Technical Report:
STPA Analysis of NextGen Interval Management Components: Ground Interval Management (GIM) and Flight Deck Interval Management (FIM)

Date: 24 September 2013
Authors: Cody H. Fleming, M. Seth Placke, and Nancy G. Leveson

EXECUTIVE SUMMARY

The next generation of air traffic management systems will involve significant changes from the way ATC (air traffic control) is done today. Reliance on software is increasing and allowing greater system complexity. Humans are assuming supervisory roles over automation, requiring more cognitively complex human decision-making. Control is shifting from the ground to the aircraft and shared responsibilities. In addition, coupling and interconnection between land, airborne, and space systems introduces more potential for accidents stemming from unsafe and unintended component interactions.

Traditional hazard analysis and risk management techniques, most of which were created 50 or more years ago for the much simpler systems of that time, cannot effectively handle the more complex systems being developed today. More powerful hazard analysis methods are needed.

Systems-Theoretic Process Analysis (STPA) is a new type of hazard analysis technique based on a very different type of paradigm and assumptions about the causes of accidents. Traditional approaches to safety assume accidents are caused by component faults and failures. Those approaches therefore focus on component reliability enhancement and do not adequately handle accidents caused by unsafe and unintended interactions among non-failed components. Such unsafe interactions usually stem from system design errors, software requirements errors, or operator errors.

In addition, traditional approaches to safety treat human error as random or stochastic. Human error, and all human behavior, is affected by the context and system design in which it occurs. For purposes of improving safety and designing to reduce errors, it is more useful to provide information about *why* the error occurred, which is needed to eliminate or mitigate errors in the system design, than to assign a probability of error.

STPA can handle the advanced features of NextGen and the complexity of the proposed operational improvements. It provides a rigorous process to assist subject matter experts, in other words, it allows an "organized inquiry." There is potential for automated assistance in the analysis and many of the basic steps in STPA have already been automated.

Most current hazard analysis techniques are usable only late in the development process, when the major design decisions have already been made and a concrete design is available to be analyzed. However, in addition to analyzing and verifying an existing design, designers of complex systems need assistance and analysis techniques during early concept development. Seventy to ninety percent of safety-related design decisions are made before most hazard analysis techniques are applicable [2]. STPA works early in concept design so that decisions can be evaluated before they are very costly to change. It identifies potential causal scenarios leading to system hazards and the system and subsystem design requirements to mitigate or control these potential design flaws.

In extensive use and industrial comparisons of STPA with traditional hazard analysis techniques, the results have shown that STPA finds more potential accident causes then the traditional hazard analysis techniques and more than a group of experts alone. It has proven to be easily learned and used by non-specialists in safety engineering and to be much less costly than more traditional methods.

Systems-Theoretic Process Analysis (STPA) is demonstrated in this report as a potential alternative or addition to the traditional hazard analysis techniques. The demonstration is done on Interval Management and Spacing (IM-S), an important component of Trajectory-Based Operations (TBO). IM-S is an arrival spacing enhancement in en route areas that automatically specifies scheduled times of arrival across flow management points. The automation then issues speed advisories to achieve these schedule times, and en route controllers are responsible for issuing these IM-related clearances to the appropriate aircraft. The STPA hazard analysis is performed on two implementations of IM-S: Ground-based Interval Management (GIM-S) and Flight deck-based Interval Management (FIM-S). GIM-S uses ground-based automation to issue speed advisories, while FIM-S uses flight deck-based automation to calculate appropriate trajectory modifications.

For GIM-S, the STPA hazard analysis identifies unsafe control actions of en route air traffic controllers. Because FIM-S involves advanced decision making capability from the flight deck, the FIM-S analysis identifies unsafe control actions of flight crews in addition to en route air traffic controllers. The STPA analysis identifies causes of these unsafe actions for both GIM-S and FIM-S and then requirements are written and allocated to system components to prevent these causes. Requirements are allocated to surveillance systems, traffic monitoring systems, ground- and flight deck-based automation, air traffic controllers, pilots, trajectory modeling systems, and weather monitoring and prediction systems. Requirements are also allocated to ensure appropriate coordination between these components.

Because STPA includes non-linear, indirect, and feedback relationships among events and actors, many of the scenarios identified in this report include more than just component failure. Therefore many of the requirements identified by the STPA analysis go beyond reliability and relate to the behavior of system components (both human controllers and automation) and the information that those components receive and exchange. The hazard analysis identified several scenarios and/or causal factors that are not considered in the IM-S Concept of Operations [24]. These additional scenarios and causal factors can be used for future revisions of the IM-S ConOps as well as in the development of detailed design documents or future revisions of IM-S platforms.

The causal factors identified by STPA but not included in the IM-S ConOps include potential lack of coordination between controllers both within and across sectors, timing of IM-S clearances relative to other required clearances, potential lack of synchronization between surveillance sources provided to controllers and their tools, and conflicts between IM automation and other tools and ATC tasks.

While the results by themselves will help stakeholders make more informed decisions with respect to delegating authority, responsibility, procedural control, and algorithmic control within the NAS, extensions to the basic STPA analysis done in this report could assist in ascertaining relative levels of risk associated with different design and control decisions. For example, GIM-S is hierarchical and centralized, which is closer to the paradigm used in the current NAS. Alternatively, FIM-S, a flight deck-based interval management solution, is highly de-centralized. A hierarchical, centralized structure with clearly delineated control authority might be more appropriate for tactical (short-term) resolutions. On the other hand, decentralized control may be more appropriate during strategic (long-term) negotiations. The different types of hazard causes that result from changes in control structure, different time horizons (or timing requirements), and goals could be compared. STPA could then be used as a part of a safety-guided design effort, where the safety controls are created to ensure(s) system safety under different operational modes.

STPA does not require changes in the current Air Traffic Organization (ATO) Safety Management System and fits within it in three places. It could be used to identify hazards in the Safety Risk Management (SRM) pillar. It also provides a useful way to describe systems in the first step of the SRM process. The functional control structure generated to perform STPA includes all the system aspects currently described for this SRM descriptive step as well as a more complete description of system functional behavior than that currently described as a minimum for SRM. Finally, it could be used in the Safety Assurance pillar to identify what needs to be assured, including audit procedures to verify that safety is not degrading as behavior changes over time. And, of course, because STPA works early in the system design process, it can be used to assist in developing and finding gaps in the ConOps and other design documentation.

TABLE OF CONTENTS

Executive Summary 1

Table of Contents 4

Figures and Tables 5

1 Introduction 7

1.1 An Introduction to STPA and its Application to NextGen 7

1.2 STPA Process, Inputs, Outputs, and Participants 14

1.3 Evaluations and Comparisons of STPA with Traditional Hazard Analysis Techniques . 15

1.4 Comprehensiveness and Completeness 16

1.5 Additional Practical Considerations 19

1.6 Potential Role of STPA in the FAA SMS (Safety Management System) 19

1.7 Summary 21

2 Scope & Assumptions of the STPA Demonstration 22

2.1 Interval Management for Spacing (IM-S,GIM-S, FIM-S) 22

2.2 Analysis Scope 25

3 The STPA Hazard Analysis for GIM-S and FIM-S 28

3.1 Results for GIM-S 28

3.2 FIM-S Results 55

4 Conclusions from the STPA Demonstration on FIM-S and GIM-S 82

5 possible Future Extensions to the Analysis 84

List of Acronyms 86

References 87

A. Hazard Analysis Results 89

FIGURES AND TABLES

Figure 1: An Example Safety Control Structure 10

Figure 2: Safety Control Structure for In-Trail Procedure 11

Figure 3: Control Agent Process Model 12

Figure 4: The STPA Process 14

Figure 5: IM-S Concept [24] 24

Figure 6: Organizational Structure of and Interactions among the Different Roles [24] 26

Figure 7: Basic TFM/IM-S Control Structure 29

Figure 8: Detailed TBFM/IM-S Safety Control Structure 31

Figure 9: Structure of a hazardous control action (adapted from [25]) 40

Figure 10: General Control Loop with Causal Factors 44

Figure 11: STPA Step 2 Control Loop for En Route ATC 46

Figure 12: En Route ATC Process Model States 47

Figure 13: Example Scenario for Loss of Separation (UCA.6.S) 54

Figure 14: FIM-S Control Structure (includes GIM-S functionality) 57

Figure 15: STPA Step 2 Control Loop for ATC (FIM-S) 68

Figure 16: STPA Control Loop for Flight Crew (FIM-S) 76

Figure 17: Flight Crew Process Model States (FIM-S) 77

Figure 18: Example Scenario for Loss of Separation, FIM 81

Table 1: Actor Responsibilities in ConOps 27

Table 2: Potentially Unsafe Control Actions for the En Route ATC – General Clearance 34

Table 3: Potentially Unsafe Control Actions for the En Route ATC – Modify Speed 35

Table 4: Potentially Unsafe Control Actions for the En Route ATC – Vector Clearance 36

Table 5: Potentially Unsafe Control Actions for the En Route ATC – Modify Altitude 37

Table 6: Example Unsafe Control Actions Using Automated Method 42

Table 7: FIM-S Terminology (adapted or quoted from [28]) 56

Table 8: Air Traffic Control Unsafe Control Actions for generic “IM Clearance” (FIM-S) 59

Table 9: Air Traffic Control Unsafe Control Actions for Maintain Current Spacing clearance (FIM-S) 60

Table 10: Air Traffic Control Unsafe Control Actions for Achieve-by then Maintain (FIM-S).. 62

Table 11: Air Traffic Control Unsafe Control Actions for IM Turn Clearance (FIM-S) 64

Table 12: Flight Crew Unsafe Control Actions for IM Execution (FIM-S) 65

Table 13: Example Requirement from STPA - Interference 83

Table 14: Full Set of Unsafe Control Actions using Automated Method..... 90

Table 15: ATC Unsafe Control Actions for GIM-S 95

1 INTRODUCTION

In 2012 Lincoln Laboratory conducted a survey of Risk-Based Modeling (RBM) techniques to support NextGen concept assessment and validation [17]. From the report:

> Effective safety analysis should begin as early as possible during a system's life cycle in order to have maximum impact. Ideally, safety considerations should play a role even during a new system's concept definition and development. Elements of the Next Generation Air Transportation System (NextGen) are currently progressing through these early phases.
>
> NextGen will increasingly rely on integrating multiple systems and information sources together to enable improved efficiency, safety, and reduced environmental impact. … for example, Trajectory Based Operations (TBO) will require components and interactions spanning ground automation systems, ADS-B surveillance, cockpit flight management systems and displays, precision navigation, datacomm, new operating procedures, and communications and collaboration tools between cockpit, facilities, and airlines—all while also supporting legacy systems and procedures as the National Airspace System transitions into NextGen.
>
> Ensuring that such complex interconnected systems are developed to meet safety goals requires corresponding advances in RBM and safety assessment approaches. Homogeneous safety analysis tools used in the past—such as fault trees—for relatively self-contained systems cannot simply be expanded to cover these larger and more complex interactions.

The report identified STPA (Systems-Theoretic Process Analysis), a hazard analysis methodology developed at MIT, as a tool capable of analyzing risk and identifying potential hazards during a system's development process. In order to explore this conclusion more thoroughly, this follow-on report delves more deeply into STPA and how it handles common features of complex systems. The bulk of the report contains an example application of STPA to TBO-related increments of the Operational Improvement "Point-in-Space Metering" (104120) in order to evaluate STPA's practicality and potential advantages.

1.1 An Introduction to STPA and its Application to NextGen

The next generation of air traffic management will include increased coupling and interconnectivity among airborne, ground, and satellite systems and intensive use of computers and software in safety-critical roles. Control will be shifting from the ground to the aircraft and to shared responsibility for safety among ATC (air traffic control), pilots, and airline operations centers. The planned coupling and interconnection between land, airborne, and satellite systems introduces more potential for accidents stemming from unsafe and unintended component interactions. To be able to assess and reduce risk in such systems, the hazard analysis techniques used must be able to handle these new accident causes.

Traditional approaches to safety analysis assume that accidents are caused by component failures and therefore focus on reliability analysis. Almost all the hazard analysis techniques listed in Appendix G of the FAA ATO (Air Traffic Organization) Safety Management System Manual [1] are 30 to 40 years old and predate the extensive use of computers. The goal of these analysis methods is to identify sequences of component failures (including human "failures")

that together will lead to an accident or loss event. Failures may be single or multiple and are usually assumed to be random with a constant failure rate (exponentially distributed). After the component failure scenarios are identified, engineers use fault tolerance or fail-safe techniques to protect against the hazards caused by the identified failures.

This approach to safety made sense for the relatively simple, pure electro-mechanical systems of the past where system components could be effectively decoupled, allowing relatively simple interactions among components. System design errors could, for the most part, be identified and eliminated by testing and what remained after development were random hardware failures. Operational procedures could be completely specified and operator error mostly involved skipping a step or performing a step incorrectly. Reliability and safety were, therefore, closely related in these relatively simple designs.

This situation is now changed. Software has become an integral part of most systems, allowing much more complex systems to be constructed. Operators have increasingly assumed supervisory roles over automation, which requires more cognitively complex human decision making. Accidents more often result from interactions among components and not just individual or multiple component failures.

While software design errors may exist that result in the software not implementing the stated requirements, the role of software in accidents and safety-related incidents is much more likely to result from inadequate software requirements [10]. The software can be perfectly reliable (it does the same thing continually given the same inputs) and perfectly implement its requirements, but it may still be unsafe if the behavior specified by the requirements is unsafe (including both requirements of the system being changed and the other systems with which it interfaces).

The problems are similar for human operators. Assumptions about the role of human operators in safety have always been oversimplified. Most human factors experts now accept the fact that behavior is affected by the context in which it occurs and humans do not "fail" in a random fashion (see, for example, Rasmussen 1997 [3], Dekker 2006 [4], Flach 1995 [5], Norman 2002 [6]).

The basic problem is complexity. Complexity has increased in current advanced engineering systems to the point where all the potential interactions among system components cannot be anticipated, identified, and guarded against in design and operations. *Component interaction accidents* (as opposed to *component failure accidents*) are occurring where no components have "failed" but a system design flaw results in accidents caused by previously unidentified, unsafe component interactions and component requirements specification errors. Hazard analysis techniques based on reliability theory and assumptions that accidents are caused by component failures do not apply to component interaction accidents.

As a result of these changes, new types of accidents are occurring and, in particular, are resulting from new causal factors, such as mode confusion or requirements incompleteness flaws. The changes in the ATM system planned for NextGen take all these changes and system design complexity to the next level and will require a new approach to safety assessment that is not based solely on component reliability assessment.

STPA is a new hazard analysis technique that differs from the traditional ones in that it is based on a new theoretical model of how accidents occur called STAMP (System-Theoretic Accident Model and Processes). This model, which is based on systems theory (which also

underlies system engineering), extends the types of accidents and causes that can be considered by including non-linear, indirect, and feedback relationships among events. In this way, the traditional causality model is extended to consider new types of accident causality brought about by component interactions (rather than just component failures), cognitively complex human mistakes, management and organizational errors, software errors (particularly requirements errors), etc. Accidents or unacceptable losses can result not only from system component failures but also from interactions among system components—both physical and social—that violate *system safety constraints*. For example, an important safety constraint in ATC is that airborne aircraft are always separated by a minimum safe distance.

In systems theory, emergent properties are those system properties that arise in the interactions among components. Safety is a type of emergent property. The emergent properties associated with a set of components are related to constraints upon the degree of freedom of those components' behavior. There are always constraints or controls that exist on the interactions among components in any complex system. These behavioral controls may include physical laws, designed fail-safe mechanisms to handle component failures, policies, and procedures, etc. Such controls must be designed such that the safety constraints are enforced on the potential interactions between the system components. In air traffic control, for example, the system is designed to prevent loss of separation among aircraft.

System safety, then, can be reformulated as a system *control* problem rather than a component *reliability* problem: Accidents or losses occur when component failures, external disturbances, and/or potentially unsafe interactions among system components are not handled adequately or controlled—where controls may be managerial, organizational, physical, operational, or manufacturing—leading to the violation of required safety constraints on component behavior (such as maintaining minimum separation).

In STAMP, the safety controls in a system are embodied in the *hierarchical safety control structure.* Note that a Safety Management System is a particular implementation of a safety control structure. Hierarchies are a basic concept in systems theory. At any given level of a hierarchical model of complex systems, it is often possible to describe and understand mathematically the behavior of individual components when the behavior is completely independent of other components at the same or other levels. But emergent system properties (such as safety) do not satisfy this assumption and require a description of the acceptable interactions among components at a level higher than the components; these interactions are controlled through the imposition of constraints upon the interactions of components at the level below. Figure 1 shows an example of a hierarchical safety control structure for a typical regulated industry, such as commercial aircraft, in the U.S. Higher level controllers may provide overall safety policy, standards, and procedures, and get feedback about their effects in various types of reports, including incident and accident reports. The feedback provides the ability to learn and to improve the effectiveness of the safety controls.

There are two basic hierarchical control structures in Figure 1—one for system development (on the left) and one for system operation (on the right)—with interactions between them. An aircraft manufacturer, for example, might only have system development under its immediate control, but safety involves both development and operational use of the aircraft and neither can be accomplished successfully in isolation: safety must be designed into the aircraft, and safety during operation depends partly on the original design and partly on effective control over

operations. Manufacturers must communicate to their customers the assumptions about the operational environment in which the original safety analysis was based, for example, maintenance procedures and quality, as well as information about safe aircraft operating procedures. The operational environment, in turn, provides feedback to the manufacturer about the performance of the system during operations. Each component in the hierarchical safety control structure has responsibilities for enforcing safety constraints appropriate for that component, and together these responsibilities should result in enforcement of the overall system safety constraint.

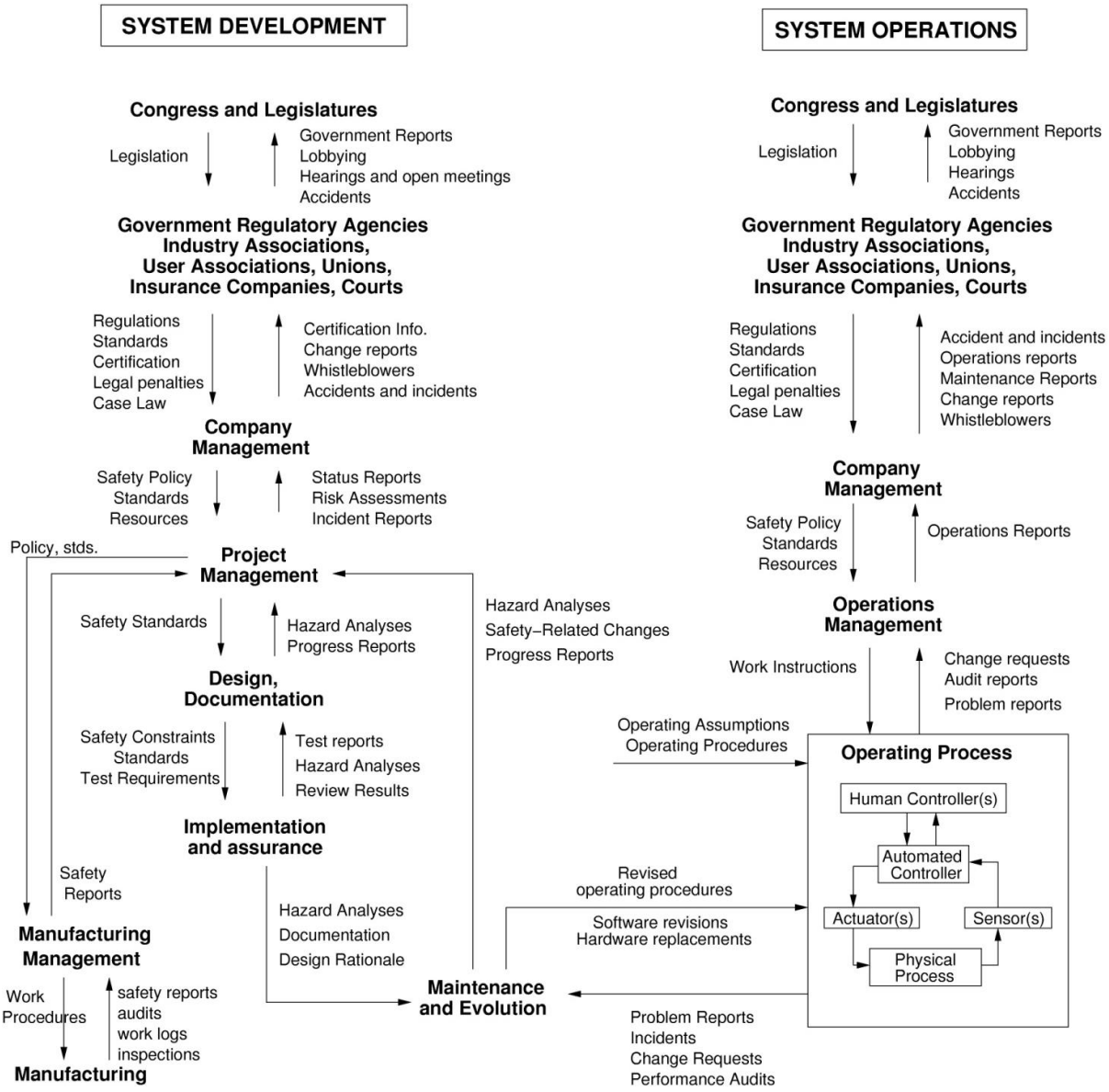


Figure 1: An Example Safety Control Structure

The safety control structure integrates the organizational and managerial aspects of systems with the operating technical system. This report does not include the organizational aspects of NextGen in its example analysis.

An example of a more detailed control structure for the operating process (the lower right hand box in Figure 1) is shown in Figure 2.

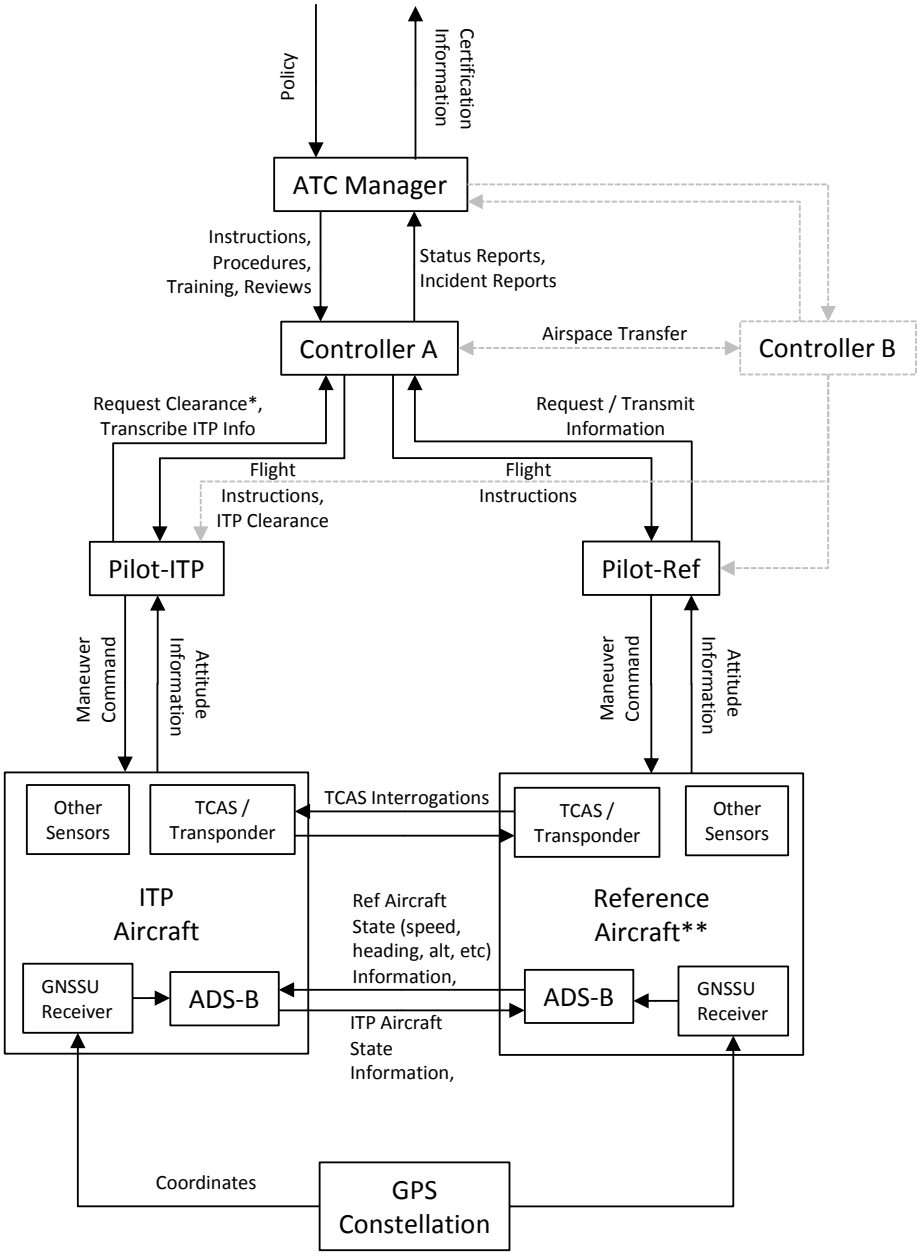


Figure 2: Safety Control Structure for In-Trail Procedure

Figure 3 shows the control structure for an early component of NextGen called In-Trail-Procedure (ITP) that will allow more passing opportunities in the aircraft tracks over the North

Atlantic. The structure includes all the human and technical components of the ITP operating process that have any impact or are affected by ITP, both human (pilots and air traffic controllers) and physical (ADS-B, GPS, etc.).

The relationship between components at different levels of the control structure is a classic feedback control loop. Control actions are provided by the control agent at the higher level and feedback provides information about the state of the controlled process. For example, in Figure 2, the pilots provide maneuvering commands to the aircraft and receive feedback about the current state of the aircraft. As another example, in ITP a pilot can request permission to perform the passing maneuver and ATC will either approve or deny it. The pilot is responsible for ensuring that ITP safety criteria are satisfied before passing the reference aircraft.

Although not shown in these figures, the responsibilities of each of the components in the control structure must be specified.[1] Together these responsibilities should ensure the safety of the system (the enforcement of the safety constraints) if they are properly implemented. In an air traffic control system, for example, the air traffic controller may be assigned responsibility for maintaining safe separation between aircraft. The controller issues advisories to the aircraft to ensure that minimum separation requirements are enforced. Pilots have their own responsibilities, such as to follow the advisories provided by ATC if they do not have information (perhaps visual) that the advisory is unsafe.

A third important concept in STAMP, besides safety constraints and hierarchical safety control structures, is a process model (Figure 3). Any control agent contains both a control algorithm (although this may be changeable in a human control agent) and a process model.

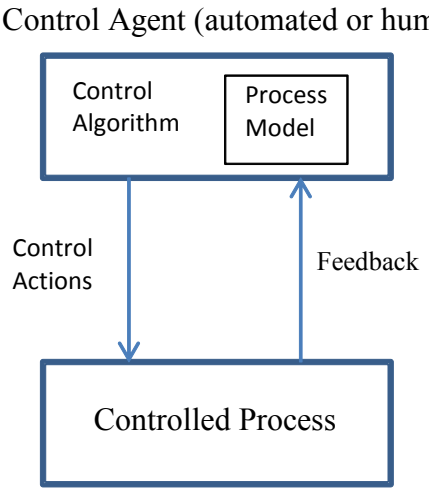


Figure 3: Control Agent Process Model

[1] The responsibilities for the (non-technical) components of the FAA SMS are specified in the SMS implementation manuals such as the ATO SMS Manual.

The *control algorithm* uses information about the process state (contained in the *process model*) to generate those control actions that will cause the process to achieve the requirements or maintain the safety constraints. In a human controller, the process model is usually called a "mental model." This process model or mental model includes assumptions about how the controlled process operates and the current state of the controlled process. The control agent uses his/her process model to determine what control actions are necessary to keep the system operating effectively.

For example, if a simple thermostat is controlling the temperature in a room, it will determine whether the temperature of the room is at a commanded set point. If not, the thermostat generates control actions using the designed control algorithm to either start or stop the furnace and perhaps start or stop an air conditioning unit if air conditioning is provided in the system. For a more complex process, the requirements can be more complex than simply maintaining a set point. In the air traffic control example, the air traffic controller issues advisories to the pilots to maintain separation constraints while ensuring adequate throughput in the system.

One way an accident can occur in such a system is that the control agent's process model becomes inconsistent with the real state of the controlled process and an unsafe control action is provided. For example, the pilot of the aircraft that wants to pass another aircraft thinks the conditions are safe to perform the ITP passing maneuver when they are not and a collision results. When there are multiple control agents controlling the same process (including the case where the control agents may be a mixture of humans and computers, as will occur in NextGen), accidents can also result when conflicting control actions are provided, perhaps due to inconsistencies in the control agents' process models. Part of the challenge in designing an effective safety control structure is to provide the feedback and inputs necessary to keep the control agents' models consistent with the actual state of the controlled process and with each other.

There are four general types of unsafe behavior by the control agent:

1. An unsafe control action is provided that creates a hazard (e.g., an air traffic controller issues an advisory that leads to loss of separation that would not otherwise have occurred)
2. A required control action is not provided to avoid a hazard (e.g., the air traffic controller does not issue an advisory when one is required to maintain safe separation)
3. A potentially safe control action is provided too late, too early, or in the wrong order
4. A continuous safe control action is provided too long or is stopped too soon (e.g., the pilot executes a required ascent maneuver but continues it past the assigned flight level)

There is a fifth scenario where a control action required to enforce the safety constraint (avoid a hazard) is provided but not followed because of inadequate behavior (perhaps a failure or a delay) in a part of the control structure other than the control agent (e.g., the actuator, the controlled process, the sensors, or the communication links).[2]

These five scenarios are a much better model of accident causes related to actions by a human or a computer than is simply a model that says they "failed" with no other information about

[2] Note that any of the parts of the control structure may be an engineered device or may be a human.

why. Without understanding the causes of the "failures," options for eliminating or reducing them are limited.

STPA is a hazard analysis technique based on the STAMP accident causality model. STPA examines the control loops in the safety control structure, using defined procedures, to find potential flaws and the potential for and causes of unsafe control. The procedures use the four types of unsafe control actions, along with the fifth reason for unsafe control, to identify potential causes of hazardous behavior, including that involving software or a human. The identified scenarios (hazard causes) can then be used by the system designers to eliminate the causes from the system or, if that is not possible or practical, to mitigate them. Mitigation might involve changing any part of the control loop (the assigned responsibilities, the design of the controlled process, the control algorithm, the process model, the control actions, designed feedback, communication links, etc).

1.2 STPA Process, Inputs, Outputs, and Participants

STPA consists of three parts: (1) creating a high-level control structure based on the functions described in the system architecture, (2) identification of potentially unsafe control actions, and (3) causal analysis of the unsafe control actions identified. Figure 4 shows these steps graphically along with their relationships to general system engineering activities. Figure 4 also shows who should be involved during each step of the analysis and illustrates the iterative nature of hazard analysis when it is used to guide the design. The participants in an STPA analysis should be no different than any other hazard analysis.

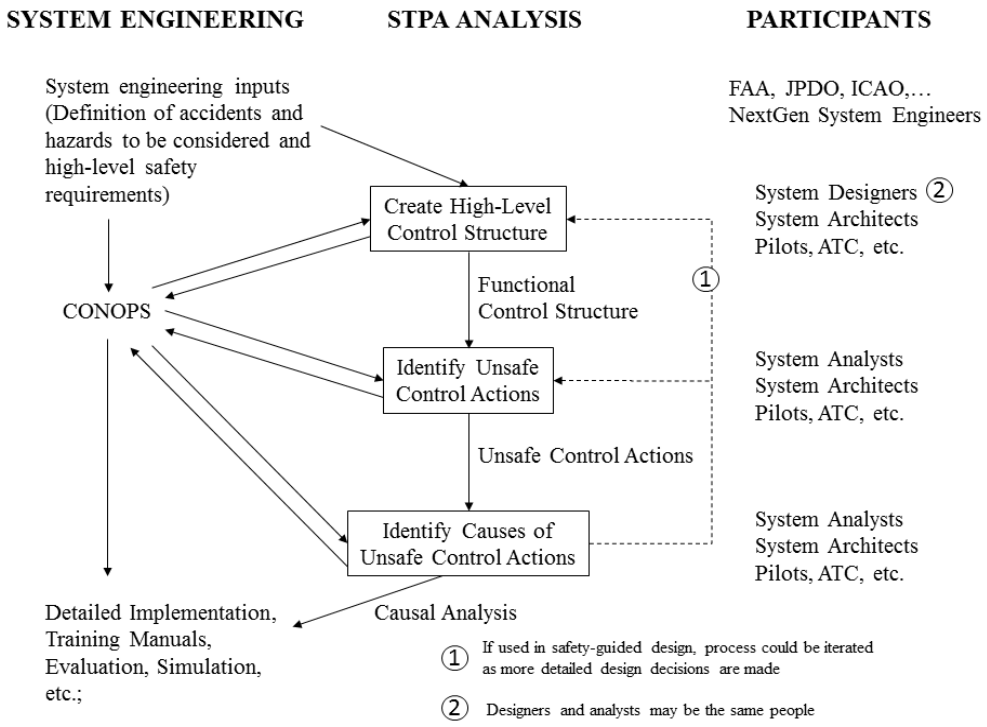


Figure 4: The STPA Process

The first step in STPA is the creation of the functional control structure for the system. Figure 2 is an example of such a structure for the NextGen In-Trail Procedure (ITP). The information to create this structure comes from basic system engineering inputs such as the system goals and early concept of operations. This structure may, and probably will, change as information is derived from the hazard analysis. Even at this very early stage in analysis, gaps or weaknesses in the ConOps can be identified.

The functional control structure is then used to identify potential hazardous control actions, such as the air traffic controller providing an altitude modification that leads to a loss of separation or the flight crew deviating from their reported flight plan. Information will again be derived from the ConOps and flaws in the ConOps can be identified.

The final step in STPA is to identify the potential causes of unsafe control actions. An example might be that the process models of the air traffic controller and the automation become inconsistent, perhaps due to inadequate feedback and coordination.

STPA can be performed on a very high-level design and iterated as design decisions are made (perhaps as a result of the STPA analysis results) and the system design becomes more detailed.

As with any hazard analysis, usefulness of the results will be enhanced by the participation of system experts in the analysis. As discussed later, STPA has been found to be very easy to learn and use by the design engineers and does not require use only by special experts in STPA.

1.3 Evaluations and Comparisons of STPA with Traditional Hazard Analysis Techniques

Because STAMP extends current accident models and thus includes component failure accidents, STPA can identify the hazard scenarios identified by fault tree, event tree, and other traditional hazard analysis methods, but it also can find those factors not included or poorly handled in these traditional methods such as software requirements errors, component interaction accidents, complex human errors (mistakes vs. slips), inadequate coordination among multiple control agents, and unsafe management and regulatory decision making.

While this comparison of STPA and the traditional hazard analysis methods shows STPA to be *theoretically* more powerful, does STPA actually identify more causal scenarios when used on real systems? There have been a lot of real-world comparisons made and in each of these STPA outperformed the traditional hazard analysis methods.

One of the first industrial uses of STPA, in 2003, was on the new U.S. Missile Defense System in order to assess the risk associated with the hazard of inadvertent launch [7]. The system had been subjected to standard hazard analysis methods, but one more additional analysis was required before the system could be deployed and field tested. STPA found so many flaws during just a limited three month analysis by two people that deployment was delayed for six months to fix the newly identified hazardous scenarios [7]. In many of these newly identified scenarios, all the components were operating exactly as intended, but the complexity of the component interactions led to unanticipated system behavior. These unidentified scenarios included things like missing cases in software requirements and subtle timing errors in communication (sending and receiving messages) between the system components. STPA also identified component failures in the system that could cause hazards. Most traditional hazard analysis methods consider only these types of component failure events.

The Japanese Aerospace Exploration Agency (JAXA) used STPA experimentally on their unmanned spacecraft, called the HTV, which delivers cargo to the International Space Station. STPA found everything identified in the HTV fault tree analysis (required by NASA) plus it found additional hazardous scenarios, mostly related to system design flaws and to software but also related to hazardous interactions among the multiple HTV control agents (astronauts, HTV software, NASA mission controllers and JAXA mission controllers) [9].

Experimental application of STPA to the NextGen In-Trail Procedure (ITP) in a recent MIT research project identified more scenarios than the fault tree and event tree mixture used in the official ITP safety analysis and documented in DO-312 [8]. STPA identified all the hazard causes produced by the official analysis, but found many more that had been omitted. Using STPA, more safety-related requirements for ITP were generated than are listed in the official RTCA requirements document [8]. The official fault tree/event tree analysis in DO-312 produced a probabilistic risk number for an accident—which was almost certainly not accurate as it omitted many potential causal factors in the analysis—while STPA instead identified the potential safety weaknesses in the system so they could be fixed or mitigated.

EPRI (Electric Power Research Institute) ran a comparative evaluation of fault trees, event trees, HAZOP, FMEA, and a few other traditional techniques as well as STPA on a real nuclear power plant design. Each hazard analysis technique was applied by experts on the techniques. STPA was the only one that found a scenario for a real accident that had occurred on that plant design (which, of course, the analysts did not know about).

The original FMEA for a blood gas analyzer (a medical device) that had been recalled by the FDA because of a serious adverse event took a team of people a year to perform and found 75 hazardous scenarios. It did not find the scenario leading to the recall. STPA performed by one person in 10 days found 175 scenarios including 9 leading to the hazardous behavior involved in the recall, including the one that actually occurred [8].

To evaluate usefulness and learnability for subject matter experts and system designers, two one-day workshops have been held to teach the technique in the morning and then have the experts apply it to their own system in the afternoon. In both cases, the engineers, even though they had just learned STPA, identified safety design flaws in the systems they were designing or evaluating that they had not noticed before. One typical comment was “We never realized that [system design feature] was important for safety or could lead to an accident.” In these two informal evaluations, one resulted in a recommendation to adopt STPA (for use on a radiation therapy device) and the other to conduct a larger controlled comparison (for U.S. Air Force mission assurance).

There have been many more successful uses of STPA in most every type of industry. Not only did STPA find more causes of hazards (which could have been predicted from a theoretical comparison), but it much less time and fewer resources to perform.

A demonstration of STPA on some new TBO-related capabilities is presented later in this report to further evaluate its power.

1.4 Comprehensiveness and Completeness

How comprehensive or complete is an STPA analysis? No identification of hazards and hazard causes, using any method, can be proven to be complete as completeness is

mathematically undefined in this context. In addition, some hazards may be purposely omitted from consideration.

One factor in the comprehensiveness of any causal analysis is the defined scope of the analysis. STPA starts with a short list of the high-level hazardous states of the application. For this report, the application is air traffic management excluding ground operations. The high-level list is then refined iteratively into more detailed hazards and their causes for the specific part of the system being considered. For example, the high-level hazards used in this report are

H1: Aircraft violate minimum separation (LOS or loss of separation)

H2: Aircraft enters restricted area

H3: Aircraft enters unsafe atmospheric region

H4: Aircraft enters uncontrolled state

H5: Aircraft assumes unsafe attitude

There are some hazards that have purposely been omitted from this list, for example, a meteorite comes through the fusilage and kills a member of the crew or a passenger. There are two different reasons for the omission. One is that it has never happened in the entire history of flight and NextGen will not change any conditions that could lead to that hazard (i.e., increase the probability of being hit by a meteorite). The other is that there is no way to design NextGen to avoid that hazard. It is just not a hazard that aviation has been concerned about in the past or will likely be concerned about in the future. This is an example of "incompleteness" that we know about and accept as a community.

The list must include any potential new hazards that arise only with NextGen and have not had to be considered in the past. With the current conception of NextGen, it does not appear that there are new system-level hazards. There will be new hazard *causes* related to changed or new designs and procedures, but not new hazardous states at the system level. The new causes of the list of five hazards are the things that engineers need to concentrate on in the design of NextGen operational increments.

Why not start with a long list of hazards (i.e., by just generating every potentially unsafe system state and cause one can think of)? Because then it is difficult (impossible?) to determine whether anything has been missed—the list is too long and at too many different levels of abstraction. One of the most powerful ways human minds deal with complexity is by using hierarchical abstraction and refinement. By starting at a high level of abstraction with a small list and then refining that list with a more detailed list at each step (working top down), one can be more confident about completeness because each of the longer list of causes (refined hazards or causes) can be traced to one or more of the small starting list (and vice versa). With that traceability, it is also easier for human reviewers to find any incompleteness. We say "more confident" because such a list can never be proven to be complete—there is no formal (mathematical) model of the entire system and how it will operate. Human participation in the analysis and human review of the results will always be required and, therefore, incompleteness will always be possible. But structuring the process in a way that optimizes human processing and review will reduce any potential incompleteness.

A second aspect of completeness is whether all hazard causes are identified. STPA considers more *types* of hazard causes than the other hazard analysis methods and includes those types

identified by other methods. So theoretically, it is more complete than existing methods. Whether the actual analysis is complete or more complete depends on how well it is conducted and the time and effort expended. In practice, where comparisons have been possible (see Section 1.3), STPA found more hazard causes in total, including types that were not (and, in fact, could not be) found by the other methods,

Another question that has come up is whether STPA includes all the hazards and the relationships between their causes during the analysis or, as in other top-down analysis methods, is a different analysis performed for each system-level hazard at a time. The answer is that all hazards are considered together, with a qualification. STPA will find the causes that are related to the part of NextGen that is being analyzed at the time. So, for example, the STPA analysis of GIM will identify causes related to the operation of GIM that relate to all five hazards and, potentially, identify other hazards beyond the initial five if any important ones have been omitted. The analysis process starts with a short list of hazards that limit the scope and document what the designers want to consider with respect to safety, that is, to document what is being considered in the hazard analysis. But STPA looks at all the control actions within the documented scope to identify those that are unsafe and traces those unsafe control actions to one or more of the five high-level hazards.

The list of unsafe control actions is used to generate a list of their potential causes. Here is where STPA differs from bottom-up methods like FMEA and Event Tree Analysis. Bottom-up analysis techniques start by identifying all possible failures. This list can be very long if there are a lot of components and all the permutations and combinations of component failures are considered. For example, the FMEA used on the Space Shuttle identified 20,000 safety-critical failures. And that list does not include non-critical failures and the causes of a space shuttle accident that do not involve component failures at all. STPA, in contrast, only identifies the failures and other causes that can lead to a system hazard and does not start by identifying all possible failures and removing all non-critical failures from the list.

In addition, in the top-down STPA analysis approach, the analyst can stop refining causes at the point where an effective mitigation can be identified and not go down any further in detail. The analyst only has to continue refining causes if an acceptable mitigation cannot be designed. That is the major difference between STPA and FMEA (and any other bottom-up technique) and explains the differences in time and effort required, as noted in Section 1.3.

Event tree analysis is another “bottom-up” technique that examines all failures to identify those that can lead to a loss although the types of failures considered and the ordering of their occurrence are much more limited than FMEA (which is why it is less resource intensive than a FMEA). The problem with event trees is that they necessarily have to leave many things out and even then are impractical for complex systems. Event tree analysis was created for the safety systems in nuclear power plants, which are purposely kept simple to ensure very high reliability and availability. As such, event tree analysis is totally inappropriate for NextGen, although people are using it. The analyses we have seen using event trees on NextGen components are very incomplete in terms of the cases considered.

What about other top-down analysis methods like fault trees? Their refinement can potentially be stopped at any point too. The difference is that STPA can find more types of causes than fault trees, and STPA has a structured process to follow in doing the analysis (fault tree analysis does not) that is likely to result in a more complete result. Section 1.3 described comparisons and

evaluations that have been made in many different industries.. In these cases, the fault tree analysts were usually experts and the users of STPA were usually beginners. In all the comparisons done by us and others so far (that we know about), STPA found all the causes found by fault trees and found more, particularly those related to computers and to human operational mistakes.

1.5 Additional Practical Considerations

One practical consideration is learnability and how much time it takes to learn to use a technique. The traditional techniques have been used for so long that there are many people who already know how to perform them. So the important question is how easy is it to learn to use STPA adequately. Because engineers are usually familiar with basic control loop concepts, we have found that engineers with just a half day of training have been able to find significant previously undiscovered problems using STPA on their designs. Our classes for industry now run from two to three days, after which the trainees have used STPA on their systems. In addition, people have been picking it up just from reading Leveson's book and looking at some sample analyses that have been published. For the most part, we have found that they did an excellent job without any formal training. The FAA and their subcontractors could do an STPA analysis themselves and would not need to rely on outside experts.

Another practical question is about the time and cost involved in an STPA analysis. We have been surprised to find that STPA takes less time and effort than the equivalent traditional techniques in the empirical comparisons that have been made by us and by others. For bottom-up, labor and time intensive reliability analysis techniques like FMEA or FMECA, this fact should not be surprising. For the other top-down hazard analysis techniques, it is somewhat surprising as STPA is more powerful and identifies more causal scenarios. We initially assumed STPA would be harder and take more resources, but the evidence so far is that this assumption is untrue. Part of the explanation may lie in the detailed steps and guidance in an STPA analysis. Fault trees are difficult and often incomplete, for example, because there is no real guidance on how to produce the tree and what to include in it.

Any cost comparisons are necessarily limited because analysis using any method can be incomplete and therefore take less time or effort. There appears to be enough data now from real projects, however, to show that STPA is not more costly and may be less. The automated tools for assisting with STPA that are now being created should also reduce the effort and time involved.

1.6 Potential Role of STPA in the FAA SMS (Safety Management System)

STPA fits into the SMS Safety Risk Management (SRM) pillar under the steps requiring the identification of hazards (which in the SMS appears to include identifying the causes of hazards). There is a long list of old (and many never widely used) techniques in Appendix G of the ATO Safety Management System Manual (Version 2.1, 2008). Almost all of these are *not* applicable to a system of this size, type, and complexity. The only change to the SMS manual that would be required would be to add STPA to the list in that appendix as an additional choice.

STPA also fits in the current SMS process by providing a way to describe the system in the first step of the SRM process. The STPA functional control diagram includes all the things currently described in this SMS requirement as well as a more complete description of the

system functional behavior than seems to be required as a minimum for SRM. The more complete description provided in the STPA functional control diagram will be needed for system design and maintenance and particularly for any future changes that are made. In the extensive use of STPA in other industries, one of the most common responses from users is that the functional control diagram produced for STPA is the best and most useful documentation they have about the functional design of the system, even in a decades long development program near its end, as was the case for the application of STPA on the U.S. Missile Defense System. Most industry documentation, particularly graphical documentation, focuses on the physical system design and not the functional design.

A third place where STPA would be extremely useful is in the Safety Assurance pillar of the SMS process. The STPA causal analysis can be used to identify what needs to be assured, including audit procedures to verify that safety is not degrading as behavior changes over time.

STPA does have a slightly different definition of hazard than included in the SMS Manual. The official definition in the SMS manual is "a condition that is prerequisite to an accident or incident." The drawback of that definition is that there are a very large if not infinite number of conditions that precede an accident. Aircraft being in the airspace is prerequisite to an accident or incident, but we cannot eliminate that condition, i.e., not allow any planes in the airspace. The definition used in STPA restricts hazards to be conditions or states that nobody ever wants to occur, such as a violation of minimum separate standards. These conditions, once they are identified, can be eliminated or controlled in the system design and operations. All prerequisites to an accident (the SMS definition) cannot be considered (and do not need to be) as they include almost all conditions that occur during operations.

In practice, we suspect that the actual hazards identified in any SMS hazard identification process will be those that fit the STPA definition. Otherwise, such a listing would be impossible. This was the case for the safety analysis of ITP. In fact, official ITP analysis identified fewer hazards than STPA because it only considered component failures. The same is true for the techniques currently listed in Appendix G of the ATO SMS Manual. As such, the hazards identified by the Appendix G methods will be a proper subset of those identified by STPA (assuming both are competently executed).

There may be implications for the use of STPA on the process of assessing risk in SMS. Because human errors and non-failure scenarios can be identified by STPA, it will not be possible in many, or maybe even most, cases to assess a probability for these hazards. A different type of assessment will be needed. One solution to this dilemma is simply to ignore the scenarios for which probabilities cannot be derived, which is effectively what is being done now because those scenarios are never identified even though they exist. The result is (and would be) an inaccurate value. Unfortunately, there is no way to evaluate the accuracy of such probabilistic risk assessments (without waiting a thousand years to see what happens) so they are usually just accepted as true without validation. Non-probabilistic assessment methods will be needed, but this conclusion has little to do with STPA and everything to do with the nature of hazards in complex, tightly coupled, distributed systems. The possibility of using qualitative methods for risk assessment is included in the SMS Manual so the change necessary will be in practices used rather than in the definition of and requirements for risk assessment in SMS.

STPA has no impact on the SMS processes involving identifying mitigations and controls. STPA is an analysis technique, not a design technique. If used on a design that already exists,

STPA does not tell the engineers how to redesign the system but it does provide important information including, whether adequate controls already exist or if new ones are needed. The method can also potentially be applied to various alternatives to see which one(s) are preferable from a safety standpoint. If used early in the design process, as in this report, STPA can generate the safety design requirements for the system being considered so that better decisions can be made during concept formation and early design. Assessing safety after the design is complete usually limits the types of hazard mitigations that are possible and results in extremely costly (both in terms of money and time) rework. Designing safety in as the design concepts and decisions are made can result in safety costing very little or even nothing extra.

Another potential use for STPA in the SMS process, although not explored in this report, is to evaluate the independence and safety impact of potential changes and upgrades in ATC capabilities. The Preliminary Safety Analysis defined in the SMS Manual requires determining whether a change can impact safety and therefore requires more extensive analysis. This process is actually much more difficult than people think. An informal impact analysis (and even one using the traditional hazard analysis techniques) can only identify the direct relationships between the changes proposed and the current system. Indirect effects are not easily identified. In a nuclear power plant demonstration of STPA recently completed for the NRC, we found several ways that the non-safety system can impact the safety system indirectly and potentially lead to a catastrophe. In nuclear power design, major reliance is placed on the safety system to react when there is a disturbance in the plant and certification is usually focused on the safety system. Therefore, one of the most fundamental design requirements is that the successful operation of the safety system must be independent from the non-safety components of the plant. We demonstrated that the way the nuclear power community currently determines independence is flawed as it relies on identifying only direct relationships between the components and not indirect ones. The indirect relationships tend to be obscure and difficult to find. STPA can do this.

STPA has one other implication for SMS. Because STPA can be performed earlier than the traditional techniques, potential design flaws can be found earlier and eliminated from the design when more and cheaper design changes and options are available. This feature would appear to impact the current SMS design by allowing hazard analysis to begin earlier and to be more tightly intertwined with the original concept definition and architectural development rather than being only an after-the-fact analysis process. This advantage of STPA could save a lot of time and money in rework due to changes required late in the process.

1.7 Summary

Traditional approaches to safety assume accidents are caused by component faults and failures. They therefore focus on component reliability enhancement. They do not handle accidents caused by unsafe and unintended interactions among non-failed components, usually stemming from system design errors, software requirements errors, or operator errors. In the extensive use and comparisons of STPA with traditional hazard analysis techniques done so far in many industries, the results have shown that STPA finds more things than the traditional analysis techniques and more than a group of experts alone.

In addition, traditional approaches to safety treat human error as random and assign probabilities to them. Human behavior, including human error, is always affected by the context

and system design in which it occurs. Assigning a probability to such errors assumes that context and system design is unimportant unless such probabilities are carefully derived from the specific design changes involved and from extensive simulation and operational use information, which is often impractical. In addition, the probabilities do not provide information about *why* the error occurred, which is required in order to eliminate it or mitigate it in the system design.

Finally, most of the current hazard analysis techniques are usable only late in the development process, when the major design decisions have already been made and a concrete design is available to be analyzed [17]. However, designers of complex systems need assistance and analysis techniques also in early concept development. Seventy to ninety percent of safety-related design decisions are made before most hazard analysis techniques are applicable.

These traditional approaches, as such, will not handle the changes and complexity envisioned for NextGen. Reliance on software is increasing and allowing greater system complexity. Humans are assuming supervisory roles over automation, requiring more cognitively complex human decision making, which is not captured by probabilistic assessments. Control is shifting from the ground to the aircraft and shared responsibilities. In addition, coupling and interconnection between land, airborne, and space systems introduces more potential for accidents stemming from unsafe and unintended component interactions. More powerful hazard analysis methods are needed to handle these NextGen changes.

STPA is the only hazard analysis technique currently available that can handle these features of NextGen. It also provides a rigorous process to assist subject matter experts, in other words, it allows an "organized inquiry." There is potential for automated analysis, and we can already automate most of the process of generating the safety requirements for a system and its subsystems.

The remainder of this report contains a demonstration of STPA on two increments of the TBO-related Operation Improvement "Point-in-Space Metering (104120). Section 2 documents assumptions about TBFM and IM-S (the TBO capabilities selected), including their concepts of operation and delegated responsibilities of the various actors and tools. Section 3 presents the STPA analysis results. Section 4 summarizes the results of the demonstration

2 SCOPE & ASSUMPTIONS OF THE STPA DEMONSTRATION

One of the purposes of the work reported here is to demonstrate and evaluate STPA for NextGen and, in particular, TBO. IM-S (GIM-S and FIM-S) was selected for the study because of its potential contribution to the overall achievement of TBO, its relatively higher level of design definition with respect to other capabilities in TBO, and its potential to provide immediate improvements in trajectory optimization. It is a stepping stone to full TBO capabilities, such as collaborative decision making, automated conflict prediction and resolution, and real-time trajectory feedback and negotiation via data link.

2.1 Interval Management for Spacing (IM-S,GIM-S, FIM-S)

The IM-S concept broadly involves capable aircraft being assigned spacing goals behind target aircraft by ATC [15]. The application utilizes Automatic Dependent Surveillance–Broadcast (ADS-B) when available. Interval management will improve accuracy in trajectory prediction and facilitate more efficient spacing control through the use of speed advisories. Note

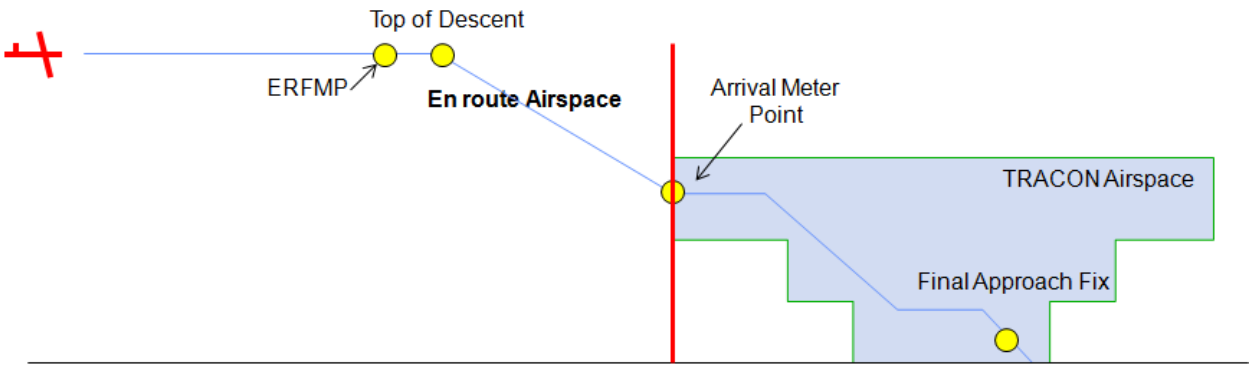
that interval management is subtly different from time-based management, or metering, in that merging and spacing is achieved through precise station-keeping of the aircraft, predicted miles-in-trail constraints and other techniques—as opposed to time-based metering across a fix. In addition, IM-S uses Extended Metering, where meter fixes are extended much farther away from terminal operations.

Assumptions and model descriptions for IM-S draw largely from the FAA's IM-S Concept of Operations for the Mid-Term Timeframe [23]. IM-S contains two variants: Ground-based Interval Management and Flight Deck-based Interval Management.

2.1.1 Ground-based Interval Management (GIM-S)

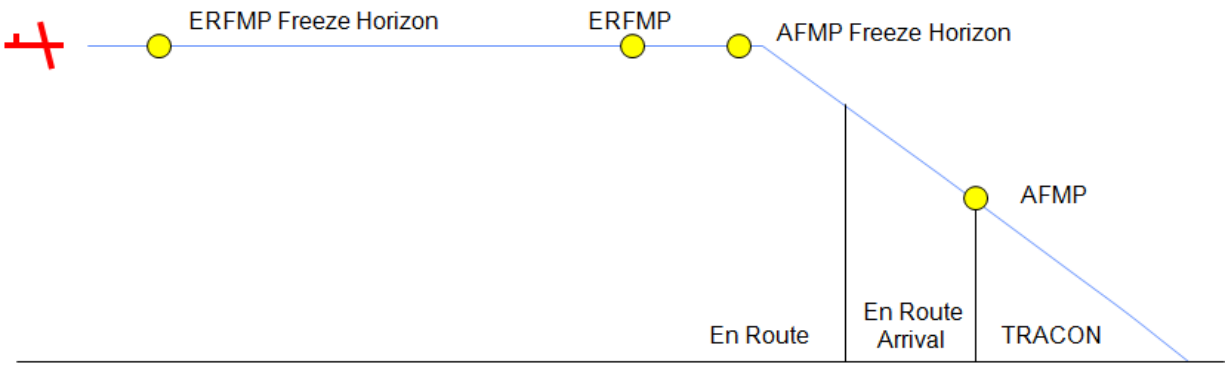
Time-Based Flow Management (TBFM, another component of TBO) will help to mitigate congestion in terminal areas by providing advisories to en route controllers to delay aircraft through speed changes or through path stretching. Once the aircraft is nearing its top of descent,[3] the speed control of IM-S begins engagement. Ground-based Interval Management (GIM-S) will provide controllers with speed advisories to ensure aircraft do not lose separation at any point in the trajectory. Speed advisories help to resolve predicted future loss of separation when aircraft spacing compresses near the transition from en route to terminal approach airspace.

Under the GIM-S framework, there will be two control points for which aircraft are metered: En Route Flow Management Point (ERFMP) and Arrival Flow Management Point (AFMP). For the purposes of interval management the points should be well separated in time and space, because a violation of this assumption could be hazardous. Figure 5 illustrates these assumptions notionally. Part (a) of Figure 4 represents conventional arrival operations, while part (b) represents operations under IM-S. In order to maintain sufficient spacing between aircraft, conventional operations typically require leveling and other maneuvers during descent. With improved prediction and trajectory modeling, IM-S will provide the accurate and consistent arrival spacing for arrival streams as necessary to support optimized descents and fully utilize the runways [24].



(a)

[3] This will occur at the En-Route Flow Management Point (ERFMP) Freeze Horizon, prior ERFMP



(b)

Figure 5: IM-S Concept [24]

Ensuring proper spacing through interval management is particularly valuable in enabling Optimized Descent Profiles (OPD) A difficulty with OPDs is that aircraft that are well-spaced near the top of descent may become compressed at some point along the descent trajectory to the airport because they are slowing to different speeds, which are based on each aircraft's specific aerodynamic properties. Safe management of these trajectories requires accurate trajectory prediction using wind forecasting and other tools.

Our analysis assumes that GIM-S support tools do pairwise comparisons between trajectories in order to generate speed advisories to ensure aircraft maintain proper separation. When applying GIM-S, it is the responsibility of the relevant controller or traffic manager to determine whether the advisory is appropriate based on the conditions outside of the pairwise comparison algorithm—for example, cascading effects to upstream or downstream aircraft in the flow, conflicts with aircraft outside the arrival stream, or weather constraints [24].

The GIM-S support tools are not guaranteed to enforce conflict-free trajectories in all operational situations. As with any software output, the advisories may be inappropriate if based on incorrect or delayed inputs, which include surveillance data, weather data, and flight plan data.

2.1.2 Flight Deck-based Interval Management (FIM-S)

Flight deck-based Interval Management (FIM-S) is similar to GIM-S in concept, but FIM-S delegates responsibilities differently than GIM-S. GIM-S has a centralized automation tool, and speed advisories are issued by en route ATC. Alternatively, in FIM-S, air traffic controllers provide an interval requirement to a FIM-capable aircraft, such as "60 second spacing to target aircraft X" [28]. Individual aircraft are equipped with automation tools, and flight management systems or flight crews individually decide(s) whether or how to implement the advisories coming from air traffic control using the flight deck (FIM) equipment.

Our analysis focuses on the Ground-based flow component (GIM-S), and also includes preliminary analysis of FIM-S. Future work may involve more comprehensive analysis of the flight deck-based component (FIM-S) and mixed equipage.

2.2 Analysis Scope

The analysis includes those components that have a functional role in the NAS. Broadly these components include Air Traffic Controllers, Flight Crews, Flight Operation Centers and the Air Navigation Service Provider. In particular, the analysis focuses on En Route Air Traffic Controllers (ARTCC) and the ARTCC's relevant decision support tools.

2.2.1 Operational Environment

One benefit of TBFM enhancements is increased use of traffic management techniques during non-routine situations such as weather events or unplanned airspace restrictions (see Section 1.1). Such situations will be critical for safety and require careful attention. IM-S operations are not intended for re-route operations, however, and thus inclement weather is expected to be a major impediment to IM-S implementation [24].

Our analysis does not consider events and influences outside the NAS such as crew incapacitation, malicious intervention (terrorism), natural disaster anomalies or other events that are highly infrequent and change the underlying assumptions that enable air travel. These could be included but are omitted because they are outside the scope of the IM-S Concept of Operations.

2.2.2 Time/Distance Horizon

Our analysis focuses on en route (approach) operations and activities affecting approach and descent flight phases: it does not explicitly include surface operations. However, as the NAS becomes more tightly integrated and focused on trajectory optimization, it is both necessary and informative to extend the boundaries of the analysis beyond what would traditionally be considered "approach operations". The generation and maintenance of safe trajectories near the airport (say 5 nautical miles) depends on appropriate behavior upstream in the process. Because IM-S needs sufficient time (and thus distance) to be effective, the analysis includes scenarios up to 300 NM away from terminal airports.

The ending point of these en route IM-S scenarios will be the transition point from TRACON's arrival control to local airport control tower, which is generally 5 to 10 NM away from the airport—a point after which major trajectory changes are less likely and less effective. Future analyses may include scenarios from the Final Approach Fix to touch down and may even include ground operations at the airports.

2.2.3 Actors (System Components) and Responsibilities

Figure 6 shows the actors and their interactions in IM-S. Table 1 shows the relevant actors and their responsibilities that are considered in our safety analysis of IM-S. According to [24], "The information flows between the Command Center and the Centers are Collaborative Decision Making (CDM) information flows among those facilities (the corresponding capabilities are not shown because they are beyond the scope of this document)".

As shown in the figure, the Center TFM capability (TBFM) will provide (1) FMT constraint information (with TFM-generated speed advisories) to the en route ATC automation for notification to the sector controllers and (2) Constrained Departure Time (CDT) constraint

information to the terminal ATC automation for display in Constraint Lists for the tower controllers.

The flight deck capabilities may include ADS-B Out to broadcast the aircraft's position information to the ATC automation. Otherwise aircraft surveillance is provided by primary or secondary radar and fused track reports.

The en route ATC automation will send speed advisory acceptance and cancellation information to the Center TFM capability. As in today's system, the en route ATC automation will provide all flight plan amendments as updates, as well as fused radar track reports. Flight plans that are maintained will be available to Center TFM, en route ATC, and terminal ATC automation as in today's system. When available, en route ATC automation will send TFM automation ADS-B reported position, altitude, velocity, and Time of Applicability-position information to enhance the trajectory predictions made by TBFM.

Actor responsibilities, information flows, and the assumptions outlined in sections 2.1 and 2.2 are derived from [24]. Section 4 provides requirements and constraints relating to surveillance, responsibilities, and information flow.

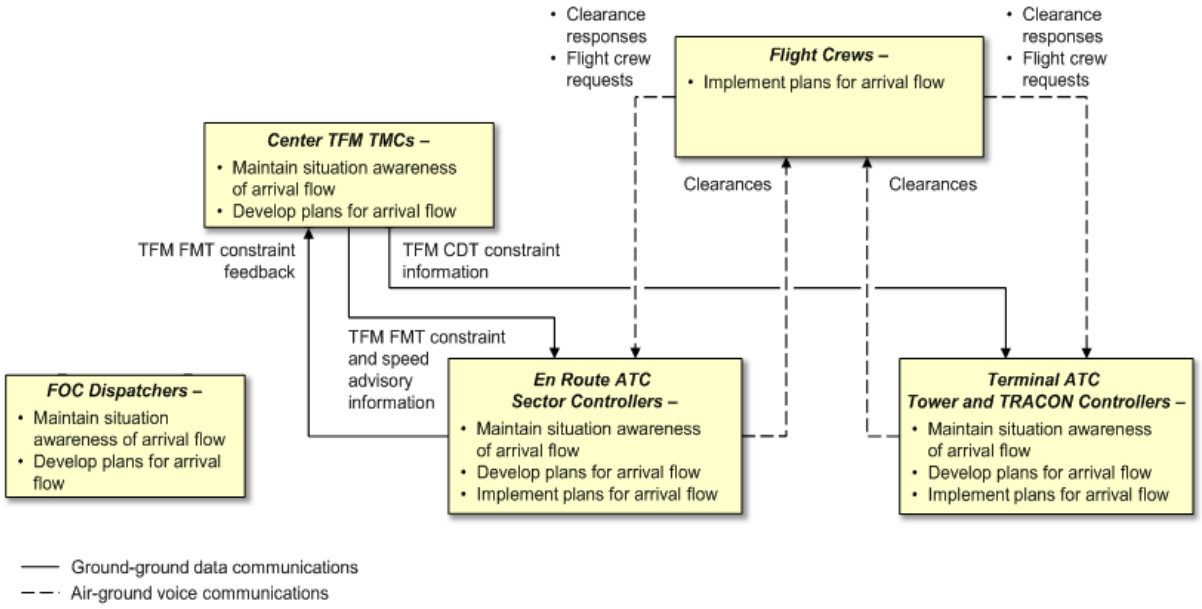


Figure 6: Organizational Structure of and Interactions among the Different Roles [24]

Table 1: Actor Responsibilities in ConOps

Actor	Responsibilities
Center TFM TMCs	The Center TFM is responsible for generating IM-S speed advisories and sending these speed advisories to the relevant air traffic control centers. Center TFM includes the traffic management coordinators (TMC), who are responsible for manually manipulating constraints, as well as the automated tools that will generate constraints and advisories automatically. TFM capabilities should include: • Trajectory modeling • Controlled Departure Time (CDT) / Flow Management Time (FMT) constraint assignment • Speed advisory generation and validation without sector-level problem status
En Route ATC Sector Controllers	En route controllers are responsible for issuing IM-S speed advisories, in addition to traditional responsibilities of separation and flow management. En route controllers are expected to interact with IM-S automated tools in order to provide interval management. En route IM-related automation is expected to provide • Notification of new advisories • Indication of whether an advisory is current or out-of-date (stale) • Interface for response from ATC, including acceptance or rejection • Display control, or interaction between user interface and controller
Flight Crews	Flight crew responsibilities differ depending on the implementation of IM-S. For GIM-S, flight crew responsibilities remain the same as in traditional operations but change slightly for FIM-S. • Execute speed advisories per ATC instruction (GIM-S) • Determine and execute trajectory to meet ATC-prescribed interval requirement (FIM-S)
FOC Dispatchers	No explicit tactical requirements
Terminal ATC Tower and TRACON Controllers	Terminal (tower) controllers are expected to provide a constraint list to the Center TFM, which allows the Center TFM to calculate the interval time based on terminal capacity.

Actor	Responsibilities
TFM Automation	Compute additional distance necessary to absorb delays; compute and propose closed form lateral paths; check candidate advisories for conflicts; compute ETA, STA and delay times; display meter lists and DCT on radar scopes; schedule metered flights to CSPs; estimates of likely flight deviations in response to weather; track cumulative delay across sectors

3 THE STPA HAZARD ANALYSIS FOR GIM-S AND FIM-S

The analysis in this report focuses on TBFM and IM-S and identifies hazardous behavior due to component interaction, human behavior, and software requirements. The results from this study points to areas where the two systems may potentially exhibit dysfunctional interaction. Follow-on work will demonstrate how different alternatives can be traded off in order to reconcile two different operational improvements.

Two graduate students conducted the majority of the analysis in this report over the course of four months, including learning about air traffic control and TBO as neither student previously had much air traffic control knowledge. The graduate students had assistance gaining access to technical documentation from researchers at Lincoln Laboratories and the contract monitors at the FAA. During the course of the analysis there was one technical interchange meeting, which included at least one air traffic controller and design engineer.

3.1 Results for GIM-S

3.1.1 Identifying System Hazards and Control Structure

As in traditional safety analysis, the STPA process starts by identifying hazards, although hazards are not equated to failures, as is often the case. Instead, a hazard is defined as a system state that under worst-case environmental conditions will lead to a loss or accident. This definition encompasses more than simply the states following component failures but includes undesired states that can result from any cause.

The five hazards included are listed in Section 1.3 and reproduced here:

H1: Aircraft violate minimum separation (LOS or loss of separation)

H2: Aircraft enters restricted area

H3: Aircraft enters unsafe atmospheric region

H4: Aircraft enters uncontrolled state

H5: Aircraft assumes unsafe attitude

These hazards were chosen because they are at a high-level of abstraction, they have been used in past ATM systems, and they seem to be complete with those concerns important to safety in the NAS. They are refined into a longer and more detailed list as the analysis proceeds.

For the introduction of IM-S, hazard H-1 is the most relevant and leads to the high-level system safety requirement/constraint: "The speed advisory must not cause a pair of controlled aircraft to violate minimum separation standards." The other hazards are, however, also included in the STPA analysis. The hazard analysis identifies system and component requirements necessary to enforce the safety requirements/constraints associated with all five hazards as they relate to the specific parts of IM-S that are included in the analysis.

STPA uses a functional control model of the system. Figure 7 shows a high level control structure for IM-S. This high-level control structure can be expanded in breadth and detail as the analysis moves forward.

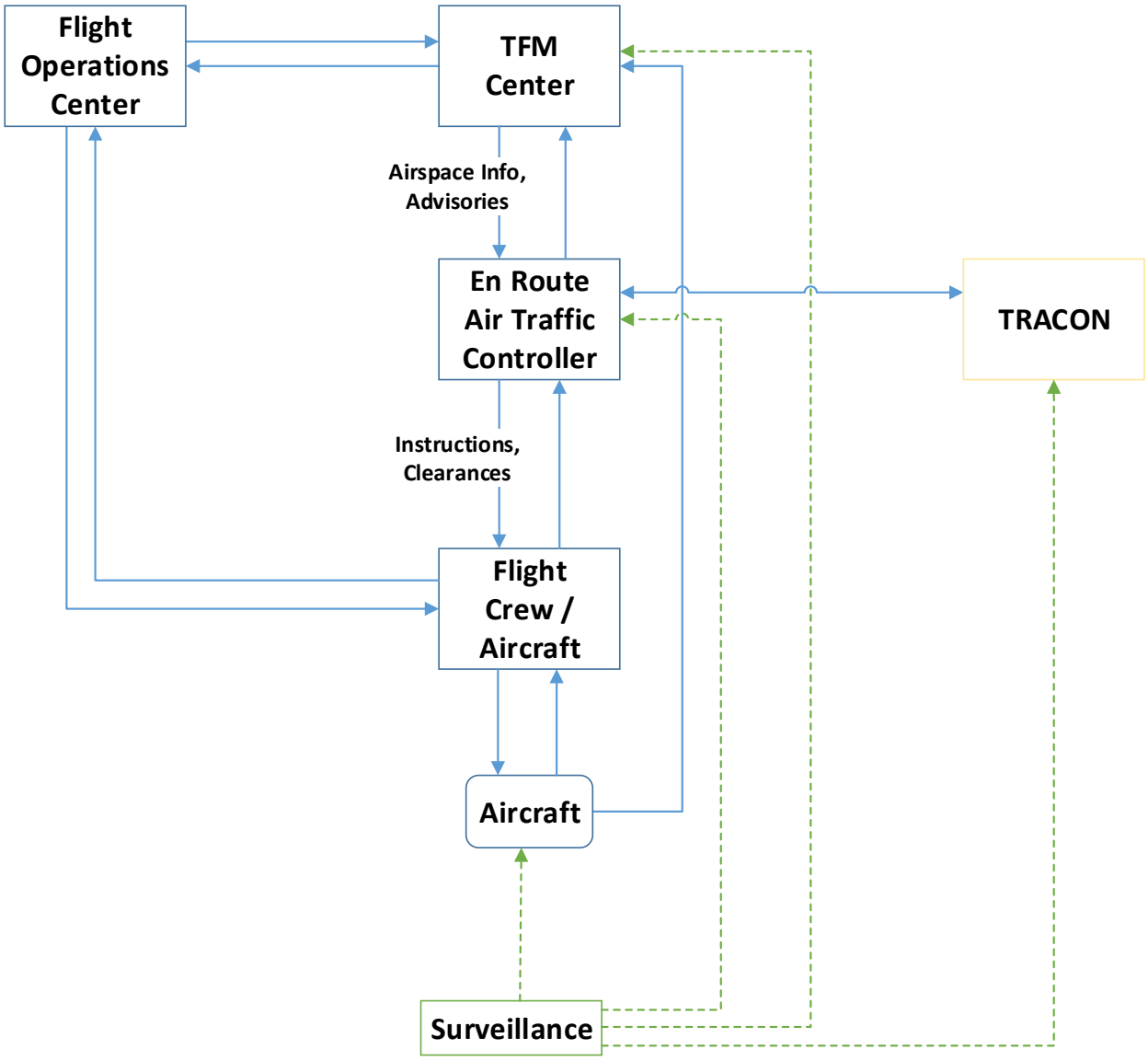
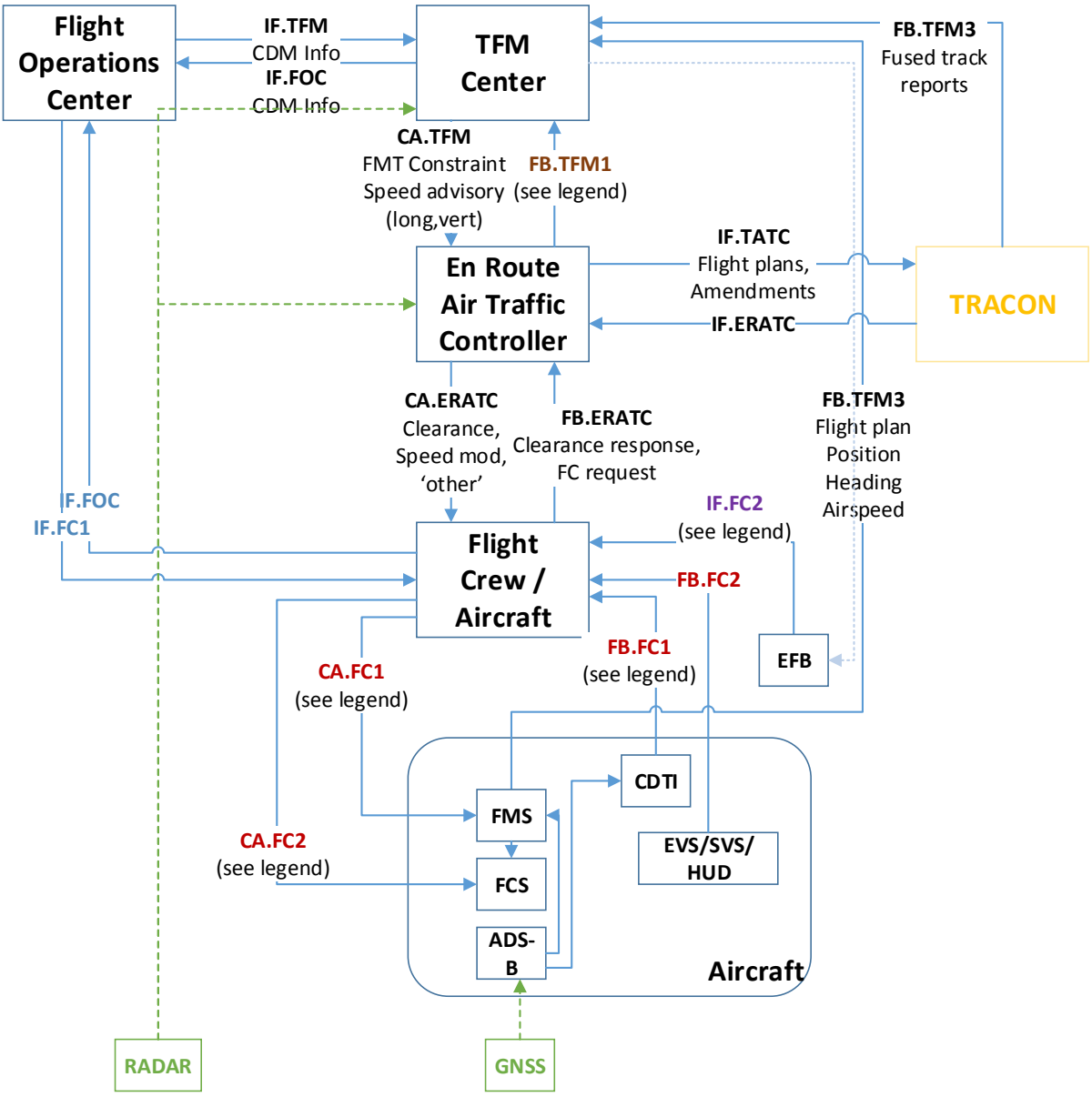


Figure 7: Basic TFM/IM-S Control Structure

The scope of the model shown in Figure 8 can be extended to include additional actors and the fidelity of the structure will increase as large functional actors such as the En Route ATC are broken into sub-groups with unique control responsibilities and information flows. Figure 7 shows a more detailed TFM/IM-S control structure, which is derived from information in the most recent IM-S Concept of Operations [24].

The analysis of each operational improvement begins with the creation of the hierarchical control structure. When analyzing FIM or other operational improvements, multiple control structures are produced that are then compared and combined when evaluating the coupled implementation of several OIs.



LEGEND

CA.FC1
- Input flight plan
- Modify flight plan

CA.FC2
- Modify airspeed
- Modify altitude
- Modify heading

FB.FC1
- Ownship position
- Other a/c position
- Weather

FB.FC2
- Heading
- Angle of attack
- Airspeed

IF.FC2
- Nav charts
- Op manual for a/c

FB.TFM1
- Speed advisory acceptance & cancellation
- Flight plans and amendments
- Fused radar track reports
- ADS-B reported position, alt, speed, and Time of Applicability (position)

Figure 8: Detailed TBFM/IM-S Safety Control Structure

3.1.2 STPA Step 1: Identifying Unsafe Control Actions for GIM-S

STPA Step 1 identifies hazardous control actions for each component that can lead to one or more of the defined system hazards. These identified unsafe control actions are used to refine the high-level safety constraint/requirements into more detailed safety requirements. The four general types of unsafe control actions are shown in Table 5. Additional analysis must also include consideration of why and how a control action required for safety might not be followed (scenario 5 in Section 1.1) but that is done in Step 2 of STPA.

The control actions can be arranged in a table to document the hazardous control actions identified, as in Table 2. The hazardous control actions can then be translated into high-level system and component safety requirements and constraints.

Each row of the table represents a control action that is part of the safety-related responsibilities of the control agent. These control responsibilities may be derived from a system's concept of operations, procedures, software algorithm or pseudocode, or any other available design documentation. The columns represent each of the four types of unsafe control actions. Finally, each entry of the table points to the hazard or hazard involved in that particular unsafe control action.

Consider the potential control action En Route ATC "Provides Clearance" in Table 2. If the En Route ATC does not provide a new clearance, hazard H-1 may result when the current aircraft trajectories will result in an immediate conflict (Column 2). In addition, not providing a speed advisory could have longer-term implications on aircraft separation such as downstream-sector saturation. Alternatively, there are several conditions under which providing the control action (such as modify speed) could lead to the hazard, for example: new airspeed given that causes loss of separation with leading, trailing, or crossing aircraft (Column 3). There are also potentially unsafe control actions related to timing. A hazard could arise if a clearance that was previously safe is provided too late after the aircraft initiation a different set of maneuvers (Column 4). A potentially safe control action could become unsafe if it is applied too long, for example if a speed advisory continues after environmental conditions have changed (Column 5).

General control actions for the En Route ATC are: Modify speed, Modify altitude, Provide Vector, and Give Time-to-Fix clearance. These control actions are not mutually exclusive. For example, an air traffic controller may instruct a flight crew to change direction (vector) while also increasing speed and altitude. Therefore, to maintain generality and traceability, Table 2 lists the unsafe control actions for providing a generic clearance, which may include any of the available control actions.

Specific unsafe control actions for speed modification, vector clearances, and altitude modification are listed in Table 3 through Table 5, respectively. Every unsafe control action for speed advisories, vectors, or altitude advisories in Table 3 through Table 5 has a "parent" unsafe control action in Table 2. A "child" unsafe control action is similar to its parent, but the context of the unsafe control will be different. For example, the first unsafe control actions in are: (1) UCA1.C.a. Not providing a vector clearance is hazardous when the current trajectory leads to LOS and speed modification is not given, and (2) UCA1.C.b. Not providing a vector clearance is hazardous when the current speed leads to LOS and appropriate speed mod exceeds aircraft

capability. In other words, the context for an unsafe control action for speed modification includes the presence, or lack thereof, of other control actions.

Per the IM-S Concept of Operations, speed modifications are explicitly related to IM-S [24] and therefore this report only includes causal analysis of unsafe control actions related to speed modifications (Table 3). Unsafe control actions for vector clearances (Table 4) and altitude modifications (Table 5) are included to illustrate the fact that air traffic controllers have many different actions and combinations at their disposal. Though the unsafe control actions for vector clearances and altitude modifications are not explicitly analyzed for causal factors in this report, some of the causal factors of speed modifications relate to other types of clearances. For example, one potentially unsafe use of a speed modification is when the speed is insufficient to maintain separation and a vector is required (see STPA-G.4S.5.2 in Section 3.1.3).

Table 2: Potentially Unsafe Control Actions for the En Route ATC – General Clearance

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence[5]	Stopped too soon, applied too long
Clearance	UCA1. Not providing a clearance when current trajectory leads to LOS. ↑[H-1]	UCA4. Providing a clearance that leads to LOS. ↑[H-1]	UCA7. Providing a clearance to an aircraft that was previously safe if given too late after a different clearance[1] has been executed by same or other aircraft ↑[H-1]	UCA10. Providing clearance where modified trajectory is applied too long and traffic/weather exists 'downstream[2]' from initiation of maneuver. ↑[H-1;H-2;H-5]
	UCA2. Not providing a clearance when there is convective (or other) weather in the path of the current trajectory ↑[H-3; H-4; H-5]	UCA5. Providing a clearance to the wrong aircraft. ↑[H-1;H-2;H-3;H-4;H-5]	UCA8. Providing a clearance to an aircraft that was previously safe if given too soon before a different clearance has been executed by same or other aircraft ↑[H-1]	UCA11. Providing clearance where modified trajectory is not applied long enough and separation not achieved. ↑[H-1]
	UCA3. Not providing a clearance when prohibited airspace is in the path of the current trajectory ↑[H-2]	UCA6. Providing a clearance that exceeds the aircraft capability. ↑[H-4;H-5]	UCA9. Providing clearance too late after environmental conditions (e.g. weather, aircraft speed, heading, etc) have changed ↑[H-1;H-2;H-3;H-4;H-5]	

Table 3: Potentially Unsafe Control Actions for the En Route ATC – Modify Speed

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Modify Speed[3]	UCA1.S. Not providing a speed modification when the current speed leads to LOS and vector is not given. ↑[H-1]	UCA4.S. Providing a speed modification that leads to LOS. ↑[H-1]	UCA7.S. Providing a speed modification to an aircraft that was previously safe if given too late after a different clearance has been executed by same or other aircraft ↑[H-1]	UCA10.S. Providing speed modification where modified speed is applied too long and traffic/weather exists 'downstream[2]' from initiation of maneuver. ↑[H-1;H-2;H-5]
	UCA2.S. Not providing a speed modification when there is convective (or other) weather in the path of the current trajectory ↑[H-3; H-4; H-5]	UCA5.S. Providing a speed modification to the wrong aircraft. ↑[H-1;H-2;H-3;H-4;H-5]	UCA8.S. Providing a speed modification to an aircraft that was previously safe if given too soon before a different clearance has been executed by same or other aircraft ↑[H-1]	UCA11.S. Providing speed modification where modified speed is not applied long enough and separation not achieved. ↑[H-1]
		UCA6.S. Providing a speed modification that exceeds the aircraft capability (overspeed or stall). ↑[H-4; H-5]	UCA9.S. Providing speed modification too late after environmental conditions (e.g. weather, aircraft speed, heading, etc) have changed ↑[H-1;H-2;H-3;H-4;H-5]	

Table 4: Potentially Unsafe Control Actions for the En Route ATC – Vector Clearance

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Vector Clearance[3]	UCA1.C.a Not providing a vector clearance when the current trajectory leads to LOS and speed modification is not given. ↑[H-1]	UCA4.C. Providing a vector clearance where the new heading leads to LOS ↑[H-1]	UCA7.C. Providing a vector to an aircraft that was previously safe if given too late after a different clearance has been executed by same or other aircraft ↑[H-1]	UCA10.C. Providing vector clearance if vectored heading is applied too long and traffic/weather exists 'downstream[2]' from initiation of maneuver. ↑[H-1;H-2;H-3]
	UCA1.C.b Not providing a vector clearance when the current speed leads to LOS and appropriate speed mod exceeds aircraft capability. ↑[H-1; H-4; H-5]	UCA5.C. Providing a vector clearance where the required maneuvers exceed the aircraft capability ↑[H-4; H-5]	UCA8.C. Providing a vector to an aircraft that was previously safe if given too soon before a different clearance has been executed by same or other aircraft ↑[H-1]	UCA11.C. Vectored heading is not maintained long enough, so that necessary separation is not achieved/maintained. ↑[H-1]
	UCA2.C. Not providing a vector clearance if there is convective (or other) weather in the path of the current trajectory ↑[H-3]	UCA6.C. Providing a vector clearance when there is convective weather in the path of the cleared trajectory ↑[H-3]	UCA9.C. Providing vector too late after environmental conditions (e.g. weather, aircraft speed, heading, etc) have changed ↑[H-1;H-2;H-3;H-4;H-5]	

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
	UCA3.C. Not providing a vector clearance when there is prohibited airspace in the path of the current trajectory ↑[H-2]			

Table 5: Potentially Unsafe Control Actions for the En Route ATC – Modify Altitude

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Modify Altitude[3,4]	UCA1.A. Not providing an altitude modification when the current trajectory leads to LOS and vector AND speed mod is not given. ↑[H-1]	UCA4.A. Providing an altitude modification that leads to LOS. ↑[H-1]	UCA7.A. Providing an altitude modification to an aircraft that was previously safe if given too late after a different clearance has been executed by same or other aircraft ↑[H-1]	UCA10.A. Providing altitude modification where altitude is applied too long and traffic/weather exists 'downstream' at the modified altitude. ↑[H-1;H-2;H-3]
	UCA2.A. Not providing an altitude modification when there is convective (or other) weather in the path of the current trajectory and spd/vec not given ↑[H-3]	UCA5.A. Providing an altitude modification to the wrong aircraft. ↑[H-1;H-2;H-3;H-4;H-5]	UCA8.A. Providing an altitude modification to an aircraft that was previously safe if given too soon before a different clearance has been executed by same or other aircraft ↑[H-1]	UCA11.A. Providing altitude modification where modified altitude is not applied long enough when passing over/under traffic. ↑[H-1]

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
		UCA6.A. Providing an altitude modification that exceeds the aircraft capability (stall). ↑[H-4; H-5]	UCA9.A. Providing altitude modification too late after environmental conditions (e.g. weather, aircraft speed, heading, etc) have changed ↑[H-1;H-2;H-3;H-4;H-5]	

[1] Related clearance (speed or other) used to de-conflict aircraft "j" with aircraft "i" or other. Could be imminent conflict or for downstream flow management

[2] Vector clearance is initially safe and would be if applied for the "correct" time and then aircraft is vectored back towards initial stream.

[3] Each control action assumes that no other clearances are provided to that same aircraft (e.g. speed clearance assumes heading, alt remain the same)

[4] Altitude clearance also includes vertical speed requirement

[5] "Too soon, too late, out of sequence" unsafe control actions are all relative to other clearances. A clearance that is simply too soon or too late is a sub-set of the previous two categories. For example, clearance provided too late (without any context of other clearances) is already captured in the "Not Provided" category, and likewise a clearance provided too soon is captured by the "Providing causes hazard category".

Once the tables are created, the identified unsafe control actions are rewritten as high-level system safety constraints. The constraints are refined further, in a top-down system engineering process, during STPA Step 2. The high-level safety constraints related to the controller unsafe control actions are listed in below. Each constraint contains a reference to the relevant unsafe control action(s) and hazard(s).

[SC-1] ATC must provide a speed modification when the current speed leads to a loss of separation and no other clearance is given. ←UCA1.S, ↑[H-1]

[SC-2] ATC must provide a speed modification when there is convective weather in the path of the current trajectory and no other clearance is given. ←UCA1.S, ↑[H-3;H-4;H-5]

[SC-3] ATC must not provide a speed modification if the new speed leads to loss of separation. ←UCA4.S, ↑[H-1]

[SC-4] ATC must provide speed modifications to the correct aircraft. ←UCA5.S, ↑[H-1;H-2;H-3;H-4;H-5]

[SC-5] ATC must provide speed modifications that are within aircraft capability (overspeed or stall limits). ←UCA6.S, ↑[H-4; H-5]

[SC-6] ATC must verify that aircraft under speed modifications maintain sufficient separation throughout the speed modification clearance. Aircraft may modify their trajectories due to other clearances, weather, or onboard circumstances. ←UCA7.S, UCA8.S, ↑[H-1]

[SC-7] ATC must reject or terminate speed advisories when environmental conditions become detrimental to aircraft control. ←UCA9.S, ↑[H-1;H-2;H-3;H-4;H-5]

[SC-8] Speed advisory must be terminated when current speed will cause aircraft to enter into airspace with saturated traffic or inclement weather. ←UCA10.S, ↑[H-1;H-2;H-5]

[SC-9] ATC must apply speed modification for sufficient duration to achieve and maintain separation. ←UCA11.S, ↑[H-1]

The GIM-S analysis intentionally does not include an analysis of the Flight Crew, as the Flight Crew's role remains unchanged with the use of ground-based automation. Flight Crew analysis is a significant aspect of FIM-S, however. This process of identifying unsafe control actions and translation to safety constraints is repeated for FIM-S, the Flight Crew, and the simultaneous usage of all of these.

3.1.3 Identifying Unsafe Control Actions using Formalized Extension

Though the method presented in the previous sub-section provides a systematic, guided process for generating unsafe control actions, we have created ways to automate the process to reduce effort and, most important, to ensure completeness and rigor [25][26]. As seen in the examples in Table 2 through Table 5, a control action by itself does not provide enough information to determine whether it is safe or hazardous—additional information is required

about the context or environment in which the control action is given. Figure 9 illustrates a generic structure that applies to the hazardous control actions that can be identified.

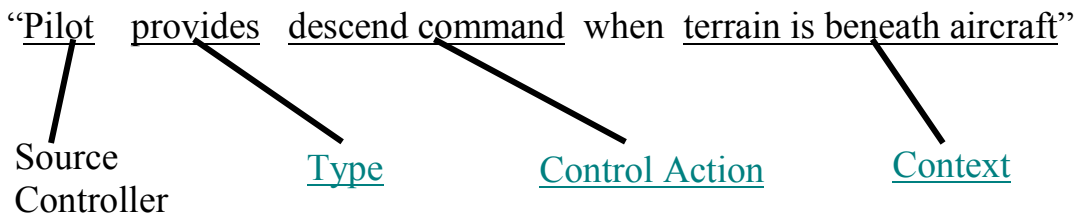


Figure 9: Structure of a hazardous control action (adapted from [25])

According to Thomas [25]:

> The structure in Figure 9 decomposes control actions into four main elements: source controller, type, control action, and context. The source controller is a controller that has the capability to provide the specified control action. The type of a hazardous control action identifies whether the specified action is provided or not provided—either of which could be hazardous. Finally, the context describes the conditions in the system and environment that make action (or inaction) hazardous.
>
> The task of identifying hazardous control actions requires identifying the potentially hazardous contexts of each control action. Although the controllers and control actions are described in the system control structure and are not difficult to identify, hazardous contexts can be more challenging and some contexts may be overlooked using an ad-hoc method. By decomposing the context further it is possible to provide additional guidance and reduce the possibility that important contexts are overlooked.

Consider the example in Figure 9. The Pilot is the source. The type is "provides", and the control action is "descend." Providing this control action is unsafe in a particular context, i.e., there is terrain beneath the aircraft.

Defining a general format for all unsafe control actions allows the analyst to rigorously check all combinations of source, type, control action, and context for hazardous and non-hazardous scenarios and creates the possibility of automated support.

For GIM-S and for air traffic control in general, the structure of unsafe control actions can be decomposed as follows. The source of the control actions is the air traffic controller, and (s)he has the option to give altitude clearances, speed clearances, vector clearances, or any combination of these. In other words, to change the 4-dimensional trajectory of any aircraft, the air traffic controller can request a change in altitude, speed, or direction.

Exposure to loss of separation, unsafe atmospheric conditions, and/or terrain should be avoided. Therefore, the context of unsafe control actions relates to the presence of other aircraft on the trajectory of a given aircraft (which can be decomposed into the other aircrafts' paths, speeds, and altitudes); the presence of inclement weather, and the presence of terrain. The high level, generic structure of ATC unsafe control actions can be decomposed as follows:

- Source: Air Traffic Control (ARTCC or TRACON for GIM-S)
- Control Action & Type:
  - Speed Modification
    - Not Provided
    - Increase Speed*
    - Decrease Speed*
  - Vector Clearance
    - Not Provided
    - Turn Heading*
  - Altitude Modification
    - Not Provided
    - Change Altitude*
- Context
  - Target
    - Lateral to current path (will not cross)
    - Same path, leading (e.g. within 15 degree heading)
    - Same path, trailing (e.g. within 15 degree heading)
    - Crossing
  - Δ-Speed (relative speed between aircraft under instruction and 'target')
    - >0kts
    - <=0kts
  - Vertical Separation
    - >1000'
    - <1000'
  - Terrain
    - Not present
    - Present, in current path
    - Present, lateral to current path
  - Weather (convective or other inclement environment)
    - Not present
    - Present, in current path
      Present, lateral to current path

The example in Figure 9 shows a controller with one specific control action, but an air traffic controller has many different actions to choose from. While there is the potential for combinatorial explosion, in real systems there are a limited number of combinations that are physically possible or relevant.

The analyst can set up rules for unsafe control actions and implement an automatic checker to ensure that all the possible states have been checked without having to emumerate or check all of them. For example, if there is a leading aircraft that is going slower than the IM aircraft, it is obvious that either not providing a speed advisory or telling the aircraft to increase speed (and not vectoring the aircraft or modifying altitude) is hazardous. Our automated tools include a very readable representation for expressing the rules to be used to prune the table.

Table 10 shows three example rules. The rules are represented by the combination ("AND"ing of states (rows) in a column. Any rows that have a star (*) indicate that that particular state does not contribute to the hazardous condition. Rule 1 states that it is always hazardous if there is inclement weather in the path of the aircraft and the aircraft is not vectored in a different direction. More formally, Rule 1 should be interpreted as "Vector clearance not provided AND weather in the path of the aircraft leads to a hazard". The situation is hazardous regardless of the state of other aircraft.

Likewise, it is always hazardous if there is loss of separation between aircraft, regardless of the presence of weather or terrain (Rule 2). Formally this is stated as "An increase in speed is provided AND no other clearance is provided AND another aircraft in its path leads to a hazard".

The columns (or rules) of Table 6 should be read using "OR" logic. There is a potential hazard associated with Rule 1 "or" Rule 2 "or" Rule 3.

Table 6: Example Unsafe Control Actions Using Automated Method

	Rule 1	Rule 2	Rule 3
Speed Modification	*	**Increase V**	*
Vector Clearance	**Not Provided**	**Not Provided**	**Turn Heading**
Altitude Modification	*	**Not Provided**	**NP**
Presence of other Aircraft	*	**Same-Leading**	**Lateral**
Speed Differential of other aircraft	*	**<=0kts**	*
Vertical Separation	*	**<1000**	**<1000**
Presence of Terrain	*	*	*
Presence of Weather	**In Path**	*	*

The automated tools can also detect conflicts in the table. For example, consider Rule 1 and Rule 3 in Table 6. To avoid the hazard in Rule 1, the air traffic controller should vector the aircraft to avoid inclement weather. However, Rule 3 states that it is hazardous to vector the aircraft if there are adjacent aircraft (Presence of other Aircraft = Lateral). This example is somewhat trivial, as the air traffic controller has many other means for resolving such a conflict, including an infinite number of directions to vector the aircraft. The example does illustrate how this automated checking can illuminate conflicts in the goals, hazards, and/or design of a system.

Note that the analysis in this section has assumed worst-case conditions. For example, if there is traffic (or weather or terrain) lateral to the aircraft being controlled, the analysis assumes that a vector clearance is unsafe. Of course, this clearance is *potentially* unsafe. But if a vector

clearance to, say, “50 degrees left” would result in a loss of separation; it might still be safe to turn only 20 degrees, or to turn 50 degrees to the right. The analysis could be extended to include a series of different vector clearances (say 15, 20, 25, etc. and -15, -20, etc.) as well as a series of lateral traffic scenarios. Similar precision could be added to the altitude, terrain, and weather components of the analysis. However, the associated unsafe control actions in Table 6 (with the full set of results in Table 14 of Appendix A) provide a means for checking whether all of the potentially unsafe control actions have been properly accounted for. Furthermore, decomposing the structure of the unsafe control action this way assists in the next step, which is identifying causes of unsafe control actions.

Table 14 in Appendix A shows all of the cases that were considered in the analysis, along with the rules applied to each case.

3.1.4 STPA Step 2: Identifying Causes of Unsafe Control Actions for GIM-S

The next step of STPA examines each control loop in the safety structure to identify potential causal factors for each hazardous control action, i.e., the scenarios that could lead to providing or executing one of the unsafe control actions or to not executing a control action required for safety. Figure 10 shows the generic types of control loop flaws that are examined during the causal analysis.

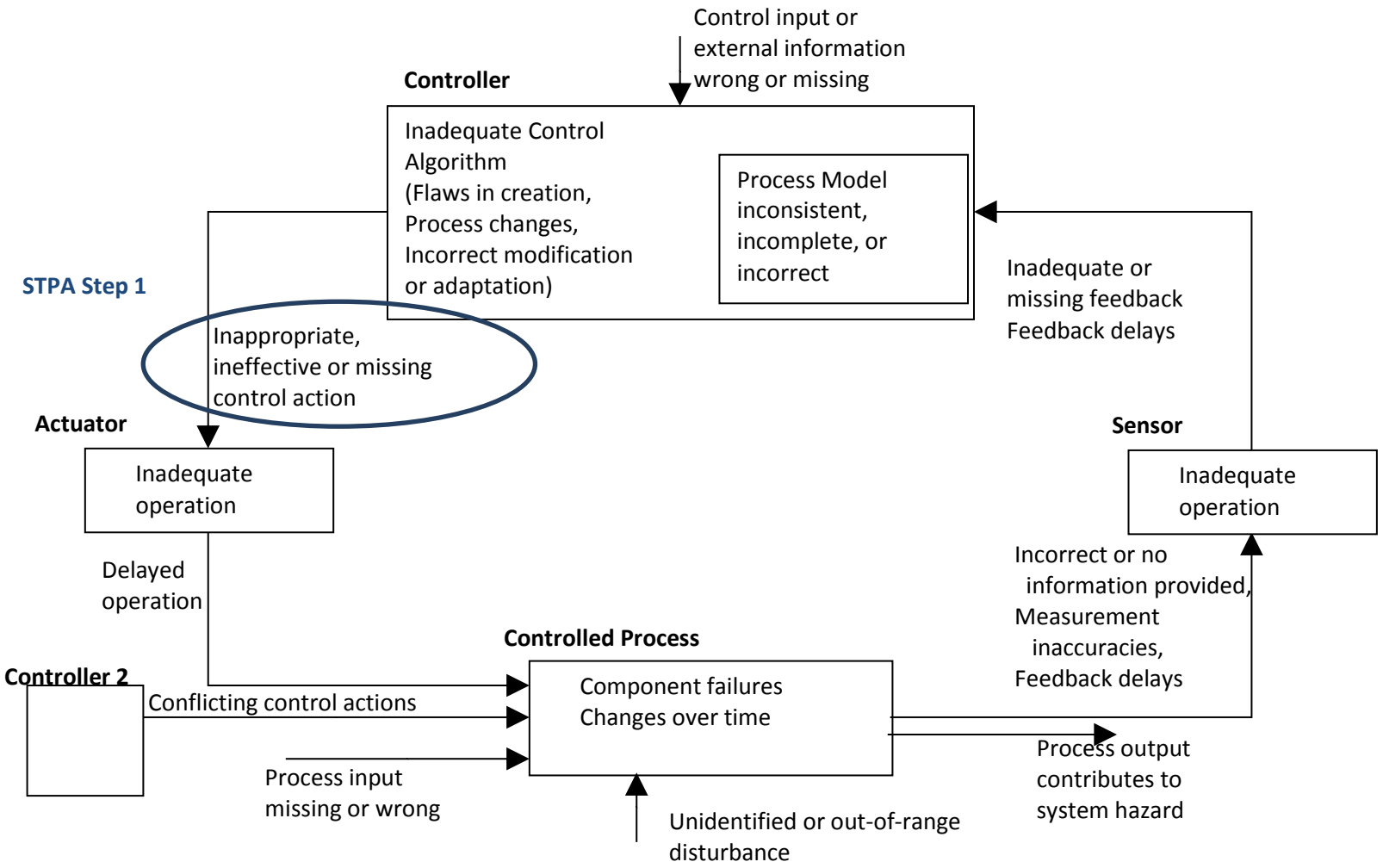
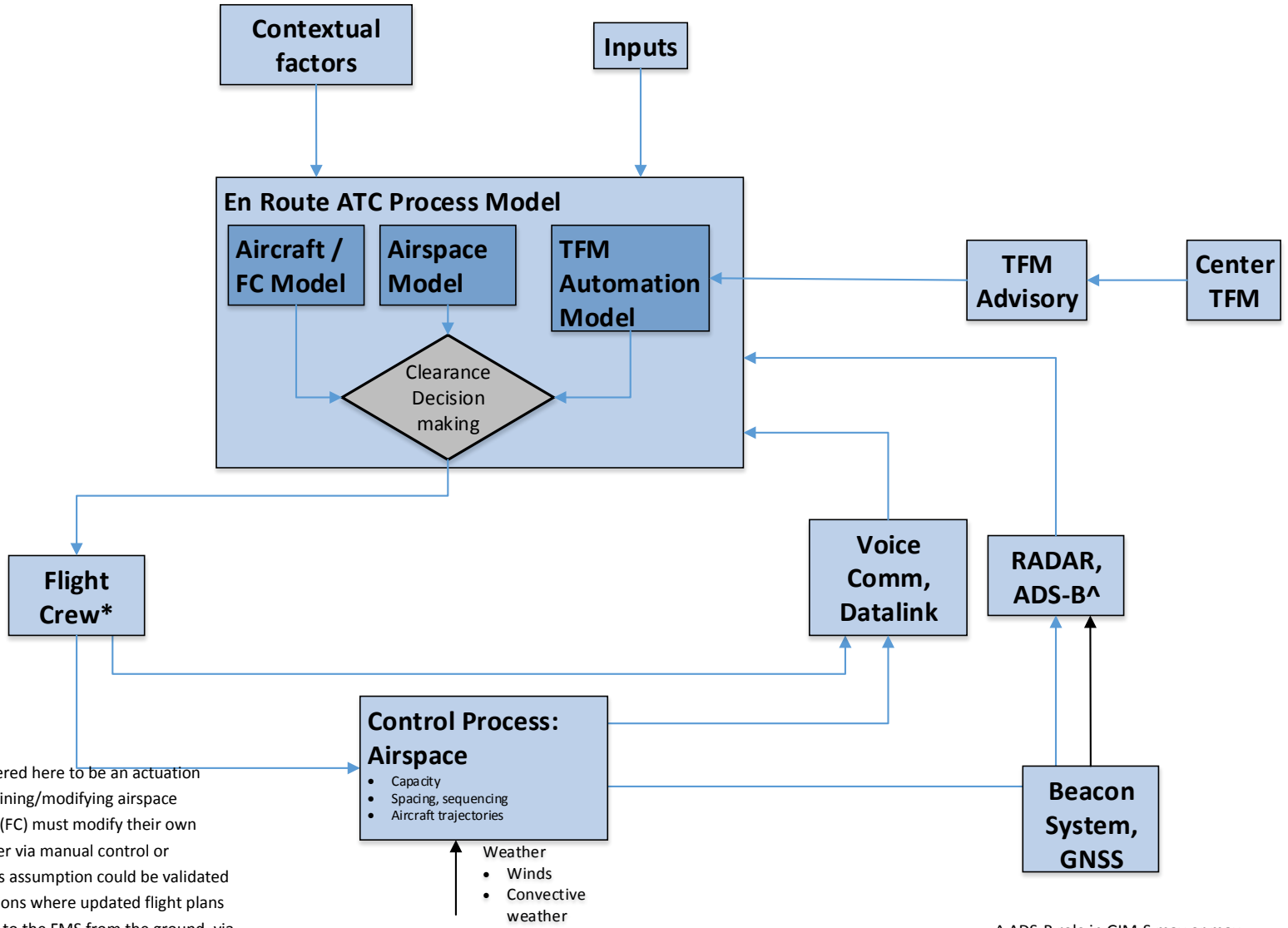


Figure 10: General Control Loop with Causal Factors

Figure 11 shows a sample control loop for the En Route ATC, which identifies the feedback and inputs given to the controller. Feedback paths for air traffic control include voice communication with the flight crews, data communication from the flight deck, and surveillance data from either/both of the radar system or Global Navigation Space System (GNSS) for ADS-B equipped aircraft. Inputs to ATC include procedures from the FAA, capacity demands and constraints from upstream and downstream sectors, and TFM advisories from the TFM automation. In addition, there are contextual factors that influence ATC behavior, including prioritization of system-wide goals such as traffic optimization.

Figure 12 shows the process model states for an En Route Air Traffic Controller who must implement IM-S. The air traffic controller must have a model of the individual aircraft, including aircraft type, capability, current 3-D location, and any advisories the aircraft might be under. The ATC must also have a model of the general airspace, which includes separation requirements, current and predicted separation, current and predicted capacity demands, the environment, and sequence/flow goals. Each of the previous process model variables is identified using the IM-S CONOPS [24]. Finally, the ATC must have a model of any automated tools being used. For GIM-S, the controller must have a model of the TFM automation. A human control agent that is interacting with (overseeing) automation must have a model of that automation including an understanding of how the automation algorithm behaves, what the automation uses in its trajectory model to generate a constraint list, and how to interact with the automation.



* Flight crew is considered here to be an actuation mechanism for maintaining/modifying airspace conditions. Thus, they (FC) must modify their own aircraft trajectory either via manual control or updating FMS, etc. This assumption could be validated in future implementations where updated flight plans could be input directly to the FMS from the ground, via ATC or operation center, or other.

Figure 11: STPA Step 2 Control Loop for En Route ATC

^ ADS-B role in GIM-S may or may not be required, according to the IM-S ConOps.

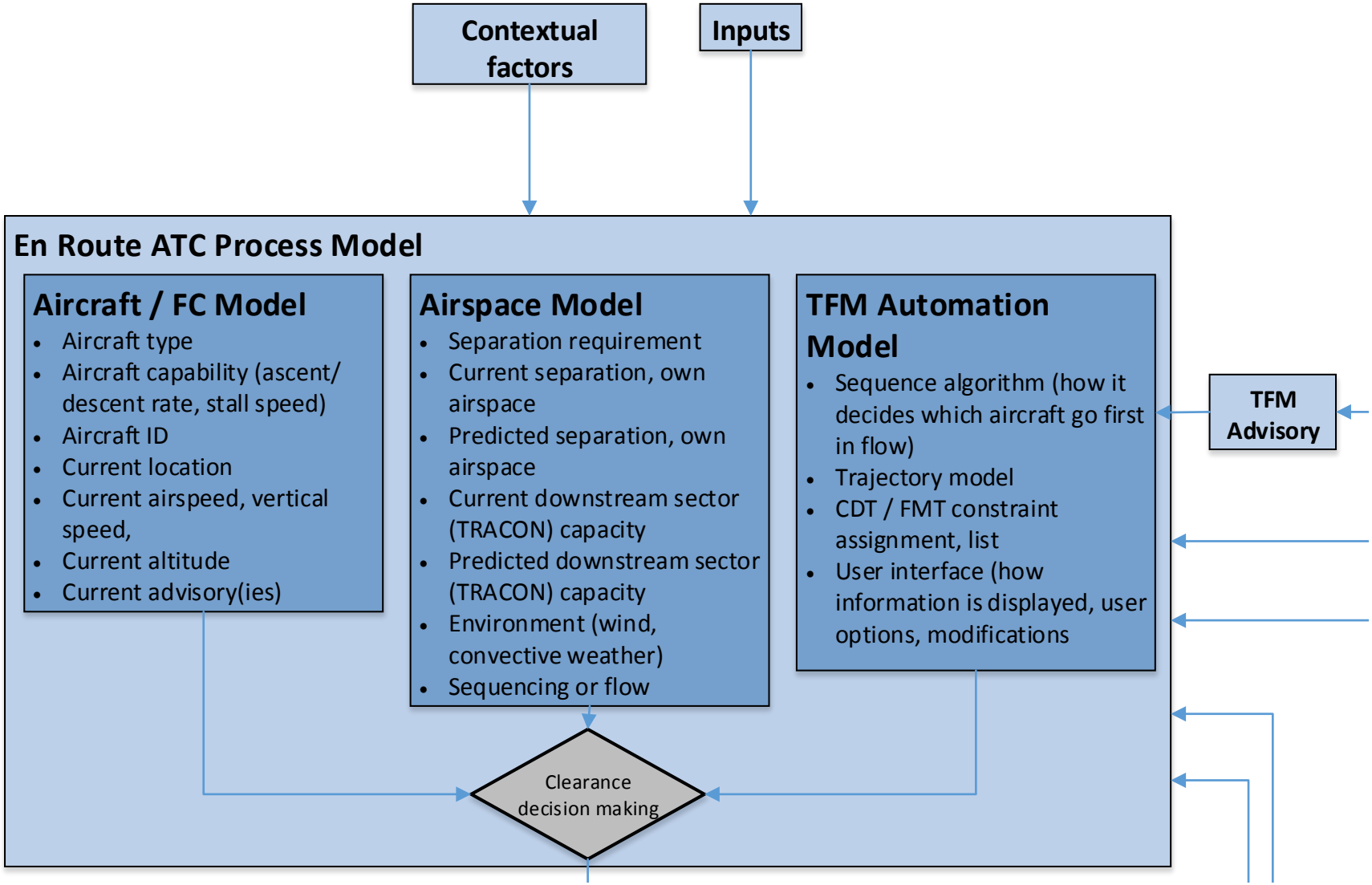


Figure 12: En Route ATC Process Model States

Following is a list of hazardous scenarios and causal factors for a specific control action "Not providing a speed modification is hazardous when the current speed leas to a loss of separation and a vector is not given". The scenarios are related to potential flaws in the controller's process model or inadequate execution by an actuator. The associated causal factors are identified using the generic control loop in Figure 10. To gather information about how the hazard could occur, the guidewords in Figure 9 help the analyst identify where feedback is missing, incorrect, or delayed; disturbances cause the process to behave unexpectedly; actuators behave inadequately; or multiple controllers and processes interact ineffectively. The following list shows scenarios and causal factors related to each guideword in Figure 9.

To improve traceability, the causal analysis (and associated requirements) use the following hierarchical identification scheme:

STPA indicates that the result is identified using STPA hazard analysis

STPA-G indicates which operation, "G" is for GIM-S and "F" is for FIM-S

STPA-G.1S traces to the relevant unsafe control action, "1S" is for UCA.1S

STPA-G.1S.1 represents a scenario related either to process model flaws or inadequate actuator operation

STPA-G.1S.1.1 is a causal factor related to the process model flaw, using the guidewords in Figure 9

Safety-related requirements can be derived from the causal analysis. All of the requirements are children of the parent requirement "ATC must provide a speed modification when the current speed leads to a loss of separation and no other clearance is given" (SC-1 from the previous section). Safety-related requirements have the depth:

STPA-G.1S.1.1.1 is a safety-related requirement or constraint for the particular causal factor

UCA.1S Unsafe Control Action for EnRoute ATC: Not providing a speed modification is **hazardous when the current speed leads to LOS and vector is not given. ↑[H-1]**

STPA-G.1S.1 ATC believes advisory is outside of aircraft envelope, therefore does not provide clearance. [ATC process model of Aircraft / FC incorrect]

STPA-G.1S.1.1 Flight crew / aircraft not flying the reported flight plan

STPA-G.1S.1.1.1 Flight crew must fly the reported flight plan or request a clearance to deviate from the plan. (Allocated to: Flight Crew, FMS)

STPA-G.1S.1.2 Change in environment prevents aircraft from achieving advised airspeed (e.g. headwinds, tailwinds)

STPA-G.1S.1.2.1 ATC and flight crew must monitor compliance with IM speeds. (Allocated to: ATC, Flight Crews)

STPA-G.1S.1.2.2 TFM automation must monitor aircraft compliance with speed advisory and provide an alert if discrepancy exceeds TBD. (Allocated to: TFM Automation)

STPA-G.1S.1.3 TFM calculates that no speed advisories are possible, but other clearance is necessary (but ATC misunderstands as 'no speed advisory')

STPA-G.1S.1.3.1 ATC must issue conflict resolution advisories regardless of state of IM advisory. (Allocated to: ATC)

STPA-G.1S.1.4 ATC incorrectly mistrusts TFM advisory (when it is in fact correct) - e.g. many past false advisories

STPA-G.1S.1.4.1 False advisories must not occur more than TBD percentage of total advisories. (Allocated to:TFM Automation)

STPA-G.1S.1.5 TFM trajectory model predictions use different time-horizon than ATC real-time control

STPA-G.1S.1.5.1 TFM trajectory model time horizon must be synchronized with ATC tools, or TFM Automation,

STPA-G.1S.1.5.2 The time horizon prediction must be presented to ATC. (Allocated to: ERAM)

STPA-G.1S.1.6 Center TFM update rate is too slow"

STPA-G.1S.1.6.1 TFM must update its status every TBD seconds. (Allocated to: TFM Automation)

STPA-G.1S.1.7 Signal gets jammed, corrupted or IM clearance interferes with other clearances

STPA-G.1S.1.7.1 Protection must be provided against jamming or corruption of the signal between Center TFM and ARTCC centers. System-level requirement. See the following two rows for requirement allocation

STPA-G.1S.1.7.2 Protection must be provided against jamming or corruption of the signal between ARTCC centers and flight decks. (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders)

STPA-G.1S.1.7.3 The system must control against radio interference or other types of communication interference. (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders TFM Center software, receivers, transponders)

STPA-G.1S.1.7.4 The IM/TFM system must not interfere with existing ATC systems or procedures. (Allocated to: TFM automation, IM automation, IM user interface)

STPA-G.1S.1.8 Surveillance data is inaccurate

STPA-G.1S.1.8.1 ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.1S.1.8.2 The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation, ADS-B)

STPA-G.1S.1.8.3 TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to:TFM Automation, ADS-B)

STPA-G.1S.1.9 Screen/GUI refresh rate too slow

STPA-G.1S.1.9.1 User interface must refresh every TBD seconds or provide indication that it is not updating. (Allocated to: IM-S Automation)

STPA-G.1S.1.9.2 ATC must not give clearance based on a user interface that is not updating. (Allocated to: ATC, FAA Procedures)

STPA-G.1S.1.10 TFM automation generates advisory outside of aircraft envelope

STPA-G.1S.1.10.1 TFM must generate advisories within aircraft capabilities. (Allocated to: TFM Automation, Airline Operators, Airframe Manufacturers)

STPA-G.1S.1.11 ATC recognizes unsafe TFM advisory, rejects it (or lets it time out), but does not provide appropriate advisory in its place

STPA-G.1S.1.11.1 ATC must provide appropriate action in the event of an unsafe TFM advisory. ATC should reject (or let time out) the advisory and either maintain the previous trajectory if it is safe or issue a new clearance. (Allocated to: ATC)

STPA-G.1S.2 ATC maintains current speed of aircraft i in order to meet downstream sector capacity/ requests [ATC process model of airspace incorrect]

STPA-G.1S.2.1 ATC mistakenly prioritizes downstream saturation over immediate conflict

STPA-G.1S.2.1.1 ATC must give priority to immediate conflict over any downstream demands. (Allocated to: ATC, Conflict detection tools, Interface layout)

STPA-G.1S.2.2 TFM advisory is currently being followed and leads to LOS"

STPA-G.1S.2.2.1 ATC must monitor aircraft under IM speed advisories for conflicts. (Allocated to: ATC, Conflict detection tools)

STPA-G.1S.2.3 ATC does not ‘see’ or account for crossing traffic that will result in near term / immediate conflict

STPA-G.1S.2.3.1 ATC must monitor traffic adjacent to IM traffic flow for conflicts. (Allocated to: ATC, ERAM, Surveillance screens ("glass"))

STPA-G.1S.3 ATC waits for TFM automation to generate speed advisories, and TFM does not provide a de-conflicting advisory [ATC process model of TFM Automation incorrect]

STPA-G.1S.3.1 TFM attempts to generate an advisory for downstream sequencing, but cannot find a valid speed

STPA-G.1S.3.1.1 ATC must issue conflict resolution clearance (not limited to speed modification) even if TFM cannot calculate a valid speed advisory. (Allocated to: ATC, FAA Procedures)

STPA-G.1S.3.2 Over time, ATC develops process of using TFM for all speed advisories, and other tools/mental cues for other types of control actions (e.g. vectors)

STPA-G.1S.3.2.1 ATC must provide appropriate action in the event of an unsafe TFM advisory. (Allocated to: ATC, FAA Procedures)

STPA-G.1S.3.3 TFM does not have accurate aircraft information due to non-updated flight plans

STPA-G.1S.3.3.1 Flight operators (or another entity, TBD) must send updated flight plans to TFM center. Provision must be made to ensure that plan has not been changed due to conflict or other reason. (Allocated to: Airline operators [Potentially ATC, crews, or avionics]

STPA-G.1S.3.4 TFM does not have correct surveillance information and therefore does not or cannot generate speed advisory

STPA-G.1S.3.4.1 TFM must not generate speed advisories with incomplete surveillance data. (Allocated to: TFM automation)

STPA-G.1S.3.4.2 TFM must be provided with airspeed, heading, altitude, vertical speed, and aircraft type for all aircraft in flow. See requirements STPA-G.1.12-14 below for protection against incorrect or inaccurate information. (Allocated to: ADS-B, GNSS, Radar, ERAM)

STPA-G.1S.4 ATC mistrusts TFM automation, ignoring automation even when it generates safe advisories [ATC process model of TFM Automation incorrect]

STPA-G.1S.4.1 Repeated 'bad' (i.e. unsafe or inefficient) advisories from TFM

STPA-G.1S.4.1.1 False advisories must not occur more than TBD percentage of the time. See requirements STPA-G.1S.1.12 - 14 above for protection against incorrect information. (Allocated to: TFM Automation)

STPA-G.1S.5 Aircraft / Flight crew does not perform necessary speed modification, leading to LOS. This may be due to one or a combination of the following factors [Inadequate actuator operation]

STPA-G.1S.5.1 Flight crew does not update FMS

STPA-G.1S.5.1.1 Flight crew must enter IM speed into FMS, or (see STPA-G.1S.5.2 - 5) . (Allocated to: Flight Crew)

STPA-G.1S.5.2 Flight crew flies incorrect speed

STPA-G.1S.5.2.1 Flight crew must manually fly IM speed (see STPA-G.1S.5.3) . (Allocated to: Flight Crew)

STPA-G.1S.5.2.2 Flight crew must not deviate from the IM speed provided unless IM speed leads to a hazard. (Allocated to: Flight Crew)

STPA-G.1S.5.2.3 Flight crew must notify ATC of intentional deviation from IM speed and why. (Allocated to: Flight Crew)

STPA-G.1S.5.4.1 Flight crew must alert ATC of degraded aircraft performance. (Allocated to: Flight Crew)

STPA-G.1S.5.3 FMS does not follow flight plan

STPA-G.1S.5.3.1 FMS must follow flight plan to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) . (Allocated to: FMS)

STPA-G.1S.5.3.2 TFM must be provided with surveillance data to verify if flight is performing as expected to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) . (Allocated to: ADS-B, Radar)

STPA-G.1S.5.3.3 TFM must check that flight performance is within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed). (Allocated to: TFM automation, [ERAM])

STPA-G.1S.5.3.4 TFM (or other tool such as ATC automation) must provide alert when performance is not within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed). (Allocated to: TFM automation, [ERAM])

STPA-G.1S.5.4 Degraded performance of aircraft

STPA-G.1S.5.4.1 Flight crew must alert ATC of degraded aircraft performance. (Allocated to: Flight Crew)

Once the final step of STPA has been applied to determine potential causes for each hazardous control action identified in STPA Step 1, the causes should be eliminated or controlled in the design at the system-level or detailed behavior requirements must be levied on the system components. The STPA process will be repeated during the analysis of FIM. It is expected that during the analysis of the combined GIM and FIM OIs, this step will reveal gaps and/or conflicts between the procedures and infrastructure associated with both.

Listed above are the causal factors and scenarios related to the ATC process model and the unsafe control action "Providing a speed modification to an aircraft that was previously safe if given too late after a different clearance has been executed by same or other aircraft". The following example depicts such a scenario related to this hazard (Figure 13(a)). At time t_0, TFM generates a speed advisory for AC_1 for its interval with AC_2. However, ATC gives a different advisory to AC_1 and actually instructs a greater speed change in order to resolve the conflict with the crossing aircraft, AC_k. Meanwhile, ATC lets the TFM-generated advisory time-out.

At time t_1, TFM generates a *new* speed advisory for AC_1, using assumptions about the speed and position from the t_0 condition (but updated to account for the passage of time). Because there are no new conflicts and the new speed advisory appears to be reasonable, ATC accepts the new TFM-generated speed. This part of the scenario is shown in Figure 13(b).

At time t_1, TFM did not have an updated model of the aircraft trajectory, and the fused-track data was not current or accurate. This latency or inaccuracy could be due to incorrect ADS-B data, low refresh rate of primary/secondary radar, other nominally expected conditions, or some other type of anomaly. Additionally, ATC did not update the flight plan into the automation due to the cognitive load of de-conflicting AC_1 and AC_k. Therefore, at time t_2, AC_1 and AC_2 lose separation, shown in Figure 13(c).

This example scenario illustrates several important types of design problems that STPA can identify. First, timing is important, both in terms of when a control action is (or is not) issued

and also in terms of when feedback is (or is not) provided to the various control agents. Second, it is vital that the control agents have a mutually consistent and accurate model of the controlled process, which in this case is the airspace traffic. Finally, it is important that control agents have a mutually consistent model of how the other agents make control decisions. It must be emphasized that GIM-related automation tools are not intended to recognize and eliminate traffic conflicts. The lack of conflict detection has implications temporally on events immediately beyond a potential conflict. In fact, as Figure 13 briefly shows, the limitations of the automation may manifest themselves well after a potential conflict has been resolved. The lack of conflict resolution (and any other limitation) must constantly be a part of the air traffic controller's model of the automation.

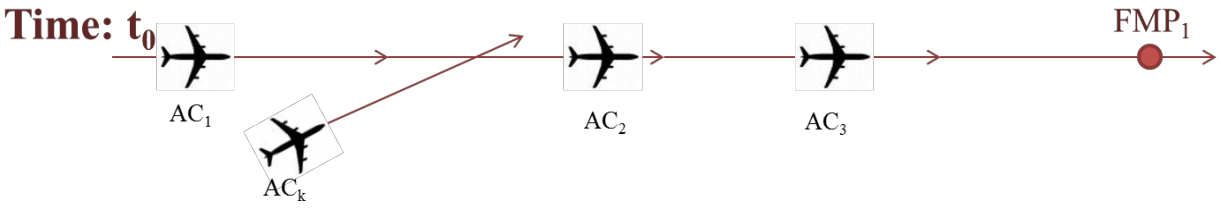


Figure13 (a)

Figure13 (b)

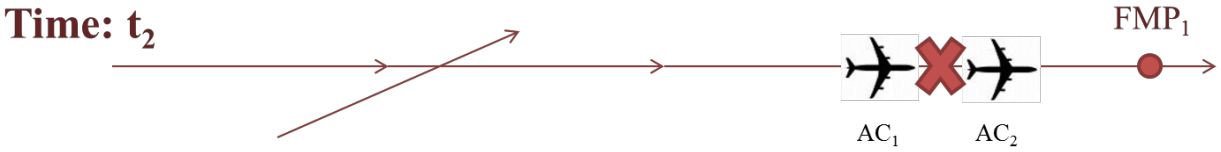


Figure 13 (c)

Figure 13: Example Scenario for Loss of Separation (UCA.6.S)

3.2 FIM-S Results

The FIM-S hazard analysis draws largely on the GIM-S analysis, particularly for the early steps. Both the hazards (Section 3.1.1) and the control structure are essentially identical between GIM-S and FIM-S. Factors that are significantly different, however, include the clearances available to the air traffic controller and the lower-level actions available to the flight crews. The control structure (Figure 11) is modified slightly to reflect the available actions and safety-related responsibilities outlined in [28]. The main differences are the additional clearances that the ATC may grant:

- Maintain Current Spacing Clearance: used when the controller wants the IM Aircraft to maintain the current Spacing Interval, as determined by the FIM Equipment, until the Planned Termination Point.

- Achieve-by Then Maintain Clearance: used when the controllers want the IM Aircraft to achieve the Assigned Spacing Goal at the Achieve-by Point and then maintain the Assigned Spacing Goal until the Planned Termination Point

- IM Turn Clearance: used when the controller wants the IM Aircraft to adjust its horizontal path to help achieve the Assigned Spacing Goal at the Achieve-by Point. The "controller identifies the Intercept Point, Achieve-by Point, and Assigned Spacing Goal. The FIM Equipment provides the IM Turn Point position and the flight crew follows its current navigation clearance until the IM Turn Point is reached and the turn to the Intercept Point is executed." [28]

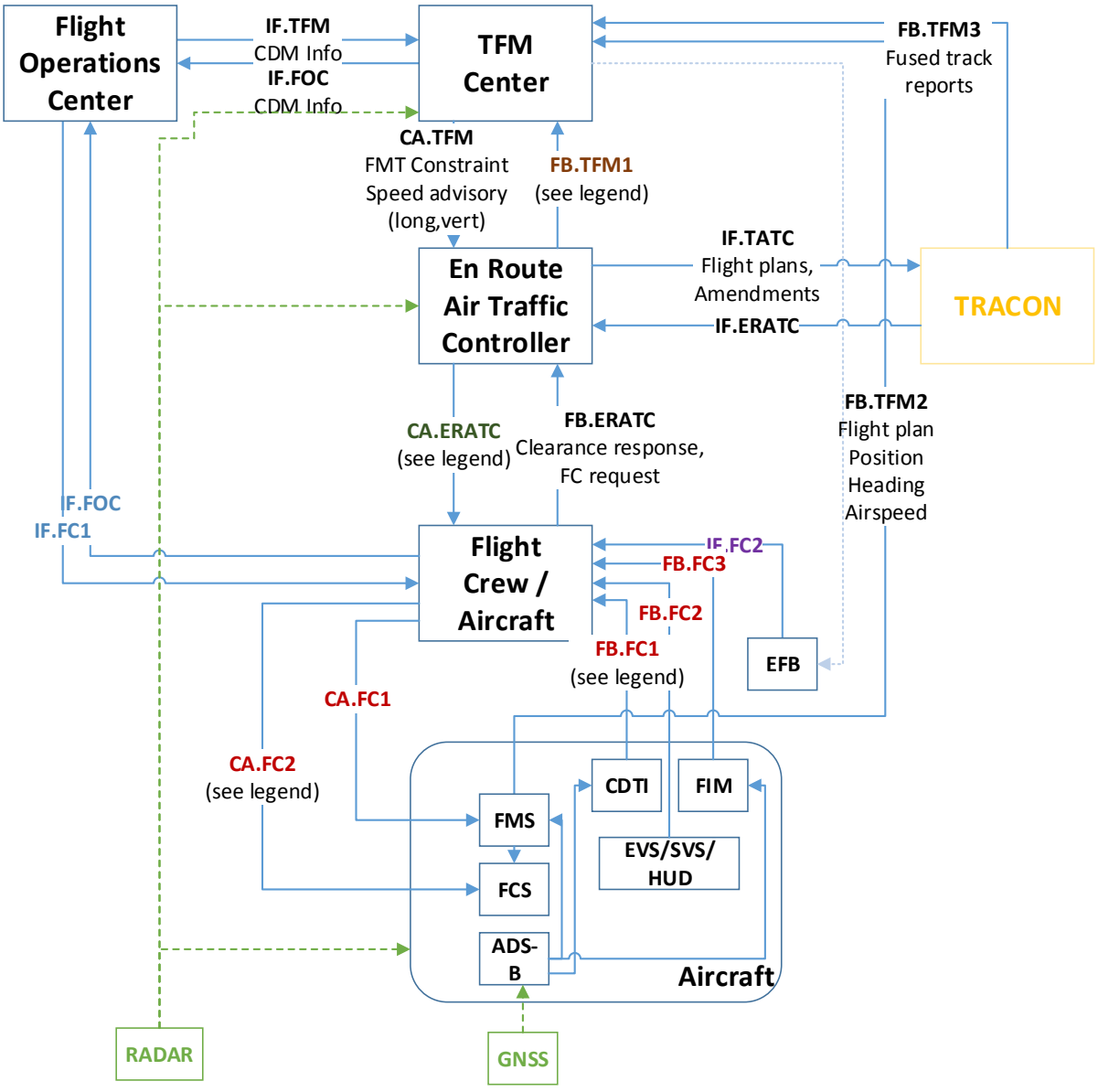
The flight crews do not have any explicitly new control actions, but the crews will receive instructions from FIM automation and must guide their aircraft to achieve whichever FIM clearance they receive from ATC and flight parameters from FIM automation. Therefore, the feedback/input mechanisms in Figure 14 are also slightly modified from the GIM-S version.

In addition to the different IM clearance types, controllers can assign different spacing goal types. Spacing goal types include Precise Value spacing, Closed Interval spacing, and No Closer than Interval spacing. As the name suggests, Precise Value spacing is when an aircraft is required to achieve and maintain a precise time interval relative to a Target Aircraft. Closed Interval spacing requires that an aircraft achieve an interval between a minimum and maximum assigned value (e.g. spacing must be between 60 and 120 seconds). DO-328 states that a closed interval is used when the maximum traffic capacity is not the principal concern [28]. Finally, No Closer than Interval requires that the IM aircraft achieve/maintain a spacing that is greater than or equal to a specified value.

See Table 8 for a list of terminology and descriptions related to FIM-S.

Table 7: FIM-S Terminology (adapted or quoted from [28])

Term	Description
IM Aircraft	An aircraft that is equipped with FIM Equipment that is instructed to perform an IM Operation
Target Aircraft	The aircraft against which the IM Aircraft is performing the IM Operation
Assigned Spacing Goal	Time or distance interval between the IM Aircraft and Target Aircraft assigned by the controller as part of the IM Operation
Intercept Point	As part of an IM Turn, a point along the IM Aircraft's Intended Flight Path to which the aircraft turns direct to in order to complete the IM Turn.
Achieve-by Point	Point on the IM Aircraft's Intended Flight Path, where the Spacing Interval is expected to be within the IM Tolerance of the Assigned Spacing Goal.
IM Turn Clearance	Controller wants the IM Aircraft to adjust its horizontal path to help achieve the Assigned Spacing Goal at the Achieve-by Point
Maintain Current Spacing clearance	Controller wants the IM Aircraft to maintain the current Spacing Interval, as determined by the FIM Equipment, until the Planned Termination Point
Achieve-by then Maintain clearance	Controllers want the IM Aircraft to achieve the Assigned Spacing Goal at the Achieve-by Point and then maintain the Assigned Spacing Goal until the Planned Termination Point
Precise Value spacing	IM aircraft required to achieve precise value relative to Target
Closed Interval spacing	IM aircraft required to achieve spacing between two assigned values relative to Target
No Closer than Interval	IM Aircraft is required to achieve and/or maintain a spacing that is greater than or equal to the value specified



LEGEND

CA.FC1
- Input flight plan
- Modify flight plan

CA.FC2
- Modify airspeed
- Modify altitude
- Modify heading

CA.ERATC
- Maintain clearance
- Achieve-by
- IM Turn
- IM parameters
- Other clearnc

FB.FC1
- Ownship position
- Other a/c position
- Weather

FB.FC2
- Heading
- Angle of attack
- Airspeed

FB.FC3
- IM Speed
- Turn Point

IF.FC2
- Nav charts
- Op manual for a/c

FB.TFM1
- Speed advisory acceptance & cancellation
- Flight plans and amendments
- Fused radar track reports
- ADS-B reported position, alt, speed, and Time of Applicability (position)

Figure 14: FIM-S Control Structure (includes GIM-S functionality)

3.2.1 Identifying Unsafe Control Actions for FIM-S

The four general types of unsafe control actions are shown in Table 5 in Section 3.1.2. Because FIM-S is a supplement to the existing air traffic management system, as opposed to a replacement for some types of clearances, the generic unsafe control actions in Table 2 (page 34) still apply. In addition to these general unsafe control actions, FIM-S introduces a new set of related unsafe control actions related to specific IM clearances granted by ATC. Moreover, since a greater degree of authority is granted to flight crews and their aircraft equipment, there are an additional set of unsafe control actions related to flight crew execution of IM clearances.

Table 8 through Table 11 contain the FIM-S-related unsafe control actions for ATC. Table 12 contains the FIM-S-related unsafe control actions for IM flight crews.

Table 8: **Air Traffic Control Unsafe Control Actions for generic "IM Clearance" (FIM-S)**

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
IM Clearance	UCA13. Not providing IM clearance when no other clearances given and current aircraft trajectories will lose separation ↑[H-1]	UCA14. Providing IM clearance where new trajectory will lead to loss of separation with target aircraft ↑[H-1]	UCA18. Providing an IM clearance to an aircraft that was previously safe if given too late after a different clearance has been executed by same or target (or non-target) aircraft ↑[H-1]	UCA21. IM Clearance applied too long as separation requirements changed, e.g. capacity demands change or flight segment necessitates different spacing ↑[H-1]
		UCA15. Providing IM clearance where new trajectory will lead to loss of separation with non-target aircraft ↑[H-1]	UCA19. Providing an IM clearance to an aircraft that was previously safe if given too soon before a different clearance has been executed by same or target (or non-target) aircraft ↑[H-1]	
		UCA16. Providing IM clearance where trajectory exceeds aircraft capability ↑[H-4]	UCA20. Providing IM clearance too late after enviornmental conditions (e.g. weather, aircraft speed, heading, etc) have changed ↑[H-1;H-2;H-3;H-4;H-5]	
		UCA17. Providing a IM clearance if there is convective weather in the path of the IM trajectory ↑[H-2; H-3; H-5]		

Table 9: Air Traffic Control Unsafe Control Actions for Maintain Current Spacing clearance (FIM-S)

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Maintain Current Spacing Clearance	UCA13.M. Maintain Current Spacing clearance not provided, and no other clearance provided, when current speed is too fast and leads to loss of separation with leading (or merging/crossing) aircraft or too slow and leads to LOS with trailing aircraft ↑[H-1]	UCA14.M. Maintain Current Spacing clearance provided when current spacing between FIM and target is too little ↑[H-1]	UCA18.M. Maintain Current Spacing clearance provided before or after a (non-target, could be in a different IM clearance) aircraft is instructed to merge into flow or aircraft in flow changes speeds ↑[H-1]	UCA21.M. Maintain Current Spacing clearance applied too long as separation requirements changed, e.g. capacity demands change or flight segment necessitates different spacing ↑[H-1]
		UCA15.M. Maintain Current Spacing clearance provided when spacing will cause receive aircraft to be incorrect speed for merging aircraft or non-target aircraft in flow ↑[H-1]	UCA19.M. Maintain Current Spacing clearance executed where target aircraft modifies speed during Maintain clearance and exceeds receiving aircraft capability ↑[H-4]	UCA22.M. Maintain Current Spacing clearance stopped too soon as non-target aircraft merge into flow based on assumption of longer Maintain clearance ↑[H-1]
		UCA16.M. Maintain Current Spacing clearance that results in trajectory which exceeds FIM aircraft capability ↑[H-1]	UCA20.M. Maintain Current Spacing clearance provided too long before or after environmental conditions change ↑[H-2]	

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
		UCA17.M. Maintain Current Spacing clearance is hazardous if given in lieu of vector (turn) clearance when trajectory of target leads to convective weather or restricted airspace [H-2; H-3; H-5]		

Table 10: Air Traffic Control Unsafe Control Actions for Achieve-by then Maintain (FIM-S)

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Achieve-by then Maintain	See UCA 13.M	See UCA 14.M	UCA18.AB. Achieve-by then Maintain clearance provided before or after a (non target, could be in a different IM clearance) aircraft is instructed to merge into flow or aircraft in flow changes speeds ↑[H-1]	See UCA 21.M
	UCA13.AB. Achieve-by aspect of clearance not provided, and achieve-by is necessary to achieve separation with non-target aircraft ↑[H-1]	See UCA 15.M	UCA19.AB. Achieve-by then Maintain clearance is hazardous if target aircraft modifies speed during Maintain clearance and exceeds receiving aircraft capability ↑[H-4]	See UCA 22.M
		See UCA 16.M	UCA20.AB. Achieve-by then Maintain clearance provided after environmental conditions change ↑[H-2]	

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
		See UCA 17.M		
		UCA14.AB. Achieve-by point given that causes loss of separation with other (non-target) merging or in-path aircraft ↑[H-1]		
		UCA15.AB. Achieve-by point given that causes aircraft to increase / decrease airspeeds to levels that exceed overspeed / stall capability of aircraft ↑[H-4]		

Table 11: Air Traffic Control Unsafe Control Actions for IM Turn Clearance (FIM-S)

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
IM Turn Clearance	See all Maintain / Achieve-by unsafe control actions, with addition of Intercept Point	See all Maintain / Achieve-by unsafe control actions, with addition of Intercept Point	See all Maintain / Achieve-by unsafe control actions, with addition of Intercept Point	See all Maintain / Achieve-by unsafe control actions, with addition of Intercept Point
	UCA13.T. IM Turn Clearance not provided when speed-only clearance would not prevent loss of separation with target, merging, or in-track aircraft ↑[H-1]	UCA14.T. IM Turn Clearance provided where Intercept Point results in loss of separation with traffic that was previously off-track ↑[H-1]	UCA18.T. IM Turn clearance is given after IM aircraft reaches its IM turn point, resulting in a trajectory that potentially exceeds aircraft capability ↑[H-4]	
	UCA22.T. IM Turn Clearance not provided when speed-only clearance would exceed aircraft capability ↑[H-4]	UCA15.T. IM Turn Clearance provided where Intercept Point exceeds aircraft capability, including turn rate ↑[H-3; H-4]		
	UCA23.T. IM Turn Clearance not provided when IM spacing is needed and convective weather or restricted airspace is in previous aircraft path ↑[H-2; H-5]	UCA16.T. IM Turn Clearance provided where turn-back or Intercept Point is in restricted airspace or convective weather ↑[H-2; H-5]		

Table 12: Flight Crew Unsafe Control Actions for IM Execution (FIM-S)

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Execute IM Clearance	UCA.FC.1. Flight crew does not execute IM clearance, which is necessary to maintain safe separation from other aircraft ↑[H-1]	UCA.FC.2. Flight crew executes different type of IM clearance than was given by ATC (e.g. executes maintain current instead of achieve-by) and causes loss of separation ↑[H-1]	UCA.FC.7. Flight crew executes IM clearance too long after it has been requested/accepted and traffic pattern has changed ↑[H-1]	UCA.FC.10. Flight crew continues IM clearance after termination point and other aircraft trajectories' separation(s) are based on IM aircraft stopping at termination point ↑[H-1]
		UCA.FC.3. Flight crew executes IM clearance with incorrect parameters (e.g. wrong speed, incorrect turn, incorrect Spacing Goal Type) ↑[H-1]	UCA.FC.8. Flight crew executes IM clearance too long after it has been requested/accepted and environment has changed ↑[H-1; H-2]	UCA.FC.11. Flight crew terminates IM clearance before termination point and other aircraft trajectories' separation(s) are based on IM aircraft continuing to termination point ↑[H-1]
		UCA.FC.4. Flight crew executes IM clearance instead of other maneuver, where other maneuver is necessary to maintain separation ↑[H-1]	UCA.FC.9. Flight crew executes IM clearance too soon before it is actually accepted by ATC ↑[H-1]	

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
		UCA.FC.5. Flight crew executes IM clearance outside of performance bounds or at extremum of performance bounds ↑[H-3; H-4]		
		UCA.FC.6. Flight crew executes IM clearance instead of other maneuver, where other maneuver is necessary to avoid inclement weather, terrain, or restricted airspace ↑[H-2; H-5]		

3.2.2 Identifying Causes of Unsafe Control Actions for FIM-S

Recall that the next step of STPA examines each control loop in the safety structure to identify potential causal factors for each hazardous control action, i.e., the scenarios that could lead to providing or executing one of the unsafe control actions. Figure 15 shows a sample control loop for the En Route ATC, which identifies the feedback and inputs given to the controller. Feedback paths for air traffic control include voice communication with the flight crews, data communication from the flight deck, and surveillance data from either/both of the radar system or Global Navigation Space System (GNSS) for Automatic Dependent Surveillance-Broadcast (ADS-B) equipped aircraft. Inputs to ATC include procedures from the FAA, capacity demands and constraints from upstream and downstream sectors, and potential IM advisories from the IM automation. As Figure 15 notes, we are unsure whether decision support tools or automation are suggested or required for flight deck-based IM. In addition, there are contextual factors that influence ATC behavior, including prioritization of system-wide goals such as traffic optimization.

A current and accurate process model is important for each control agent in the system. The process model for FIM-S (Figure 15) is slightly different than that for GIM-S (Figure 11). The air traffic controller must consider aspects that are specific to FIM operations, such as the Starting Event, Achieve-by Point, Intercept Point, Planned Termination Point, IM Tolerance, clearance type, and others. Some of these process model variables are similar to those required for providing traditional clearances, such as vectoring to a certain fix or applying bounds around a desired interval range. There are, however, differences in nomenclature as well as differences in the level of autonomy granted to flight crews.

Other factors in the control loop of Figure 15 are similar to that of GIM-S, although there might be greater influence in keeping track of “Current advisories / Clearance types” for aircraft under IM. The rationale for this statement again has to do with the authority granted to flight crews, and their equipment, under FIM-S.

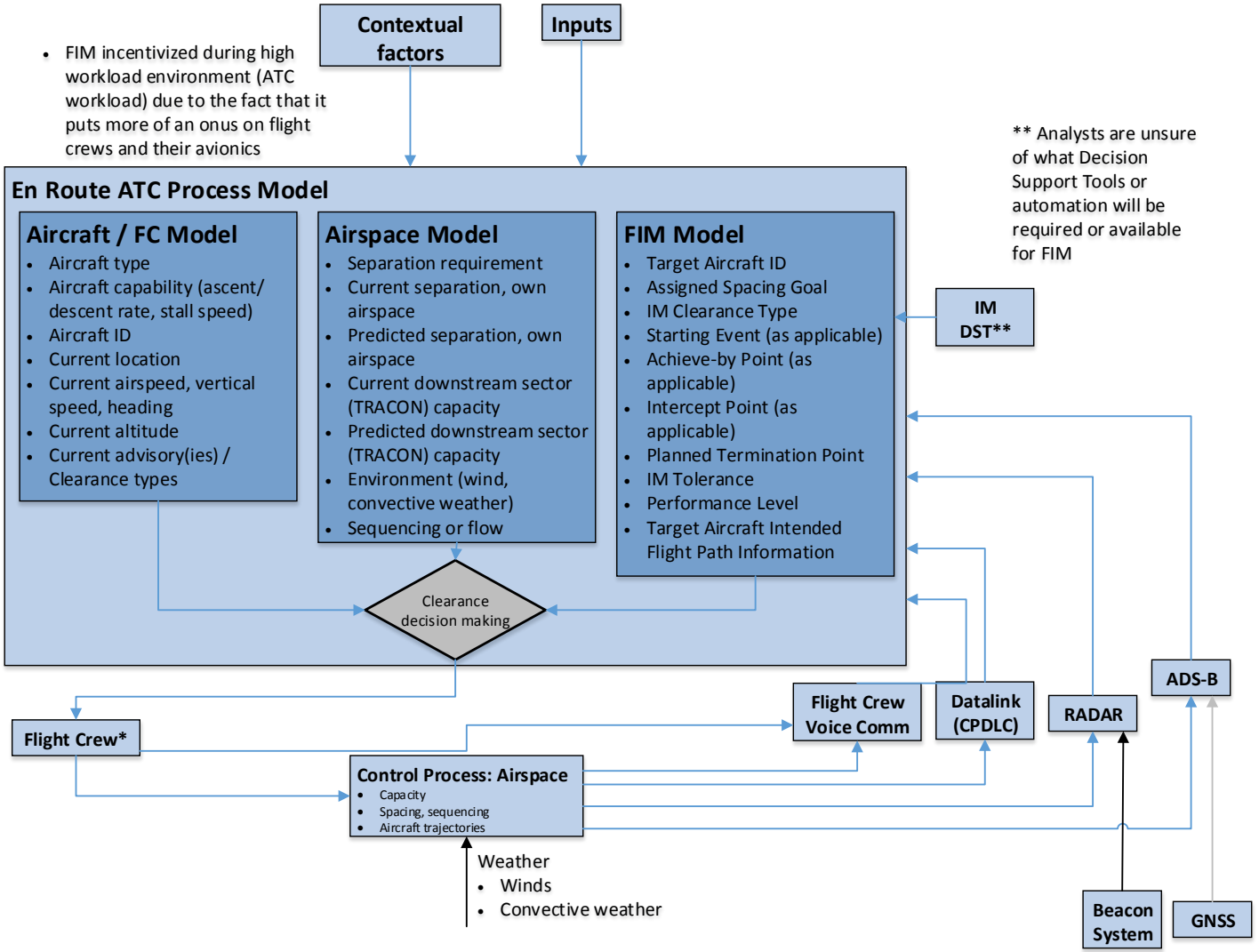


Figure 15: STPA Step 2 Control Loop for ATC (FIM-S)

Following are the causal analysis results for one of the FIM-S unsafe control action: "Maintain Current Spacing clearance provided when spacing will cause receive aircraft to be incorrect speed for merging aircraft or non-target aircraft in flow". See Section 3.1.3 for an explanation of identification scheme.

UCA15.M. Unsafe Control Action for EnRoute ATC: Maintain Current Spacing clearance provided when spacing will cause receive aircraft to be incorrect speed for merging aircraft or non-**target aircraft in flow ↑[H-1]**

STPA-F.14T.1 ATC believes that FC is (or will be) flying a different speed, therefore ATC assumes that separation requirements will be met, and/or issues other clearances based on this assumption. [Process Model Flaw: Aircraft / FC Model]

STPA-F.14T.1.1 Incorrect aircraft ID on radar or flight strip

STPA-F.15T.1.1.1 Modified flight plans or new clearances must be sent to FIM automation within TBD seconds for all aircraft in sector (Allocated to: Operators, Controllers)

STPA-F.15T.1.1.2 The design of user interfaces must not contribute to ATC, flight crew, or airline operator error. (Allocated to: ERAM, FIM Automation, Other ATC or Operator Interfaces)

STPA-F.15T.1.1.3 User interfaces must provide a clear, consistent means for entering aircraft data. (Allocated to: ERAM, FIM Automation, Other ATC or Operator Interfaces)

STPA-F.15T.1.1.4 Airline operator must verify that the registration/call sign matches the associated aircraft data file (Allocated to: Airline operators)

STPA-F.15T.1.1.5 ATC and flight crews must communicate and verify aircraft information per FAA standards (Allocated to: ATC, Flight Crew)

STPA-F.15T.1.1.6 Data must be generated and translated per internationally recognized standards (Allocated to: ERAM, FIM Automation, Other ATC or Operator automation, Communication networks)

STPA-F.15T.1.1.7 Aircraft data file must be provided to TFM automation and ATC in standardized format. (Allocated to: Airline operators,)

STPA-F.15T.1.1.8 Aircraft data includes certification, airworthiness, and other regulations. (Allocated to: Airframe manufacturers)

STPA-F.15T.1.1.9 Aircraft data file must be updated every flight or any time maintenance is performed that changes flight characteristics (Allocated to: Airline operators)

STPA-F.15T.1.2.1 TFM automation must have access to real-time wind data for the airspace. (Allocated to: ATC Weather Service)

STPA-F.15T.1.2.2 FIM automation must calculate maximum and minimum allowed speeds for given real-time data. (Allocated to: FIM Automation, Airframe manufacturers)

STPA-F.15T.1.2.3 Flight crew must notify ATC of inclement weather (Allocated to: Flight crew)

STPA-F.15T.1.3.1 Flight crew must alert ATC of degraded aircraft performance. (Allocated to: Flight Crew)

STPA-F.15T.1.3.2 FIM automation must provide alert when aircraft does not meet performance requirements (Allocated to: FIM Automation)

STPA-F.15T.1.3.3 FIM alerts must not interfere with or supersede other safety-critical warnings (Allocated to: FIM Automation, FMS, TCAS, aircraft health monitoring systems, and others)

STPA-F.15T.1.3.4 Ground-based tools must be provided with surveillance data to verify if flight is performing as expected to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: ADS-B, Radar)

STPA-F.15T.1.3.5 Ground-based tools must check that flight performance is within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: IM-related automation, [ERAM])

STPA-F.15T.1.3.6 Ground-based tools must provide alert when performance is not within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: IM-related automation, [ERAM])

STPA-F.15T.1.4.1 ATC and associated IM-S automation must use real-time surveillance data for generating IM clearances. See STPA-F.14.1 for requirement related to flight plans. See STPA-F.14.18-21 for requirements related to surveillance (Allocated to: ATC, IM-related automation)

STPA-F.15T.1.5.1 ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.15T.1.5.2 The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-F.15T.1.5.3 TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.15T.1.5.4 TFM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, Radar)

STPA-F.15T.1.6. ATC must verify that there are no conflicting aircraft in the proposed IM clearance. Conflicting aircraft could include crossing, in-track, non-ADS-B equipped aircraft, and others. (Allocated to: ATC, Conflict detection tools)

STPA-F.14T.1.2 Environmental changes result in modified aircraft capability

STPA-F.14T.1.3 Aircraft cannot achieve desired speed due to anomaly aboard

STPA-F.14T.1.4 ATC using filed flight plan for decision instead of real-time fused track data

STPA-F.14T.1.5 Fused track data is inaccurate due to spurious ADS-B information or long distance to radar beacon

STPA-F.14T.1.6 Non-FIM aircraft not included in IM automation computations and air traffic controller(s) does(do) not recognize potential conflict

STPA-F.14T.2 Airspace (in particular, a traffic flow) is saturated, and ATC believes that maintain current spacing between two will alleviate potential spacing issues, neglecting non-FIM aircraft maneuvers. [Process Model Flaw: Airspace]

STPA-F.14T.2.1 Downstream sector (TRACON or other ARTCC) does not report change in capacity

STPA-F.15T.2.1.1 ATC and associated IM automation must have access to predicted capacity demands and capacity constraints of all adjacent sectors up to TBD hours. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.15T.2.1.2 ATC and associated IM automation must have access to real-time capacity demands and capacity constraints of all adjacent sectors. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.15T.2.1.3 Downstream or adjacent sector capacity must be considered stale after TBD minutes. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.15T.2.1.4 ATC must not issue IM clearances that will saturate downstream or own airspace (Allocated to: ATC)

STPA-F.15T.2.2.1 ATC Centers must have access to real-time weather data, current runway status, updated flight plans, and real-time surveillance. (Allocated to: Tower, tower automation, ATC Weather Service, ATC, Airline operators, ADS-B, GNSS, Radar, ERAM)

STPA-F.15T.2.2.2 Capacity calculations must include real-time weather data, current runway status, updated flight plans, and real-time surveillance. (Allocated to: ATC Centers and associated automation (automation and/or operators that calculate capacity))

STPA-F.15T.2.2.3 Capacity demands must be updated whenever any of the above components is updated. (Allocated to: ATC Centers and associated automation (automation and/or operators that calculate capacity))

STPA-F.15T.2.3.1 FIM or ground-based automation must not issue IM clearances that will saturate downstream or own airspace (Allocated to: FIM-S Automation [Ground-based automation])

STPA-F.14T.2.2 Downstream sector (TRACON or other ARTCC) incorrectly estimates capacity

STPA-F.14T.2.3 FIM or ground-based automation contains incorrect time interval rules for given capacity demands

STPA-F.14T.3 ATC correctly selects FIM-equipped aircraft based on TFM advisory, but neglects non-FIM aircraft in flow. [Process Model Flaw: FIM Procedure]

STPA-F.14T.3.1 FIM automation not designed to consider non-FIM-equipped aircraft and ATC does not understand limitation

STPA-F.15T.3.1.1 ATC must verify that there are no conflicting aircraft in the proposed IM clearance. (Allocated to: ATC,)

STPA-F.15T.3.1.2 Conflicting aircraft could include crossing, in-track, non-ADS-B equipped aircraft, and others. (Allocated to: Conflict detection tools)

STPA-F.15T.3.2.1 ATC must verify that separation standards are maintained during IM clearance. (Allocated to: ATC,)

STPA-F.15T.3.2.2 Aircraft that join the flow between the FIM and target aircraft invalidate the clearance. (Allocated to: Conflict detection tools)

STPA-F.15T.3.3.1 ATC must verify that separation standards are maintained during IM clearance, including aircraft that cross the trajectory of the FIM aircraft, the target aircraft, or in between the two aircraft. (Allocated to: ATC, Conflict detection tools)

STPA-F.15T.3.4.1 Downstream or adjacent sector controllers must have access to IM clearances being flown by aircraft entering the sector (Allocated to: Sector Automation, IM-related Automation)

STPA-F.15T.3.4.2 Downstream or adjacent sector controllers must have access to IM speed advisories that have not yet been issued to aircraft entering the sector. (Allocated to: Sector Automation, IM-related Automation)

STPA-F.15T.3.5.1 All controllers within a sector must have access to IM speed advisories (Allocated to: IM-S Automation, user interface(s))

STPA-F.15T.3.5.2 Controllers must not issue conflicting IM speed clearances (Allocated to: ATC, IM-S Procedures)

STPA-F.14T.3.2 Non-FIM aircraft join the flow after FIM advisory has been generated and accepted

STPA-F.14T.3.3 Non-FIM aircraft cross the flow after FIM advisory has been generated and accepted

STPA-F.14T.3.4 Non-FIM aircraft join the flow after crossing sector boundary

STPA-F.14T.3.5 Non-FIM aircraft join the flow after transferring work or changing shifts

STPA-F.14T.4 ATC incorrectly trusts IM or other ground-based automation [Process Model Flaw: FIM Automation/DST]

STPA-F.14T.4.1 Target aircraft does not fly its intended flight path

STPA-F.15T.4.1.1 Target aircraft must fly its intended flight path to within TBD NM horizontal position, TBD feet altitude, TBD vertical speed, and TBD velocity. These predictions must be TBD% accurate for TBD second time horizon prediction. (Allocated to: Target aircraft Flight Crew, FMS)

STPA-F.15T.4.1.2 ATC and/or flight crew must monitor target aircraft trajectory. (Allocated to: ATC, FIM Flight Crew)

STPA-F.15T.4.2.1 Target aircraft must notify ATC of intention to modify trajectory. Target aircraft flight crew must request amended clearance. (Allocated to: Target aircraft flight crew)

STPA-F.15T.4.2.2 ATC must confirm that modified target aircraft trajectory allows for a safe IM clearance. (Allocated to: ATC)

STPA-F.15T.4.2.3 If target aircraft is in a compromised state, ATC must not include the aircraft in IM clearance. (Allocated to:)

STPA-F.15T.4.3.1 ATC must verify target aircraft intended flight path before issuing IM clearance. (Allocated to: ATC)

STPA-F.14T.4.2 Target aircraft modifies trajectory from ATC prediction

STPA-F.14T.4.3 ATC misinterprets target aircraft intended flight path

STPA-F.14T.5 Aircraft FIM automation calculates incorrect speed to execute FIM separation [Inadequate Actuator Operation]

STPA-F.14T.5.1 Incorrect ADS-B/fused-track data for ownship

STPA-F.15T.5.1.1 ADS-B must provide 0.1/0.3 NM (95%) accuracy for FIM aircraft. (Allocated to: ADS-B, GNSS)

STPA-F.15T.5.1.2 The design must protect against use of data that is not in the 95% accuracy range for FIM aircraft. (Allocated to: IM-related Automation, ERAM)

STPA-F.15T.5.1.3 IM-related automation must check when surveillance data is outside of 95% requirement for FIM aircraft. (Allocated to: IM-related Automation, ERAM)

STPA-F.15T.5.1.4 IM-related automation must have access to fused track data that includes sources other than ADS-B for FIM aircraft. (Allocated to: ERAM, Radar)

STPA-F.14T.5.2 Incorrect ADS-B/fused-track data for target aircraft

STPA-F.15T.5.2.1 ADS-B must provide 0.1/0.3 NM (95%) accuracy for target aircraft. (Allocated to: ADS-B, GNSS)

STPA-F.15T.5.2.2 The design must protect against use of data that is not in the 95% accuracy range for target aircraft. (Allocated to: IM-related Automation, ERAM)

STPA-F.15T.5.2.3 IM-related automation must check when surveillance data is outside of 95% requirement for target aircraft. (Allocated to: IM-related Automation, ERAM)

STPA-F.15T.5.2.4 IM-related automation must have access to fused track data that includes sources other than ADS-B for target aircraft. (Allocated to: ERAM, Radar)

STPA-F.15T.5.2.5 ATC and IM flight crew must verify the accuracy and integrity of both target and FIM aircraft surveillance data. (Allocated to: ATC, Flight crews)

STPA-F.15T.5.3 Incorrect trajectory model in FIM automation

STPA-F.15T.5.3.1 FIM automation must predict target aircraft trajectory to within TBD NM horizontal position, TBD feet altitude, TBD vertical speed, and TBD velocity. These predictions must be TBD% accurate for TBD second time horizon prediction. (Allocated to: FIM Automation)

STPA-F.15T.5.4 FIM automation updates speed modification too late

STPA-F.15T.5.4.1 FIM automation must be provided with updated target aircraft state every TBD seconds. Target aircraft state includes altitude, position, velocity, and vertical speed. (Allocated to: ADS-B or fused-track surveillance)

STPA-F.15T.5.4.2 FIM automation must update target aircraft state every TBD seconds. Target aircraft state includes altitude, position, velocity, and vertical speed. (Allocated to: FIM Automation,)

STPA-F.15T.5.5 Flight crew fails to identify non-FIM aircraft along or adjacent to flight path due to lack of air traffic information

STPA-F.15T.5.5.1 Flight crew must identify conflicting aircraft during IM operations. (Allocated to: Flight Crew)

STPA-F.15T.5.6 Flight crew fails to identify non-FIM aircraft along or adjacent to flight path due to conflict with other on-deck responsibilities

STPA-F.15T.5.6.1 Conflict detection and resolution responsibilities must supersede IM responsibilities. (Allocated to: Flight Crew)

STPA-F.15T.5.6.2 Conflict detection and resolution tools, including alerts, must be more prominent than IM tools. (Allocated to: TCAS or other conflict resolution tool)

STPA-F.15T.5.7 Flight deck-based automation does account for non-FIM aircraft

STPA-F.15T.5.7.1 Conflict detection and resolution responsibilities must supersede IM responsibilities. (Allocated to: Flight Crew)

STPA-F.15T.5.7.2 Conflict detection and resolution tools, including alerts, must be more prominent than IM tools. (Allocated to: TCAS or other conflict resolution tool)

STPA-F.15T.5.8 FMS does not receive speed updates from FIM automation

STPA-F.15T.5.8.1 FIM automation must send updated speed or modified trajectory information to FMS, (Allocated to: FIM Automation, FMS), OR

STPA-F.15T.5.8.2 FIM automation must prominently display updated speed or modified trajectory information to the flight crew via the user interface. (Allocated to: FIM Automation)

STPA-F.15T.5.8.3 Flight crew must verify the safety of the updated FIM information. If the updated FIM trajectory is safe, flight crew must fly the trajectory or issue a rejection to ATC. (Allocated to: FIM Automation)

The FIM-S causal analysis includes more causes related to flight crew execution of clearance than the analysis for GIM-S. The increased emphasis on flight crew and aircraft performance is due to the increased responsibilities allocated to the flight deck for FIM-S operations. This increased responsibility is relative to both traditional (pre-NextGen) operations as well as the ground-based version of interval management. Figure 16 and Figure 17 show the STPA control loop and process model for the flight crew. The control loops and process model for the flight crew are very similar to those of the air traffic controller for FIM, due to the delegated nature of separation responsibilities. The causal analysis for specific flight crew unsafe control actions is included in Appendix A.

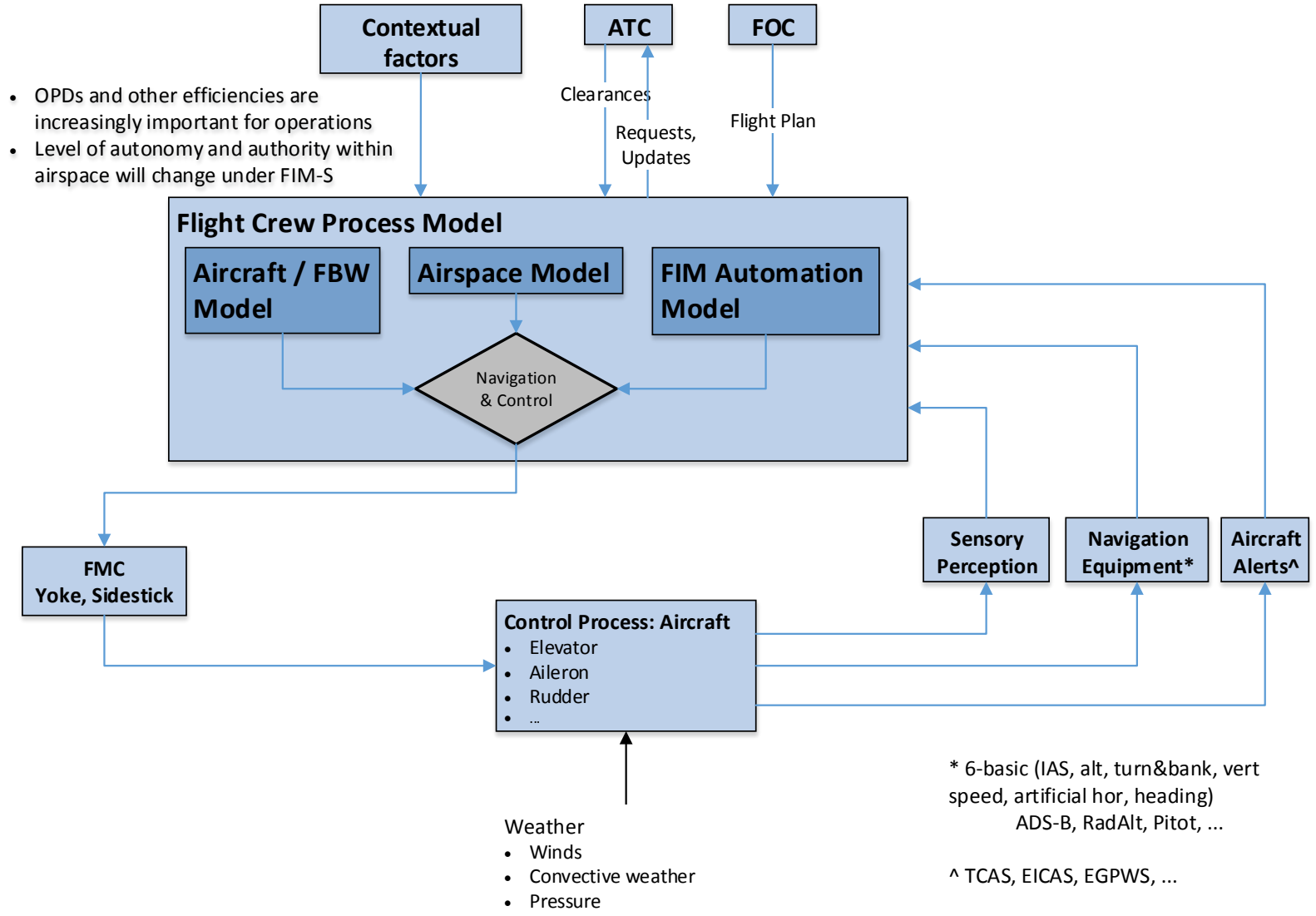


Figure 16: STPA Control Loop for Flight Crew (FIM-S)

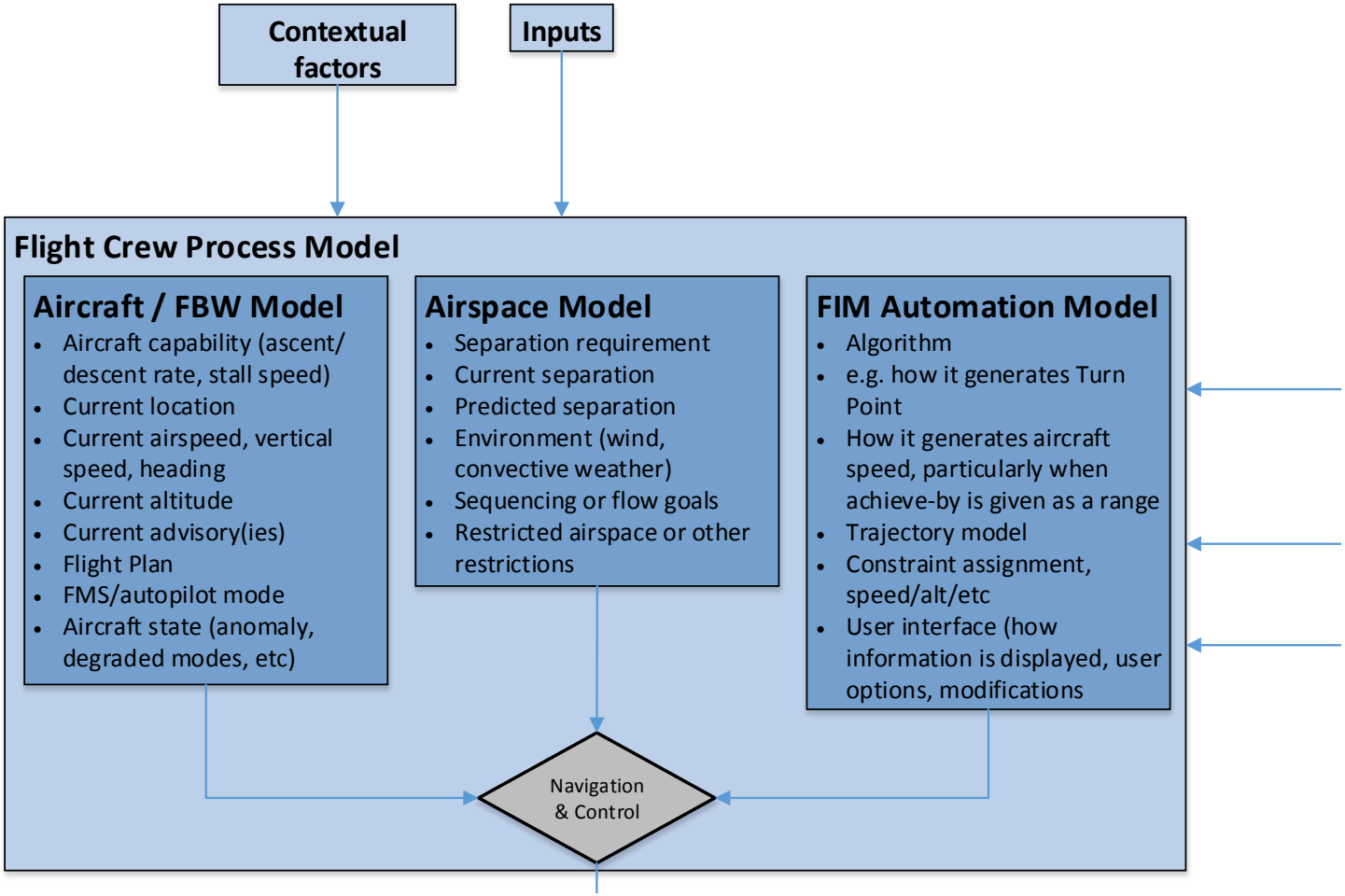


Figure 17: Flight Crew Process Model States (FIM-S)

The previous sub-section lists causal factors and scenarios related to the ATC process model and the unsafe control action "UCA15.M. Maintain Current Spacing clearance provided when spacing will cause receive aircraft to be incorrect speed for merging aircraft or non-target aircraft in flow". The following example depicts such a scenario related to this hazard. Observe Figure 18(a). At time t_0, the controller in $ARTCC_j$ generates an Interval Management clearance for FM_1 for its interval with TG_1. At the same time (or at any time before FM2/TG2 cross the sector boundary), the controller in $ARTCC_k$ gives an IM clearance for FM_2 relative to aircraft TG_2. Both sets of aircraft are supposed to cross into the adjacent TRACON and continue on a descent[4], and both IM clearances are set precisely to 60 second intervals.

At time t_1, both the respective target aircraft (TG_1, TG_2) have entered the TRACON. Without observing that both aircraft are leading aircraft in different IM clearances, the TRACON controller issues another IM clearance. In this case, TG_1 will follow TG_2 by 60 seconds. This part of the scenario is shown in Figure 18(b).

At time t_1, the TRACON controller feels (s)he has achieved adequate separation between the aircraft arriving from sectors j and k, and thus diverts his or her attention towards other potential conflicts within the sector. At time t_2, FM_1 and TG_2 lose separation because both aircraft are under a 60 second interval relative to TG_1.

As in Section 3.1.1, this example scenario illustrates several important results that STPA can find. Again, timing is important, both in terms of when a control action is (or is not) issued and also in terms of when feedback is (or is not) provided to the various control agents. Second, the control agents must have a mutually consistent and accurate model of the controlled process, which in this case is the set of IM clearances that various aircraft are under. The control agents must also have a mutually consistent model of how the other agents make control decisions. For FIM-S, the relative change in authority and the move of automation to the flight deck may have detrimental impacts on inter-sector (and intra-sector) communication. While FIM-related advisories are intended to ensure pairwise separation, the controllers must maintain sector- and system-level awareness and objectives, as they do now.

[4] This scenario is not specifically related to a merge in a TRACON and top-of-descent. It could occur at any airspace boundary where different streams of aircraft must merge into one stream.

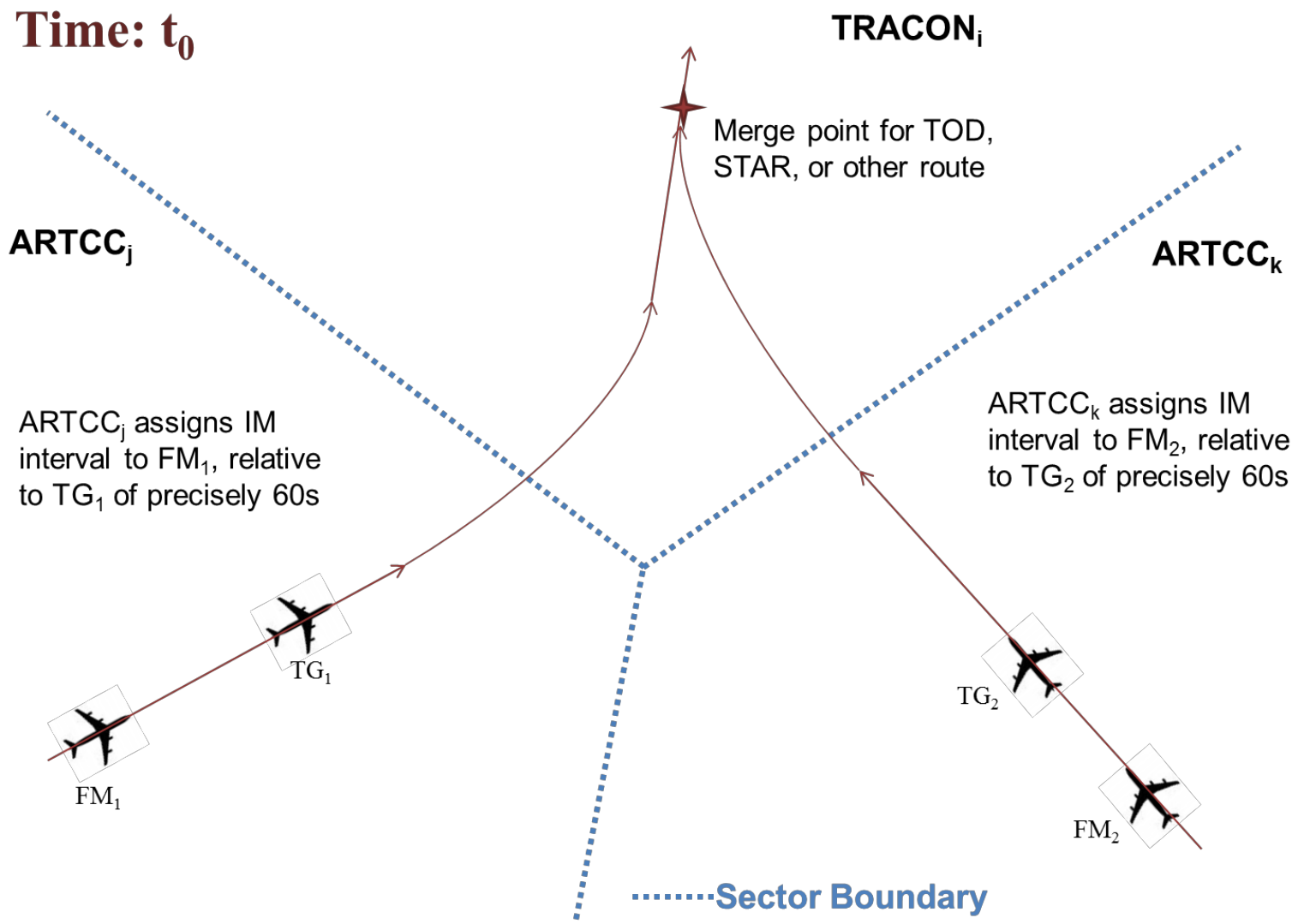

Time: t_0
TRACON$_i$
Merge point for TOD, STAR, or other route
ARTCC$_j$
ARTCC$_k$
ARTCC$_j$ assigns IM interval to FM$_1$, relative to TG$_1$ of precisely 60s
ARTCC$_k$ assigns IM interval to FM$_2$, relative to TG$_2$ of precisely 60s
TG$_1$
FM$_1$
TG$_2$
FM$_2$
Sector Boundary

Figure 18 (a)

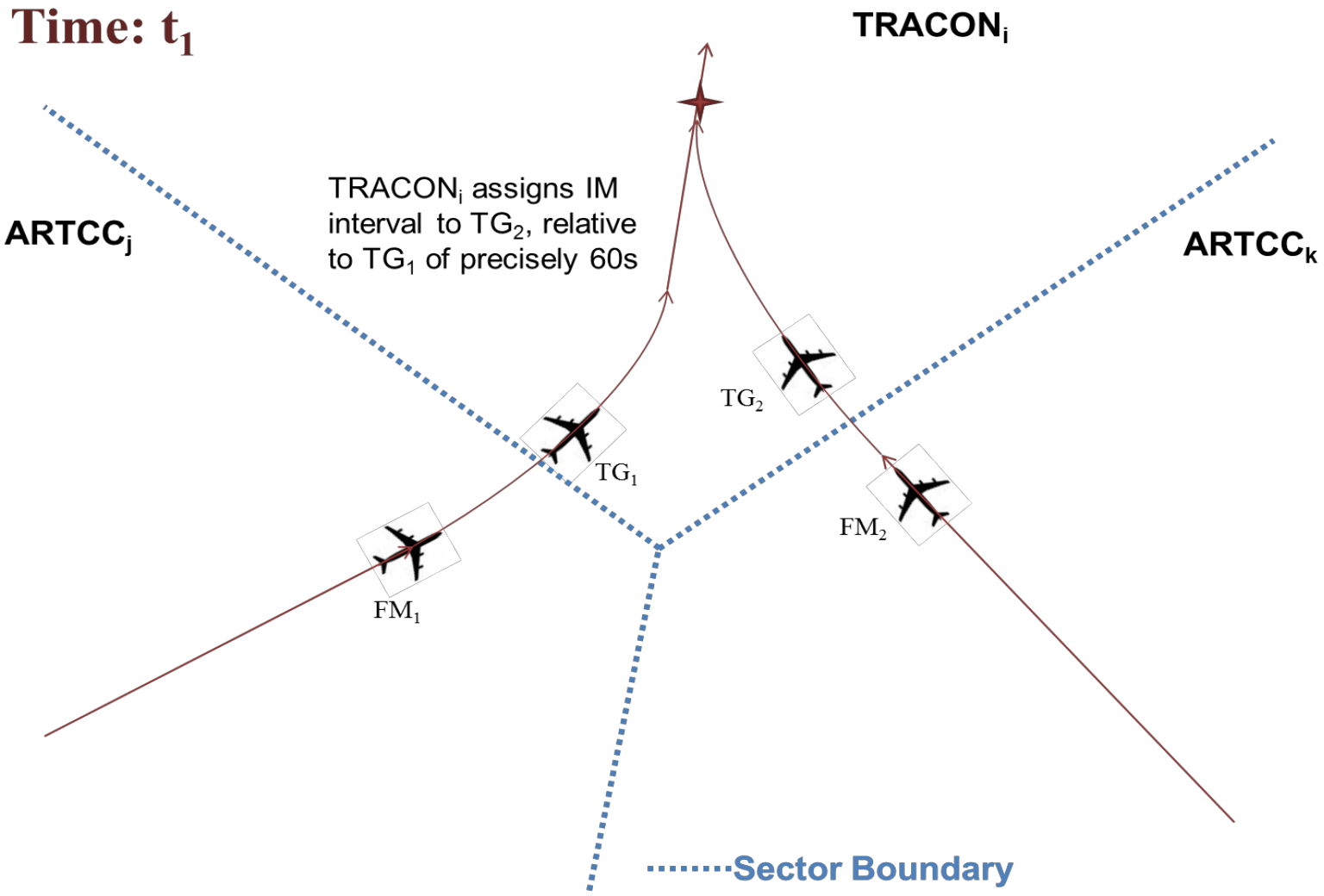

Time: t_1
TRACON$_i$
ARTCC$_j$
TRACON$_i$ assigns IM interval to TG$_2$, relative to TG$_1$ of precisely 60s
ARTCC$_k$
TG$_2$
TG$_1$
FM$_2$
FM$_1$
Sector Boundary

Figure 18 (b)

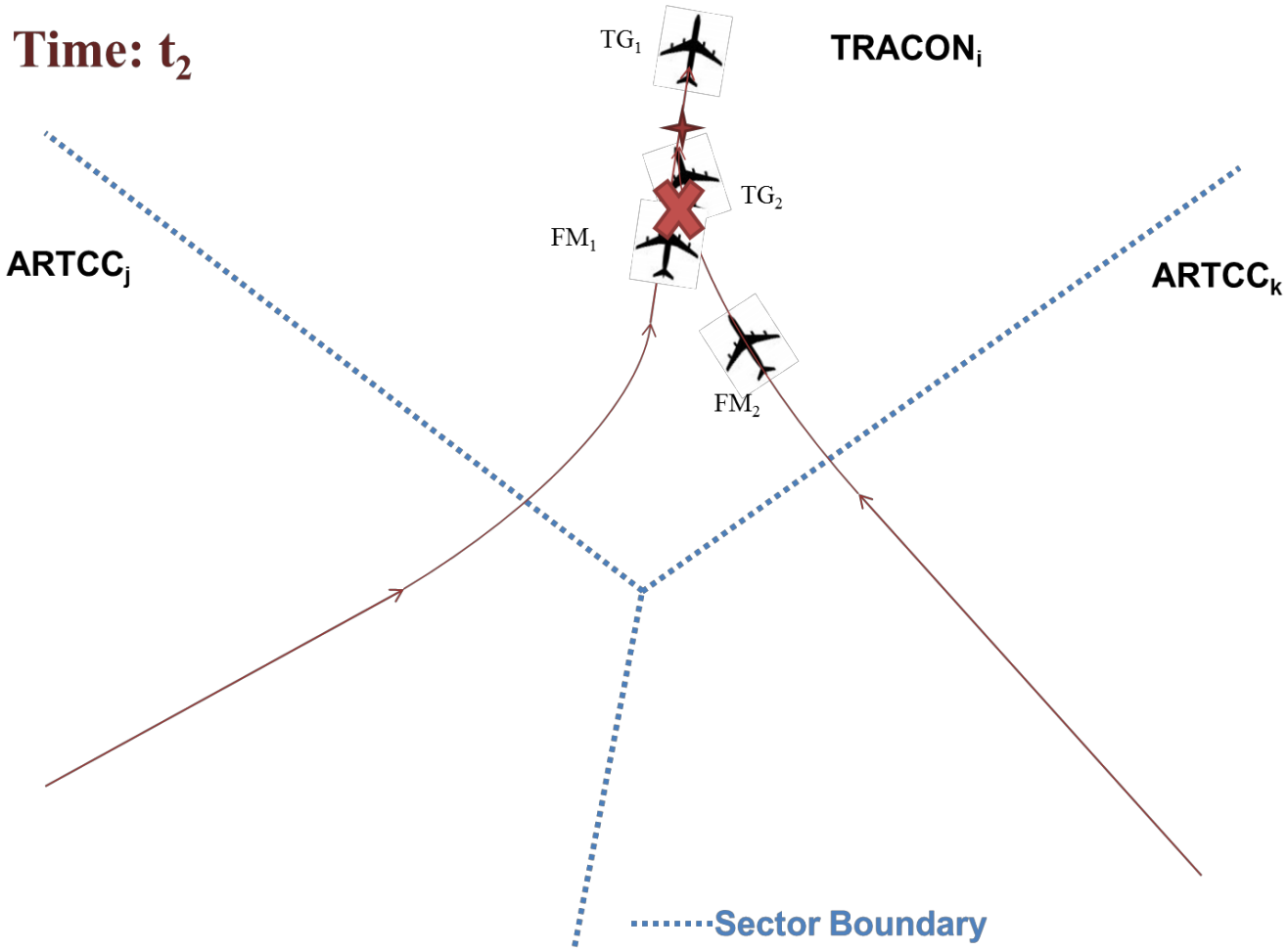


Figure 18 (c)

Figure 18: Example Scenario for Loss of Separation, FIM

4 CONCLUSIONS FROM THE STPA DEMONSTRATION ON FIM-S AND GIM-S

This report describes a new hazard analysis technique called Systems-Theoretic Process Analysis, or STPA, which is based on an accident causality rooted in systems theory and applies it to components of IM-S that are in the concept development and preliminary design or implementation stages.

Because STPA includes non-linear, indirect, and feedback relationships among events and actors, many of the scenarios identified in this report include more than just component failure. Therefore many of the requirements go beyond reliability and relate to the behavior of actors (both human controllers and automation) in the system and the information that those actors receive and exchange. These requirements are shown in the previous section along with recommendations for further investigation. See Section 3.1.3, 3.2.2, and Appendix A.

The hazard analysis identified several scenarios and/or causal factors that are not considered in the IM-S Concept of Operations [24]. These additional scenarios and causal factors can be used for future revisions of the IM-S ConOPS as well as in the development of detailed design documents or future revisions of IM-S platforms.

Causal factors identified by STPA but not included in the IM-S ConOPS include potential lack of coordination between controllers both within and across sectors, timing of IM clearances relative to other required clearances, potential lack of synchronization between surveillance sources provided to controllers and their tools, and conflicts between IM automation and other tools and ATC tasks.

Consider the example scenarios in Table 12. Requirement STPA-G.7S.1.2.3 states that “All controllers within a sector must have access to TFM-generated speed advisories”, which is allocated to IM-S Automation and controllers’ user interfaces. This requirement ensures that not only do all sectors have access to information about aircraft under IM advisories, but also that different controllers within a sector can coordinate clearances based on a common understanding of both the current state of the airspace and controller goals. Another example is STPA-G.1S.1.7.4, which states, “The IM/TFM system must not interfere with existing ATC systems” and the rationale for this requirement is “Interference includes both signal interference and interference with other controller tools”. A related requirement for a different scenario is STPA-G.4S.5.1.3: “Conflict detection advisories must take precedence over IM advisories”. The comment for STPA-G.4S.5.1.3 states that “These constraints could be implemented with aural alerts as well (e.g. conflict detection alerts are louder than IM), although that does not appear to be part of NextGen planning”.

Table 13: Example Requirement from STPA - Interference

Scenario	Associated Causal Factors	Requirement	Allocated To	Comments
STPA-G.7S.1 [Process Model Flaw: Aircraft / FC Model] ATC is unaware of another clearance the Aircraft/FC is executing or has requested.	STPA-G.7S.1.2 Aircraft / FC has recently passed to new controller (sector or shift change) and in-process clearance was not conveyed	STPA-G.7S.1.2.3 All controllers within a sector must have access to TFM-generated speed advisories	IM-S Automation, user interface(s)	This requirement refers to: (1) multiple controllers within a room (2) controllers that are physically separated but working in the same airspace (3) controllers working in the same airspace but during different shifts
STPA-G.1S.1 [Process Model Flaw: Aircraft / FC Model] ATC believes advisory is outside of aircraft envelope, therefore does not provide clearance. The flaw in the ATC's process model may be due to one or a combination of the following factors:	STPA-G.1S.1.7 Signal gets jammed, corrupted or IM clearance interferes with other clearances	STPA-G.1S.1.7.4 The IM/TFM system must not interfere with existing ATC systems	TFM automation, IM automation, IM user interface	Interference includes both signal interference and interference with other controller tools
STPA-G.4S.5 [Process Model Flaw: TFM Automation] ATC misinterprets TFM automatic advisory and gives incorrect speed clearance. The flaw in ATC's process model may be due to:	STPA-G.4S.5.1 TFM provides an incorrect speed advisory and ATC believes it is correct and follows it	STPA-G.4S.5.1.3 Conflict detection advisories must take precedence over IM advisories.	ATC, FAA Procedures, IM-S Interface Design	Precedence may be ensured (or encouraged) by making conflict resolution more visually prominent than IM advisories. These constraints could be implemented with aural alerts as well

Scenario	Associated Causal Factors	Requirement	Allocated To	Comments
				(e.g. conflict detection alerts are louder than IM), although that does not appear to be part of NextGen planning.

None of these requirements are related to component failure. The requirements are intended to ensure coordination between controllers, coordination between controller tools (also prevention of interference between tools), and design precedence for controller tools as well as FAA procedures. These are the kinds of causal factors that can be identified by, and requirements that can be derived from, an STPA hazard analysis. STPA also finds causes related to reliability and integrity, such as the ADS-B surveillance requirements that are found throughout Appendix A.

5 POSSIBLE FUTURE EXTENSIONS TO THE ANALYSIS

This report documents how to generate hazardous scenarios for systems with different control modes and different underlying assumptions. These results by themselves will help stakeholders make more informed decisions with respect to delegating authority, responsibility, procedural control, and algorithmic control within the NAS. Additional analysis could involve the synthesis of these hazardous scenarios into control system level trades, which will allow the stakeholder to ascertain relative levels of risk associated with different types of controls.

Of particular interest is the analysis of fundamentally different types of control and how these designs can be compared and/or merged. Broadly, Time-Based Flow Management can be considered hierarchical and centralized, which is closer to the paradigm used in the current NAS. Alternatively, FIM-S, a flight deck-based interval management solution, is highly de-centralized. Extensions to STPA could be used to identify how these solutions can be merged or how the system can migrate or transition from one paradigm to the other.

For example, a hierarchical, centralized structure with clearly delineated control authority might be more appropriate for tactical (short-term) resolutions. On the other hand, decentralized control may be more appropriate during strategic (long-term) negotiations. The different types of hazard causes that result from changes in control structure, different time horizons (or timing

requirements), and goals could be compared[5]. STPA can then be used as a part of a safety-guided design effort, where the safety control structure(s) are created to ensure(s) system safety under different operational modes.

STPA in this report looked only at the high-level technical system. Theoretically, STPA could be used to analyze NextGen operations (include more of the hierarchical safety control structure) and to dig deeper into technical issues that need to be resolved.

[5] Examples of different goals include: strategic goals of optimizing flight trajectories versus short-term tactical goals of de-conflicting aircraft or modifying flows around convective weather. Of course trajectory optimization still has safety as a goal, but the emphasis is slightly different.

LIST OF ACRONYMS

4DT	4-dimensional Trajectory (3 spatial, 1 temporal)
ANSP	Air Navigation Service Provider
ARTCC	Air Route Traffic Control Center
ATO	Air Traffic Organization
CDT	Constrained Departure Time
ERAM	En Route Automation Modernization
FIM-S	Flight Deck-Based Interval Management Spacing
FMP	Flow Management Point
GIM-S	Ground-Based Interval Management Spacing
IM-S	Interval Management and Spacing
ITP	In-Trail Procedure
NAS	National Airspace System
NWS	National Airspace Weather Service
OI	Operational Improvement
OPD	Optimized Profile Descent
PDMP	Pre-Defined Meter Points
RNAV	Area Navigation
RNP	Required Navigation Performance
RTP	Required Time Performance
STAMP	Systems Theoretic Accident Model and Process
STPA	Systems Theoretic Process Analysis (hazard analysis)

TBFM	Time Based Flow Management
TFM	Traffic Flow Management (more general term than TBFM)
TRACON	Terminal Radar Approach Control Facilities

REFERENCES

[1] FAA Air Traffic Organization, ATO Safety Management System Manual, Version 2.1, May 2008.

[2] Frola, F. R., and C. O. Miller. System safety in aircraft management, Logistics Management Institute, Washington DC (1984).

[3] Jens Rasmussen, 1997. Risk management in a dynamic society: A modelling problem, Safety Science, 27 (2-3), pp. 183-213

[4] Dekker, S.W.A. The Field Guide to Understanding Human Error, Ashgate Publishing Co., 2006.

[5] Flach, J., Hancock, P.A., Caird, J., and Vicente, K.J. Global Perspectives on the Ecology of Human-Machine Systems, CRC Press, 1995.

[6] Norman, D. The Design of Everyday Things, Basic Books, 2002.

[7] Pereira, Steven J., Grady Lee, and Jeffrey Howard. A System-Theoretic Hazard Analysis Methodology for a Non-advocate Safety Assessment of the Ballistic Missile Defense System, Proceedings of the 2006 AIAA Missile Sciences Conference, Monterey, California, November 2006.

[8] Balgos, Vincent H. A Systems Theoretic Application to Design for the Safety of Medical Diagnostic Devices, MIT Master's Thesis, February 2012.

[9] Takuto Ishimatsu, Nancy G. Leveson, John P. Thomas, Cody H. Fleming, Masafumi Katahira, Yuko Miyamoto, Ryo Ujiie, Haruka Nakao, and Nobuyuki Hoshino, Hazard Analysis of Complex Spacecraft using STPA, AIAA Journal of Spacecraft and Rockets, in press 2013.

[10] Leveson, N.G. *Engineering a Safer World*, MIT Press, 2011.

[11] Leveson, N.G. A New Approach to Hazard Analysis for Complex Systems. International Conference of the System Safety Society, Ottawa, August 2003.

[12] Fleming, C.H.; Spencer, M.; Leveson, N.; and Wilkinson, C. Safety Assurance in NextGen, NASA Technical Report NASA/CR–2012-217553, 2012.

[13] Fleming, C.H. .; Spencer, M.; Thomas, J.; Leveson, N.; and Wilkinson, C. Safety assurance in NextGen and complex transportation systems, Safety Science Volume 55, June 2013.

[14] Federal Aviation Administration, NextGEN Implementation, 2013.

[15] Penhallegon, W.J, et al, Flight Deck-Based Interval Management-Spacing During Departures: Flight Crew Human-In-The-Loop Simulation, 9th USA/Europe Air Traffic Management Research and Development Seminar, 2011.

[16] RTCA/DO-312. Safety, Performance, and Interoperability Requirements Document for the In-Trail Procedure in Oceanic Airspace (ATSA-ITP) Application, RTCA Incorporate, Washington DC.
[17] Harkleroad, E., Vela, A.E., Kuchar, J. White Paper on Risk-Based Modeling to Support NextGen Concept Assessment & Validation, MIT Lincoln Laboratories.
[18] Nolan, M. *Fundamental of Air Traffic Control*, 4th Edition. Brooks/Cole 2004.
[19] Joint Planning and Development Office, JPDO Trajectory-Based Operations (TBO) Study Team Report, December 4, 2011.
[20] Joint Planning and Development Office, Capability Safety Assessment of Trajectory Based Operations, February 9, 2012.
[21] Reason, J. The Contribution of Latent Human Failures to the Breakdown of Complex Systems, Philosophical Transactions of the Royal Society of London, Series B, Biological Sciences, 12 April 1990.
[22] FAA Air Traffic Organization, Concept of Operations for Time-Based Flow Management (TBFM), 31 October 2012. (DRAFT)
[23] Federal Aviation Administration Surveillance and Broadcast Services (SBS) Program Office. Arrival Interval Management – Spacing (IMS) Concept of Operations for the Mid-Term Timeframe. PMO-010, Rev. 01, Version 4.0, August 06, 2012.
[24] Capezzuto, V. Surveillance and Broadcast Services (SBS) Concept of Operations Arrival Interval Management – Spacing (IM-S) Concept of Operations for the Mid-Term Timeframe, PMO-010, Revision 02, Final March 1, 2013
[25] Thomas, J. Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis, Doctoral Thesis, Massachusetts Institute of Technology, Engineering Systems Division, 2013.
[26] Thomas, J. Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis SAND2012-4080, Sandia National Labroratories, 2012.
[27] Leveson, N.G., Heimdahl, M. and Reese, J.D. Designing Specification Languages for Process Control Systems: Lessons Learned and Steps to the Future, presented at SIGSOFT FOSE '99 (Foundations of Software Engineering), Toulouse, September 1999.
[28] RTCA/DO-328. Safety, Performance, and Interoperability Requirements Document for Airborne Spacing – Flight Deck Interval Management (ASPA-FIM), RTCA Incorporate, Washington DC, 2011.
[29] Walker, M. ATO-E Program Operations Conceptual Use Case, Arrival Interval Management – Spacing (IM-S). Ground based Interval Management for Spacing (GIM-S). FAA ATO, 19 November 2012.
[30] Federal Aviation Administration, Air Traffic Control Policy, FAA Order JO 7110.65U, 9 February 2012.

A. Hazard Analysis Results

All of the hazard analysis will go here.

A.1 GIM-S

Insert here

A.1.1.1 STPA Step 1

Section 3.1.2 describes the identification of unsafe control actions, and those sections contain all the necessary and relevant information. Table 14 contains the full set of unsafe control actions identified using the new automated method. These formalized unsafe control actions can be mapped to the prose statements in Table 15 (identical to Table 3 in the main body text but reiterated here for navigation).

Table 14: Full Set of Unsafe Control Actions using Automated Method

	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6
Speed Modification	*	*	*	NP	NP	NP
Vector Clearance	NP	NP	*	NP	NP	NP
Altitude Modification	*	*	NP	NP	NP	NP
Presence of other Aircraft	*	*	*	Crossing	Same-Leading	Same-Trailing
Speed Differential of other aircraft	*	*	*	*	<=0kts	>0kts
Vertical Separation	*	*	*	<1000	<1000	<1000
Presence of Terrain	*	In Path	In Path	*	*	*
Presence of Weather	In Path	*	*	*	*	*

Table 14 continued

	Rule 8	Rule 9	Rule 10	Rule 11	Rule 12	Rule 13
Speed Modification	*	*	NP	NP	NP	Increase V
Vector Clearance	Turn Heading	Turn Heading	NP	NP	NP	NP
Altitude Modification	*	NP	Change Alt	Change Alt	Change Alt	Change Alt
Presence of other Aircraft	*	Lateral	Same-Leading	Crossing	Same-Trailing	Same-Leading
Speed	*	*	<=0kts	*	>0kts	<=0kts

Differential of other aircraft						
Vertical Separation	*	**<1000**	**>1000**	**>1000**	**>1000**	**>1000**
Presence of Terrain	**Lateral**	*	*	*	*	*
Presence of Weather	*	*	*	*	*	*

Table 14 continued

	Rule 15	Rule 16	Rule 17
Speed Modification	*	**Decrease V**	**Decrease V**
Vector Clearance	**Turn Heading**	**NP**	**NP**
Altitude Modification	**Change Alt**	**NP**	**Change Alt**
Presence of other Aircraft	**Lateral**	**Same-Trailing**	**Same-Trailing**
Speed Differential of other aircraft	*	**>0kts**	**>0kts**
Vertical Separation	**>1000**	**<1000**	**>1000**
Presence of Terrain	*	*	*
Presence of Weather	*	*	*

Table 15: ATC Unsafe Control Actions for GIM-S

Control Action	Not Provided when required for safety	Providing Causes Hazard	Too soon, too late, out of sequence	Stopped too soon, applied too long
Modify Speed	UCA1.S. Not providing a speed modification when the current speed leads to LOS and vector is not given. ↑[H-1]	UCA4.S. Providing a speed modification that leads to LOS. ↑[H-1]	UCA7.S. Providing a speed modification to an aircraft that was previously safe if given too late after a different clearance has been executed by same or other aircraft ↑[H-1]	UCA10.S. Providing speed modification where modified speed is applied too long and traffic/weather exists 'downstream[2]' from initiation of maneuver. ↑[H-1;H-2;H-5]
	UCA2.S. Not providing a speed modification when there is convective (or other) weather in the path of the current trajectory ↑[H-3; H-4; H-5]	UCA5.S. Providing a speed modification to the wrong aircraft. ↑[H-1;H-2;H-3;H-4;H-5]	UCA8.S. Providing a speed modification to an aircraft that was previously safe if given too soon before a different clearance has been executed by same or other aircraft ↑[H-1]	UCA11.S. Providing speed modification where modified speed is not applied long enough and separation not achieved. ↑[H-1]
		UCA6.S. Providing a speed modification that exceeds the aircraft capability (overspeed or stall). ↑[H-4; H-5]	UCA9.S. Providing speed modification too late after environmental conditions (e.g. weather, aircraft speed, heading, etc) have changed ↑[H-1;H-2;H-3;H-4;H-5]	

High level safety constraints are derived from these unsafe control actions. This is described in the main body, section 3.1.2. The constraints are reiterated here:

[SC-1] ATC must provide a speed modification when the current speed leads to a loss of separation and no other clearance is given. ←UCA1.S, ↑[H-1]

[SC-2] ATC must provide a speed modification when there is convective weather in the path of the current trajectory and no other clearance is given. ←UCA1.S, ↑[H-3;H-4;H-5]

[SC-3] ATC must not provide a speed modification if the new speed leads to loss of separation. ←UCA4.S, ↑[H-1]

[SC-4] ATC must provide speed modifications to the correct aircraft. ←UCA5.S, ↑[H-1;H-2;H-3;H-4;H-5]

[SC-5] ATC must provide speed modifications that are within aircraft capability (overspeed or stall limits). ←UCA6.S, ↑[H-4; H-5]

[SC-6] ATC must verify that aircraft under speed modifications maintain sufficient separation throughout the speed modification clearance. Aircraft may modify their trajectories due to other clearances, weather, or onboard circumstances. ←UCA7.S, UCA8.S, ↑[H-1]

[SC-7] ATC must reject or terminate speed advisories when environmental conditions become detrimental to aircraft control. ←UCA9.S, ↑[H-1;H-2;H-3;H-4;H-5]

[SC-8] Speed advisory must be terminated when current speed will cause aircraft to enter into airspace with saturated traffic or inclement weather. ←UCA10.S, ↑[H-1;H-2;H-5]

[SC-9] ATC must apply speed modification for sufficient duration to achieve and maintain separation. ←UCA11.S, ↑[H-1]

A.1.1.2 STPA Step 2

The following hazard causes and scenarios are related to the GIM-S Hazard Analysis described in Section 3.1. For a more detailed discussion of how these scenarios are generated, please see that section. Each of the scenarios and causal factors are related to the STPA control loops in Figure 11 and Figure 12 using the guidewords in Figure 10 (all figures in section 3.1.3). Detailed safety requirements, labeled STPA-G.ucaS.x.y.z, are derived from the scenarios and causes with the shared ID number.

Unsafe Control Action: UCA1.S. Not providing a speed modification when the current speed leads to LOS a**nd vector is not given. ↑[H-**1]

STPA-G.1S.1. ATC believes advisory is outside of aircraft envelope, therefore does not provide clearance [Process Model Flaw: Aircraft / FC Model]

STPA-G.1S.1.1. Flight crew / aircraft not flying the reported flight plan

STPA-G.1S.1.1.1. Flight crew must fly the reported flight plan or request a clearance to deviate from the plan (Allocated to: Flight Crew, FMS)

STPA-G.1S.1.2. Change in environment prevents aircraft from achieving advised airspeed (e.g. headwinds, tailwinds)

STPA-G.1S.1.2.1. ATC and flight crew must monitor compliance with IM speeds (Allocated to: ATC, Flight Crews)

STPA-G.1S.1.2.2. TFM automation must monitor aircraft compliance with speed advisory and provide an alert if discrepancy exceeds TBD (Allocated to: TFM Automation)

STPA-G.1S.1.3. TFM calculates that no speed advisories are possible, but other clearance is necessary (but ATC misunderstands as 'no speed advisory')

STPA-G.1S.1.3.1. ATC must issue conflict resolution advisories regardless of state of IM advisory (Allocated to: ATC)

STPA-G.1S.1.4. ATC incorrectly mistrusts TFM advisory (when it is in fact correct) - e.g. many past false advisories

STPA-G.1S.1.4.1. False advisories must not occur more than TBD percentage of total advisories. (Allocated to: TFM Automation)

STPA-G.1S.1.5. TFM trajectory model predictions use different time-horizon than ATC real-time control

STPA-G.1S.1.5.1. TFM trajectory model time horizon must be synchronized with ATC tools, or (Allocated to: TFM Automation,)

STPA-G.1S.1.5.2. The time horizon prediction must be presented to ATC (Allocated to: ERAM)

STPA-G.1S.1.6. Center TFM update rate is too slow

STPA-G.1S.1.6.1. TFM must update its status every TBD seconds (Allocated to: TFM Automation)

STPA-G.1S.1.7. Signal gets jammed, corrupted or IM clearance interferes with other clearances

STPA-G.1S.1.7.1. Protection must be provided against jamming or corruption of the signal between Center TFM and ARTCC centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.1S.1.7.2. Protection must be provided against jamming or corruption of the signal between ARTCC centers and flight decks (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders)

STPA-G.1S.1.7.3. The system must control against radio interference or other types of communication interference. (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders, TFM Center software, receivers, transponders)

STPA-G.1S.1.7.4. The IM/TFM system must not interfere with existing ATC systems or procedures (Allocated to: TFM automation, IM automation, IM user interface)

STPA-G.1S.1.8. Surveillance data is inaccurate

STPA-G.1S.1.8.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.1S.1.8.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation, ADS-B)

STPA-G.1S.1.8.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation, ADS-B)

STPA-G.1S.1.9. Screen/GUI refresh rate too slow

STPA-G.1S.1.9.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: IM-S Automation)

STPA-G.1S.1.9.2. ATC must not give clearance based on a user interface that is not updating (Allocated to: ATC, FAA Procedures)

STPA-G.1S.1.10. TFM automation generates advisory outside of aircraft envelope

STPA-G.1S.1.10.1. TFM must generate advisories within aircraft capabilities (Allocated to: TFM Automation, Airline Operators, Airframe Manufacturers)

STPA-G.1S.1.11. ATC recognizes unsafe TFM advisory, rejects it (or lets it time out), but does not provide appropriate advisory in its place

STPA-G.1S.1.11.1. ATC must provide appropriate action in the event of an unsafe TFM advisory. ATC should reject (or let time out) the advisory and either maintain the previous trajectory if it is safe or issue a new clearance (Allocated to: ATC)

STPA-G.1S.2. ATC maintains current speed of aircraft i in order to meet downstream sector capacity/ requests [Process Model Flaw: Airspace]

STPA-G.1S.2.1. ATC mistakenly prioritizes downstream saturation over immediate conflict

STPA-G.1S.2.1.1. ATC must give priority to immediate conflict over any downstream demands (Allocated to: ATC, Conflict detection tools, Interface layout)

STPA-G.1S.2.2. TFM advisory is currently being followed and leads to LOS

STPA-G.1S.2.2.1. ATC must monitor aircraft under IM speed advisories for conflicts (Allocated to: ATC, Conflict detection tools)

STPA-G.1S.2.3. ATC does not 'see' or account for crossing traffic that will result in near term / immediate conflict

STPA-G.1S.2.3.1. ATC must monitor traffic adjacent to IM traffic flow for conflicts (Allocated to: ATC, ERAM, Surveillance screens ("glass"))

STPA-G.1S.3. ATC waits for TFM automation to generate speed advisories, and TFM does not provide a de-conflicting advisory [Process Model Flaw: TFM Automation]

STPA-G.1S.3.1. TFM attempts to generate an advisory for downstream sequencing, but cannot find a valid speed

STPA-G.1S.3.1.1. ATC must issue conflict resolution clearance (not limited to speed modification) even if TFM cannot calculate a valid speed advisory (Allocated to: ATC, FAA Procedures)

STPA-G.1S.3.2. Over time, ATC develops process of using TFM for all speed advisories, and other tools/mental cues for other types of control actions (e.g. vectors)

STPA-G.1S.3.2. ATC must provide appropriate action in the event of an unsafe TFM advisory. (Allocated to: ATC, FAA Procedures)

STPA-G.1S.3.3. TFM does not have accurate aircraft information due to non-updated flight plans

STPA-G.1S.3.3.1. Flight operators (or another entity, TBD) must send updated flight plans to TFM center. Provision must be made to ensure that plan has not been changed due to conflict or other reason. (Allocated to: Airline operators [Potentially ATC, crews, or avionics])

STPA-G.1S.3.4. TFM does not have correct surveillance information and therefore does not or cannot generate speed advisory

STPA-G.1S.3.4.1. TFM must not generate speed advisories with incomplete surveillance data. (Allocated to: TFM automation)

STPA-G.1S.3.4.2. TFM must be provided with airspeed, heading, altitude, vertical speed, and aircraft type for all aircraft in flow. See requirements STPA-G.1.12-14

below for protection against incorrect or inaccurate information (Allocated to: ADS-B, GNSS, Radar, ERAM)

STPA-G.1S.4. ATC mistrusts TFM automation, ignoring automation even when it generates safe advisories [Process Model Flaw: TFM Automation]

STPA-G.1S.4.1. Repeated 'bad' (i.e. unsafe or inefficient) advisories from TFM

STPA-G.1S.4.1.1. False advisories must not occur more than TBD percentage of the time. See requirements STPA-G.1S.1.12 - 14 above for protection against incorrect information (Allocated to: TFM Automation)

STPA-G.1S.5. Aircraft / Flight crew does not perform necessary speed modification, leading to LOS. This may be due to one or a combination of the following factors [Inadequate Actuator Operation]

STPA-G.1S.5.1. Flight crew does not update FMS

STPA-G.1S.5.1.1. Flight crew must enter IM speed into FMS, or (see STPA-G.1S.5.2 - 5) (Allocated to: Flight Crew)

STPA-G.1S.5.2. Flight crew flies incorrect speed

STPA-G.1S.5.2.1. Flight crew must manually fly IM speed (see STPA-G.1S.5.3) (Allocated to: Flight Crew)

STPA-G.1S.5.2.2. Flight crew must not deviate from the IM speed provided unless IM speed leads to a hazard. (Allocated to: Flight Crew)

STPA-G.1S.5.2.3. Flight crew must notify ATC of intentional deviation from IM speed and why. (Allocated to: Flight Crew)

STPA-G.1S.5.3. FMS does not follow flight plan

STPA-G.1S.5.3.1. FMS must follow flight plan to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: FMS)

STPA-G.1S.5.3.2. TFM must be provided with surveillance data to verify if flight is performing as expected to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: ADS-B, Radar)

STPA-G.1S.5.3.3. TFM must check that flight performance is within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: TFM automation, [ERAM])

STPA-G.1S.5.3.4. TFM (or other tool such as ATC automation) must provide alert when performance is not within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: TFM automation, [ERAM])

STPA-G.1S.5.4. Degraded performance of aircraft

STPA-G.1S.5.4.1. Flight crew must alert ATC of degraded aircraft performance. (Allocated to: Flight Crew)

Unsafe Control Action: UCA2.S. Not providing a speed modification when there is **convective (or other) weather in the path of the current trajectory ↑[H-3; H-4; H-5]**

STPA-G.2S.1. ATC believes the aircraft is flying a different trajectory than it actually is. ATC does not believe aircraft is near convective weather [ATC process model of Aircraft / FC is incorrect]

STPA-G.2S.1.1. Flight crew / aircraft not flying the reported flight plan

STPA-G.2S.1.1.1. Flight crew must fly the reported flight plan or request a clearance to deviate from the plan (Allocated to: Flight Crew, FMS)

STPA-G.2S.1.2. Change in environment causes aircraft to be in a different state than expected (e.g. headwinds, tailwinds)

STPA-G.2S.1.2.1. ATC and flight crew must monitor compliance with IM speeds (Allocated to: ATC, Flight Crews)

STPA-G.2S.1.2.2. TFM automation must monitor aircraft compliance with speed advisory and provide an alert if discrepancy exceeds TBD (Allocated to: TFM Automation)

STPA-G.2S.1.3. Signal gets jammed, corrupted or IM clearance interferes with other clearance

STPA-G.2S.1.3.1. Protection must be provided against jamming or corruption of the signal between Center TFM and ARTCC centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.2S.1.3.2. Protection must be provided against jamming or corruption of the signal between ARTCC centers and flight decks (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders)

STPA-G.2S.1.3.3. The system must control against radio interference or other types of communication interference. (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders, TFM Center software, receivers, transponders)

STPA-G.2S.1.3.4. The IM/TFM system must not interfere with existing ATC systems or procedures. (Allocated to: TFM automation, IM automation, IM user interface)

STPA-G.2S.1.4. Inaccurate or inadequate surveillance

STPA-G.2S.1.4.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.2S.1.4.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: ERAM, ADS-B)

STPA-G.2S.1.4.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: ERAM, ADS-B)

STPA-G.2S.1.4.4. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, Radar)

STPA-G.2S.2. ATC is unaware of the presence of convective weather [ATC process model of airspace is incorrect]

STPA-G.2S.2.1. Inclement weather forms rapidly, before ATC can be made aware

STPA-G.2S.2.1.1. Flight crews may request an amended clearance due to inclement weather if the crew deams it necessary (Allocated to: Flight Crews)

STPA-G.2S.2.1.2. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NAS Weather Service (NWS))

STPA-G.2S.2.2. Flight crews do not report experiencing turbulance or observing inclement weather

STPA-G.2S.2.2.1. Flight crews must report turbulance and/or observation of inclement weather (Allocated to: Flight crews)

STPA-G.2S.2.2.2. Flight crews must report location, heading, altitude, and airspeed when reporting inclement (Allocated to: Flight crews)

STPA-G.2S.2.2.3. Flight crews must report type of weather, including turbulence, lightning, poor visibility, and others. Flight crews must report weather according to severity level in FAA standards (Allocated to: Flight crews)

STPA-G.2S.2.3. NAS weather service surveillance is inaccurate

STPA-G.2S.2.3.1. Precipitation measurements must be within TBD dBZ with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-G.2S.2.3.2. Wind measurements must be within TBD kts with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-G.2S.2.3.3. NAS weather service must notify ATC of accuracy and resolution of weather data, or notify ATC when the above requirements are not met. (Allocated to: NWS)

STPA-G.2S.2.4. ATC misinterprets or misunderstands"Resolution" or accuracy of weather service

STPA-G.2S.2.4.1. The weather service user interface must clearly present the spatial resolution of weather surveillance (Allocated to: NWS User Interface)

STPA-G.2S.2.4.2. The weather service user interface must clearly present the time of applicability of weather surveillance (Allocated to: NWS User Interface)

STPA-G.2S.2.5. NAS weather service does not update its surveillance fast enough

STPA-G.2S.2.5.1. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NWS (AWIPS, WARP, or other))

STPA-G.2S.2.6. Weather monitoring interface does not update fast enough

STPA-G.2S.2.6.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: NWS Automation)

STPA-G.2S.2.6.. ATC must not give clearance based on a user interface that is not updating (Allocated to: ATC, FAA Procedures)

STPA-G.2S.2.7. ATC has incorrect understanding of location of weather

STPA-G.2S.2.7.1. The weather service user interface must have the same scale and perspective as aircraft surveillance surveillance screens (Plan position indicator) (Allocated to: NWS Automation)

STPA-G.2S.2.8. Weather data is displayed incorrectly or in a confusing manner

STPA-G.2S.2.8.1. Weather data must be presented in a consistent format, within and across sectors (Allocated to: NWS, Tower, TRACON, ARTCC facilities)

STPA-G.2S.2.9. ATC receives report of inclement weather from flight crew but misinterprets location of aircraft

STPA-G.2S.2.9.1. ATC must verify location of aircraft per FAA standards (Allocated to: ATC, FAA Procedures)

STPA-G.2S.2.10. Incorrect surveillance of aircraft

STPA-G.2S.2.10.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.2S.2.10.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: ERAM, ADS-B)

STPA-G.2S.2.10.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: ERAM, ADS-B)

STPA-G.2S.2.10.4. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, Radar)

STPA-G.2S.2.11. Incorrect identification of aircraft

STPA-G.2S.2.11.1. Airline operator must verify that the registration/call sign matches the associated aircraft data file (Allocated to: Airline operators)

STPA-G.2S.2.11.2. ATC and flight crews must communicate and verify aircraft information per FAA standards (Allocated to: ATC, Flight Crew)

STPA-G.2S.2.11.3. Data must be generated and translated per internationally recognized standards (Allocated to: ERAM, Other ATC or Operator automation, Communication networks)

STPA-G.2S.2.11.4. Aircraft data file must be provided to TFM automation and ATC in standardized format. (Allocated to: Airline operators,)

STPA-G.2S.2.11.5. Aircraft data includes certification, airworthiness, and other regulations. (Allocated to: Airframe manufacturers)

STPA-G.2S.2.11.6. Aircraft data file must be updated every flight or any time maintenance is performed that changes flight characteristics (Allocated to: Airline operators)

STPA-G.2S.2.12. ATC has incorrect understanding of magnitude or severity of weather

STPA-G.2S.2.12.1. Severity of weather must be presented or communicated in a consistent format within and across sectors (Allocated to: NWS Surveilance, NWS User Interface)

STPA-G.2S.2.13. Flight crew report underestimates severity

STPA-G.2S.2.13.1. Precipitation must communicated in terms of "Light", "Moderate", "Heavy", and "Extreme" paired with appropriate dBZ range of precipitation intensity level (Allocated to: FAA Procedures, NWS)

STPA-G.2S.2.14. ATC misinterprets NAS weather service surveillance (e.g. wrong colors on radar screen)

STPA-G.2S.2.14.1. Presentation of weather data in user interface must be consistent with ATC Weather Radar Terms (Allocated to: NWS User Interface)

STPA-G.2S.2.15. NAS weather service weather prediction/modeling is incorrect

STPA-G.2S.2.15.1. Current weather surveillance data supercedes forecasted data (Allocated to: ATC, FAA Procedures, NWS)

STPA-G.2S.2.15.2. ATC must issue weather avoidance clearances based on real-time weather surveillance data (Allocated to: ATC, FAA Procedures)

STPA-G.2S.2.16. ATC generates control actions (lack thereof) based on inappropriate time horizon.

STPA-G.2S.2.16.1. Short range forecasts must be updated every TBD hours (Allocated to: NWS)

STPA-G.2S.2.16.2. Medium range forecasts must be updated every TBD days (Allocated to: NWS)

STPA-G.2S.2.16.3. ATC must be presented with time of applicability of all weather forecasts (Allocated to: NWS)

STPA-G.2S.2.16.4. User interface must indicate when forecasts become invalid (Allocated to: NWS)

STPA-G.2S.2.17. ATC misinterprets confidence in weather modeling. For example, weather service has only 40% accuracy currently but ATC assumes a much better prediction

STPA-G.2S.2.17.1. Quantitative forecasts must include meteorological rationale underlying the model (Allocated to: NWS)

STPA-G.2S.3. ATC relies too heavily on automation to clear aircraft around weather [ATC process model of TFM Automation is incorrect]

STPA-G.2S.3.1. ATC believes that TFM accounts for convective weather in its algorithm for generating advisories (and TFM does NOT generate weather-avoidance advisories).

STPA-G.2S.3.1.1. Weather alerts take precedence over TFM-generated speed advisories (Allocated to: ATC, FAA Procedures, NWS, IM-S)

STPA-G.2S.3.2. IM-S automation interferes with weather tracking

STPA-G.2S.3.2.1. Protection must be provided against jamming or corruption of the signal between Center TFM, ARTCC centers, and NWS centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.2S.3.3. Signal interference or data corruption

STPA-G.2S.3.3.1. The system must control synchronous garbling, nonsynchronous garbling, multipath signals. (Allocated to: NWS avionics, ARTCC software, receivers, transponders, TFM Center software, receivers, transponders)

STPA-G.2S.3.4. Interference with user interface

STPA-G.2S.3.4.1. The IM/TFM system must not interfere with NAS weather service surveillance systems (Allocated to: TFM automation, IM automation, IM user interface, NWS user interface)

STPA-G.2S.3.5. IM-S automation interferes with weather conflict automation

STPA-G.2S.3.5.1. Protection must be provided against jamming or corruption of the signal between Center TFM, ARTCC centers, and NWS centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.2S.3.6. Signal interference or data corruption

STPA-G.2S.3.6.1. The system must control synchronous garbling, nonsynchronous garbling, multipath signals. (Allocated to: NWS avionics, ARTCC software, receivers, transponders, TFM Center software, receivers, transponders)

STPA-G.2S.3.7. Interference with user interface

STPA-G.2S.3.7.1. The IM/TFM system must not interfere with NAS weather service warning systems (Allocated to: TFM automation, IM automation, IM user interface, NWS warning systems)

STPA-G.2S.4. ATC prioritizes sequencing and flow over avoiding convective weather [Incorrect understanding of FAA procedures and priorities]

STPA-G.2S.4.1. ATC must give priority to inclement weather over any IM advisories

STPA-G.2S.4.1.1. ATC, FAA Procedures (Allocated to: I.e. current speeds optimize the sequence so ATC does not modify the speed)

STPA-G.2S.4.2. Weather advisories must take precedence over IM advisories.

STPA-G.2S.4.2.1. ATC, FAA Procedures, IM-S Interface Design, NWS User Interface (Allocated to: Precedence may be ensured (or encouraged) by making weather advisories more visually prominent than IM advisories. These constraints could be implemented with aural alerts as well (e.g. weather alerts are louder than IM))

STPA-G.2S.5. Aircraft / Flight crew does not perform necessary speed modification, resulting in a trajectory with inclement weather. This may be due to one or a combination of the following factors [Inadequate actuator operation]

STPA-G.2S.5.1. Flight crew does not update FMS

STPA-G.2S.5.1.1. Flight crew must enter IM speed into FMS, or (Allocated to: Flight Crew)

STPA-G.2S.5.2. Flight crew flies incorrect speed

STPA-G.2S.5.2.1. Flight crew must manually fly IM speed (Allocated to: Flight Crew)

STPA-G.2S.5.2.2. Flight crew must not deviate from the IM speed provided unless IM speed leads to a hazard. (Allocated to: Flight Crew)

STPA-G.2S.5.2.3. Flight crew must notify ATC of intentional deviation from IM speed and why. (Allocated to: Flight Crew)

STPA-G.2S.5.3. FMS does not follow flight plan

STPA-G.2S.5.3.1. FMS must follow flight plan to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: FMS)

STPA-G.2S.5.3.2. TFM must be provided with surveillance data to verify if flight is performing as expected to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: ADS-B, Radar)

STPA-G.2S.5.3.3. TFM must check that flight performance is within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: TFM automation, [ERAM])

STPA-G.2S.5.3.4. TFM (or other tool such as ATC automation) must provide alert when performance is not within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: TFM automation, [ERAM])

STPA-G.2S.5.4. Degraded performance of aircraft

STPA-G.2S.5.4.1. Flight crew must alert ATC of degraded aircraft performance. (Allocated to: Flight Crew)

STPA-G.2S.5.4.2. ATC must issue special clearances to degraded aircraft in order to avoid inclement weather (Allocated to: ATC)

STPA-G.2S.5.4.3. ATC may request Meteorological assistance from a Center Weather Service Unit (CWSU) (Allocated to: ATC, NWS)

Unsafe Control Action: UCA4.S. Providing a speed modification where the new speed leads **to LOS. ↑[H-1]**

STPA-G.4S.1. ATC has incorrect understanding of aircraft status or predicted status, therefore provides unsafe speed mod. The flaw in the ATC's process model may be due to one or a combination of the following factors: [Process Model Flaw: Aircraft / FC Model]

STPA-G.4S.1.1. ATC and/or TFM automation has incorrect location for aircraft, issues clearance accordingly

STPA-G.4S.1.1.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.4S.1.1.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-G.4S.1.1.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-G.4S.1.1.4. TFM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, Radar)

STPA-G.4S.1.2. Missing or inaccurate flight plans

STPA-G.4S.1.2.1. Updated flight plans must be sent to TFM automation within TBD seconds (Allocated to: Airline operators, ATC)

STPA-G.4S.1.3. Flights plans have been modified, but not updated in database / GUI

STPA-G.4S.1.3.1. TFM automation must check for consistency between flight plan and real-time surveillance data (Allocated to: TFM Automation)

STPA-G.4S.1.3.2. TFM must use updated flight plan in trajectory modeling if the flight plan is consistent with real-time surveillance data to within TBD NM (Allocated to: TFM Automation)

STPA-G.4S.1.3.3. TFM must not issue speed advisories if flight plan is inconsistent with real-time surveillance data (Allocated to: TFM Automation)

STPA-G.4S.1.4. Model of immediate airspace is incorrect or out of date (Radar/GNSS outage, datalink update delay, unequipped aircraft present, etc...)

STPA-G.4S.1.4.1. TFM must have access to accurate surveillance data for all aircraft within TBD NM of an aircraft when generating a speed advisory for that aircraft (Allocated to: ADS-B, GNSS, Radar, ERAM)

STPA-G.4S.1.4.2. Airspace model must be updated every TBD minutes. The airspace model should include aircraft type, altitude, vertical speed, horizontal position, and heading for every aircraft in sector. (Allocated to: ADS-B, GNSS, Radar, ERAM, Operators)

STPA-G.4S.1.5. Surveillance data is inaccurate

STPA-G.4S.1.5.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.4S.1.5.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-G.4S.1.5.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-G.4S.1.5.4. TFM must have access to fused track data that includes sources other than ADS-B (Allocated to: ADS-B, GNSS, Radar, ERAM)

STPA-G.4S.1.6. Inadequate surveillance systems (outage, jamming, corrupted or delayed signal)

STPA-G.4S.1.6.1. Protection must be provided against jamming or corruption of the signal between Center TFM and ARTCC centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.4S.1.6.2. Protection must be provided against jamming or corruption of the signal between ARTCC centers and flight decks (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders)

STPA-G.4S.1.6.3. The system must control against radio interference or other types of communication interference (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders, TFM Center software, receivers, transponders)

STPA-G.4S.1.6.4. The IM/TFM system must not interfere with existing ATC systems and procedures (Allocated to: TFM automation, IM automation, IM user interface)

STPA-G.4S.1.7. ATC and/or TBFM automation believes an aircraft has followed a prior advisory when it has yet to do so, and then uses that assumed new trajectory in calculating and issuing the advisory

STPA-G.4S.1.7.1. Flight crew (or datacomm) must confirm the acceptance and execution of IM speed advisory or explicitly deny the advisory. (Allocated to: Flight crew, CPDLC)

STPA-G.4S.1.7.2. ATC and TFM must have a way to confirm that aircraft have followed advisories. (Allocated to: Surveillance (ADS-B, radar, fused track reports))

STPA-G.4S.1.7.3. ATC and TBFM must confirm that prior advisories have been followed before issuing a new advisory. (Allocated to: ATC, TFM Automation)

STPA-G.4S.1.7.4. ATC or TFM automation must verify that aircraft is within TBD (airspeed or mach) of speed advisory (Allocated to: ATC, TFM Automation)

STPA-G.4S.1.7.5. ATC (or automated tool) must advise TFM automation of a denied speed advisory (Allocated to: ATC, IM-S Automation)

STPA-G.4S.1.7.6. Flight crew must fly IM speed within TBD (knots or mach) of speed advisory (Allocated to: Flight Crew, FMS)

STPA-G.4S.1.8. Radar screen mismatches IM(TFM) presentation of sequence

STPA-G.4S.1.8.1. Aircraft data must presented in IM automation in the same format as on radar screens (Allocated to: Ground-based Automation)

STPA-G.4S.1.9. ATC has a different understanding of sequence based on bird's eye view (plan position indicator) of relative aircraft positions

STPA-G.4S.1.9.1. ATC must verify that IM speed advisory is consistent with current surveillance information (Allocated to: ATC, FAA Procedures)

STPA-G.4S.1.10. ATC misinterprets TFM sequencing algorithm and therefore issues advisory to incorrect aircraft

STPA-G.4S.1.10.1. ATC must verify that the IM speed advisory is going to the correct aircraft (see also surveillance requirements) (Allocated to: ATC, FAA Procedures)

STPA-G.4S.1.11. Mismatch between TFM algorithm and ATC goals and procedures

STPA-G.4S.1.11.1. ATC must verify that IM advisories are consistent with ATC's desired merging pattern (Allocated to: ATC, FAA Procedures)

STPA-G.4S.1.12. TFM sequences aircraft incorrectly (B before A instead of A before B) relative to ATC's desired merging pattern

STPA-G.4S.1.12.1. ATC must not accept IM speed advisory if ATC's desired merging pattern is inconsistent with IM advisory (Allocated to: ATC, FAA Procedures)

STPA-G.4S.1.13. Communication on incorrect frequency

STPA-G.4S.1.13.1. ATC and flight crews must communicate on frequency allocation per FAA standards (Allocated to: ATC, Flight Crew, Communications network)

STPA-G.4S.1.14. Wrong aircraft ID in TFM automation

STPA-G.4S.1.14.1. TFM must have access to aircraft ID (Allocated to: Airline operators)

STPA-G.4S.1.15. Incorrect call sign / identifier

STPA-G.4S.1.15.1. Operators and flight crew must verify call sign of aircraft (Allocated to: Flight crew, Airline operators, ATC)

STPA-G.4S.1.16. Wrong aircraft ID in TFM automation

STPA-G.4S.1.16.1. TFM must have access to aircraft ID (Allocated to: Airline operators)

STPA-G.4S.2. Wrong aircraft ID in TFM automation

STPA-G.4S.2.1. Flight crew misidentifies ownship

STPA-G.4S.2.1.1. Airline operator must verify that the registration/call sign matches the associated aircraft data file (Allocated to: Airline operators)

STPA-G.4S.2.2. Garbled text message (for CPDLC or datalink application)

STPA-G.4S.2.2.1. ATC and flight crews must communicate and verify aircraft information per FAA standards (Allocated to: ATC, Flight Crew)

STPA-G.4S.2.3. Misinterpration of text message (for CPDLC or datalink application)

STPA-G.4S.2.3.1. Data must be generated and translated per internationally recognized standards (Allocated to: ERAM, Other ATC or Operator automation, Communication networks)

STPA-G.4S.2.4. Automation misinterprets or scrambles message

STPA-G.4S.2.4.1. Aircraft data file must be provided to TFM automation and ATC in standardized format. (Allocated to: Airline operators,)

STPA-G.4S.2.5. Inconsistent format

STPA-G.4S.2.5.1. Aircraft data includes certification, airworthiness, and other regulations. (Allocated to: Airframe manufacturers)

STPA-G.4S.2.6. Manual error in entering message

STPA-G.4S.2.6.1. Aircraft data file must be updated every flight or any time maintenance is performed that changes flight characteristics (Allocated to: Airline operators)

STPA-G.4S.2.7. "Manual" error in receiving message (misread or misinterpret)

STPA-G.4S.2.7.1. (Allocated to:)

STPA-G.4S.3. ATC has incorrect understanding of adjacent aircraft or environment, therefore provides unsafe speed mod. The flaw in the ATC's process model may be due to one or a combination of the following factors: [Process Model Flaw: Airspace]

STPA-G.4S.3.1. ATC mistakenly prioritizes downstream saturation over immediate conflict

STPA-G.4S.3.1.1. ATC must give priority to immediate conflict over any downstream demands (Allocated to: ATC, FAA Procedures)

STPA-G.4S.3.2. ATC does not 'see' or account for crossing traffic that will result in near term / immediate conflict

STPA-G.4S.3.2.1. ATC must verify that there is no crossing traffic before issuing an IM speed advisory (Allocated to: ATC, FAA Procedures)

STPA-G.4S.3.2.2. ATC must verify that there will be no crossing traffic during the entirety of an IM speed advisory (Allocated to: ATC, FAA Procedures)

STPA-G.4S.3.2.3. If there is an occurrence of crossing traffic during an IM speed advisory, ATC must issue conflict resolution clearance(s) to one or all of the aircraft involved (Allocated to: ATC, FAA Procedures)

STPA-G.4S.3.3. ATC is basing control actions on incorrect understanding of downstream capacity / demands. ATC thinks that downstream capacity is higher (lower) than it actually is, and creates an arrival flow with too many aircraft (see below, next process model flaw)

STPA-G.4S.3.3.1. ATC and TFM must have access to predicted capacity demands and capacity constraints of all adjacent sectors up to TBD hours. (Allocated to: TRACON, Tower, ARTCC)

STPA-G.4S.3.3.2. ATC and TFM must have access to real-time capacity demands and capacity constraints of all adjacent sectors. (Allocated to: TRACON, Tower, ARTCC)

STPA-G.4S.3.3.3. Downstream or adjacent sector capacity must be considered stale after TBD minutes. (Allocated to: TRACON, Tower, ARTCC)

STPA-G.4S.3.3.4. ATC must not issue IM clearances that will saturate downstream or own airspace (Allocated to: ATC)

STPA-G.4S.4. ATC or TFM automation has incorrect assumption about leading (or trailing) aircraft speed or trajectory, therefore provides unsafe speed mod. The flaw in the ATC's process model may be due to one or a combination of the following factors: [Process Model Flaw: Airspace]

STPA-G.4S.4.1. Leading aircraft flying a lower final approach speed than expected

STPA-G.4S.4.1.1. TFM automation must have access to surveillance data of all aircraft in flow (Allocated to: ADS-B, GNSS, Radar, Fused track reports, ERAM)

STPA-G.4S.4.1.2. TFM must check that aircraft fly the final approach at the required speed. (Allocated to: TFM Automation)

STPA-G.4S.4.1.3. TFM must issue a new speed advisory if leading aircraft airspeed is TBD below airspeed in TFM trajectory model (Allocated to: TFM Automation)

STPA-G.4S.4.2. Trailing aircraft flying a faster final approach speed than expected

STPA-G.4S.4.2.1. TFM must issue a new speed advisory if trailing aircraft airspeed is TBD above airspeed in TFM trajectory model (Allocated to: TFM Automation)

STPA-G.4S.4.3. Leading/trailing aircraft fly a different approach than expected in TFM automation model

STPA-G.4S.4.3.1. Flight crews or associated automation must notify ATC of intent to modify approach (Allocated to: Flight crews, Flight deck avionics)

STPA-G.4S.4.3.2. ATC or sector automation must notify TFM Center of aircraft's modified approach (Allocated to: ATC, ATC automation, Datalink)

STPA-G.4S.5. ATC has incorrect understanding of downstream airspace demands and capacity, therefore provides unsafe speed mod. The flaw in the ATC's process model may be due to one or a combination of the following factors: [Process Model Flaw: Airspace]

STPA-G.4S.5.1. Arrival rate is not updated or input into TFM automation

STPA-G.4S.5.1.1. Updated arrival rate constraints must be included in TFM model (Allocated to: TFM Automation)

STPA-G.4S.5.2. Arrival rate changes unexpectedly (many causes, included something on the runway)

STPA-G.4S.5.2.1. Arrival rate constraints must be updated every TBD minutes (Allocated to: TRACON, Tower, ARTCC)

STPA-G.4S.5.2.2. Updated arrival rate constraints must be sent to or communicated with upstream sectors (Allocated to: TRACON, Tower, ARTCC)

STPA-G.4S.5.3. Arrival rate not communicated or misunderstood with upstream ATC

STPA-G.4S.5.3.1. ATC sectors must communicate desired arrival rate constraints with upstream sectors (Allocated to: TRACON, Tower, ARTCC)

STPA-G.4S.5.3.2. Updated arrival rates must be sent to TFM centers (Allocated to: TRACON, Tower, ARTCC)

STPA-G.4S.5.3.3. ATC must be provided a means for comparing arrival rates used by TFM automation with arrival rates communicated or sent by downstream sectors (Allocated to: ERAM, other)

STPA-G.4S.5.3.4. ATC or sector automation must check for consistency between downstream arrival rates and arrival rates being used by TFM automation (Allocated to: ATC, IM-S Automation)

STPA-G.4S.5.3.5. ATC must not issue IM clearance if the downstream arrival rates and arrival rates used by TFM automation are inconsistent (Allocated to: ATC, FAA Procedures)

STPA-G.4S.5.4. Wake Vortex separation requirements change

STPA-G.4S.5.4.1. ATC sectors must have access to updated wake turbulence separation requirements for determination of separation requirements and capacity (Allocated to: FAA Procedures)

STPA-G.4S.5.5. Wake Vortex separation requirements incorrect for aircraft type or sequence

STPA-G.4S.5.5.1. ATC sectors must have access to aircraft type for determination of separation requirements and capacity due to wake turbulence (Allocated to: FAA Procedures, Airline operators, Airframe manufacturers)

STPA-G.4S.6. ATC misinterprets TFM automatic advisory and gives incorrect speed clearance. The flaw in ATC's process model may be due to: [Process Model Flaw: TFM Automation]

STPA-G.4S.6.1. TFM provides an incorrect speed advisory and ATC believes it is correct and follows it

STPA-G.4S.6.1.1. False advisories must not occur more than TBD percentage of total advisories. (Allocated to: TFM Automation)

STPA-G.4S.6.1.2. ATC must give priority to conflict over any IM advisories (Allocated to: ATC, FAA Procedures)

STPA-G.4S.6.1.3. Conflict detection advisories must take precedence over IM advisories. (Allocated to: ATC, FAA Procedures, IM-S Interface Design)

STPA-G.4S.6.1.4. Conflict detection tools should be more prominent in ATC display ("glass") than IM tools (Allocated to: ATC, FAA Procedures, IM-S Interface Design)

STPA-G.4S.6.2. TFM provides advisory for downstream sequencing, but immediate conflict exists

STPA-G.4S.6.2.1. ATC must give priority to conflict over any IM advisories (Allocated to: ATC, FAA Procedures)

STPA-G.4S.6.3. ATC misinterprets TFM advisory

STPA-G.4S.6.3.1. ATC or TFM automation must verify that aircraft is within TBD (airspeed or mach) of speed advisory (Allocated to: ATC, IM-S Automation)

STPA-G.4S.6.3.2. User interface must clearly present desired speed, including whether the speed advisory is in terms of Mach number or in airspeed (Allocated to: IM-S Interface Design)

STPA-G.4S.7. Aircraft / Flight crew executes incorrect speed, leading to LOS. This may be due to one or a combination of the following factors [Inadequate Actuator Operation]

STPA-G.4S.7.1. Flight crew does not follow advisory due to misunderstanding of clearance and flies at incorrect speed

STPA-G.4S.7.1.1. ATC must include in clearance whether the speed is in Mach number or airspeed (Allocated to: ATC, FAA Procedures)

STPA-G.4S.7.2. Flight crew flies at incorrect speed due to other types of feedback not available to ATC or automation

STPA-G.4S.7.2.1. Flight crew must notify ATC if crew intentionally does not fly or cannot fly IM speed (Allocated to: Flight Crew)

STPA-G.4S.7.2.2. ATC must reject IM speed advisories for aircraft intentionally not flying IM speed (Allocated to: ATC, FAA Procedures)

STPA-G.4S.7.3. Aircraft cannot fly at correct speed due to environment factors such as change in winds, pressure, etc

STPA-G.4S.7.3.1. TFM automation and ATC must be provided surveillance data to verify if flight is performing as expected to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: ADS-B, GNSS, Radar, ERAM, Fused track data reports)

STPA-G.4S.7.4. Aircraft cannot fly at correct speed due to degraded performance (e.g. reduced thrust due to engine failure or degradation)

STPA-G.4S.7.4.1. Flight crew must notify ATC of degraded performance (Allocated to: Flight Crew)

STPA-G.4S.7.4.2. ATC must reject IM speed advisories for degraded aircraft (Allocated to: ATC, FAA Procedures)

Unsafe Control Action: UCA5.S. Providing a speed modification that exceeds the aircraft **capability (overspeed or stall). ↑[H-4; H-5]**

STPA-G.5S.1. ATC believes advisory is within aircraft envelope, therefore provides clearance. The flaw in the ATC's process model may be due to one or a combination of the following factors: [Process Model Flaw: Aircraft / FC Model]

STPA-G.5S.1.1. Data file with aircraft equipage is incorrect

STPA-G.5S.1.1.1. Aircraft data file must be provided to TFM automation and ATC in standardized format. (Allocated to: Airline operators,)

STPA-G.5S.1.1.2. Aircraft data includes certification, airworthiness, and other regulations. (Allocated to: Airframe manufacturers)

STPA-G.5S.1.1.3. Aircraft data file must be updated every flight (Allocated to: Airline operators)

STPA-G.5S.1.1.4. V speeds must be provided to TFM automation in a standardized format (Allocated to: Airframe manufacturers)

STPA-G.5S.1.1.5. (Allocated to:)

STPA-G.5S.1.1.6. Stall speeds and speed limits must be provided to TFM automation (Allocated to: Airframe manufacturers)

STPA-G.5S.1.2. Aircraft location (position/alt/speed) data is incorrect, stall/over-speed limits are then incorrect

STPA-G.5S.1.2.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.5S.1.2.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-G.5S.1.2.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-G.5S.1.2.4. TFM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, Radar, Fused-track data reports)

STPA-G.5S.1.2.5. Protection must be provided against jamming or corruption of the signal between Center TFM and ARTCC centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.5S.1.2.6. Protection must be provided against jamming or corruption of the signal between ARTCC centers and flight decks (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders)

STPA-G.5S.1.2.7. The system must control against radio interference or other types of communication interference (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders, TFM Center software, receivers, transponders)

STPA-G.5S.1.2.8. The IM/TFM system must not interfere with existing ATC systems and procedures (Allocated to: TFM automation, IM automation, IM user interface)

STPA-G.5S.1.3. Aircraft is in different configuration than what ATC believes

STPA-G.5S.1.3.1. ATC must verify that aircraft is in level flight (Allocated to: ATC, FAA Procedures)

STPA-G.5S.1.3.2. Flight crew must notify ATC of inability to meet IM speed (Allocated to: Flight Crew)

STPA-G.5S.1.3.3. ATC or TFM automation must be provided information about off-nominal flight characteristics (non-cruise, non-level flight) (Allocated to: Flight Crew, ADS-B, GNSS, Radar, Altimeters)

STPA-G.5S.1.3.4. ATC or TFM automation must verify that flight is in cruise configuration and at level flight. (Allocated to: ATC, TFM Automation)

STPA-G.5S.1.3.5. If aircraft does not meet these conditions, TFM must not issue IM speed advisory, and/or ATC must reject advisory (Allocated to: TFM Automation)

STPA-G.5S.1.3.6. Flight crew must notify ATC of degraded performance (Allocated to: Flight Crew)

STPA-G.5S.1.3.7. ATC must reject IM speed advisories for degraded aircraft (Allocated to: ATC, FAA Procedures)

STPA-G.5S.2. ATC has incorrect understanding of environmental conditions surrounding aircraft, therefore provides unsafe speed mod. [Process Model Flaw: Airspace]

STPA-G.5S.2.1. ATC console displays information about aircraft x while allowing modification of aircraft y

STPA-G.5S.2.1.1. ATC must be provided with surveillance information for all aircraft on the IM advisory list (Allocated to: ADS-B, GNSS, Radar, ERAM, Fused track data reports)

STPA-G.5S.2.1.2. Aircraft identification format for IM interface must match the format used in traffic situation or surveillance interface (Allocated to: IM-S Automation [Possibly levied on other ATC tools])

STPA-G.5S.2.2. Weather/wind data is incorrect, actual load on aircraft for given speed/alt is not understood correctly

STPA-G.5S.2.2.1. TFM automation must have access to real-time wind data for the airspace. (Allocated to: ATC Weather Service)

STPA-G.5S.2.2.2. TFM automation must calculate maximum and minimum allowed speeds for given real-time data. (Allocated to: TFM Automation, Airframe manufacturers)

STPA-G.5S.2.2.3. TFM automation must not issue speed advisories outside of maximum and minimum allowed speeds. (Allocated to: TFM Automation)

STPA-G.5S.2.2.4. Flight crew must verify that clearance is within aircraft capability (Allocated to: Flight crew, FMS)

STPA-G.5S.2.2.5. Flight crew must request amendment to clearance if IM speed exceeds capability. Amendment request should explicitly state that speed exceeds aircraft capability (Allocated to: Flight Crew)

STPA-G.5S.2.3. ATC gives speed mod clearance to incorrect aircraft

STPA-G.5S.2.3.1. ATC must verify aircraft before and after issuing IM clearance. This verification should include aircraft call sign (Allocated to: ATC)

STPA-G.5S.2.3.2. TFM automation must include aircraft call sign with all advisories (Allocated to: TFM Automation)

STPA-G.5S.2.4. Meter points are too closely spaced for aircraft to meet time demands

STPA-G.5S.2.4.1. Meter points must be sufficiently spaced to allow aircraft to meet time of arrival demands. (Allocated to: TFM Automation, FAA Procedures)

STPA-G.5S.3. ATC has incorrect interpretation of TFM capability, therefore accepts an unsafe TFM advisory. [Process Model Flaw: TFM Automation]

STPA-G.5S.3.1. Automation prioritizes and/or only considers FMT or separation (disregarding capability) and issues advisory accordingly

STPA-G.5S.3.1.1. System must check that IM speed advisories are within the capability of the aircraft (Allocated to: ATC, TFM, Flight crews, FMS, or other automation (see the following requirements))

STPA-G.5S.3.1.2. TFM must not issue speed advisory that exceeds aircraft capability, including stall and overspeed (Allocated to: TFM Automation)

STPA-G.5S.3.1.3. ATC must not issue clearance that exceeds aircraft capability, including stall and overspeed (Allocated to: ATC, FAA Procedures)

STPA-G.5S.3.1.4. Flight crew must reject a clearance that exceeds aircraft capability, including stall and overspeed (Allocated to: Flight Crew)

STPA-G.5S.3.1.5. Flight crew must request an amended clearance and state that existing clearance exceeds aircraft capability. (Allocated to: Flight Crew)

STPA-G.5S.3.2. Automation presents clearance in format inconsistent with ATC understanding (e.g. in IAS instead of mach)

STPA-G.5S.3.2.1. IM interface must present speed advisory with associated units, either indicated airspeed or mach number. (Allocated to: IM-S Interface)

STPA-G.5S.3.2.2. ATC must issue clearance with appropriate unit (airspeed or mach) (Allocated to: ATC)

STPA-G.5S.4. Flight Crew executes a speed modification that exceeds aircraft capability [Inadequate Actuator Operation]

STPA-G.5S.4.1. Flight crew inadvertently enters wrong speed into FMS

STPA-G.5S.4.1.1. Flight crew must fly aircraft to IM speed if the speed is within aircraft capability. Otherwise flight crew must request amended clearance. (Allocated to: Flight crew, FMS)

STPA-G.5S.4.1.2. TFM must be provided with surveillance data to verify if flight is performing as expected to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: ADS-B, GNSS, Radar, ERAM, Fused track data reports)

STPA-G.5S.4.1.3. TFM must check that flight performance is within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: TFM Automation, ERAM)

STPA-G.5S.4.1.4. TFM (or other tool such as ATC IM automation) must provide alert when performance is not within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: TFM Automation, ERAM, IM-S Automation)

STPA-G.5S.4.2. Flight crew flies aircraft in different configuration than what was assumed during issuance of clearance

STPA-G.5S.4.2.1. Flight crew must execute IM speed in cruise configuration and at level flight (Allocated to: Flight Crew)

STPA-G.5S.4.2.2. Flight crew must notify ATC if aircraft is not in cruise configuration or level flight (Allocated to: Flight Crew)

Unsafe Control Action: UCA6.S. Providing a speed modification that leads to inclement **weather.** ↑**[H**-3;H-4;H-5]

STPA-G.6S.1. ATC believes the aircraft is flying a different trajectory than it actually is. ATC believes aircraft is in a different position relative to convective weather [ATC process model of Aircraft / FC is incorrect]

STPA-G.6S.1.1. ATC incorrectly believes that speed modification will result in avoidance of inclement weather

STPA-G.6S.1.1.1. ATC should avoid the use of speed advisories in the presence of inclement weather, to the extent possible (Allocated to: ATC, FAA Procedures)

STPA-G.6S.1.2. Flight crew / aircraft not flying the reported flight plan

STPA-G.6S.1.2.1. Flight crew must fly the reported flight plan or request a clearance to deviate from the plan (Allocated to: Flight Crew, FMS)

STPA-G.6S.1.3. Change in environment causes aircraft to be in a different state than expected (e.g. headwinds, tailwinds)

STPA-G.6S.1.3.1. ATC and flight crew must monitor compliance with IM speeds (Allocated to: ATC, Flight Crews)

STPA-G.6S.1.3.2. TFM automation must monitor aircraft compliance with speed advisory and provide an alert if discrepancy exceeds TBD (Allocated to: TFM Automation)

STPA-G.6S.1.4. Signal gets jammed, corrupted or IM clearance interferes with other clearance

STPA-G.6S.1.4.1. Protection must be provided against jamming or corruption of the signal between Center TFM and ARTCC centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.6S.1.4.2. Protection must be provided against jamming or corruption of the signal between ARTCC centers and flight decks (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders)

STPA-G.6S.1.4.3. The system must control against radio interference or other types of communication interference (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders
TFM Center software, receivers, transponders)

STPA-G.6S.1.4.4. The IM/TFM system must not interfere with existing ATC systems and procedures (Allocated to: TFM automation, IM automation, IM user interface)

STPA-G.6S.1.5. Inaccurate or inadequate surveillance

STPA-G.6S.1.5.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.6S.1.5.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: ERAM, ADS-B)

STPA-G.6S.1.5.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: ERAM, ADS-B)

STPA-G.6S.1.5.4. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, Radar)

STPA-G.6S.2. ATC is unaware of the presence of convective weather [ATC process model of airspace is incorrect]

STPA-G.6S.2.1. Inclement weather forms rapidly, before ATC can be made aware

STPA-G.6S.2.1.1. Flight crews may request an amended clearance due to inclement weather if the crew deams it necessary (Allocated to: Flight Crews)

STPA-G.6S.2.1.2. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NAS Weather Service (NWS))

STPA-G.6S.2.2. Flight crews do not report experiencing turbulance or observing inclement weather

STPA-G.6S.2.2.1. Flight crews must report turbulance and/or observation of inclement weather (Allocated to: Flight crews)

STPA-G.6S.2.2.2. Flight crews must report location, heading, altitude, and

airspeed when reporting inclement (Allocated to: Flight crews)

STPA-G.6S.2.2.3. Flight crews must report type of weather, including turbulence, lightning, poor visibility, and others.

Flight crews must report weather according to severity level in FAA standards (Allocated to: Flight crews)

STPA-G.6S.2.3. NAS weather service surveillance is inaccurate

STPA-G.6S.2.3.1. Precipitation measurements must be within TBD dBZ with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-G.6S.2.3.2. Wind measurements must be within TBD kts with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-G.6S.2.3.3. NAS weather service must notify ATC of accuracy and resolution of weather data, or notify ATC when the above requirements are not met. (Allocated to: NWS)

STPA-G.6S.2.4. ATC misinterprets or misunderstands"Resolution" or accuracy of weather service

STPA-G.6S.2.4.1. The weather service user interface must clearly present the spatial resolution of weather surveillance (Allocated to: NWS User Interface)

STPA-G.6S.2.4.2. The weather service user interface must clearly present the time of applicability of weather surveillance (Allocated to: NWS User Interface)

STPA-G.6S.2.5. NAS weather service does not update its surveillance fast enough

STPA-G.6S.2.5.1. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NWS (AWIPS, WARP, or other))

STPA-G.6S.2.6. Weather monitoring interface does not update fast enough

STPA-G.6S.2.6.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: NWS Automation)

STPA-G.6S.2.6.2. ATC must not give clearance based on a user interface that is not updating (Allocated to: ATC, FAA Procedures)

STPA-G.6S.2.7. ATC has incorrect understanding of location of weather

STPA-G.6S.2.7.1. The weather service user interface must have the same scale and perspective as aircraft surveillance surveillance screens (Plan position indicator) (Allocated to: NWS Automation)

STPA-G.6S.2.8. Weather data is displayed incorrectly or in a confusing manner

STPA-G.6S.2.8.1. Weather data must be presented in a consistent format, within and across sectors (Allocated to: NWS, Tower, TRACON, ARTCC facilities)

STPA-G.6S.2.9. ATC receives report of inclement weather from flight crew but misinterprets location of aircraft

STPA-G.6S.2.9.1. ATC must verify location of aircraft per FAA standards (Allocated to: ATC, FAA Procedures)

STPA-G.6S.2.10. Incorrect surveillance of aircraft

STPA-G.6S.2.10.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.6S.2.10.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: ERAM, ADS-B)

STPA-G.6S.2.10.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: ERAM, ADS-B)

STPA-G.6S.2.10.4. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, Radar)

STPA-G.6S.2.11. Incorrect identification of aircraft

STPA-G.6S.2.11.1. Airline operator must verify that the registration/call sign matches the associated aircraft data file (Allocated to: Airline operators)

STPA-G.6S.2.11.2. ATC and flight crews must communicate and verify aircraft information per FAA standards (Allocated to: ATC, Flight Crew)

STPA-G.6S.2.11.3. Data must be generated and translated per internationally recognized standards (Allocated to: ERAM, Other ATC or Operator automation,

Communication networks)

STPA-G.6S.2.11.4. Aircraft data file must be provided to TFM automation and ATC in standardized format. (Allocated to: Airline operators)

STPA-G.6S.2.11.5. Aircraft data includes certification, airworthiness, and other regulations. (Allocated to: Airframe manufacturers)

STPA-G.6S.2.11.6. Aircraft data file must be updated every flight or any time maintenance is performed that changes flight characteristics (Allocated to: Airline operators)

STPA-G.6S.2.12. ATC has incorrect understanding of magnitude or severity of weather

STPA-G.6S.2.12.1. Severity of weather must be presented or communicated in a consistent format within and across sectors (Allocated to: NWS Surveilance, NWS User Interface)

STPA-G.6S.2.13. Flight crew report underestimates severity

STPA-G.6S.2.13.1. Precipitation must communicated in terms of "Light", "Moderate", "Heavy", and "Extreme" paired with appropriate dBZ range of precipitation intensity level (Allocated to: FAA Procedures, NWS)

STPA-G.6S.2.14. ATC misinterprets NAS weather service surveillance (e.g. wrong colors on radar screen)

STPA-G.6S.2.14.1. Presentation of weather data in user interface must be consistent with ATC Weather Radar Terms (Allocated to: NWS User Interface)

STPA-G.6S.2.15. NAS weather service weather prediction/modeling is incorrect

STPA-G.6S.2.15.1. Current weather surveillance data supercedes forecasted data (Allocated to: ATC, FAA Procedures, NWS)

STPA-G.6S.2.15.2. ATC must issue weather avoidance clearances based on real-time weather surveillance data (Allocated to: ATC, FAA Procedures)

STPA-G.6S.2.16. ATC generates control actions (lack thereof) based on inappropriate time horizon.

STPA-G.6S.2.16.1. Short range forecasts must be updated every TBD hours (Allocated to: NWS)

STPA-G.6S.2.16.2. Medium range forecasts must be updated every TBD days (Allocated to: NWS)

STPA-G.6S.2.16.3. ATC must be presented with time of applicability of all weather forecasts (Allocated to: NWS)

STPA-G.6S.2.16.4. User interface must indicate when forecasts become invalid (Allocated to: NWS)

STPA-G.6S.2.17. ATC misinterprets confidence in weather modeling. For example, weather service has only 40% accuracy currently but ATC assumes a much better prediction

STPA-G.6S.2.17.1. Quantitative forecasts must include meteorological rationale underlying the model (Allocated to: NWS)

STPA-G.6S.3. ATC relies too heavily on automation to clear aircraft around weather [ATC process model of TFM Automation is incorrect]

STPA-G.6S.3.1. ATC believes that TFM accounts for convective weather in its algorithm for generating advisories (and TFM does NOT generate weather-avoidance advisories).

STPA-G.6S.3.1.1. Weather alerts take precedence over TFM-generated speed advisories (Allocated to: ATC, FAA Procedures, NWS, IM-S)

STPA-G.6S.3.2. IM-S automation interferes with weather tracking

STPA-G.6S.3.2.1. Protection must be provided against jamming or corruption of the signal between Center TFM, ARTCC centers, and NWS centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.6S.3.3. Signal interference or data corruption

STPA-G.6S.3.3.1. The system must control synchronous garbling, nonsynchronous garbling, multipath signals. (Allocated to: NWS avionics, ARTCC software, receivers, transponders

TFM Center software, receivers, transponders)

STPA-G.6S.3.4. Interference with user interface

STPA-G.6S.3.4.1. The IM/TFM system must not interfere with NAS weather service surveillance systems (Allocated to: TFM automation, IM automation, IM user interface, NWS user interface)

STPA-G.6S.3.5. IM-S automation interferes with weather conflict automation

STPA-G.6S.3.5.1. Protection must be provided against jamming or corruption of the signal between Center TFM, ARTCC centers, and NWS centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.6S.3.6. Signal interference or data corruption

STPA-G.6S.3.6.1. The system must control synchronous garbling, nonsynchronous garbling, multipath signals. (Allocated to: NWS avionics, ARTCC software, receivers, transponders
TFM Center software, receivers, transponders)

STPA-G.6S.3.7. Interference with user interface

STPA-G.6S.3.7.1. The IM/TFM system must not interfere with NAS weather service warning systems (Allocated to: TFM automation, IM automation, IM user interface, NWS warning systems)

STPA-G.6S.4. ATC prioritizes sequencing and flow over avoiding convective weather [Incorrect understanding of FAA procedures and priorities]

STPA-G.6S.4.1. ATC must give priority to inclement weather over any IM advisories

STPA-G.6S.4.1.1. ATC,
FAA Procedures (Allocated to: I.e. current speeds optimize the sequence so ATC does not modify the speed)

STPA-G.6S.4.1.2. Weather advisories must take precedence over IM advisories. (Allocated to: ATC,
FAA Procedures,
IM-S Interface Design,

NWS User Interface)

STPA-G.6S.5. Aircraft / Flight crew executes speed modification incorrectly, resulting in a trajectory with inclement weather. This may be due to one or a combination of the following factors [Inadequate actuator operation]

STPA-G.6S.5.1. Flight crew does update FMS incorrectly

STPA-G.6S.5.1.1. Flight crew must enter IM speed into FMS, or (Allocated to: Flight Crew)

STPA-G.6S.5.2. Flight crew flies incorrect speed

STPA-G.6S.5.2.1. Flight crew must manually fly IM speed (Allocated to: Flight Crew)

STPA-G.6S.5.2.2. Flight crew must not deviate from the IM speed provided unless IM speed leads to a hazard. (Allocated to: Flight Crew)

STPA-G.6S.5.2.3. Flight crew must notify ATC of intentional deviation from IM speed and why. (Allocated to: Flight Crew)

STPA-G.6S.5.3. FMS does not follow flight plan

STPA-G.6S.5.3.1. FMS must follow flight plan to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: FMS)

STPA-G.6S.5.3.2. TFM must be provided with surveillance data to verify if flight is performing as expected to within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: ADS-B, Radar)

STPA-G.6S.5.3.3. TFM must check that flight performance is within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: TFM automation, [ERAM])

STPA-G.6S.5.3.4. TFM (or other tool such as ATC automation) must provide alert when performance is not within TBD NM horizontal position, TBD feet altitude, and TBD mach (or airspeed) (Allocated to: TFM automation, [ERAM])

STPA-G.6S.5.4. Degraded performance of aircraft

STPA-G.6S.5.4.1. Flight crew must alert ATC of degraded aircraft performance. (Allocated to: Flight Crew)

STPA-G.6S.5.4.2. ATC must issue special clearances to degraded aircraft in order to avoid inclement weather (Allocated to: ATC)

STPA-G.6S.5.4.3. ATC may request Meteorological assistance from a Center Weather Service Unit (CWSU) (Allocated to: ATC, NWS)

Unsafe Control Action: UCA7.S. Providing a speed modification to an aircraft that was previously safe if given too late after a different clearance has been executed by same or other ai**rcraft ↑[H**-1]

STPA-G.7S.1. ATC is unaware of another clearance the Aircraft/FC is executing or has requested. [Process Model Flaw: Aircraft / FC Model]

STPA-G.7S.1.1. Flight crew / aircraft not flying the flight plan visible to the ATC

STPA-G.7S.1.1.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.7S.1.1.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation, ATC Automation, ATC, Flight Crew)

STPA-G.7S.1.1.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-G.7S.1.1.4. TFM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM)

STPA-G.7S.1.1.5. ATC must have access to surveillance data (Allocated to: ERAM)

STPA-G.7S.1.2. Aircraft / FC has recently passed to new controller (sector or shift change) and in-process clearance was not conveyed

STPA-G.7S.1.2.1. Downstream or adjacent sector controllers must have access to IM clearances being flown by aircraft entering the sector (Allocated to: Sector Automation, IM-S Automation)

STPA-G.7S.1.2.2. Downstream or adjacent sector controllers must have access to IM speed advisories that have not yet been issued to aircraft entering the sector.

This requirement refers to TFM-generated IM speed advisories that have (1) not been accepted by ATC or (2) the clearance for modified speed has not yet been issued. (Allocated to: Sector Automation, IM-S Automation)

STPA-G.7S.1.2.3. All controllers within a sector must have access to TFM-generated speed advisories (Allocated to: IM-S Automation, user interface(s))

STPA-G.7S.1.2.4. All controllers within a sector must have access to IM clearances that are currently being flown (Allocated to: IM-S Automation, user interface(s), Controllers)

STPA-G.7S.1.2.5. Controllers must not issue conflicting IM speed clearances (Allocated to: ATC, IM-S Procedures)

STPA-G.7S.1.3. Other clearance for same aircraft was not entered into TFM automation upon issuance or execution

STPA-G.7S.1.3.1. TFM must have access to new clearances that have been issued by ATC (Allocated to: ATC, IM-S user interface)

STPA-G.7S.1.3.2. Modified flight plans or new clearances must be sent to TFM automation within TBD seconds for all aircraft in sector (Allocated to: Operators, Controllers)

STPA-G.7S.1.4. Center TFM update rate is too slow, new trajectory is not computed until after different clearance is issued

STPA-G.7S.1.4.1. TFM automation must update speed advisories every TBD seconds. (Allocated to: TFM automation)

STPA-G.7S.1.4.2. TFM automation must update speed advisories with TBD seconds of receiving new flight plans or convective weather data (Allocated to: TFM automation)

STPA-G.7S.1.5. Signal gets jammed, corrupted

STPA-G.7S.1.5.1. Protection must be provided against jamming or corruption of the signal between Center TFM and ARTCC centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.7S.1.5.2. Protection must be provided against jamming or corruption of the signal between ARTCC centers and flight decks (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders)

STPA-G.7S.1.5.3. The system must control against radio interference or other types of communication interference (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders, TFM Center software, receivers, transponders)

STPA-G.7S.1.5.4. The IM/TFM system must not interfere with existing ATC systems and procedures (Allocated to: TFM automation, IM automation, IM user interface)

STPA-G.7S.1.6. Aircraft position/speed is incorrect due to surveillance delay so ATC is not aware of mismatch

STPA-G.7S.1.6.1. ADS-B surveillance data must be refreshed every 1 second (Allocated to: ADS-B)

STPA-G.7S.1.6.2. Radar surveillance data must be refreshed every 12 seconds (Allocated to: Radar)

STPA-G.7S.2. ATC is unaware a clearance being issued to another aircraft. [Process Model Flaw: Airspace]

STPA-G.7S.2.1. Clearance for another aircraft was not entered into TFM automation

STPA-G.7S.2.1.1. Modified flight plans or new clearances must be sent to TFM automation within TBD seconds for all aircraft in sector (Allocated to: Operators, Controllers)

STPA-G.7S.3. TFM and/or ATC is not aware of how changing environmental conditions affect prior clearances [Process Model Flaw: Airspace – predicted separation]

STPA-G.7S.3.1. Trajectory information is incorrect because dead-reckoning or other predictive strategy has incorrect/insufficient wind data

STPA-G.7S.3.1.1. TFM automation must have access to real-time surveillance data (Allocated to: TFM automation)

STPA-G.7S.3.1.2. TFM automation must update trajectory model if real-time trajectory deviates from predicted trajectory (Allocated to: TFM automation)

STPA-G.7S.3.2. Strategies and trajectories are modified due to the presence or prediction of convective weather

STPA-G.7S.3.2.1. TFM weather models and weather data must be synchronized with system-wide weather models and weather data (Allocated to: ATC Weather

Service)

STPA-G.7S.3.2.2. ATC must turn off IM tool or reject IM clearances if flight crews report weather that is not included in system-wide models (Allocated to: Controller,)

STPA-G.7S.3.2.3. Flight crews must report the presence of inclement weather (Allocated to: Flight Crews)

STPA-G.7S.4. ATC prioritizes issuing clearance to another aircraft [Process Model Flaw: Airspace – sequence & flow]

STPA-G.7S.4.1. Conflict involving other aircraft is imminent and requires immediate action

STPA-G.7S.4.1.1. ATC must give priority to immediate conflict over any downstream demands (Allocated to: ATC, FAA Procedures)

STPA-G.7S.4.1.2. ATC must monitor aircraft under IM speed advisories for conflicts (Allocated to: ATC)

STPA-G.7S.4.1.3. ATC must monitor traffic adjacent to IM traffic flow for conflicts (Allocated to: ATC)

STPA-G.7S.4.1.4. ATC must issue conflict resolution clearance (not limited to speed modification) even if TFM cannot calculate a valid speed advisory (Allocated to: ATC, FAA Procedures)

STPA-G.7S.4.1.5. ATC must provide appropriate action in the event of an unsafe TFM advisory. (Allocated to: ATC)

STPA-G.7S.4.2. Clearance in conflict with onboard RA

STPA-G.7S.4.2.1. TCAS or other resolution advisory takes precedence over IM speed advisory (Allocated to: ATC, FAA Procedures, Flight Crews)

STPA-G.7S.5. Process Model Flaw: TFM Automation]

STPA-G.7S.5.1. TFM model of airspace is different than ATC model

STPA-G.7S.5.1.1. TFM surveillance data must be synchronized with ATM

system-wide surveillance (Allocated to: ERAM, TFM Automation, ADS-B, GNSS, Radar)

STPA-G.7S.5.1.2. Flight operators (or another entity, TBD) must send updated flight plans to TFM center. Provision must be made to ensure that plan has not been changed due to conflict or other reason. (Allocated to: Airline operators)

STPA-G.7S.5.2. Modified flight plans are not input into TFM trajectory model

STPA-G.7S.5.2.1. TFM must have access to flight plans (Allocated to: Operators (airlines))

STPA-G.7S.5.2.2. Modified flight plans must be sent to TFM automation within TBD seconds (Allocated to: Operators, Controllers)

STPA-G.7S.5.3. Flight plans are input incorrectly into TFM automation

STPA-G.7S.5.3.1. Flight plans must be generated in a consistent, standardized format (Allocated to: FAA Standards, Operators, Controllers)

STPA-G.7S.5.3.2. TFM automation must verify that real-time surveillance data is consistent with flight plans (Allocated to: TFM Automation)

STPA-G.7S.6. Aircraft / Flight crew delays execution of clearance. [Inadequate Actuator Operation]

STPA-G.7S.6.1. FC distraction

STPA-G.7S.6.1.1. Flight crew must verify that the clearance is safe, including whether the clearance does not violate separation standards, is within aircraft capability, and there is no presence of inclement weather or restricted airspace. (Allocated to: Flight Crews)

STPA-G.7S.6.1.2. Flight crew must confirm and accept IM clearance after verification (Allocated to: Flight Crews)

STPA-G.7S.6.1.3. Flight crew must issue a response (acceptance or request of amended clearance) within TBD seconds of ATC issuing clearance. (Allocated to: Flight Crews)

STPA-G.7S.6.2. FMS prevents timely entry and execution

STPA-G.7S.6.2.1. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS)

STPA-G.7S.6.2.2. Flight crew must enter IM speed into FMS or manually fly IM speed within TBD seconds (Allocated to: Flight Crew)

STPA-G.7S.6.3. FC workload is too great to execute in a timely manner

STPA-G.7S.6.3.1. ATC must assume that IM clearance is not being flown if flight crew response is not received in a timely manner, or within TBD seconds of issuance. (Allocated to: ATC (Controllers))

Unsafe Control Action: UCA8.S. Providing a speed modification to an aircraft that was previously safe if given too soon before a different clearance has been executed by same or **other aircraft ↑[H-1]**

STPA-G.8S.1. ATC is unaware that same or another Aircraft/FC has yet to complete or has strayed from another clearance [Process Model Flaw: Aircraft / FC Model]

STPA-G.8S.1.1. Flight crew / aircraft not flying the flight plan visible to the ATC

STPA-G.8S.1.1.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-G.8S.1.1.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation, ATC Automation, ATC, Flight Crew)

STPA-G.8S.1.1.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-G.8S.1.1.4. TFM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM)

STPA-G.8S.1.1.5. ATC must have access to surveillance data (Allocated to: ERAM)

STPA-G.8S.1.2. Aircraft / FC has recently passed to new controller (sector or shift change) and in-process clearance (or alteration) was not conveyed

STPA-G.8S.1.2.1. Downstream or adjacent sector controllers must have access to IM clearances being flown by aircraft entering the sector (Allocated to: Sector Automation, IM-S Automation)

STPA-G.8S.1.2.2. Downstream or adjacent sector controllers must have access to IM speed advisories that have not yet been issued to aircraft entering the sector.

This requirement refers to TFM-generated IM speed advisories that have (1) not been accepted by ATC or (2) the clearance for modified speed has not yet been issued. (Allocated to: Sector Automation, IM-S Automation)

STPA-G.8S.1.2.3. All controllers within a sector must have access to TFM-

generated speed advisories (Allocated to: IM-S Automation, user interface(s))

STPA-G.8S.1.2.4. All controllers within a sector must have access to IM clearances that are currently being flown (Allocated to: IM-S Automation, user interface(s), Controllers)

STPA-G.8S.1.2.5. Controllers must not issue conflicting IM speed clearances (Allocated to: ATC, IM-S Procedures)

STPA-G.8S.1.3. Other clearance for same aircraft was not entered into TFM automation upon issuance or execution

STPA-G.8S.1.3.1. TFM must have access to new clearances that have been issued by ATC (Allocated to: ATC, IM-S user interface)

STPA-G.8S.1.3.2. Modified flight plans or new clearances must be sent to TFM automation within TBD seconds for all aircraft in sector (Allocated to: Operators, Controllers)

STPA-G.8S.1.4. Center TFM update rate is too slow, new trajectory is not computed until after different clearance is issued

STPA-G.8S.1.4.1. TFM automation must update speed advisories every TBD seconds. (Allocated to: TFM automation)

STPA-G.8S.1.4.2. TFM automation must update speed advisories with TBD seconds of receiving new flight plans or convective weather data (Allocated to: TFM automation)

STPA-G.8S.1.5. Signal gets jammed, corrupted

STPA-G.8S.1.5.1. Protection must be provided against jamming or corruption of the signal between Center TFM and ARTCC centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.8S.1.5.2. Protection must be provided against jamming or corruption of the signal between ARTCC centers and flight decks (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders)

STPA-G.8S.1.5.3. The system must control against radio interference or other types of communication interference (Allocated to: Flight deck avionics, ARTCC software, receivers, transponders TFM Center software, receivers,

transponders)

STPA-G.8S.1.5.4. The IM/TFM system must not interfere with existing ATC systems and procedures (Allocated to: TFM automation, IM automation, IM user interface)

STPA-G.8S.1.6. Aircraft position/speed is incorrect due to surveillance delay so ATC is not aware of mismatch

STPA-G.8S.1.6.1. ADS-B surveillance data must be refreshed every 1 second (Allocated to: ADS-B)

STPA-G.8S.1.6.2. Radar surveillance data must be refreshed every 12 seconds (Allocated to: Radar)

STPA-G.8S.1.7. ATC is not able to assess when another clearance is complete or when an aircraft has reached "steady state"

STPA-G.8S.1.7.1. ATC must not issue IM speed advisories while any aircraft in flow are in the midst of a maneuver (Allocated to: ATC, Surveillance, Flight plans)

STPA-G.8S.1.7.2. ATC must be provided information about the execution of manuever (Allocated to: Surveillance, ERAM, Flight plans, Flight crews, ATC (other controllers who have issued clearances))

STPA-G.8S.2. ATC is unaware a clearance has been issued to another aircraft. [Process Model Flaw: Airspace]

STPA-G.8S.2.1. Clearance for another aircraft was not entered into TFM automation

STPA-G.8S.2.1.1. Modified flight plans or new clearances must be sent to TFM automation within TBD seconds for all aircraft in sector (Allocated to: Operators, Controllers)

STPA-G.8S.2.2. ATC rushes or inappropriately batches the issuing of clearances

ATC tries to optimize workflow by "batching" clearances

STPA-G.8S.2.2.1. Minimize the number of amended clearances for aircraft in a

given space to the extent possible. (Allocated to: ATC, FAA Procedures)

STPA-G.8S.2.3. Pressure to finish clearances ahead of shift change

STPA-G.8S.2.3.1. Clearances, including IM-S speed advisories, should not be expedited due to shift changes, changes in control responsibilty, or aircraft leaving/entering airspace. (Allocated to: ATC, FAA Procedures)

STPA-G.8S.2.3.2. Downstream or adjacent sector controllers must have access to IM clearances being flown by aircraft entering the sector (Allocated to: Sector Automation, IM-S Automation)

STPA-G.8S.2.3.3. Downstream or adjacent sector controllers must have access to IM speed advisories that have not yet been issued to aircraft entering the sector.

This requirement refers to TFM-generated IM speed advisories that have (1) not been accepted by ATC or (2) the clearance for modified speed has not yet been issued. (Allocated to: Sector Automation, IM-S Automation)

STPA-G.8S.2.3.4. All controllers within a sector must have access to TFM-generated speed advisories (Allocated to: IM-S Automation, user interface(s))

STPA-G.8S.2.3.5. All controllers within a sector must have access to IM clearances that are currently being flown (Allocated to: IM-S Automation, user interface(s), Controllers)

STPA-G.8S.2.3.6. Controllers must not issue conflicting IM speed clearances (Allocated to: ATC, IM-S Procedures)

STPA-G.8S.3. TFM and/or ATC is not aware of how changing environmental conditions affect prior clearances [Process Model Flaw: Airspace – predicted separation]

STPA-G.8S.3.1. Trajectory information is incorrect because dead-reckoning or other predictive strategy has incorrect/insufficient wind data

STPA-G.8S.3.1.1. TFM automation must have access to real-time surveillance data (Allocated to: TFM automation)

STPA-G.8S.3.2. Strategies and trajectories are modified due to the presence or

prediction of convective weather

STPA-G.8S.3.2.1. TFM automation must update trajectory model if real-time trajectory deviates from predicted trajectory (Allocated to: TFM automation)

STPA-G.8S.4. ATC uses IM-S automation inappropriately due to misunderstanding of automation's design [Process Model Flaw: TFM Automation]

STPA-G.8S.4.1. TFM model of airspace is different than ATC model

STPA-G.8S.4.1.1. TFM weather models and weather data must be synchronized with system-wide weather models and weather data (Allocated to: ATC Weather Service)

STPA-G.8S.4.2. Modified flight plans are not input into TFM trajectory model

STPA-G.8S.4.2.1. ATC must turn off IM tool or reject IM clearances if flight crews report weather that is not included in system-wide models (Allocated to: Controller,)

STPA-G.8S.4.3. Flight plans are input incorrectly into TFM automation

STPA-G.8S.4.3.1. Flight crews must report the presence of inclement weather (Allocated to: Flight Crews)

STPA-G.8S.4.4. ATC uses IM-S automation for tasks other than sequencing

STPA-G.8S.4.4.1. ATC must give priority to conflict over any IM advisories (Allocated to: ATC, FAA Procedures)

STPA-G.8S.4.5. ATC prioritizes IM-S sequencing over conflict resolution

STPA-G.8S.4.5.1. Conflict detection advisories must take precedence over IM advisories. (Allocated to: ATC, FAA Procedures, IM-S Interface Design)

STPA-G.8S.4.6. ATC incorrectly relies on automation for conflict prediction, avoidance, and resolution

STPA-G.8S.4.6.1. Conflict detection tools should be more prominent in ATC display (“glass”) than IM tools (Allocated to: ATC, FAA Procedures, IM-S

Interface Design)

STPA-G.8S.5. Aircraft / Flight crew executes a clearance prematurely [Inadequate Actuator Operation]

STPA-G.8S.5.1. FC distraction

STPA-G.8S.5.1.1. Flight crew must verify that the clearance is safe, including whether the clearance does not violate separation standards, is within aircraft capability, and there is no presence of inclement weather or restricted airspace. (Allocated to: Flight Crews)

STPA-G.8S.5.1.2. Flight crew must confirm and accept IM clearance after verification (Allocated to: Flight Crews)

STPA-G.8S.5.1.3. Flight crew must issue a response (acceptance or request of amended clearance) within TBD seconds of ATC issuing clearance. (Allocated to: Flight Crews)

STPA-G.8S.5.1.4. ATC must clearly state the starting point criteria as part of clearance (Allocated to: ATC)

STPA-G.8S.5.1.5. Flight crew must verify that the IM clearance has a delayed starting point (Allocated to: Flight Crews)

STPA-G.8S.5.2. FC enters clearance into FMS but does not, or forgets to, delay execution

STPA-G.8S.5.2.1. Flight crew must include starting point (time) in command to FMS, when IM clearance includes starting point (Allocated to: Flight Crews)

STPA-G.8S.5.2.2. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS)

STPA-G.8S.5.2.3. Flight crew must enter IM speed into FMS or manually fly IM speed within TBD seconds of starting point (Allocated to: Flight Crew)

STPA-G.8S.5.3. FC executes clearance early in anticipation of increased workload

STPA-G.8S.5.3.1. ATC must verify that IM clearance is not being flown until

TBD seconds of planned starting point. (Allocated to: ATC (Controllers))

Unsafe Control Action: UCA9.S. Providing speed modification too late after environmental conditions (e.g. weather, aircraft speed, heading, etc) have changed ↑[**H**-1;H-2;H-3;H-4;H-5]

STPA-G.9S.1. TFM takes too long to generate IM-S speed advisory [ATC has incorrect process model about automation]

STPA-G.9S.1.1. Transmission from TFM center to ATC ground-based automation takes longer than expected

STPA-G.9S.1.1.1. Transmission of TFM data to ATC sectors must take no longer than TBD seconds (Allocated to: TFM Center, Communication network)

STPA-G.9S.1.1.2. Protection must be provided against jamming or corruption of the signal between TFM centers and ARTCC centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.9S.1.1.3. The system must control against radio interference or other types of communication interference (Allocated to: ARTCC software, receivers, transponders TFM Center software, receivers, transponders)

STPA-G.9S.1.1.4. The IM/TFM system must not interfere with existing ATC systems and procedures (Allocated to: TFM automation, IM automation, IM user interface)

STPA-G.9S.1.2. Model updates too slow, or takes to long to compute advisories based on surveillance that becomes stale

STPA-G.9S.1.2.1. TFM modeling algorithm must generate new trajectory models within TBD seconds of receiving new surveillance or amended flight plans (Allocated to: TFM automation)

STPA-G.9S.1.2.2. TFM automation must generate IM-S speed advisories within TBD seconds of receiving new trajectory models (Allocated to: TFM automation)

STPA-G.9S.1.3. User interface updates too slow

STPA-G.9S.1.3.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: IM-S Automation)

STPA-G.9S.1.4. ATC does not see update soon enough or does not return to screen

to see new speeds

STPA-G.9S.1.4.1. ATC must issue IM clearance within TBD seconds of accepting and confirming IM speed (Allocated to: ATC, FAA Procedures)

STPA-G.9S.1.5. ATC waits too long after accepting TFM-generated IM-S speed advisory to issue clearance

STPA-G.9S.1.5.1. ATC must issue IM speed advisory within TBD seconds of accepting the advisory or before accepting advisory (Allocated to: ATC, FAA Procedures)

STPA-G.9S.2. ATC incorrectly believes that environmental conditions remain the same as when the IM advisory was issued [ATC incorrect process model about airspace]

STPA-G.9S.2.1. Transmission from NWS center to ATC ground-based automation takes longer than expected

STPA-G.9S.2.1.1. Transmission of NWS weather data to ATC sectors must take no longer than TBD seconds (Allocated to: NWS, Communication network)

STPA-G.9S.2.1.2. Protection must be provided against jamming or corruption of the signal between NWS centers and ARTCC centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-G.9S.2.1.3. The system must control synchronous garbling, nonsynchronous garbling, multipath signals. (Allocated to: NWS software, transponders and receivers, ARTCC software, receivers, transponders, TFM Center software, receivers, transponders)

STPA-G.9S.2.1.4. The IM/TFM system must not interfere with NWS systems (Allocated to: TFM automation, IM automation, IM user interface)

STPA-G.9S.2.2. Weather surveillance update takes too long

STPA-G.9S.2.2.1. Real-time weather surveillance must be updated every TBD seconds (Allocated to: NWS)

STPA-G.9S.2.3. Weather surveillance updates are out-of-sync with TFM model update rate

STPA-G.9S.2.3.1. TFM trajectory modeling time horizon must be synchronized with NWS forecast time horizon, OR (Allocated to: TFM automation, NWS forecasting models)

STPA-G.9S.2.3.2. TFM automation must clearly present trajectory modeling time horizon to ATC (Allocated to: TFM automation, TFM user interface)

STPA-G.9S.2.4. Weather changes more rapidly than what is forecasted

STPA-G.9S.2.4.1. Real-time weather surveillance takes precedence over forecasts for clearances related to aircraft within TBD NM of weather advisory (Allocated to: ATC, FAA Procedures, NWS)

STPA-G.9S.2.4.2. Short term forecasts take precendence over real-time weather surveillance for clearances related to aircraft in TBD-TBD NM bands of weather advisory (Allocated to: ATC, FAA Procedures, NWS)

STPA-G.9S.2.4.3. Long term forecasts should not be used for generating or issuing speed modification clearances (Allocated to: ATC, FAA Procedures, NWS)

STPA-G.9S.2.5. ATC uses incorrect weather forecast range

STPA-G.9S.2.5.1. Weather tracking automation must clearly present trajectory modeling time horizon to ATC (Allocated to: NWS Automation)

STPA-G.9S.3. Flight crew / aircraft takes to long too execute speed change

STPA-G.9S.3.1. Flight crew takes too long to enter new speed into FMS

STPA-G.9S.3.1.1. Flight crew must enter IM speed into FMS or manually fly IM speed within TBD seconds ATC cancellation of speed advisory (Allocated to: Flight Crew)

STPA-G.9S.3.2. Flight crew takes too long to manually modify speed

STPA-G.9S.3.2.1. (Allocated to: Flight Crew)

STPA-G.9S.3.3. FMS takes too long to implement change

STPA-G.9S.3.3.1. FMS must begin modifying aircraft speed within TBD

seconds of receiving updated plan from Flight Crew (Allocated to: FMS)

STPA-G.9S.3.3.2. ATC must verify that new desired speed is reached within TBD seconds of issuing cancellation of IM speed advisory (Allocated to: ATC (Controllers))

STPA-G.9S.3.4. Aircraft dynamics are different than ATC expectations (takes 60 seconds to reach steady-state IM speed as opposed to 30 sec)

STPA-G.9S.3.4.1. TFM trajectory modeling must be provided with aircraft performance data on expected time-to-steady-state for completing speed changes. This time should include environmental considerations such as wind, barometric pressure, angle-of-attach, and other relevant factors for flight dynamics (Allocated to: Airline operators, Airframe manufacturers)

STPA-G.9S.3.5. Aircraft performance is different than expected due to environmental conditions such as headwinds or tailwinds

STPA-G.9S.3.5.1. Flight crews must verify that speed modification is feasible given current environmental conditions (Allocated to: Flight crew)

STPA-G.9S.3.5.2. Flight crews must request an amended clearance if speed modificaiton is infeasible (Allocated to: Flight crew)

Unsafe Control Action: UCA10.S. Providing speed modification if modified speed is **applied too long and traffic/weather exists 'downstream' from initiation of maneuver. ↑[H-1;H-2;H-5]**

STPA-G.10S.1. ATC believes that desired separation has not yet been satisfied and inappropriately continues advisory [Inadequate process model of aircraft and airspace]

STPA-G.10S.1.1. Downstream traffic situation changes after initiation of advisory

STPA-G.10S.1.1.1. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-G.10S.1.1.2. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-G.10S.1.1.3. TFM automation must have access to changes in downstream capacity and demands (Allocated to: ATC, Ground-based automation)

STPA-G.10S.1.2. Downstream capacity demands are modified after initiation of advisory, but model/algorithm for generating clearances is not updated

STPA-G.10S.1.2.1. ATC must communicate amended clearances and amended flight plans within TBD seconds of amendment. Communication could be verbal or in the form of datalink or text with other controllers within and across sectors (Allocated to: ATC)

STPA-G.10S.1.3. Aircraft are unexpectedly diverted into flow due to other reasons (weather, airport conditions change)

STPA-G.10S.1.3.1. ATC must have access to amended clearances and amended flight plans within sector (Allocated to: ATC, Ground-based automation)

STPA-G.10S.1.3.2. ATC must have access to amended clearances and amended flight plans within sector (Allocated to: ATC, Ground-based automation)

STPA-G.10S.1.3.3. ATC must be provided with rationale for amended clearances and amended flight plans within and across sectors (Allocated to: ATC)

STPA-G.10S.1.4. Number of aircraft in downstream traffic flow increases after initiation of advisory

STPA-G.10S.1.4.1. ATC must have access to downstream traffic flow within sector, including capacity, sequencing, and spacing (Allocated to: Surveillance user interface, ERAM, Ground-based automation, TFM automation)

STPA-G.10S.1.4.2. ATC must have access to downstream traffic flow in adjacent and other sectors, including capacity, sequencing, and spacing (Allocated to: Surveillance user interface, ERAM, Ground-based automation, TFM automation)

STPA-G.10S.1.4.3. ATC must have access to TFM assumptions about downstream capacity and spacing (Allocated to: TFM automation, TFM user interface)

STPA-G.10S.1.4.4. ATC must verify that downstream capacity is consistent with assumptions in TFM model prior to initiation of IM speed advisory (Allocated to: ATC, FAA procedures)

STPA-G.10S.1.4.5. ATC must reject IM speed advisory and provide new clearance if downstream traffic situation changes after initation of IM speed advisory (Allocated to: ATC, FAA procedures)

STPA-G.10S.1.4.6. TFM must provide updated speed advisories if downstream traffic situation changes after initiation of IM speed advisory (Allocated to: TFM automation, TFM user interface)

STPA-G.10S.1.5. Number of aircraft and location of those aircraft in traffic flow is not updated in model in appropriate time

STPA-G.10S.1.5.1. TFM must update traffic flow information every 1 second (Allocated to: TFM automation)

STPA-G.10S.1.6. Downstream environment changes after initiation of advisory

STPA-G.10S.1.6.1. ATC must monitor downstream and adjacent environment before and during execution of advisory (Allocated to: ATC, NWS)

STPA-G.10S.1.6.2. IM-S speed advisory becomes invalid if weather severity is downgraded before or during execution of advisory (Allocated to: TFM automation, ATC, NWS)

STPA-G.10S.1.6.3. IM-S trajectory modeling refresh rate must be synchronized with weather forecasting and surveillance refresh rates (Allocated to: TFM

automation, NWS)

STPA-G.10S.1.7. Aircraft are unexpectedly diverted into flow due change in weather that is unpredicted or incorrectly predicted by NWS

STPA-G.10S.1.7.1. TFM trajectory modeling time horizon must be synchronized with weather forecast time horizon (Allocated to: TFM automation, NWS forecasting)

STPA-G.10S.1.7.2. IM-S speed advisory becomes invalid if capacity in flow changes by more than TBD aircraft per NM, before or during execution of advisory (Allocated to: TFM automation, ATC, ADS-B or radar surveillance, ERAM)

STPA-G.10S.1.8. Number of available runways change

STPA-G.10S.1.8.1. TFM must have access to number of runways and runway capacity of each airport (Allocated to: Tower controllers, Airport operators)

STPA-G.10S.1.8.2. All controllers must have access to number of runways and runway capacity of each airport (Allocated to: Tower controllers, Airport operators)

STPA-G.10S.1.8.3. Runway availability and capacity must be updated every TBD minutes (Allocated to: Tower controllers, Airport operators)

STPA-G.10S.1.8.4. TFM modeling of capacity must be synchronized with runway availability and capacity refresh rates (Allocated to: TFM automation)

STPA-G.10S.1.9. Approach conditions change, and not updated in model (e.g. switching direction or runway due to changes in winds)

STPA-G.10S.1.9.1. TFM automation must have access to changes in runway configurations and approach routes (Allocated to: Tower ATC, TRACON, Ground-based automation)

STPA-G.10S.1.9.2. En route ATC must have access to changes in runway configurations and approach routes (Allocated to: Tower ATC, TRACON, Ground-based automation)

STPA-G.10S.1.9.3. ATC must have access to runway and approach configurations being used by TFM modeling (Allocated to: TFM automation,

TFM user interface)

STPA-G.10S.1.9.4. TFM and other en route tools must be notified of configuration change within TBD seconds of change (Allocated to: Tower ATC, TRACON, Ground-based automation)

STPA-G.10S.1.10. Environment around aircraft changes after initiation of advisory, causing fulfillment of separation goal (timing constraint) to be achieved earlier than expected

STPA-G.10S.1.10.1. ATC must monitor aircraft state relative to separation / timing goal after initial execution of IM speed advisory. (Allocated to: ATC)

STPA-G.10S.2. Target aircraft, or other aircraft in flow, flies a different speed than expected after initiation of advisory (e.g. leading target flies slower than expected so goal is attained quicker)

STPA-G.10S.2.1. Target aircraft (or other aircraft in IM-S flow) degraded performance

STPA-G.10S.2.1.1. IM-S speed advisory becomes invalid if any aircraft in traffic flow are not within TBD mach (or knots) of predicted speed (Allocated to: IM-S automation)

STPA-G.10S.2.2. Target aircraft (or other aircraft in IM-S flow) incorrect execution

STPA-G.10S.2.2.1. Any aircraft in traffic flow must fly within TBD mach (or knots) of predicted speed (Allocated to: Flight crews)

STPA-G.10S.2.3. Change in environment, and target aircraft (or other aircraft in IM-S flow) have different flight dynamics relative to environment

STPA-G.10S.2.3.1. TFM must have access to aircraft performance given expected environmental conditions, including wind, pressure, altitude, airspeed (Allocated to: Airline operators, Airframe manufacturers)

STPA-G.10S.2.4. Target aircraft (or other aircraft in IM-S flow) must avoid conflict

STPA-G.10S.2.4.1. ATC must be informed about conflict resolutions for any aircraft in traffic flow (Allocated to: TCAS, Flight crews, Ground-based automation)

STPA-G.10S.2.4.2. ATC may reject or modify IM-S clearance based on a conflict resolution of any aircraft in traffic flow or adjacent airspace (Allocated to: ATC, FAA procedures)

STPA-G.10S.2.5. ATC does not "see" target aircraft (or other aircraft in IM-S flow) due to sector boundary

STPA-G.10S.2.5.1. ATC may reject or modify IM-S clearance based on a conflict resolution of any aircraft in traffic flow or adjacent, downstream, or upstream sectors (Allocated to: ATC, FAA procedures)

STPA-G.10S.3. ATC uses incorrect spacing goal* and therefore continues advisory to meet incorrect goal [Inadequate process model of airspace]

STPA-G.10S.3.1. ATC spacing goal mismatches spacing in TFM model

STPA-G.10S.3.1.1. ATC must have access to TFM spacing goal (Allocated to: TFM automation, TFM user interface)

STPA-G.10S.3.1.2. ATC may reject IM-S speed advisories if controller deems the TFM spacing goals to be appropriate (Allocated to: ATC, FAA procedures)

STPA-G.10S.3.2. Spacing goal changes due to change in capacity or demands

STPA-G.10S.3.2.1. TFM must synchronize spacing goals with available capacity and demands (Allocated to: TFM automation)

STPA-G.10S.3.3. Spacing goal changes due to change in quality of surveillance

STPA-G.10S.3.3.1. TFM must synchronize spacing goals with quality of surveillance data (Allocated to: TFM automation)

STPA-G.10S.4. TFM incorrectly continues speed advisory, ATC over reliance on automation [Inadequate process model of TFM automation]

STPA-G.10S.4.1. TFM computation / model does not update correctly and last valid update included advisory

STPA-G.10S.4.1.1. TFM must update trajectory model and IM computation at least every 1 second (Allocated to: TFM automation)

STPA-G.10S.4.1.2. TFM must notify ATC that advisory has timed out within TBD seconds of calculating that IM speed is no longer valid (Allocated to: TFM automation, TFM user interface)

STPA-G.10S.4.2. TFM user interface does not update correctly and last valid update included advisory

STPA-G.10S.4.2.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: NWS Automation)

STPA-G.10S.4.2.2. ATC must not give IM-related clearance based on a user interface that is not updating (Allocated to: ATC, FAA Procedures)

STPA-G.10S.4.3. TFM trajectory model has incorrect parameter for how long it will take between advisory timing out and aircraft reaching new steady-state

STPA-G.10S.4.3.1. TFM trajectory modeling must be provided with aircraft performance data on expected time-to-steady-state for completing speed changes. This time should include environmental considerations such as wind, barometric pressure, angle-of-attach, and other relevant factors for flight dynamics and have upper and lower bounds (Allocated to: Airline operators, Airframe manufacturers)

STPA-G.10S.4.3.2. ATC must issue or reject IM speed advisory within TBD seconds. (Allocated to: ATC)

STPA-G.10S.5. ATC incorrectly believes that something ahead of or behind aircraft should cause advisory to be continued [Inadequate process model of airspace and automation]

STPA-G.10S.5.1. False conflict advisory

STPA-G.10S.5.1.1. False conflict alerts should occur no more than TBD% of total conflict alerts (Allocated to: TCAS, Ground-based conflict alert systems)

STPA-G.10S.5.2. False weather alert

STPA-G.10S.5.2.1. False weather alerts should occur no more than TBD% of total weather alerts (Allocated to: NWS)

STPA-G.10S.6. Flight crew incorrectly executes speed during advisory, or changes

speed after initiation [Inadequate actuator operation]

STPA-G.10S.6.1. FC distraction

STPA-G.10S.6.1.1. Flight crew must continually verify throughout speed advisory that the clearance is safe, including whether the clearance does not violate separation standards, is within aircraft capability, and there is no presence of inclement weather or restricted airspace. (Allocated to: Flight Crews)

STPA-G.10S.6.1.2. Flight crew must issue a response (request of amended clearance) within TBD seconds of observing potential conflict (Allocated to: Flight Crews)

STPA-G.10S.6.2. FC fails to enter new speed into FMS or delays entering new speed

STPA-G.10S.6.2.1. Flight crew must enter IM speed into FMS or manually fly IM speed within TBD seconds ATC cancellation of speed advisory (Allocated to: Flight Crew)

STPA-G.10S.6.2.2. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS)

STPA-G.10S.6.3. FC programs change in speed into FMS in anticipation of heavy workload and does not update speed

STPA-G.10S.6.3.1. ATC must verify that new desired speed is reached within TBD seconds of issuing cancellation of IM speed advisory (Allocated to: ATC (Controllers))

Unsafe Control Action: UCA11.S. Providing speed modification if modified speed is not **applied long enough and separation not achieved. ↑[H-1]**

STPA-G.11S.1. ATC incorrectly believes that desired separation has been satisfied and stops advisory inappropriately [Inadequate process model of aircraft and airspace]

STPA-G.11S.1.1. Downstream traffic situation changes after initiation of advisory

STPA-G.11S.1.1.1. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-G.11S.1.1.2. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-G.11S.1.1.3. TFM automation must have access to changes in downstream capacity and demands (Allocated to: ATC, Ground-based automation)

STPA-G.11S.1.2. Model/algorithm for generating clearances is updated at a faster rate than downstream capacity updates

STPA-G.11S.1.2.1. IM-S advisory algorithm update rate must be synchronized with downstream capacity update rate (Allocated to: TFM automation, Ground-based automation)

STPA-G.11S.1.2.2. Capacity update rate and clearance algorithm update rate must be synchronized (Allocated to: Ground-based automation)

STPA-G.11S.1.3. Aircraft are unexpectedly diverted into flow due to other reasons (weather, airport conditions change)

STPA-G.11S.1.3.1. ATC must have access to amended clearances and amended flight plans within sector (Allocated to: ATC, Ground-based automation)

STPA-G.11S.1.3.2. ATC must have access to amended clearances and amended flight plans within sector (Allocated to: ATC, Ground-based automation)

STPA-G.11S.1.3.3. ATC must be provided with rationale for amended clearances and amended flight plans within and across sectors (Allocated to: ATC)

STPA-G.11S.1.4. ATC incorrectly assesses presence of merging aircraft (thinks more are merging than really are) and prematurely terminates IM clearance

STPA-G.11S.1.4.1. ATC must have access to downstream traffic flow within sector, including capacity, sequencing, and spacing (Allocated to: Surveillance user interface, ERAM, Ground-based automation, TFM automation)

STPA-G.11S.1.4.2. ATC must have access to downstream traffic flow in adjacent and other sectors, including capacity, sequencing, and spacing (Allocated to: Surveillance user interface, ERAM, Ground-based automation, TFM automation)

STPA-G.11S.1.4.3. ATC must have access to TFM assumptions about downstream capacity and spacing (Allocated to: TFM automation, TFM user interface)

STPA-G.11S.1.4.4. ATC must verify that downstream capacity is consistent with assumptions in TFM model prior to initiation of IM speed advisory (Allocated to: ATC, FAA procedures)

STPA-G.11S.1.4.5. ATC must reject IM speed advisory and provide new clearance if downstream traffic situation changes after initation of IM speed advisory (Allocated to: ATC, FAA procedures)

STPA-G.11S.1.4.6. TFM must provide updated speed advisories if downstream traffic situation changes after initiation of IM speed advisory (Allocated to: TFM automation, TFM user interface)

STPA-G.11S.1.5. Number of aircraft and location of those aircraft in traffic flow is not updated in model in appropriate time

STPA-G.11S.1.5.1. TFM must update traffic flow information every 1 second (Allocated to: TFM automation)

STPA-G.11S.1.6. Model/algorithm for generating clearances is updated at a faster rate than weather surveillance updates

STPA-G.11S.1.6.1. ATC must monitor downstream and adjacent environment before and during execution of advisory (Allocated to: ATC, NWS)

STPA-G.11S.1.6.2. IM-S speed advisory becomes invalid if weather severity is downgraded before or during execution of advisory (Allocated to: TFM automation, ATC, NWS)

STPA-G.11S.1.6.3. IM-S trajectory modeling refresh rate must be synchronized with weather forecasting and surveillance refresh rates (Allocated to: TFM automation, NWS)

STPA-G.11S.1.7. ATC believes weather forecast has shorter time horizon that it really does. For example, ATC believes forecast is for 15 minutes when it is really 2 hours and therefore terminates IM

STPA-G.11S.1.7.1. TFM trajectory modeling time horizon must be synchronized with weather forecast time horizon (Allocated to: TFM automation, NWS forecasting)

STPA-G.11S.1.7.2. IM-S speed advisory becomes invalid if capacity in flow changes by more than TBD aircraft per NM, before or during execution of advisory (Allocated to: TFM automation, ATC, ADS-B or radar surveillance, ERAM)

STPA-G.11S.1.8. Number of available runways change

STPA-G.11S.1.8.1. TFM must have access to number of runways and runway capacity of each airport (Allocated to: Tower controllers, Airport operators)

STPA-G.11S.1.8.2. All controllers must have access to number of runways and runway capacity of each airport (Allocated to: Tower controllers, Airport operators)

STPA-G.11S.1.8.3. Runway availability and capacity must be updated every TBD minutes (Allocated to: Tower controllers, Airport operators)

STPA-G.11S.1.8.4. TFM modeling of capacity must be synchronized with runway availability and capacity refresh rates (Allocated to: TFM automation)

STPA-G.11S.1.9. Approach conditions change, and not updated in model (e.g. switching direction or runway due to changes in winds)

STPA-G.11S.1.9.1. TFM automation must have access to changes in runway configurations and approach routes (Allocated to: Tower ATC, TRACON, Ground-based automation)

STPA-G.11S.1.9.2. En route ATC must have access to changes in runway configurations and approach routes (Allocated to: Tower ATC, TRACON, Ground-based automation)

STPA-G.11S.1.9.3. ATC must have access to runway and approach configurations being used by TFM modeling (Allocated to: TFM automation, TFM user interface)

STPA-G.11S.1.9.4. TFM and other en route tools must be notified of configuration change within TBD seconds of change (Allocated to: Tower ATC, TRACON, Ground-based automation)

STPA-G.11S.1.10. Environment around aircraft changes after initiation of advisory, causing fulfillment of separation goal (timing constraint) to be achieved earlier than expected

STPA-G.11S.1.10.1. ATC must monitor aircraft state relative to separation / timing goal after initial execution of IM speed advisory. (Allocated to: ATC)

STPA-G.11S.2. Target aircraft, or other aircraft in flow, flies a different speed than expected after initiation of advisory (e.g. leading target flies faster than expected so goal takes longer)

STPA-G.11S.2.1. Target aircraft (or other aircraft in IM-S flow) degraded performance

STPA-G.11S.2.1.1. IM-S speed advisory becomes invalid if any aircraft in traffic flow are not within TBD mach (or knots) of predicted speed (Allocated to: IM-S automation)

STPA-G.11S.2.2. Target aircraft (or other aircraft in IM-S flow) incorrect execution

STPA-G.11S.2.2.1. Any aircraft in traffic flow must fly within TBD mach (or knots) of predicted speed (Allocated to: Flight crews)

STPA-G.11S.2.3. Change in environment, and target aircraft (or other aircraft in IM-S flow) have different flight dynamics relative to environment

STPA-G.11S.2.3.1. TFM must have access to aircraft performance given expected environmental conditions, including wind, pressure, altitude, airspeed (Allocated to: Airline operators, Airframe manufacturers)

STPA-G.11S.2.4. Target aircraft (or other aircraft in IM-S flow) must avoid conflict

STPA-G.11S.2.4.1. ATC must be informed about conflict resolutions for any aircraft in traffic flow (Allocated to: TCAS, Flight crews, Ground-based automation)

STPA-G.11S.2.4.2. ATC may reject or modify IM-S clearance based on a conflict resolution of any aircraft in traffic flow or adjacent airspace (Allocated to: ATC, FAA procedures)

STPA-G.11S.2.5. ATC does not "see" target aircraft (or other aircraft in IM-S flow) due to sector boundary

STPA-G.11S.2.5.1. ATC may reject or modify IM-S clearance based on a conflict resolution of any aircraft in traffic flow or adjacent, downstream, or upstream sectors (Allocated to: ATC, FAA procedures)

STPA-G.11S.3. ATC uses incorrect spacing goal* and therefore terminates advisory to meet incorrect goal [Inadequate process model of airspace]

STPA-G.11S.3.1. ATC spacing goal mismatches spacing in TFM model

STPA-G.11S.3.1.1. ATC must have access to TFM spacing goal (Allocated to: TFM automation, TFM user interface)

STPA-G.11S.3.1.2. ATC may reject IM-S speed advisories if controller deems the TFM spacing goals to be appropriate (Allocated to: ATC, FAA procedures)

STPA-G.11S.3.2. Spacing goal changes due to change in capacity or demands

STPA-G.11S.3.2.1. TFM must synchronize spacing goals with available capacity and demands (Allocated to: TFM automation)

STPA-G.11S.3.3. Spacing goal changes due to change in quality of surveillance

STPA-G.11S.3.3.1. TFM must synchronize spacing goals with quality of surveillance data (Allocated to: TFM automation)

STPA-G.11S.4. TFM incorrectly terminates speed advisory, ATC over reliance on automation [Inadequate process model of TFM automation]

STPA-G.11S.4.1. TFM computation / model does not update correctly and last valid update included advisory

STPA-G.11S.4.1.1. TFM must update trajectory model and IM computation at least every 1 second (Allocated to: TFM automation)

STPA-G.11S.4.1.2. TFM must notify ATC that advisory has timed out within TBD seconds of calculating that IM speed is no longer valid (Allocated to: TFM automation, TFM user interface)

STPA-G.11S.4.2. TFM user interface does not update correctly and ATC (correctly) halts IM operations

STPA-G.11S.4.2.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: NWS Automation)

STPA-G.11S.4.2.2. ATC must notify controllers within and across sectors of halted IM operations (Allocated to: ATC, FAA Procedures)

STPA-G.11S.4.2.3. ATC must issue amended clearances when premature termination of IM clearance causes loss of separation or excursion into inclement weather (Allocated to: ATC, FAA procedures)

STPA-G.11S.4.3. TFM trajectory model has incorrect parameter for how long it will take between advisory timing out and aircraft reaching new steady-state

STPA-G.11S.4.3.1. TFM trajectory modeling must be provided with aircraft performance data on expected time-to-steady-state for completing speed changes. This time should include environmental considerations such as wind, barometric pressure, angle-of-attach, and other relevant factors for flight dynamics and have upper and lower bounds (Allocated to: Airline operators, Airframe manufacturers)

STPA-G.11S.4.3.2. ATC must issue or reject IM speed advisory within TBD seconds. (Allocated to: ATC)

STPA-G.11S.5. ATC incorrectly believes that something ahead of or behind aircraft should cause advisory to be terminated [Inadequate process model of airspace and automation]

STPA-G.11S.5.1. False conflict advisory

STPA-G.11S.5.1.1. False conflict alerts should occur no more than TBD% of total conflict alerts (Allocated to: TCAS, Ground-based conflict alert systems)

STPA-G.11S.5.2. False weather alert

STPA-G.11S.5.2.1. False weather alerts should occur no more than TBD% of total weather alerts (Allocated to: NWS)

STPA-G.11S.6. Flight crew incorrectly executes speed during advisory, or changes speed after initiation [Inadequate actuator operation]

STPA-G.11S.6.1. FC distraction

STPA-G.11S.6.1.1. Flight crew must continually verify throughout speed advisory that the clearance is safe, including whether the clearance does not violate separation standards, is within aircraft capability, and there is no presence of inclement weather or restricted airspace. (Allocated to: Flight Crews)

STPA-G.11S.6.1.2. Flight crew must issue a response (request of amended clearance) within TBD seconds of observing potential conflict (Allocated to: Flight Crews)

STPA-G.11S.6.2. FC inadvertently enters new speed into FMS

STPA-G.11S.6.2.1. Flight crew must only enter new speed into FMS per issuance and verification of ATC instruction or due to TCAS or other resolution alert (Allocated to: Flight Crew)

STPA-G.11S.6.3. FC programs change in speed into FMS in anticipation of heavy workload and does not update speed

STPA-G.11S.6.3.1. ATC must verify that new desired speed is reached within TBD seconds of issuing cancellation of IM speed advisory (Allocated to: ATC (Controllers))

STPA-G.11S.6.4. Flight crew incorrectly interprets other communication or instruction as a termination of IM speed

STPA-G.11S.6.4.1. ATC must clearly state speed modification per FAA standards (Allocated to: ATC, FAA procedures)

STPA-G.11S.6.4.2. Flight crew must verify the termination of IM speed advisory (Allocated to: Flight crew, FAA procedures)

A.2 FIM-S

This section contains only the causal analysis (STPA Step 2) of the unsafe control actions identified in Section 3.2.1 of the main body text. Refer to that section for a description of unsafe control actions related to Flight deck-based Interval Management – Spacing (FIM-S) as well as a more general description of FIM-S operations. The following analysis includes scenarios, associated causal factors, and requirements for four basic sets of unsafe control actions. These four sets are related to the general classes of clearances for FIM-S: (1) Maintain Current Spacing, (2) Achieve-by then Maintain, and (3) IM Turn. Because FIM-S involves increasingly autonomous operation of aircraft relative to traditional air traffic management, the fourth category of causal analysis involves Flight Crews and FIM-related automation.

Table 8-Table 12 in the main body list the identified Unsafe Control Actions that are analyzed below.

A.2.1.1 Maintain Current Spacing Causal Analysis

Unsafe Control Action: UCA13.M. Maintain Current Spacing clearance not provided, and no other clearance provided, when current speed is too fast and leads to loss of separation with leading (or merging/crossing) aircraft or too slow and leads to LOS with trailing **aircraft ↑[H-1]**

STPA-F.13M.1. ATC incorrectly believes that aircraft are under spacing advisory or are about to begin [Inadequate process model of automation]

STPA-F.13M.1.1. ATC incorrectly interprets IM-related automation interface

STPA-F.13M.1.1.1. ATC must be provided with information regarding the acceptance, execution, and compliance of IM-related clearances (Allocated to: IM-related ground automation, ADS-B, GNSS, ERAM, Radar)

STPA-F.13M.1.1.2. ATC must verify aircraft compliance with IM clearance when using clearance for separation between non-FIM aircraft (Allocated to: ATC, FAA procedures)

STPA-F.13M.1.2. IM clearance recently terminated and ATC fails to recognize change

STPA-F.13M.1.2.1. IM-related ground automation must update its trajectory model every TBD second (Allocated to: IM-related ground automation)

STPA-F.13M.1.2.2. IM-related ground automation must update the user interface every TBD seconds (Allocated to: IM-related ground automation)

STPA-F.13M.2. ATC fails to identify crossing or merging traffic [Inadequate process model of airspace]

STPA-F.13M.2.1. Overreliance on IM-related automation

STPA-F.13M.2.1.1. Conflict detection and resolution take precedence over IM clearances (Allocated to: ATC, FAA procedures)

STPA-F.13M.2.1.2. Air traffic display and conflict resolution interfaces should be displayed more prominently than IM-related ground automation (Allocated to: ATC sectors, ground automation)

STPA-F.13M.2.2. Incorrect or delayed surveillance

STPA-F.13M.2.2.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.13M.2.2.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-F.13M.2.2.3. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.13M.2.2.4. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, Radar)

STPA-F.13M.2.2.5. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.13M.2.2.6. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.13M.2.3. Lack of coordination within workstation

STPA-F.13M.2.3.1. A single controller must have access to all clearances within a sector and adjacent sectors (Allocated to: Ground automation, user interfaces)

STPA-F.13M.2.4. Lack of coordination with other controllers within sector

STPA-F.13M.2.4.1. All controllers within a sector must have access to IM clearances, including requests, execution, and compliance (Allocated to: Ground automation, user interfaces, communication protocol)

STPA-F.13M.2.5. Lack of coordination with other controllers across sector

STPA-F.13M.2.5.1. All controllers across a sector must have access to IM clearances, including requests, execution, and compliance (Allocated to: Ground automation, user interfaces, communication protocol, comm network)

STPA-F.13M.2.6. Aircraft are unexpectedly diverted into flow due to other reasons

(weather, airport conditions change)

STPA-F.13M.2.6.1. ATC must have access to amended clearances and amended flight plans within sector (Allocated to: ATC, Ground-based automation, airline operators)

STPA-F.13M.2.6.2. ATC must have access to amended clearances and amended flight plans within sector (Allocated to: ATC, Ground-based automation, airline operators)

STPA-F.13M.2.6.3. ATC must be provided with rationale for amended clearances and amended flight plans within and across sectors (Allocated to: ATC, airline operators)

STPA-F.13M.3. ATC does not recognize that aircraft are closing [Inadequate process model of airspace]

STPA-F.13M.3.1. ATC incorrectly interprets or identifies relative speeds of aircraft

STPA-F.13M.3.1.1. Air traffic display and IM-related ground automation must clearly indicated aircraft speeds in appropriate format (Mach, IAS) (Allocated to: Ground automation, user interfaces)

STPA-F.13M.3.2. IM-related automation indicates different speeds than other surveillance interfaces (e.g. radar screen)

STPA-F.13M.3.2.1. IM-related ground automation and air traffic display must have synchronized surveillance displayed (Allocated to: IM-related ground automation, ERAM, traffic display)

STPA-F.13M.3.2.2. IM-related ground automation and air traffic display must have access to the same sources of surveillance data (Allocated to: ADS-B, GNSS, ERAM, Radar)

STPA-F.13M.3.3. Incorrect or delayed surveillance

STPA-F.13M.3.3.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.13M.3.3.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-F.13M.3.3.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.13M.3.3.4. TFM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, Radar)

STPA-F.13M.3.3.5. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.13M.3.3.6. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.13M.3.4. Flight plans are inaccurate

STPA-F.13M.3.4.1. Flight crews must follow flight plans, or (Allocated to: Flight crews)

STPA-F.13M.3.4.2. Flight crews must request amended clearances, or (Allocated to: Flight crews)

STPA-F.13M.3.4.3. Flight crews must notify ATC of a conflict resolution maneuver (Allocated to: Flight crews)

STPA-F.13M.3.5. Flight plans are inconsistent with surveillance

STPA-F.13M.3.5.1. Updated flight plans must be sent to TFM automation within TBD seconds (Allocated to: Airline operators, ATC)

STPA-F.13M.4. Flight crew does not execute maneuver

STPA-F.13M.4.1. See UCA.FC.1

STPA-F.13M.4.1.1. See UCA.FC.1 (Allocated to: See UCA.FC.1)

Unsafe Control Action: UCA14.M. Maintain Current Spacing clearance provided when **current spacing between FIM and target is too little ↑[H-1]**

STPA-F.14M.1. ATC incorrectly believes that aircraft are adequately spaced

STPA-F.14M.1.1. ATC uses incorrect spacing requirement

STPA-F.14M.1.1.1. ATC must not issue Maintain Current Spacing clearance to pair of aircraft that are in violation of spacing requirements (Allocated to: ATC, FAA Procedures)

STPA-F.14M.1.1.2. ATC must use appropriate spacing requirements when issuing Maintain Current Spacing clearance, per JO 7110.65U (Allocated to: ATC, FAA Procedures)

STPA-F.14M.1.2. ATC using filed flight plan for decision instead of real-time fused track data

STPA-F.14M.1.2.1. ATC and associated IM-S automation must use real-time surveillance data for generating IM clearances

See STPA-F.14.1 for requirement related to flight plans

See STPA-F.14.18-21 for requirements related to surveillance (Allocated to: ATC, IM-related automation)

STPA-F.14M.1.3. Fused track data is inaccurate due to spurious ADS-B information or long distance to radar beacon

STPA-F.14M.1.3.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.14M.1.3.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-F.14M.1.3.3. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.14M.1.3.4. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM,
Radar)

STPA-F.14M.1.3.5. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.14M.1.3.6. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.14M.1.4. ATC prioritizes current spacing over potential conflict

STPA-F.14M.1.4.1. Conflict detection and spacing regulations take precedence over interval management (Allocated to: ATC, FAA Procedures)

STPA-F.14M.2. IM-related ground automation suggests clearance

STPA-F.14M.2.1. Automation does not consider spacing regulations or constraints

STPA-F.14M.2.1.1. IM-related ground automation must not generate Maintain Current Spacing clearance to pair of aircraft that are in violation of spacing requirements (Allocated to: IM-related automation)

STPA-F.14M.2.1.2. IM-related ground automation must have access to current surveillance information for all potential FIM and Target aircraft (Allocated to: ADS-B, GNSS, ERAM, Radar)

STPA-F.14M.2.1.3. IM-related ground automation must have access to all spacing regulations for airspace in which the automation generates IM advisories (Allocated to: FAA)

STPA-F.14M.3. See UCA.FC.4

STPA-F.14M.3.1. See UCA.FC.4

STPA-F.14M.3.1.1. See UCA.FC.4 (Allocated to: See UCA.FC.4)

Unsafe Control Action: UCA15.M. Maintain Current Spacing clearance provided when spacing will cause receive aircraft to be incorrect speed for merging aircraft or non-target **aircraft in flow ↑[H-1]**

STPA-F.15M.1. [Process Model Flaw: Aircraft / FC Model]
ATC believes that FC is (or will be) flying a different speed, therefore ATC assumes that separation requirements will be met, and/or issues other clearances based on this assumption.

STPA-F.15M.1.1. Incorrect aircraft ID on radar or flight strip

STPA-F.15M.1.1.1. Modified flight plans or new clearances must be sent to FIM automation within TBD seconds for all aircraft in sector (Allocated to: Operators, Controllers)

STPA-F.15M.1.1.2. The design of user interfaces must not contribute to ATC, flight crew, or airline operator error. (Allocated to: ERAM,
FIM Automation,
Other ATC or Operator Interfaces)

STPA-F.15M.1.1.3. User interfaces must provide a clear, consistent means for entering aircraft data. (Allocated to: ERAM,
FIM Automation,
Other ATC or Operator Interfaces)

STPA-F.15M.1.1.4. Airline operator must verify that the registration/call sign matches the associated aircraft data file (Allocated to: Airline operators)

STPA-F.15M.1.1.5. ATC and flight crews must communicate and verify aircraft information per FAA standards (Allocated to: ATC,
Flight Crew)

STPA-F.15M.1.1.6. Data must be generated and translated per internationally recognized standards (Allocated to: ERAM,
FIM Automation,
Other ATC or Operator automation,
Communication networks)

STPA-F.15M.1.1.7. Aircraft data file must be provided to TFM automation and ATC in standardized format. (Allocated to: Airline operators,)

STPA-F.15M.1.1.8. Aircraft data includes certification, airworthiness, and other regulations. (Allocated to: Airframe manufacturers)

STPA-F.15M.1.1.9. Aircraft data file must be updated every flight or any time maintenance is performed that changes flight characteristics (Allocated to: Airline operators)

STPA-F.15M.1.2. Environmental changes result in modified aircraft capability

STPA-F.15M.1.2.1. TFM automation must have access to real-time wind data for the airspace. (Allocated to: ATC Weather Service)

STPA-F.15M.1.2.2. FIM automation must calculate maximum and minimum allowed speeds for given real-time data. (Allocated to: FIM Automation,
Airframe manufacturers)

STPA-F.15M.1.2.3. Flight crew must notify ATC of inclement weather (Allocated to: Flight crew)

STPA-F.15M.1.3. Aircraft cannot achieve desired speed due to anomaly aboard

STPA-F.15M.1.3.1. Flight crew must alert ATC of degraded aircraft performance. (Allocated to: Flight Crew)

STPA-F.15M.1.3.2. FIM automation must provide alert when aircraft does not meet performance requirements

(Allocated to: FIM Automation)

STPA-F.15M.1.3.3. FIM alerts must not interfere with or supersede other safety-critical warnings (Allocated to: FIM Automation,

FMS, TCAS, aircraft health monitoring systems, and others)

STPA-F.15M.1.3.4. Ground-based tools must be provided with surveillance data to verify if flight is performing as expected to within TBD NM horizontal position, TBD feet altitude, and TBD Mach (or airspeed) (Allocated to: ADS-B,
Radar)

STPA-F.15M.1.3.5. Ground-based tools must check that flight performance is within TBD NM horizontal position, TBD feet altitude, and TBD Mach (or airspeed) (Allocated to: IM-related automation,
[ERAM])

STPA-F.15M.1.3.6. Ground-based tools must provide alert when performance is not within TBD NM horizontal position, TBD feet altitude, and TBD Mach (or airspeed) (Allocated to: IM-related automation,
[ERAM])

STPA-F.15M.1.4. ATC using filed flight plan for decision instead of real-time fused track data

STPA-F.15M.1.4.1. ATC and associated IM-S automation must use real-time

surveillance data for generating IM clearances

See STPA-F.14.1 for requirement related to flight plans

See STPA-F.14.18-21 for requirements related to surveillance (Allocated to: ATC, IM-related automation)

STPA-F.15M.1.5. Fused track data is inaccurate due to spurious ADS-B information or long distance to radar beacon

STPA-F.15M.1.5.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.15M.1.5.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: IM-related ground automation)

STPA-F.15M.1.5.3. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related ground automation)

STPA-F.15M.1.5.4. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM,
Radar)

STPA-F.15M.1.6. Non-FIM aircraft not included in IM automation computations and air traffic controller(s) does(do) not recognize potential conflict

STPA-F.15M.1.6.1. ATC must verify that there are no conflicting aircraft in the proposed IM clearance.

Conflicting aircraft could include crossing, in-track, non-ADS-B equipped aircraft, and others. (Allocated to: ATC,
Conflict detection tools)

STPA-F.15M.2. [Process Model Flaw: Airspace]
Airspace (in particular, a traffic flow) is saturated, and ATC believes that maintain current spacing between two will alleviate potential spacing issues, neglecting non-FIM aircraft maneuvers

STPA-F.15M.2.1. Downstream sector (TRACON or other ARTCC) does not report change in capacity

STPA-F.15M.2.1.1. ATC and associated IM automation must have access to predicted capacity demands and capacity constraints of all adjacent sectors up to TBD hours. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.15M.2.1.2. ATC and associated IM automation must have access to real-time

capacity demands and capacity constraints of all adjacent sectors. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.15M.2.1.3. Downstream or adjacent sector capacity must be considered stale after TBD minutes. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.15M.2.1.4. ATC must not issue IM clearances that will saturate downstream or own airspace (Allocated to: ATC)

STPA-F.15M.2.2. Downstream sector (TRACON or other ARTCC) incorrectly estimates capacity

STPA-F.15M.2.2.1. ATC Centers must have access to real-time weather data, current runway status, updated flight plans, and real-time surveillance. (Allocated to: Tower, tower automation,
ATC Weather Service,
ATC,
Airline operators,
ADS-B, GNSS, Radar, ERAM)

STPA-F.15M.2.2.2. Capacity calculations must include real-time weather data, current runway status, updated flight plans, and real-time surveillance. (Allocated to: ATC Centers and associated automation (automation and/or operators that calculate capacity))

STPA-F.15M.2.2.3. Capacity demands must be updated whenever any of the above components is updated. (Allocated to: ATC Centers and associated automation (automation and/or operators that calculate capacity))

STPA-F.15M.2.3. FIM or ground-based automation contains incorrect time interval rules for given capacity demands

STPA-F.15M.2.3.1. FIM or ground-based automation must not issue IM clearances that will saturate downstream or own airspace (Allocated to: FIM-S Automation [Ground-based automation])

STPA-F.15M.3. [Process Model Flaw: FIM Procedure]
ATC correctly selects FIM-equipped aircraft based on TFM advisory, but neglects non-FIM aircraft in flow.

STPA-F.15M.3.1. FIM automation not designed to consider non-FIM-equipped aircraft and ATC does not understand limitation

STPA-F.15M.3.1.1. ATC must verify that there are no conflicting aircraft in the proposed IM clearance. (Allocated to: ATC,)

STPA-F.15M.3.1.2. Conflicting aircraft could include crossing, in-track, non-ADS-B equipped aircraft, and others. (Allocated to: Conflict detection tools)

STPA-F.15M.3.2. Non-FIM aircraft join the flow after FIM advisory has been generated and accepted

STPA-F.15M.3.2.1. ATC must verify that separation standards are maintained during IM clearance. (Allocated to: ATC,)

STPA-F.15M.3.2.2. Aircraft that join the flow between the FIM and target aircraft invalidate the clearance. (Allocated to: Conflict detection tools)

STPA-F.15M.3.3. Non-FIM aircraft cross the flow after FIM advisory has been generated and accepted

STPA-F.15M.3.3.1. ATC must verify that separation standards are maintained during IM clearance, including aircraft that cross the trajectory of the FIM aircraft, the target aircraft, or in between the two aircraft. (Allocated to: ATC,
Conflict detection tools)

STPA-F.15M.3.4. Non-FIM aircraft join the flow after crossing sector boundary

STPA-F.15M.3.4.1. Downstream or adjacent sector controllers must have access to IM clearances being flown by aircraft entering the sector (Allocated to: Sector Automation, IM-related Automation)

STPA-F.15M.3.4.2. Downstream or adjacent sector controllers must have access to IM speed advisories that have not yet been issued to aircraft entering the sector. (Allocated to: Sector Automation, IM-related Automation)

STPA-F.15M.3.5. Non-FIM aircraft join the flow after transferring work or changing shifts

STPA-F.15M.3.5.1. All controllers within a sector must have access to IM speed advisories (Allocated to: IM-S Automation, user interface(s))

STPA-F.15M.3.5.2. Controllers must not issue conflicting IM speed clearances (Allocated to: ATC,
IM-S Procedures)

STPA-F.15M.4. [Process Model Flaw: FIM Automation/DST] ATC incorrectly trusts IM or other ground-based automation

STPA-F.15M.4.1. Target aircraft does not fly its intended flight path

STPA-F.15M.4.1.1. Target aircraft must fly its intended flight path to within TBD NM horizontal position, TBD feet altitude, TBD vertical speed, and TBD velocity. These predictions must be TBD% accurate for TBD second time horizon prediction. (Allocated to: Target aircraft Flight Crew, FMS)

STPA-F.15M.4.1.2. ATC and/or flight crew must monitor target aircraft trajectory. (Allocated to: ATC,
FIM Flight Crew)

STPA-F.15M.4.2. Target aircraft modifies trajectory from ATC prediction

STPA-F.15M.4.2.1. Target aircraft must notify ATC of intention to modify trajectory. Target aircraft flight crew must request amended clearance. (Allocated to: Target aircraft flight crew)

STPA-F.15M.4.2.2. ATC must confirm that modified target aircraft trajectory allows for a safe IM clearance. (Allocated to: ATC)

STPA-F.15M.4.2.3. If target aircraft is in a compromised state, ATC must not include the aircraft in IM clearance. (Allocated to: ATC)

STPA-F.15M.4.3. ATC misinterprets target aircraft intended flight path

STPA-F.15M.4.3.1. ATC must verify target aircraft intended flight path before issuing IM clearance. (Allocated to: ATC)

STPA-F.15M.5. [Inadequate Actuator Operation]
Aircraft FIM automation calculates incorrect speed to execute FIM separation

STPA-F.15M.5.1. Incorrect ADS-B/fused-track data for ownship

STPA-F.15M.5.1.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy for FIM aircraft. (Allocated to: ADS-B,
GNSS)

STPA-F.15M.5.1.2. The design must protect against use of data that is not in the 95% accuracy range for FIM aircraft. (Allocated to: IM-related Automation,
ERAM)

STPA-F.15M.5.1.3. IM-related automation must check when surveillance data is outside of 95% requirement for FIM aircraft. (Allocated to: IM-related Automation,
ERAM)

STPA-F.15M.5.1.4. IM-related automation must have access to fused track data that includes sources other than ADS-B for FIM aircraft. (Allocated to: ERAM,
Radar)

STPA-F.15M.5.2. Incorrect ADS-B/fused-track data for target aircraft

STPA-F.15M.5.2.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy for target aircraft. (Allocated to: ADS-B,

GNSS)

STPA-F.15M.5.2.2. The design must protect against use of data that is not in the 95% accuracy range for target aircraft. (Allocated to: IM-related Automation, ERAM)

STPA-F.15M.5.2.3. IM-related automation must check when surveillance data is outside of 95% requirement for target aircraft. (Allocated to: IM-related Automation, ERAM)

STPA-F.15M.5.2.4. IM-related automation must have access to fused track data that includes sources other than ADS-B for target aircraft. (Allocated to: ERAM, Radar)

STPA-F.15M.5.2.5. ATC and IM flight crew must verify the accuracy and integrity of both target and FIM aircraft surveillance data. (Allocated to: ATC, Flight crews)

STPA-F.15M.5.3. Incorrect trajectory model in FIM automation

STPA-F.15M.5.3.1. FIM automation must predict target aircraft trajectory to within TBD NM horizontal position, TBD feet altitude, TBD vertical speed, and TBD velocity. These predictions must be TBD% accurate for TBD second time horizon prediction. (Allocated to: FIM Automation)

STPA-F.15M.5.4. FIM automation updates speed modification too late

STPA-F.15M.5.4.1. FIM automation must be provided with updated target aircraft state every TBD seconds. Target aircraft state includes altitude, position, velocity, and vertical speed. (Allocated to: ADS-B or fused-track surveillance)

STPA-F.15M.5.4.2. FIM automation must update target aircraft state every TBD seconds. Target aircraft state includes altitude, position, velocity, and vertical speed. (Allocated to: FIM Automation,)

STPA-F.15M.5.5. Flight crew fails to identify non-FIM aircraft along or adjacent to flight path due to lack of air traffic information

STPA-F.15M.5.5.1. Flight crew must identify conflicting aircraft during IM operations. (Allocated to: Flight Crew)

STPA-F.15M.5.6. Flight crew fails to identify non-FIM aircraft along or adjacent to flight path due to conflict with other on-deck responsibilities

STPA-F.15M.5.6.1. Conflict detection and resolution responsibilities must supersede IM responsibilities. (Allocated to: Flight Crew)

STPA-F.15M.5.6.2. Conflict detection and resolution tools, including alerts, must be more prominent than IM tools. (Allocated to: TCAS or other conflict resolution tool)

STPA-F.15M.5.7. Flight deck-based automation does account for non-FIM aircraft

STPA-F.15M.5.7.1. Conflict detection and resolution responsibilities must supersede IM responsibilities. (Allocated to: Flight Crew)

STPA-F.15M.5.7.2. Conflict detection and resolution tools, including alerts, must be more prominent than IM tools. (Allocated to: TCAS or other conflict resolution tool)

STPA-F.15M.5.8. FMS does not receive speed updates from FIM automation

STPA-F.15M.5.8.1. FIM automation must send updated speed or modified trajectory information to FMS,

OR (Allocated to: FIM Automation,
FMS)

STPA-F.15M.5.8.2. FIM automation must prominently display updated speed or modified trajectory information to the flight crew via the user interface. (Allocated to: FIM Automation)

STPA-F.15M.5.8.3. Flight crew must verify the safety of the updated FIM information. If the updated FIM trajectory is safe, flight crew must fly the trajectory or issue a rejection to ATC. (Allocated to: FIM Automation)

Unsafe Control Action: UCA16.M. Maintain Current Spacing clearance that results in **trajectory which exceeds FIM aircraft capability ↑[H-1]**

STPA-F.16M.1. ATC assigns target aircraft flying a trajectory that exceeds FIM aircraft capability [Inadequate process model of aircraft]

STPA-F.16M.1.1. Target aircraft flies too slow for FIM aircraft (Target a/c has lower stall speed) or Target aircraft flies too fast for FIM aircraft (Target a/c has higher overspeed limits)

STPA-F.16M.1.1.1. ATC or automation must verify that Target aircraft speed is within FIM aircraft capability (Allocated to: ATC, IM-related ground automation)

STPA-F.16M.1.1.2. ATC or automation must have access to aircraft type and speed limits (Allocated to: Airline operators, airframe manufacturers)

STPA-F.16M.1.1.3. FIM flight crew must have access to target aircraft speed (Allocated to: Target aircraft ADS-B or other surveillance)

STPA-F.16M.1.1.4. FIM flight crew or flight deck automation must verify that Target aircraft speed is within FIM aircraft capability (Allocated to: FIM Flight crew, FMS)

STPA-F.16M.1.1.5. FIM flight crew must reject or request amended clearance if maintain current spacing causes FIM aircraft to exceed capability (Allocated to: FIM Flight crew, datacomm)

STPA-F.16M.1.2. Target aircraft performs turn/banking that exceeds FIM aircraft capability

STPA-F.16M.1.2.1. Turning radius less than TBDm or turning rate that exceeds TBD deg/sec invalidate maintain current spacing clearances (Allocated to: ATC, FAA Procedures)

STPA-F.16M.1.2.2. ATC must issue amended clearance to FIM aircraft if target aircraft exceeds banking maneuver requirement (Allocated to: ATC, FAA Procedures)

STPA-F.16M.1.3. FIM aircraft has different capability than target with respect to altitude, winds aloft, and other environmental factors

STPA-F.16M.1.3.1. ATC or automation must have access to current environmental conditions for FIM and target aircraft (Allocated to: NWS weather surveillance)

STPA-F.16M.2. ATC incorrectly believes that target aircraft is flying within capability of FIM aircraft

STPA-F.16M.2.1. Target aircraft surveillance is incorrect or out of date

STPA-F.16M.2.1.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.16M.2.1.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: IM-related ground Automation)

STPA-F.16M.2.1.3. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related ground Automation)

STPA-F.16M.2.1.4. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, Radar)

STPA-F.16M.2.2. Target aircraft speed changes rapidly immediately before IM clearance

STPA-F.16M.2.2.1. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.16M.2.2.2. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.16M.2.2.3. ATC must not issue Maintain Current Spacing clearance if Target aircraft does not have a steady-state velocity (Allocated to: ATC, FAA Procedures)

STPA-F.16M.2.2.4. ATC or automation must verify that Target aircraft has achieved a steady state velocity (Allocated to: ATC, IM-related ground automation)

STPA-F.16M.2.2.5. Steady state velocity is achieved when aircraft speed has not deviated by more than TBD (Mach, IAS) over the last TBD samples relative to the average of last TBD samples (Allocated to: System requirement)

STPA-F.16M.3. Target aircraft performs evasive maneuver that FIM aircraft incorrectly follows

STPA-F.16M.3.1. Target aircraft receives conflict resolution alert

STPA-F.16M.3.1.1. Target aircraft flight crew must notify ATC of evasive maneuver (Allocated to: Flight crew)

STPA-F.16M.3.1.2. Maintain Current Spacing clearance becomes invalid if target aircraft performs evasive maneuver (Allocated to: FAA Procedure)

STPA-F.16M.3.2. ATC instructs target aircraft to change trajectory

STPA-F.16M.3.2.1. ATC must provide amended clearance to FIM aircraft and void maintain current spacing clearance when target aircraft performs evasive maneuver (Allocated to: ATC, FAA Procedures)

Unsafe Control Action: UCA17.M. Maintain Current Spacing clearance is hazardous if given in lieu of vector (turn) clearance when trajectory of target leads to convective weather or restricted airspace [H-2; H-3; H-5]

STPA-F.17M.1. ATC does not prioritize avoidance of convective weather and maintains spacing

STPA-F.17M.1.1. ATC incorrectly prioritizes spacing goals over avoiding hazardous weather, or ATC incorrectly prioritizes minimizing vectors (turns) over avoiding hazardous weather

STPA-F.17M.1.1.1. Convective weather (or other potentially hazardous weather) takes precedence over achieving and maintaining spacing goals (Allocated to: ATC, NWS)

STPA-F.17M.1.1.2. IM systems must not interfere with weather monitoring and forecasting systems (Allocated to: IM-S automation, NWS automation, User interfaces)

STPA-F.17M.1.1.3. Weather alerting should be more prominent than IM advisories (Allocated to: User interface design)

STPA-F.17M.1.2. ATC does not believe or misunderstands severity of weather

STPA-F.17M.1.2.1. False weather alerts should occur no more than TBD% of total weather alerts (Allocated to: NWS)

STPA-F.17M.2. ATC unaware of that weather situation has developed and neglects termination or amendment of IM clearance [Inadequate process model of airspace

STPA-F.17M.2.1. Downstream environment changes after initiation of advisory

STPA-F.17M.2.1.1. ATC must monitor downstream and adjacent environment before and during execution of advisory (Allocated to: ATC,
NWS)

STPA-F.17M.2.1.2. IM-S speed advisory becomes invalid if weather severity is downgraded before or during execution of advisory (Allocated to: TFM automation, ATC,
NWS)

STPA-F.17M.2.1.3. IM-S trajectory modeling refresh rate must be synchronized with weather forecasting and surveillance refresh rates (Allocated to: TFM automation, NWS)

STPA-F.17M.2.2. ATC incorrectly believes that speed modification will result in avoidance of inclement weather

STPA-F.17M.2.2.1. ATC should avoid the use of speed advisories in the presence of inclement weather, to the extent possible (Allocated to: ATC, FAA Procedures)

STPA-F.17M.2.3. Flight crew / aircraft not flying the reported flight plan

STPA-F.17M.2.3.1. Flight crew must fly the reported flight plan or request a clearance to deviate from the plan (Allocated to: Flight Crew, FMS)

STPA-F.17M.2.4. Change in environment causes aircraft to be in a different state than expected (e.g. headwinds, tailwinds)

STPA-F.17M.2.4.1. ATC and flight crew must monitor compliance with IM speeds (Allocated to: ATC, Flight Crews)

STPA-F.17M.2.4.2. TFM automation must monitor aircraft compliance with speed advisory and provide an alert if discrepancy exceeds TBD (Allocated to: TFM Automation)

STPA-F.17M.2.5. Inclement weather forms rapidly, before ATC can be made aware

STPA-F.17M.2.5.1. Flight crews may request an amended clearance due to inclement weather if the crew deems it necessary (Allocated to: Flight Crews)

STPA-F.17M.2.5.2. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NAS Weather Service (NWS))

STPA-F.17M.2.6. NAS weather service surveillance is inaccurate

STPA-F.17M.2.6.1. Precipitation measurements must be within TBD dBZ with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-F.17M.2.6.2. Wind measurements must be within TBD kts with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-F.17M.2.6.3. NAS weather service must notify ATC of accuracy and resolution of weather data, or notify ATC when the above requirements are not met. (Allocated to: NWS)

STPA-F.17M.2.7. ATC misinterprets or misunderstands “Resolution" or accuracy of weather service

STPA-F.17M.2.7.1. The weather service user interface must clearly present the spatial resolution of weather surveillance (Allocated to: NWS User Interface)

STPA-F.17M.2.7.2. The weather service user interface must clearly present the time of applicability of weather surveillance (Allocated to: NWS User Interface)

STPA-F.17M.2.8. NAS weather service does not update its surveillance fast enough

STPA-F.17M.2.8.1. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NWS (AWIPS, WARP, or other))

STPA-F.17M.2.9. Weather monitoring interface does not update fast enough

STPA-F.17M.2.9.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: NWS Automation)

STPA-F.17M.2.9.2. ATC must not give clearance based on a user interface that is not updating (Allocated to: ATC,
FAA Procedures)

STPA-F.17M.2.10. ATC has incorrect understanding of location of weather

STPA-F.17M.2.10.1. The weather service user interface must have the same scale and perspective as aircraft surveillance screens (Plan position indicator) (Allocated to: NWS Automation)

STPA-F.17M.2.11. Weather data is displayed incorrectly or in a confusing manner

STPA-F.17M.2.11.1. Weather data must be presented in a consistent format, within and across sectors (Allocated to: NWS,
Tower,
TRACON,
ARTCC facilities)

STPA-F.17M.2.12. ATC receives report of inclement weather from flight crew but misinterprets location of aircraft

STPA-F.17M.2.12.1. ATC must verify location of aircraft per FAA standards (Allocated to: ATC,
FAA Procedures)

STPA-F.17M.2.13. Incorrect surveillance of aircraft

STPA-F.17M.2.13.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.17M.2.13.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: ERAM,

ADS-B)

STPA-F.17M.2.13.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: ERAM,
ADS-B)

STPA-F.17M.2.13.4. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM,
Radar)

STPA-F.17M.3. Target aircraft enters restricted airspace and ATC unaware [Inadequate process model of airspace]

STPA-F.17M.3.1. Target aircraft is allowed to enter restricted airspace but FIM aircraft is not

STPA-F.17M.3.1.1. ATC should not issue IM clearances to aircraft that have different restrictions relative to airspace within sector. Suppose there is a restricted airspace within, or adjacent to, sector. If aircraft A can operate in R airspace but aircraft B cannot, then aircraft A cannot be a target for aircraft B in an IM clearance. (Allocated to: ATC, FAA Procedures)

STPA-F.17M.3.1.2. ATC must be provided information about aircraft restrictions for all classes of airspace within and across sectors. (Allocated to: FAA, US Gov't, Airline Operators, Airframe Manufacturers)

STPA-F.17M.3.2. Target aircraft incorrectly enters restricted airspace

STPA-F.17M.3.2.1. IM clearance becomes invalid if Target aircraft enters restricted airspace (Allocated to: FAA Procedures)

STPA-F.17M.3.2.2. ATC must terminate IM clearance and vector FIM aircraft away from restricted airspace if Target aircraft enters restricted airspace (Allocated to: ATC, FAA Procedures)

STPA-F.17M.3.2.3. ATC must vector target aircraft away from restricted airspace or provide restrictions to target aircraft (Allocated to: ATC, FAA Procedures)

STPA-F.17M.3.3. Airspace restriction changes and is not updated

STPA-F.17M.3.3.1. ATC must have access to restricted airspace updates within TBD seconds of update (Allocated to: FAA, US Gov't, NWS)

Unsafe Control Action: UCA18.M. Maintain Current Spacing clearance provided before or after a (non-target, could be in a different IM clearance) aircraft is instructed to merge **into flow or aircraft in flow changes speeds ↑[H-1]**

STPA-F.18M.1. ATC anticipates workload or traffic situation and prematurely issues Maintain Current spacing clearance before proper state exists [Contextual factor influences process model]

STPA-F.18M.1.1. ATC rushes or inappropriately batches the issuing of clearances

ATC tries to optimize workflow by "batching" clearances

STPA-F.18M.1.1.1. Minimize the number of amended clearances for aircraft in a given space to the extent possible. (Allocated to: ATC)

STPA-F.18M.1.2. Pressure to finish clearances ahead of shift change

STPA-F.18M.1.2.1. Clearances, including IM Maintain Current Spacing, should not be expedited due to shift changes, changes in control responsibility, or aircraft leaving/entering airspace. (Allocated to: ATC)

STPA-F.18M.1.2.2. Downstream or adjacent sector controllers must have access to IM clearances being flown by aircraft entering the sector (Allocated to: Sector Automation, IM-S Automation)

STPA-F.18M.1.2.3. Downstream or adjacent sector controllers must have access to IM clearances that have not yet been issued to aircraft entering the sector.

This requirement refers to automation- or ATC-generated IM clearance that have (1) not been accepted by ATC or (2) the clearance for maintain separation has not yet been issued. (Allocated to: Sector Automation, IM-S Automation)

STPA-F.18M.1.2.4. All controllers within a sector must have access to automation or ATC-generated IM clearances (Allocated to: IM-S Automation, user interface(s))

STPA-F.18M.1.2.5. All controllers within a sector must have access to IM clearances that are currently being flown (Allocated to: IM-S Automation, user interface(s) Controllers)

STPA-F.18M.1.2.6. Controllers must not issue conflicting IM speed clearances (Allocated to: ATC,
IM-S Procedures)

STPA-F.18M.2. ATC forgets or fails to consider that aircraft are under Maintain Current Spacing while issuing other clearances [Inadequate process model of airspace and aircraft / flight crew]

STPA-F.18M.2.1. Maintain current spacing is provided before sector boundary and merging happens after boundary

STPA-F.18M.2.1.1. ATC must verify that merging aircraft do not violate separation standards (Allocated to: ATC)

STPA-F.18M.2.1.2. When merging or crossing an aircraft between two aircraft in a flow, ATC must verify whether the in-flow aircraft are FIM and Target aircraft (Allocated to: ATC, FAA Procedures)

STPA-F.18M.2.1.3. When merging or crossing an aircraft between two aircraft in a flow, ATC may have to terminate IM Maintain Separation clearance in order to achieve separation. In particular, modifying the trajectory of a target aircraft should be considered insufficient (Allocated to: ATC, FAA Procedures)

STPA-F.18M.2.2. Maintain current spacing is provided by different personnel than controller issuing merge, cross, or speed modification

STPA-F.18M.2.2.1. ATC must verify the presence of crossing or merging aircraft, including adjacent sectors (Allocated to: ATC)

STPA-F.18M.2.2.2. ATC must not issue a Maintain Current Spacing clearance that conflicts or violates minimum separation with crossing or merging traffic (Allocated to: ATC)

STPA-F.18M.3. ATC takes too long to implement or issue clearance [Inadequate process model of airspace and dynamics]

STPA-F.18M.3.1. Transmission from trajectory modeling center to ATC ground-based automation takes longer than expected

STPA-F.18M.3.1.1. Transmission of trajectory model data to ATC sectors must take no longer than TBD seconds (Allocated to: Trajectory modeling center, Communication network)

STPA-F.18M.3.1.2. Protection must be provided against jamming or corruption of the signal between trajectory modeling and prediction centers and ARTCC centers (Allocated to: System-level requirement. See the following two rows for requirement allocation)

STPA-F.18M.3.1.3. The system must control synchronous garbling, nonsynchronous garbling, multipath signals. (Allocated to: ARTCC software, receivers, transponders TFM Center software, receivers, transponders)

STPA-F.18M.3.1.4. The IM system must not interfere with other ATC systems (Allocated to: Trajectory modeling automation, IM automation, IM user interface)

STPA-F.18M.3.2. Model updates too slow, or takes too long to compute advisories based on surveillance that becomes stale

STPA-F.18M.3.2.1. Trajectory modeling algorithm must generate new trajectory models within TBD seconds of receiving new surveillance or amended flight plans (Allocated to: Trajectory modeling automation)

STPA-F.18M.3.2.2. Trajectory modeling automation must generate IM-S speed advisories within TBD seconds of receiving new trajectory models (Allocated to: TFM automation)

STPA-F.18M.3.3. User interface updates too slow

STPA-F.18M.3.3.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: IM-S Automation)

STPA-F.18M.3.4. ATC does not see update soon enough or does not return to screen to see new speeds

STPA-F.18M.3.4.1. ATC must issue IM clearance within TBD seconds of accepting and confirming IM speed (Allocated to: ATC, FAA Procedures)

STPA-F.18M.3.5. ATC waits too long after accepting TFM-generated IM-S speed advisory to issue clearance

STPA-F.18M.3.5.1. ATC must issue IM speed advisory within TBD seconds of accepting the advisory or before accepting advisory (Allocated to: ATC, FAA Procedures)

STPA-F.18M.4. Aircraft / Flight crew executes a clearance prematurely [Inadequate Actuator Operation]

STPA-F.18M.4.1. FC distraction

STPA-F.18M.4.1.1. Flight crew must verify that the clearance is safe, including whether the clearance does not violate separation standards, is within aircraft capability, and there is no presence of inclement weather or restricted airspace. (Allocated to: Flight Crews)

STPA-F.18M.4.1.2. Flight crew must confirm and accept IM clearance after verification (Allocated to: Flight Crews)

STPA-F.18M.4.1.3. Flight crew must issue a response (acceptance or request of amended clearance) within TBD seconds of ATC issuing clearance. (Allocated to: Flight Crews)

STPA-F.18M.4.1.4. ATC must clearly state the starting point criteria as part of clearance

(Allocated to: ATC)

STPA-F.18M.4.1.5. Flight crew must verify that the IM clearance has a delayed starting point (Allocated to: Flight Crews)

STPA-F.18M.4.2. FC enters clearance into FMS but does not, or forgets to, delay execution

STPA-F.18M.4.2.1. Flight crew must include starting point (time) in command to FMS, when IM clearance includes starting point (Allocated to: Flight Crews)

STPA-F.18M.4.2.2. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS)

STPA-F.18M.4.2.3. Flight crew must enter IM speed into FMS or manually fly IM speed within TBD seconds of starting point (Allocated to: Flight Crew)

STPA-F.18M.4.3. FC executes clearance early in anticipation of increased workload

STPA-F.18M.4.3.1. ATC must verify that IM clearance is not being flown until TBD seconds of planned starting point. (Allocated to: ATC (Controllers))

STPA-F.18M.5. Flight crew / aircraft takes too long to execute speed change

STPA-F.18M.5.1. Flight crew takes too long to enter new speed into FMS

STPA-F.18M.5.1.1. Flight crew must enter Maintain clearance into FIM automation, target speed into FMS, or manually fly target speed within TBD seconds ATC cancellation of speed advisory (Allocated to: Flight Crew)

STPA-F.18M.5.2. Flight crew takes too long to manually modify speed

STPA-F.18M.5.2.1. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS, FIM automation)

STPA-F.18M.5.3. FMS takes too long to implement change

STPA-F.18M.5.3.1. ATC must verify that new desired speed is reached within TBD seconds of issuing cancellation of IM speed advisory (Allocated to: ATC (Controllers))

STPA-F.18M.5.3.2. TFM trajectory modeling must be provided with aircraft performance data on expected time-to-steady-state for completing speed changes. This time should include environmental considerations such as wind, barometric pressure, angle-of-attach, and other relevant factors for flight dynamics (Allocated to: Airline operators,
Airframe manufacturers)

STPA-F.18M.5.4. Aircraft dynamics are different than ATC expectations (takes 60 seconds

to reach steady-state IM speed as opposed to 30 sec)

STPA-F.18M.5.4.1. Flight crews must verify that Maintain Current Spacing is feasible given current environmental conditions (Allocated to: Flight crew)

STPA-F.18M.5.5. Aircraft performance is different than expected due to environmental conditions such as headwinds or tailwinds

STPA-F.18M.5.5.1. Flight crews must request an amended clearance if Maintain Current Spacing is infeasible (Allocated to: Flight crew)

STPA-F.18M.5.5.2. Flight crews must request an amended clearance if speed modification is infeasible (Allocated to: Flight crew)

Unsafe Control Action: UCA19.M. Maintain Current Spacing clearance executed where target aircraft modifies speed during Maintain clearance and exceeds receiving aircraft **capability ↑[H-4]**

STPA-F.19M.1. ATC takes too long to issue IM clearance and target modifies speed between evaluation and giving clearance [Inadequate process model of process dynamics]

STPA-F.19M.1.1. Resource constraints due to other traffic issues

STPA-F.19M.1.1.1. ATC must issue Maintain Current Spacing within TBD seconds of evaluating effectiveness and appropriateness of clearance (Allocated to: ATC, FAA Procedures)

STPA-F.19M.1.1.2. ATC must reevaluate clearance parameters if clearance is not issued within TBD seconds of most recent evaluation (Allocated to: ATC, FAA Procedures)

STPA-F.19M.1.1.3. Maintain Current spacing parameters include aircraft capability, equipage, current airspeed, altitude, heading of both aircraft and environmental conditions (Allocated to: IM Procedures)

STPA-F.19M.2. Target aircraft receives different clearance and IM not terminated [ATC inadequate process model of IM clearance]

STPA-F.19M.2.1. Target aircraft cleared to achieve objective outside of IM spacing goal

STPA-F.19M.2.1.1. FIM aircraft may request amended clearance if Target aircraft deviates from desired trajectory (Allocated to: FIM Flight crew)

STPA-F.19M.2.2. Target aircraft vectored for spacing to other aircraft

STPA-F.19M.2.2.1. ATC must reevaluate clearance parameters if Target aircraft is vectored from flight plan or predicted path (Allocated to: ATC)

STPA-F.19M.2.2.2. ATC must terminate Maintain Current Spacing clearance if vectored Target aircraft trajectory exceeds FIM aircraft capability (Allocated to: ATC)

STPA-F.19M.2.3. Target aircraft speed modification for spacing to other aircraft

STPA-F.19M.2.3.1. ATC must reevaluate clearance parameters if Target aircraft is instructed to modify speed from flight plan or predicted path (Allocated to: ATC)

STPA-F.19M.2.3.2. ATC must terminate Maintain Current Spacing clearance if speed modified Target aircraft trajectory exceeds FIM aircraft capability (Allocated to: ATC)

STPA-F.19M.2.4. Target aircraft altitude modification to avoid merging, crossing aircraft

STPA-F.19M.2.4.1. ATC must reevaluate clearance parameters if Target aircraft is given

altitude modification from flight plan or predicted path (Allocated to: ATC)

STPA-F.19M.2.4.2. ATC must terminate Maintain Current Spacing clearance if altitude modification of Target aircraft trajectory exceeds FIM aircraft capability (Allocated to: ATC)

STPA-F.19M.3. Target aircraft performs evasive maneuver and IM not terminated [ATC inadequate process model of aircraft conflicts]

STPA-F.19M.3.1. Conflict resolution alert given from flight deck

STPA-F.19M.3.1.1. Conflict resolution has priority over IM spacing objectives (Allocated to: Flight Crew)

STPA-F.19M.3.1.2. Flight crews must follow on-board conflict resolution advisories and deviate from Maintaining Current Spacing (Allocated to: Flight Crew)

STPA-F.19M.3.1.3. Flight crew must notify ATC of conflict resolution alert or advisory (Allocated to: Flight Crew)

STPA-F.19M.3.1.4. ATC must terminate Maintain Current Spacing clearance if either Target, FIM, or aircraft in their path performs a conflict resolution maneuver (Allocated to: ATC, FAA Procedures)

STPA-F.19M.3.2. ATC issues conflict resolution clearance

STPA-F.19M.3.2.1. ATC must terminate Maintain Current Spacing clearance if either Target, FIM, or aircraft in their path performs a conflict resolution maneuver (Allocated to: ATC, FAA Procedures)

STPA-F.19M.4. ATC unaware or does not consider environment changes and environment affects target and FIM aircraft dynamics differently [Inadequate process model of airspace]

STPA-F.19M.4.1. Winds aloft change and target aircraft modifies speed to take advantage of change

STPA-F.19M.4.1.1. ATC must monitor Target aircraft compliance of velocity relative to initial conditions of Maintain Current Spacing clearance (Allocated to: ATC)

STPA-F.19M.4.2. Winds aloft change and target maintains speed but FIM aircraft can no longer maintain that speed safely

STPA-F.19M.4.2.1. ATC or associated IM automation must have access to wind and other weather data (Allocated to: NWS, Flight crews)

STPA-F.19M.4.2.2. FIM Flight crew must notify ATC of inability to comply with IM airspeed (Allocated to: Flight crew)

STPA-F.19M.4.2.3. ATC must terminate Maintain Current Spacing clearance if target aircraft speed exceeds FIM aircraft capability (Allocated to: ATC)

STPA-F.19M.4.2.4. See STPA-F.16M requirements (Allocated to: See STPA-F.16M requirements)

STPA-F.19M.5. Target flight crew takes too long to execute clearance so that new trajectory occurs after IM Maintain Current Spacing begins [Inadequate actuator operation]

STPA-F.19M.5.1. Flight crew takes too long to enter new speed into FMS

STPA-F.19M.5.1.1. Flight crew must enter IM speed into FMS or manually fly IM speed within TBD seconds ATC cancellation of speed advisory (Allocated to: Flight Crew)

STPA-F.19M.5.2. Flight crew takes too long to manually modify speed

STPA-F.19M.5.2.1. (Allocated to: Flight Crew)

STPA-F.19M.5.3. FMS takes too long to implement change

STPA-F.19M.5.3.1. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS)

STPA-F.19M.5.3.2. ATC must verify that new desired speed is reached within TBD seconds of issuing cancellation of IM speed advisory (Allocated to: ATC (Controllers))

STPA-F.19M.5.4. Aircraft dynamics are different than ATC expectations (takes 60 seconds to reach steady-state IM speed as opposed to 30 sec)

STPA-F.19M.5.4.1. TFM trajectory modeling must be provided with aircraft performance data on expected time-to-steady-state for completing speed changes. This time should include environmental considerations such as wind, barometric pressure, angle-of-attach, and other relevant factors for flight dynamics (Allocated to: Airline operators,
Airframe manufacturers)

STPA-F.19M.5.5. Aircraft performance is different than expected due to environmental conditions such as headwinds or tailwinds

STPA-F.19M.5.5.1. Flight crews must verify that speed modification is feasible given current environmental conditions (Allocated to: Flight crew)

STPA-F.19M.5.5.2. Flight crews must request an amended clearance if speed modification is infeasible (Allocated to: Flight crew)

Unsafe Control Action: UCA20.M. Maintain Current Spacing clearance provided too long **before or after environmental conditions change ↑[H-2]**

STPA-F.20M.1. ATC incorrectly believes environmental conditions will not change and delays clearance

STPA-F.20M.1.1. Downstream environment changes after initiation of advisory

STPA-F.20M.1.1.1. ATC must monitor downstream and adjacent environment before and during execution of advisory (Allocated to: ATC, NWS)

STPA-F.20M.1.1.2. IM-S speed advisory becomes invalid if weather severity is downgraded before or during execution of advisory (Allocated to: TFM automation, ATC, NWS)

STPA-F.20M.1.1.3. IM-S trajectory modeling refresh rate must be synchronized with weather forecasting and surveillance refresh rates (Allocated to: TFM automation, NWS)

STPA-F.20M.1.2. Change in environment causes aircraft to be in a different state than expected (e.g. headwinds, tailwinds)

STPA-F.20M.1.2.1. ATC and flight crew must monitor compliance with IM speeds and separation (Allocated to: ATC, Flight Crews)

STPA-F.20M.1.2.2. ATC or automation must monitor aircraft compliance with Maintain Separation and predicted target aircraft speed and provide an alert if discrepancy exceeds TBD (Allocated to: IM-related ground Automation)

STPA-F.20M.1.3. Inclement weather forms rapidly, before ATC can be made aware

STPA-F.20M.1.3.1. Flight crews may request an amended clearance due to inclement weather if the crew deems it necessary (Allocated to: Flight Crews)

STPA-F.20M.1.3.2. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NAS Weather Service (NWS))

STPA-F.20M.1.4. NAS weather service surveillance is inaccurate

STPA-F.20M.1.4.1. Precipitation measurements must be within TBD dBZ with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-F.20M.1.4.2. Wind measurements must be within TBD kts with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-F.20M.1.4.3. NAS weather service must notify ATC of accuracy and resolution of weather data, or notify ATC when the above requirements are not met. (Allocated to:

NWS)

STPA-F.20M.1.5. ATC misinterprets or misunderstands "Resolution" or accuracy of weather service

STPA-F.20M.1.5.1. The weather service user interface must clearly present the spatial resolution of weather surveillance (Allocated to: NWS User Interface)

STPA-F.20M.1.5.2. The weather service user interface must clearly present the time of applicability of weather surveillance (Allocated to: NWS User Interface)

STPA-F.20M.1.6. NAS weather service does not update its surveillance fast enough

STPA-F.20M.1.6.1. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NWS (AWIPS, WARP, or other))

STPA-F.20M.1.7. Weather monitoring interface does not update fast enough

STPA-F.20M.1.7.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: NWS Automation)

STPA-F.20M.1.7.2. ATC must not give clearance based on a user interface that is not updating (Allocated to: ATC, FAA Procedures)

STPA-F.20M.1.8. ATC has incorrect understanding of location of weather

STPA-F.20M.1.8.1. The weather service user interface must have the same scale and perspective as aircraft surveillance screens (Plan position indicator) (Allocated to: NWS Automation)

STPA-F.20M.1.9. Weather data is displayed incorrectly or in a confusing manner

STPA-F.20M.1.9.1. Weather data must be presented in a consistent format, within and across sectors (Allocated to: NWS, Tower, TRACON, ARTCC facilities)

STPA-F.20M.1.10. ATC receives report of inclement weather from flight crew but misinterprets location of aircraft

STPA-F.20M.1.10.1. ATC must verify location of aircraft per FAA standards (Allocated to: ATC, FAA Procedures)

STPA-F.20M.1.11. Incorrect surveillance of aircraft

STPA-F.20M.1.11.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.20M.1.11.2. The design must protect against use of data that is not in the 95%

accuracy range. (Allocated to: ERAM, ADS-B)

STPA-F.20M.1.11.3. IM-related ground automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related ground Automation)

STPA-F.20M.1.11.4. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, ADS-B)

STPA-F.20M.2. ATC takes too long to issue IM clearance and target modifies speed between evaluation and giving clearance [Inadequate process model of process dynamics]

STPA-F.20M.2.1. Resource constraints due to other traffic issues

STPA-F.20M.2.1.1. ATC must issue Maintain Current Spacing within TBD seconds of evaluating effectiveness and appropriateness of clearance (Allocated to: ATC)

STPA-F.20M.2.1.2. ATC must reevaluate clearance parameters if clearance is not issued within TBD seconds of most recent evaluation (Allocated to: ATC)

STPA-F.20M.2.1.3. Maintain Current spacing parameters include aircraft capability, equipage, current airspeed, altitude, heading of both aircraft and environmental conditions (Allocated to: System requirement)

STPA-F.20M.3. FIM flight crew takes too long to execute clearance so that expected separation is not achieved when weather changes [Inadequate actuator operation]

STPA-F.20M.3.1. Flight crew takes too long to enter new speed into FMS

STPA-F.20M.3.1.1. Flight crew must enter Maintain clearance into FIM automation, target speed into FMS, or manually fly target speed within TBD seconds ATC cancellation of speed advisory (Allocated to: Flight Crew)

STPA-F.20M.3.2. FIM automation or FMS takes too long to implement change

STPA-F.20M.3.2.1. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS, FIM automation)

STPA-F.20M.3.2.2. ATC must verify that new desired speed is reached within TBD seconds of issuing cancellation of IM speed advisory (Allocated to: ATC (Controllers))

STPA-F.20M.3.3. Aircraft dynamics are different than ATC expectations (takes 60 seconds to reach steady-state Maintain Spacing speed as opposed to 30 sec)

STPA-F.20M.3.3.1. TFM trajectory modeling must be provided with aircraft performance data on expected time-to-steady-state for completing speed changes. This time should include environmental considerations such as wind, barometric pressure, angle-of-attach, and other relevant factors for flight dynamics (Allocated to: Airline

operators, Airframe manufacturers)

STPA-F.20M.3.4. Aircraft performance is different than expected due to environmental conditions such as headwinds or tailwinds

STPA-F.20M.3.4.1. Flight crews must verify that Maintain Current Spacing is feasible given current environmental conditions (Allocated to: Flight crew)

STPA-F.20M.3.4.2. Flight crews must request an amended clearance if Maintain Current Spacing is infeasible (Allocated to: Flight crew)

STPA-F.20M.4. Aircraft / Flight crew executes a clearance prematurely [Inadequate Actuator Operation]

STPA-F.20M.4.1. FC distraction

STPA-F.20M.4.1.1. Flight crew must verify that the clearance is safe, including whether the clearance does not violate separation standards, is within aircraft capability, and there is no presence of inclement weather or restricted airspace. (Allocated to: Flight Crews)

STPA-F.20M.4.1.2. Flight crew must confirm and accept IM clearance after verification (Allocated to: Flight Crews)

STPA-F.20M.4.1.3. Flight crew must issue a response (acceptance or request of amended clearance) within TBD seconds of ATC issuing clearance. (Allocated to: Flight Crews)

STPA-F.20M.4.1.4. ATC must clearly state the starting point criteria as part of clearance (Allocated to: ATC)

STPA-F.20M.4.1.5. Flight crew must verify that the IM clearance has a delayed starting point (Allocated to: Flight Crews)

STPA-F.20M.4.2. FC enters clearance into FMS but does not, or forgets to, delay execution

STPA-F.20M.4.2.1. Flight crew must include starting point (time) in command to FMS, when IM clearance includes starting point (Allocated to: Flight Crews)

STPA-F.20M.4.2.2. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS)

STPA-F.20M.4.2.3. Flight crew must enter IM speed into FMS or manually fly IM speed within TBD seconds of starting point (Allocated to: Flight Crew)

STPA-F.20M.4.3. FC executes clearance early in anticipation of increased workload

STPA-F.20M.4.3.1. ATC must verify that IM clearance is not being flown until TBD seconds of planned starting point. (Allocated to: ATC (Controllers))

Unsafe Control Action: UCA21.M. Maintain Current Spacing clearance applied too long as separation requirements changed, e.g. capacity demands change or flight segment **necessitates different spacing ↑[H-1]**

STPA-F.21M.1. Aircraft take longer than expected to reach termination point due to change in environmental conditions [Inadequate process model of airspace and aircraft]

STPA-F.21M.1.1. ATC is unaware of precisely how long it will take to reach termination point

STPA-F.21M.1.1.1. ATC must calculate or estimate time to termination (Allocated to: ATC)

STPA-F.21M.1.1.2. ATC must be provided information about predicted time to termination (Allocated to: IM-related ground automation)

STPA-F.21M.1.1.3. ATC or automation must include weather forecasting in prediction of time to termination (Allocated to: ATC, IM-related ground automation)

STPA-F.21M.1.1.4. ATC or automation must be provided weather forecasting for trajectory modeling (Allocated to: NWS weather modeling)

STPA-F.21M.1.1.5. ATC must monitor predicted compliance with time to termination (Allocated to: ATC, IM-related ground automation)

STPA-F.21M.1.1.6. ATC must amend or abort Maintain Current Spacing clearance if predicted compliance exceeds TBD seconds OR (Allocated to: ATC)

STPA-F.21M.2. Aircraft reach termination point later than expected due target aircraft flying a slower speed than expected

STPA-F.21M.2.1.7. ATC must amend clearances to other aircraft that conflict with new arrival new time (Allocated to: ATC)

STPA-F.21M.3. Aircraft reach termination point later than expected due target aircraft flying a slower speed than expected

STPA-F.21M.3.1. Target aircraft receives amended clearance from originator of IM clearance

STPA-F.21M.3.1.1. The controller monitoring IM aircraft must provide amended IM clearance if (s)he amends target aircraft trajectory (Allocated to: ATC)

STPA-F.21M.3.2. Target aircraft receives amended clearance from different controller in sector

STPA-F.21M.3.2.1. The controller monitoring IM aircraft must be provided with all clearances being issued to Target aircraft from within sector (Allocated to: ATC, user interfaces)

STPA-F.21M.3.3. Target aircraft receives amended clearance from different sector

STPA-F.21M.3.3.1. The controller monitoring IM aircraft must be provided with all clearances being issued to Target aircraft from adjacent sectors (Allocated to: ATC, user interfaces)

STPA-F.21M.3.3.2. The controller monitoring IM aircraft must abort or amend IM clearance if trajectory changes in target aircraft cause downstream saturation (Allocated to: ATC, user interfaces)

STPA-F.21M.3.3.3. The controller monitoring IM aircraft must abort or amend IM clearance if trajectory changes in target aircraft cause immediate conflict (Allocated to: ATC, FAA procedures)

STPA-F.21M.4. ATC believes IM clearance is consistent with capacity demands [Inadequate process model of airspace]

STPA-F.21M.4.1. ATC is unaware of or does not receive change in capacity demands

STPA-F.21M.4.1.1. ATC and associated IM automation must have access to predicted capacity demands and capacity constraints of all adjacent sectors up to TBD hours. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.21M.4.1.2. ATC and associated IM automation must have access to real-time capacity demands and capacity constraints of all adjacent sectors. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.21M.4.1.3. Downstream or adjacent sector capacity must be considered stale after TBD minutes. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.21M.4.1.4. ATC must not issue IM clearances that will saturate downstream or own airspace (Allocated to: ATC)

STPA-F.21M.5. ATC uses incorrect spacing requirement [Inadequate process model of airspace]

STPA-F.21M.5.1. ATC unaware of changes in spacing requirement

STPA-F.21M.5.1.1. ATC must terminate Maintain Current Spacing clearance when pair of aircraft that are in violation of spacing requirements (Allocated to: ATC, FAA procedures)

STPA-F.21M.5.1.2. ATC must use appropriate spacing requirements when issuing Maintain Current Spacing clearance, per JO 7110.65U (Allocated to: ATC, FAA procedures)

STPA-F.21M.5.1.3. ATC must have access to spacing requirements (Allocated to: FAA)

STPA-F.21M.5.1.4. IM-related ground automation must have access to all spacing regulations for airspace in which the automation generates IM advisories (Allocated to: FAA)

STPA-F.21M.6. ATC unaware that aircraft are under IM

STPA-F.21M.6.1. Downstream sector issues clearance to target aircraft in order to meet spacing requirements

STPA-F.21M.6.1.1. All controllers must be provided information that aircraft in their sectors and adjacent sectors are Target aircraft (Allocated to: Surveillance, user interfaces)

STPA-F.21M.6.1.2. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.21M.6.1.3. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-F.21M.6.1.4. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.21M.6.1.5. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM,
Radar)

STPA-F.21M.6.1.6. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.21M.6.1.7. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.21M.6.2. Controller does not realize FIM aircraft is a FIM aircraft and assumes it will keep flying its speed (but it continues to follow Target, which has been modified)

STPA-F.21M.6.2.1. All controllers must be provided information that aircraft in their sectors and adjacent sectors are FIM aircraft (Allocated to: Surveillance, user interfaces)

STPA-F.21M.6.2.2. ATC must verify whether aircraft are part of IM clearance before

issuing other clearances (Allocated to: ATC, FAA procedures)

STPA-F.21M.6.2.3. IM-related ground automation must have access to all capacity demands for airspace in which the automation generates IM advisories (Allocated to: Tower, TRACON, En route controllers)

STPA-F.21M.7. Flight crew takes too long to return to nominal speed

STPA-F.21M.7.1. See UCA.FC.8

STPA-F.21M.7.1.1. See UCA.FC.8 (Allocated to: Flight Crew)

Unsafe Control Action: UCA22.M. Maintain Current Spacing clearance stopped too soon as non-target aircraft merge into flow based on assumption of longer Maintain clearance ↑**[H**-1]

STPA-F.22M.1. Aircraft reach termination point earlier than expected due to change in environmental conditions

STPA-F.22M.1.1. ATC is unaware of precisely how long it will take to reach termination point

STPA-F.22M.1.1.1. ATC must calculate or estimate time to termination (Allocated to: ATC)

STPA-F.22M.1.1.2. ATC must be provided information about predicted time to termination (Allocated to: IM-related ground automation)

STPA-F.22M.1.1.3. ATC or automation must include weather forecasting in prediction of time to termination (Allocated to: ATC, IM-related ground automation)

STPA-F.22M.1.1.4. ATC or automation must be provided weather forecasting for trajectory modeling (Allocated to: NWS weather modeling)

STPA-F.22M.1.1.5. ATC must monitor predicted compliance with time to termination (Allocated to: ATC, IM-related ground automation)

STPA-F.22M.1.1.6. ATC must amend or abort Maintain Current Spacing clearance if predicted compliance exceeds TBD seconds, OR (Allocated to: ATC)

STPA-F.22M.1.1.7. ATC must amend clearances to other aircraft that conflict with new arrival new time (Allocated to: ATC)

STPA-F.22M.2. Aircraft reach termination point earlier than expected due target aircraft flying a faster speed than expected

STPA-F.22M.2.1. Target aircraft receives amended clearance from originator of IM clearance

STPA-F.22M.2.1.1. The controller monitoring IM aircraft must provide amended IM clearance if (s)he amends target aircraft trajectory (Allocated to: ATC)

STPA-F.22M.2.2. Target aircraft receives amended clearance from different controller in sector

STPA-F.22M.2.2.1. The controller monitoring IM aircraft must be provided with all clearances being issued to Target aircraft from within sector (Allocated to: ATC, user interfaces)

STPA-F.22M.2.3. Target aircraft receives amended clearance from different sector

STPA-F.22M.2.3.1. The controller monitoring IM aircraft must be provided with all clearances being issued to Target aircraft from adjacent sectors (Allocated to: ATC, user interfaces)

STPA-F.22M.2.3.2. The controller monitoring IM aircraft must abort or amend IM clearance if trajectory changes in target aircraft cause downstream saturation (Allocated to: ATC, user interfaces)

STPA-F.22M.2.3.3. The controller monitoring IM aircraft must abort or amend IM clearance if trajectory changes in target aircraft cause immediate conflict (Allocated to: ATC, FAA procedures)

STPA-F.22M.3. ATC believes insertion of aircraft into or across flow is consistent IM clearance [Inadequate process model of airspace and procedure]

STPA-F.22M.3.1. ATC is unaware of or does not receive change in IM status

STPA-F.22M.3.1.1. ATC and associated IM automation must have access to predicted IM clearances of all adjacent sectors up to TBD hours. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.22M.3.1.2. ATC and associated IM automation must have access to real-time IM clearances and capacity constraints of all adjacent sectors. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.22M.3.1.3. ATC must not issue clearances that saturate airspace with aircraft under IM clearances (Allocated to: ATC, FAA procedures)

STPA-F.22M.3.1.4. ATC must verify new target and FIM aircraft speeds after termination of IM clearance (Allocated to: ATC, FAA procedures)

STPA-F.22M.4. ATC unaware that aircraft were under IM and have stopped

STPA-F.22M.4.1. Downstream sector issues clearance to target aircraft in order to meet spacing requirements based on previous assumption of IM spacing

STPA-F.22M.4.1.1. All controllers must be provided information that aircraft in their sectors and adjacent sectors are FIM aircraft (Allocated to: Surveillance, user interfaces)

STPA-F.22M.4.1.2. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.22M.4.1.3. The design must protect against use of data that is not in the 95%

accuracy range. (Allocated to: TFM Automation)

STPA-F.22M.4.1.4. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.22M.4.1.5. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM,
Radar)

STPA-F.22M.4.1.6. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.22M.4.1.7. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.22M.4.2. Controller does not realize FIM aircraft is a FIM aircraft and assumes it will keep flying its speed (but it changes speed after termination point)

STPA-F.22M.4.2.1. All controllers must be provided information that aircraft in their sectors and adjacent sectors are FIM aircraft (Allocated to: Surveillance, user interfaces)

STPA-F.22M.4.2.2. ATC must verify whether aircraft are still part of IM clearance before issuing clearances based on that assumption (Allocated to: ATC, FAA procedures)

STPA-F.22M.5. Flight crew returns to nominal speed early in anticipation of other demands

STPA-F.22M.5.1. See UCA.FC.8

STPA-F.22M.5.1.1. See UCA.FC.8 (Allocated to: Flight Crew)

A.2.1.2 Achieve-by then Maintain Analysis

Unsafe Control Action: UCA13.AB. Achieve-by aspect of clearance not provided, and achieve-by is necessary to achieve separation with non-**target aircraft ↑[H-1]**

STPA-F.13AB.1. ATC incorrectly requests the "Achieve-by" aspect of clearance

STPA-F.13AB.1.1. ATC forgets to request Achieve-by point or requests it in confusing manner

STPA-F.13AB.1.1.1. ATC must issue Achieve-by then Maintain clearance in a clear, consistent, and standardized format that is easily distinguishable from other IM clearances (Allocated to: ATC)

STPA-F.13AB.1.1.2. IM-related ground automation must present Achieve-by then Maintain advisory in a clear, consistent, and standardized format that is easily distinguishable from other IM clearances (Allocated to: IM-related Ground Automation)

STPA-F.13AB.1.2. Flight crew interprets "Achieve-by" then maintain as just "Maintain"

STPA-F.13AB.1.2.1. Flight crew must verify the type of IM clearance before execution, or before entering IM parameters into FIM automation (Allocated to: Flight Crew)

STPA-F.13AB.1.2.2. ATC must monitor that FIM aircraft is progressing on a trajectory that will meet Achieve-by point constraints (Allocated to: ATC, IM-related Ground Automation)

STPA-F.13AB.1.3. ATC over-reliance on Maintain Current Spacing clearance

STPA-F.13AB.1.3.1. If the current separation between FIM and Target aircraft is not the desired spacing, ATC must issue an Achieve-by then Maintain clearance (Allocated to: ATC, FAA Procedures)

STPA-F.13AB.2. ATC incorrectly believes FIM and target are already spaced correctly

STPA-F.13AB.2.1. Incorrect surveillance so that aircraft appear to be separated correctly

STPA-F.13AB.2.1.1. ATC must have access to FIM and Target aircraft separation parameters. This requirement assumes that the controller will not be able to calculate or decipher separation with the precision required for IM, using only traditional surveillance tools. (Allocated to: IM-related Ground Automation, ERAM)

STPA-F.13AB.2.1.2. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,

GNSS)

STPA-F.13AB.2.1.3. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: IM-related ground Automation, FIM Automation, ATC, Flight Crew)

STPA-F.13AB.2.1.4. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related Ground Automation, FIM Automation)

STPA-F.13AB.2.1.5. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM)

STPA-F.13AB.2.1.6. ATC must have access to surveillance data (Allocated to: ERAM)

STPA-F.13AB.2.2. Incorrect interpretation of spacing goals

STPA-F.13AB.2.2.1. ATC must use appropriate spacing requirements when issuing Achieve-by then Maintain clearance, per JO 7110.65U (Allocated to: ATC, FAA procedures)

STPA-F.13AB.2.3. Spacing goals and requirements change

STPA-F.13AB.2.3.1. ATC must have access to updated spacing goals and requirements (Allocated to: FAA)

STPA-F.13AB.2.3.2. FAA or other entity must notify relevant controllers of changes in spacing goals and requirements within TBD seconds of update (Allocated to: FAA)

STPA-F.13AB.2.3.3. IM-related ground automation must have access to all spacing regulations for airspace in which the automation generates IM advisories (Allocated to: FAA)

STPA-F.13AB.2.4. Downstream demands are different than ATC expectation and therefore does not request "Achieve-by" to meet that requirement

STPA-F.13AB.2.4.1. ATC must have access to capacity demands of adjacent sectors (Allocated to: TRACON, Tower, ARTCC)

STPA-F.13AB.2.4.2. Relevant sector must notify adjacent sectors of updated capacity demands within TBD seconds update (Allocated to: TRACON, Tower, ARTCC)

Unsafe Control Action: UCA14.AB. Achieve-by point given that causes loss of separation with other (non-target) merging or in-**path aircraft ↑[H-1]**

STPA-F.14AB.1. ATC does not have correct understanding of how long it will take FIM aircraft to reach Achieve-by point [Inadequate process model of aircraft and IM procedure]

STPA-F.14AB.1.1. ATC does not attempt to determine duration of maneuver to Achieve-by Point

STPA-F.14AB.1.1.1. ATC must consider FIM aircraft trajectory characteristics to Achieve-by Point when issuing other clearances near that airspace (Allocated to: ATC, FAA Procedures)

STPA-F.14AB.1.2. ATC does not have access to predicted duration of maneuver to Achieve-by Point

STPA-F.14AB.1.2.1. IM-related Ground Automation must calculate predicted duration, required airspeed, or other necessary parameters for Achieve-by then Maintain clearance (Allocated to: IM-related Ground Automation)

STPA-F.14AB.1.2.2. IM-related Ground Automation must present predicted FIM aircraft trajectory information to ATC (Allocated to: IM-related Ground Automation)

STPA-F.14AB.1.3. Aircraft takes longer than expected to reach Achieve-by point (FIM aircraft flies slower than ATC expectations prior to Achieve-by point)

STPA-F.14AB.1.3.1. ATC must monitor FIM aircraft compliance with Achieve-by aspect of trajectory (Allocated to: ATC)

STPA-F.14AB.1.4. Aircraft takes reaches Achieve-by point faster than expected (FIM aircraft flies faster than ATC expectations prior to Achieve-by point)

STPA-F.14AB.1.4.1. ATC must terminate or amend clearance if the difference between the FIM aircraft's predicted and scheduled time of arrival to Achieve-by point exceeds TBD seconds (Allocated to: ATC, FAA Procedures)

STPA-F.14AB.1.4.2. IM-related Ground Automation or other tool must monitor FIM aircraft compliance with scheduled Achieve-by point. This requirement assumes that ATC cannot manually monitor compliance to Achieve-by Point with enough precision to support IM operations (Allocated to: IM-related Ground Automation)

STPA-F.14AB.2. Achieve-by point causes FIM aircraft to deviate from its predicted or intended path [Inadequate process model of airspace and FIM aircraft]

STPA-F.14AB.2.1. ATC has incorrect understanding of aircraft location and trajectory and believes that Achieve-by Point is along path

STPA-F.14AB.2.1.1. ATC must issue Achieve-by points that minimize deviation from FIM and target aircraft flight plans (Allocated to: ATC, FAA Procedures)

STPA-F.14AB.2.1.2. ATC must have access to FIM and Target aircraft predicted paths. This requirement could be fulfilled with existing tools and procedures (e.g. flight strips and radar screen) or supplemented with tools that show ATC the predicted paths relative to IM parameters (Allocated to: IM-related Ground Automation, ERAM)

STPA-F.14AB.2.1.3. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.14AB.2.1.4. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: IM-related ground Automation, FIM Automation, ATC, Flight Crew)

STPA-F.14AB.2.1.5. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related Ground Automation, FIM Automation)

STPA-F.14AB.2.1.6. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM)

STPA-F.14AB.2.1.7. ATC must have access to surveillance data (Allocated to: ERAM)

STPA-F.14AB.3. ATC misinterprets Achieve-by point and clears other aircraft along that trajectory [Inadequate process model of IM operation]

STPA-F.14AB.3.1. ATC misinterprets location of Achieve-by point

STPA-F.14AB.3.1.1. ATC must have access to location of Achieve-by point in format that is consistent with aircraft surveillance and airspace standards (Allocated to: IM-related Ground Automation, ERAM, Radar screen user interface)

STPA-F.14AB.3.2. ATC misinterprets timing of Achieve-by point

STPA-F.14AB.3.2.1. IM-related Ground Automation must calculate predicted duration, required airspeed, or other necessary parameters for Achieve-by then Maintain clearance (Allocated to: IM-related Ground Automation)

STPA-F.14AB.3.2.2. IM-related Ground Automation must present predicted FIM aircraft trajectory information to ATC (Allocated to: IM-related Ground Automation)

STPA-F.14AB.4. Achieve-by point causes FIM aircraft trajectory to overlap with target aircraft trajectory [Inadequate process model of airspace dynamics]

STPA-F.14AB.4.1. Achieve-by point ends up being ahead of leading target aircraft

STPA-F.14AB.4.1.1. Achieve-by Point must not cause loss of separation with leading target aircraft (Allocated to: System requirement)

STPA-F.14AB.4.1.2. Achieve-by Point must be specified such that a leading target aircraft has sufficient time and space to pass ahead of Achieve-by Point by no less than minimum required separation in NM (Allocated to: ATC, IM-related Ground Automation)

STPA-F.14AB.4.2. Achieve-by point ends up being behind trailing target aircraft

STPA-F.14AB.4.2.1. Achieve-by Point must not cause loss of separation with trailing target aircraft (Allocated to: System requirement)

STPA-F.14AB.4.2.2. Achieve-by Point must be specified such that a trailing target aircraft has sufficient time and space to avoid intruding into space behind Achieve-by Point by no less than minimum required separation in NM (Allocated to: ATC, IM-related Ground Automation)

STPA-F.14AB.5. Flight crew executes Achieve-by point incorrectly [Inadequate actuator operation]

STPA-F.14AB.5.1. See UCA.FC.3

STPA-F.14AB.5.1.1. See UCA.FC.3 (Allocated to: See UCA.FC.3)

Unsafe Control Action: UCA15.AB. Achieve-by point given that causes aircraft to increase / decrease airspeeds to levels that exceed overspeed / stall capability of aircraft ↑**[H**-4]

STPA-F.15AB.1. Incorrect FIM aircraft performance information

STPA-F.15AB.1.1. Incorrect aircraft type and performance

STPA-F.15AB.1.1.1. Aircraft data file must be provided to IM-related ground automation and ATC in standardized format. (Allocated to: Airline operators)

STPA-F.15AB.1.1.2. Aircraft data includes certification, airworthiness, and other regulations. (Allocated to: Airframe manufacturers)

STPA-F.15AB.1.1.3. Aircraft data file must be updated every flight (Allocated to: Airline operators)

STPA-F.15AB.1.1.4. V speeds must be provided to IM-related ground automation in a standardized format (Allocated to: Airframe manufacturers)

STPA-F.15AB.1.1.5. Stall speeds and speed limits must be provided to TFM automation (Allocated to: Airframe manufacturers)

STPA-F.15AB.1.2. ATC has incorrect information about current aircraft state, including speed, altitude, heading, configuration

STPA-F.15AB.1.2.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.15AB.1.2.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: IM-related ground Automation, FIM Automation, ATC, Flight Crew)

STPA-F.15AB.1.2.3. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related Ground Automation, FIM Automation)

STPA-F.15AB.1.2.4. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM)

STPA-F.15AB.1.2.5. ATC must have access to surveillance data (Allocated to: ERAM)

STPA-F.15AB.1.2.6. ATC must have access to location of Achieve-by point in format

that is consistent with aircraft surveillance and airspace standards (Allocated to: IM-related Ground Automation, ERAM, Radar screen user interface)

STPA-F.15AB.1.2.7. IM-related Ground Automation must calculate predicted duration, required airspeed, or other necessary parameters for Achieve-by then Maintain clearance (Allocated to: IM-related Ground Automation)

STPA-F.15AB.1.2.8. IM-related Ground Automation must present predicted FIM aircraft trajectory information to ATC (Allocated to: IM-related Ground Automation)

STPA-F.15AB.1.3. ATC has incorrect understanding of environmental conditions

STPA-F.15AB.1.3.1. IM-related ground automation must have access to real-time wind data for the airspace. (Allocated to: ATC Weather Service)

STPA-F.15AB.1.3.2. IM-related ground automation must calculate maximum and minimum allowed speeds for given real-time data. (Allocated to: IM-related Ground Automation, Airframe manufacturers)

STPA-F.15AB.1.3.3. IM-related ground automation must not issue Achieve-by points that result in airspeeds outside of maximum and minimum allowed speeds. (Allocated to: IM-related Ground Automation)

STPA-F.15AB.1.3.4. Flight crew must verify that clearance is within aircraft capability (Allocated to: Flight crew,
FMS)

STPA-F.15AB.1.3.5. Flight crew must request amendment to clearance if required IM speed to meet Achieve-by point exceeds capability. Amendment request should explicitly state that speed exceeds aircraft capability (Allocated to: Flight Crew)

STPA-F.15AB.2. ATC does not have correct understanding of Target aircraft speed and issues Achieve-by point according to this inadequate information [Inadequate process model of target aircraft]

STPA-F.15AB.2.1. ATC has incorrect information about Target aircraft state

STPA-F.15AB.2.1.1. See above surveillance requirements (Allocated to:)

STPA-F.15AB.2.2. Target aircraft flies different speed than ATC expectations

STPA-F.15AB.2.2.1. Target aircraft must fly expected trajectory to within TBD NM and TBD Mach (Allocated to: Flight crew)

STPA-F.15AB.2.2.2. ATC must be provided information about Target aircraft compliance with predicted trajectory. This requirement assumes that ATC cannot manually calculate compliance parameters with the accuracy required for IM

operations (Allocated to: IM-related Ground Automation)

STPA-F.15AB.2.2.3. ATC must terminate or amend Achieve-by then Maintain clearance if Target aircraft does not comply with predicted trajectory parameters (Allocated to: ATC, FAA Procedures)

STPA-F.15AB.3. ATC issues overly aggressive Achieve-by point to meet other (Non-IM) objective in the airspace

STPA-F.15AB.3.1. ATC issues overly aggressive Achieve-by point due to increased downstream demands

STPA-F.15AB.3.1.1. Issuing clearances within aircraft performance bounds takes precedence over downstream capacity demands (Allocated to: ATC, FAA Procedures)

STPA-F.15AB.3.2. ATC issues overly aggressive Achieve-by point due to potential conflict within sector (e.g. merging or crossing traffic necessitate very soon achievement of spacing)

STPA-F.15AB.3.2.1. ATC must issue conflict resolution clearances that are within aircraft performance bounds (Allocated to: ATC, FAA Procedures)

STPA-F.15AB.3.2.2. ATC must not issue IM clearances for conflict resolution (Allocated to: ATC, FAA Procedures)

STPA-F.15AB.4. Flight crew executes Achieve-by point incorrectly

STPA-F.15AB.4.1. See UCA.FC.3, 5

STPA-F.15AB.4.1.1. See UCA.FC.3, 5 (Allocated to: See UCA.FC.3, 5)

Unsafe Control Action: UCA18.AB. Achieve-by then Maintain clearance provided before or after a (non target, could be in a different IM clearance) aircraft is instructed **to merge into flow or aircraft in flow changes speeds ↑[H-1]**

STPA-F.18AB.1. ATC unaware of Achieve-by then Maintain clearance and therefore does not include this information in prediction [Inadequate process model of IM operations]

STPA-F.18AB.1.1. Originator of Achieve-by then Maintain clearance forgets existence of clearance

STPA-F.18AB.1.1.1. All controllers within a sector must have access to IM clearances that are currently being flown (Allocated to: IM-S Automation, user interface(s) Controllers)

STPA-F.18AB.1.2. Other controller within sector does not have access to information about Achieve-by then Maintain clearance

STPA-F.18AB.1.2.1. All controllers within a sector must have access to IM automation-generated clearance advisories (Allocated to: IM-S Automation, user interface(s))

STPA-F.18AB.1.3. Controller across sectors do not have access to information about Achieve-by then Maintain clearance

STPA-F.18AB.1.3.1. Downstream or adjacent sector controllers must have access to IM clearances being flown by aircraft entering the sector (Allocated to: Sector Automation, IM-S Automation)

STPA-F.18AB.1.3.2. Controllers must not issue conflicting IM clearances. (Conflicting: different type of IM clearance, or with different parameters) (Allocated to: ATC,
IM-S Procedures)

STPA-F.18AB.2. ATC unaware of expected trajectory modifications for aircraft [Inadequate model of airspace]

STPA-F.18AB.2.1. FIM aircraft has conditional start or delayed clearance

STPA-F.18AB.2.1.1. IM-related ground automation must have access to new clearances that have been issued by ATC (Allocated to: ATC,
IM-S user interface)

STPA-F.18AB.2.2. Target aircraft has conditional start or delayed clearance

STPA-F.18AB.2.2.1. Modified flight plans or new clearances must be sent to IM-related ground automation within TBD seconds for all aircraft in sector (Allocated to: Operators,
Controllers)

STPA-F.18AB.2.3. Non-IM aircraft has conditional start or delayed clearance

STPA-F.18AB.2.3.1. IM-related ground automation and ATC must have access to parameters of conditional clearances (Allocated to: ATC, IM-S automation, ERAM, Flight Crews)

STPA-F.18AB.3. ATC issues Achieve-by then Maintain clearance before it is appropriate due to expected workload demands or other pressures [Contextual factor, inadequate process model of airspace]

STPA-F.18AB.3.1. Aircraft trajectories change immediately before or after issuance of Achieve-by then Maintain clearance

STPA-F.18AB.3.1.1. ATC and/or associated automation must monitor aircraft trajectories (heading, position, airspeed) to ensure that spacing and sequencing remains consistent with assumptions when Achieve-by then Maintain clearance was originally issued (Allocated to: ATC, IM-S automation, ERAM)

STPA-F.18AB.3.2. Aircraft trajectories in IM flow or crossing IM flow have not reached steady-state (constant velocity)

STPA-F.18AB.3.2.1. ATC must issue Maintain Current Spacing within TBD seconds of evaluating effectiveness and appropriateness of clearance (Allocated to: ATC)

STPA-F.18AB.3.2.2. ATC must reevaluate clearance parameters if clearance is not issued within TBD seconds of most recent evaluation (Allocated to: ATC, IM-S automation)

STPA-F.18AB.3.2.3. ATC must terminate Achieve-by then Maintain clearance if either Target, FIM, or aircraft in their path performs a conflict resolution maneuver (Allocated to: ATC, IM-S automation)

STPA-F.18AB.3.2.4. ATC must terminate Achieve-by then Maintain clearance if either Target, FIM, or aircraft in their path performs a conflict resolution maneuver (Allocated to: ATC, IM-S automation)

STPA-F.18AB.3.2.5. ATC must monitor Target aircraft compliance of velocity relative to initial conditions of Achieve-by then Maintain clearance (Allocated to: ATC, IM-S automation)

STPA-F.18AB.4. ATC merges and/or crosses non-IM aircraft due to off-nominal or

unexpected conditions [Inadequate process model of airspace]

STPA-F.18AB.4.1. ATC neglects surge in traffic across or into traffic flow

STPA-F.18AB.4.1.1. ATC and/or associated automation must monitor traffic flow to ensure that spacing and sequencing remains consistent with assumptions when Achieve-by then Maintain clearance was originally issued (Allocated to: ATC, IM-S automation, ERAM)

STPA-F.18AB.4.2. Weather conditions in adjacent airspace cause increase in traffic within/across IM traffic flow

STPA-F.18AB.4.2.1. ATC must be informed of aircraft being diverted into airspace due to inclement weather. This information should include the fact that the reason for the increased traffic is due to weather. (Allocated to: ATC, NWS)

STPA-F.18AB.4.3. Airport delays, runway closure cause increase in traffic within/across IM traffic flow

STPA-F.18AB.4.3.1. ATC must be informed of aircraft being diverted into airspace due to airport delays. This information should include the fact that the reason for the increased traffic is due to airport delays. (Allocated to: ATC, TRACON, Tower)

STPA-F.18AB.4.4. Changes in approach configurations cause increase in traffic within/across IM traffic flow

STPA-F.18AB.4.4.1. ATC must be informed of aircraft being diverted into airspace due to changes in airspace configuration. This information should include the fact that the reason for the increased traffic is due to change in airspace configuration. (Allocated to: ATC, TRACON, Tower)

STPA-F.18AB.5. Flight crew delays execution of clearance

STPA-F.18AB.5.1. See UCA.FC8

STPA-F.18AB.5.1.1. See UCA.FC8 (Allocated to: See UCA.FC8)

STPA-F.18AB.6. Flight crew expedites execution in anticipation of other workload factors

STPA-F.18AB.6.1. See UCA.FC9

STPA-F.18AB.6.1.1. See UCA.FC9 (Allocated to: See UCA.FC9)

Unsafe Control Action: UCA19.AB. Achieve-by then Maintain clearance is hazardous if target aircraft modifies speed during Maintain clearance and exceeds receiving aircraft **capability ↑[H-4]**

STPA-F.19AB.1. ATC takes too long to issue IM clearance and target modifies speed between evaluation and giving clearance [Inadequate process model of process dynamics]

STPA-F.19AB.1.1. Resource constraints due to other traffic issues

STPA-F.19AB.1.1.1. ATC must issue Achieve-by then Maintain within TBD seconds of evaluating effectiveness and appropriateness of clearance (Allocated to: ATC, FAA Procedures)

STPA-F.19AB.1.1.2. ATC must reevaluate clearance parameters if clearance is not issued within TBD seconds of most recent evaluation (Allocated to: ATC, FAA Procedures)

STPA-F.19AB.1.1.3. Achieve-by then Maintain parameters include aircraft capability, equipage, current airspeed, altitude, heading of both aircraft and environmental conditions (Allocated to: IM Procedures)

STPA-F.19AB.2. Target aircraft receives different clearance and IM not terminated [ATC inadequate process model of IM clearance]

STPA-F.19AB.2.1. Target aircraft cleared to achieve objective outside of IM spacing goal

STPA-F.19AB.2.1.1. FIM aircraft may request amended clearance if Target aircraft deviates from desired trajectory (Allocated to: FIM Flight crew)

STPA-F.19AB.2.2. Target aircraft vectored for spacing to other aircraft

STPA-F.19AB.2.2.1. ATC must reevaluate clearance parameters if Target aircraft is vectored from flight plan or predicted path (Allocated to: ATC)

STPA-F.19AB.2.2.2. ATC must terminate Achieve-by then Maintain clearance if vectored Target aircraft trajectory exceeds FIM aircraft capability (Allocated to: ATC)

STPA-F.19AB.2.3. Target aircraft speed modification for spacing to other aircraft

STPA-F.19AB.2.3.1. ATC must reevaluate clearance parameters if Target aircraft is instructed to modify speed from flight plan or predicted path (Allocated to: ATC)

STPA-F.19AB.2.3.2. ATC must terminate Achieve-by then Maintain clearance if speed modified Target aircraft trajectory exceeds FIM aircraft capability (Allocated to: ATC)

STPA-F.19AB.2.4. Target aircraft altitude modification to avoid merging, crossing aircraft

STPA-F.19AB.2.4.1. ATC must reevaluate clearance parameters if Target aircraft is given altitude modification from flight plan or predicted path (Allocated to: ATC)

STPA-F.19AB.2.4.2. ATC must terminate Achieve-by then Maintain clearance if altitude modification of Target aircraft trajectory exceeds FIM aircraft capability (Allocated to: ATC)

STPA-F.19AB.3. Target aircraft performs evasive maneuver and IM not terminated [ATC inadequate process model of aircraft conflicts]

STPA-F.19AB.3.1. Conflict resolution alert given from flight deck

STPA-F.19AB.3.1.1. Conflict resolution has priority over IM spacing objectives (Allocated to: Flight Crew)

STPA-F.19AB.3.1.2. Flight crews must follow on-board conflict resolution advisories and deviate from Maintaining Current Spacing (Allocated to: Flight Crew)

STPA-F.19AB.3.1.3. Flight crew must notify ATC of conflict resolution alert or advisory (Allocated to: Flight Crew)

STPA-F.19AB.3.1.4. ATC must terminate Achieve-by then Maintain clearance if either Target, FIM, or aircraft in their path performs a conflict resolution maneuver (Allocated to: ATC, FAA Procedures)

STPA-F.19AB.3.2. ATC issues conflict resolution clearance

STPA-F.19AB.3.2.1. ATC must terminate Achieve-by then Maintain clearance if either Target, FIM, or aircraft in their path performs a conflict resolution maneuver (Allocated to: ATC, FAA Procedures)

STPA-F.19AB.4. ATC unaware or does not consider environment changes and environment affects target and FIM aircraft dynamics differently [Inadequate process model of airspace]

STPA-F.19AB.4.1. Winds aloft change and target aircraft modifies speed to take advantage of change

STPA-F.19AB.4.1.1. ATC must monitor Target aircraft compliance of velocity relative to initial conditions of Achieve-by then Maintain clearance (Allocated to: ATC)

STPA-F.19AB.4.2. Winds aloft change and target maintains speed but FIM aircraft can no longer maintain that speed safely

STPA-F.19AB.4.2.1. ATC or associated IM automation must have access to wind and other weather data (Allocated to: NWS, Flight crews)

STPA-F.19AB.4.2.2. FIM Flight crew must notify ATC of inability to comply with IM airspeed (Allocated to: Flight crew)

STPA-F.19AB.4.2.3. ATC must terminate Achieve-by then Maintain clearance if target aircraft speed exceeds FIM aircraft capability (Allocated to: ATC)

STPA-F.19AB.4.2.4. See STPA-F.16M requirements (Allocated to: See STPA-F.16M requirements)

STPA-F.19AB.5. ATC believes new Target aircraft speed is valid for maintain clearance

but neglects to check Achieve-by point

STPA-F.19AB.5.1. Target aircraft modifies speed that is within FIM aircraft capability to Maintain but not within capability to meet Achieve-by point

STPA-F.19AB.5.1.1. Achieve-by Point becomes invalid if Target aircraft modifies speed by more than TBD (Mach or IAS) after clearance has begun (Allocated to: FAA Procedure, IM Operations)

STPA-F.19AB.5.1.2. ATC must issue a new Achieve-by point that results in a speed within FIM aircraft capability (Allocated to: ATC)

STPA-F.19AB.5.2. Change in winds aloft results in a maintain clearance that is feasible but Achieve-by exceeds FIM aircraft capability

STPA-F.19AB.5.2.1. ATC must have access to winds aloft data (Allocated to: NWS, Flight crews)

STPA-F.19AB.5.2.2. ATC must not issue Achieve-by Point that exceeds aircraft capability given wind conditions (Allocated to: ATC)

STPA-F.19AB.5.2.3. FIM Flight crew must notify ATC of inability to comply with Achieve-by point (Allocated to: Flight crew)

STPA-F.19AB.6. Target flight crew takes too long to execute clearance so that new trajectory occurs after IM Achieve-by then Maintain begins [Inadequate actuator operation]

STPA-F.19AB.6.1. Flight crew takes too long to enter new speed into FMS

STPA-F.19AB.6.1.1. Flight crew must enter IM speed into FMS or manually fly IM speed within TBD seconds ATC cancellation of speed advisory (Allocated to: Flight Crew)

STPA-F.19AB.6.2. Flight crew takes too long to manually modify speed

STPA-F.19AB.6.2.1. (Allocated to: Flight Crew)

STPA-F.19AB.6.3. FMS takes too long to implement change

STPA-F.19AB.6.3.1. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS)

STPA-F.19AB.6.3.2. ATC must verify that new desired speed is reached within TBD seconds of issuing cancellation of IM speed advisory (Allocated to: ATC (Controllers))

STPA-F.19AB.6.4. Aircraft dynamics are different than ATC expectations (takes 60 seconds to reach steady-state IM speed as opposed to 30 sec)

STPA-F.19AB.6.4.1. TFM trajectory modeling must be provided with aircraft performance data on expected time-to-steady-state for completing speed changes. This time should include environmental considerations such as wind, barometric pressure, angle-of-attach, and other relevant factors for flight dynamics (Allocated to: Airline operators,
Airframe manufacturers)

STPA-F.19AB.6.5. Aircraft performance is different than expected due to environmental conditions such as headwinds or tailwinds

STPA-F.19AB.6.5.1. Flight crews must verify that speed modification is feasible given current environmental conditions (Allocated to: Flight crew)

STPA-F.19AB.6.5.2. Flight crews must request an amended clearance if speed modification is infeasible (Allocated to: Flight crew)

Unsafe Control Action: UCA20.AB. Achieve-by then Maintain clearance provided **before or after environmental conditions change ↑[H-2]**

STPA-F.20AB.1. ATC incorrectly believes environmental conditions will not change and delays clearance

STPA-F.20AB.1.1. Downstream environment changes after initiation of advisory

STPA-F.20AB.1.1.1. ATC must monitor downstream and adjacent environment before and during execution of advisory (Allocated to: ATC, NWS)

STPA-F.20AB.1.1.2. IM-S speed advisory becomes invalid if weather severity is downgraded before or during execution of advisory (Allocated to: TFM automation, ATC, NWS)

STPA-F.20AB.1.1.3. IM-S trajectory modeling refresh rate must be synchronized with weather forecasting and surveillance refresh rates (Allocated to: TFM automation, NWS)

STPA-F.20AB.1.2. Change in environment causes aircraft to be in a different state than expected (e.g. headwinds, tailwinds)

STPA-F.20AB.1.2.1. ATC and flight crew must monitor compliance with IM speeds and separation (Allocated to: ATC, Flight Crews)

STPA-F.20AB.1.2.2. ATC or automation must monitor aircraft compliance with Maintain Separation and predicted target aircraft speed and provide an alert if discrepancy exceeds TBD (Allocated to: IM-related ground Automation)

STPA-F.20AB.1.3. Inclement weather forms rapidly, before ATC can be made aware

STPA-F.20AB.1.3.1. Flight crews may request an amended clearance due to inclement weather if the crew deems it necessary (Allocated to: Flight Crews)

STPA-F.20AB.1.3.2. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NAS Weather Service (NWS))

STPA-F.20AB.1.4. NAS weather service surveillance is inaccurate

STPA-F.20AB.1.4.1. Precipitation measurements must be within TBD dBZ with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-F.20AB.1.4.2. Wind measurements must be within TBD kts with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-F.20AB.1.4.3. NAS weather service must notify ATC of accuracy and resolution of weather data, or notify ATC when the above requirements are not met. (Allocated to: NWS)

STPA-F.20AB.1.5. ATC misinterprets or misunderstands "Resolution" or accuracy of weather service

STPA-F.20AB.1.5.1. The weather service user interface must clearly present the

spatial resolution of weather surveillance (Allocated to: NWS User Interface)

STPA-F.20AB.1.5.2. The weather service user interface must clearly present the time of applicability of weather surveillance (Allocated to: NWS User Interface)

STPA-F.20AB.1.6. NAS weather service does not update its surveillance fast enough

STPA-F.20AB.1.6.1. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NWS (AWIPS, WARP, or other))

STPA-F.20AB.1.7. Weather monitoring interface does not update fast enough

STPA-F.20AB.1.7.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: NWS Automation)

STPA-F.20AB.1.7.2. ATC must not give clearance based on a user interface that is not updating (Allocated to: ATC, FAA Procedures)

STPA-F.20AB.1.8. ATC has incorrect understanding of location of weather

STPA-F.20AB.1.8.1. The weather service user interface must have the same scale and perspective as aircraft surveillance screens (Plan position indicator) (Allocated to: NWS Automation)

STPA-F.20AB.1.9. Weather data is displayed incorrectly or in a confusing manner

STPA-F.20AB.1.9.1. Weather data must be presented in a consistent format, within and across sectors (Allocated to: NWS, Tower, TRACON, ARTCC facilities)

STPA-F.20AB.1.10. ATC receives report of inclement weather from flight crew but misinterprets location of aircraft

STPA-F.20AB.1.10.1. ATC must verify location of aircraft per FAA standards (Allocated to: ATC, FAA Procedures)

STPA-F.20AB.1.11. Incorrect surveillance of aircraft

STPA-F.20AB.1.11.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.20AB.1.11.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: ERAM, ADS-B)

STPA-F.20AB.1.11.3. IM-related ground automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related ground Automation)

STPA-F.20AB.1.11.4. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, ADS-B)

STPA-F.20AB.2. ATC takes too long to issue IM clearance and target modifies speed between evaluation and giving clearance [Inadequate process model of process dynamics]

STPA-F.20AB.2.1. Resource constraints due to other traffic issues

STPA-F.20AB.2.1.1. ATC must issue Achieve-by then Maintain within TBD seconds of evaluating effectiveness and appropriateness of clearance (Allocated to: ATC)

STPA-F.20AB.2.1.2. ATC must reevaluate clearance parameters if clearance is not issued within TBD seconds of most recent evaluation (Allocated to: ATC)

STPA-F.20AB.2.1.3. Achieve-by then Maintain parameters include aircraft capability, equipage, current airspeed, altitude, heading of both aircraft and environmental conditions (Allocated to: System requirement)

STPA-F.20AB.3. Inclement weather unexpectedly develops between initiation of clearance and aircraft reaching Achieve-by point [Inadequate process model of airspace and aircraft trajectory]

STPA-F.20AB.3.1. ATC does not attempt to determine duration of maneuver to Achieve-by Point

STPA-F.20AB.3.1.1. ATC must consider FIM aircraft trajectory characteristics to Achieve-by Point when issuing other clearances near that airspace (Allocated to: ATC, FAA Procedures)

STPA-F.20AB.3.2. ATC does not have access to predicted duration of maneuver to Achieve-by Point

STPA-F.20AB.3.2.1. IM-related Ground Automation must calculate predicted duration, required airspeed, or other necessary parameters for Achieve-by then Maintain clearance (Allocated to: IM-related Ground Automation)

STPA-F.20AB.3.2.2. IM-related Ground Automation must present predicted FIM aircraft trajectory information to ATC (Allocated to: IM-related Ground Automation)

STPA-F.20AB.3.3. Aircraft takes longer than expected to reach Achieve-by point (FIM aircraft flies slower than ATC expectations prior to Achieve-by point)

STPA-F.20AB.3.3.1. ATC must monitor FIM aircraft compliance with Achieve-by aspect of trajectory (Allocated to: ATC)

STPA-F.20AB.3.4. Aircraft takes reaches Achieve-by point faster than expected (FIM aircraft flies faster than ATC expectations prior to Achieve-by point)

STPA-F.20AB.3.4.1. ATC must terminate or amend clearance if the difference between the FIM aircraft's predicted and scheduled time of arrival to Achieve-by point exceeds TBD seconds (Allocated to: ATC, FAA Procedures)

STPA-F.20AB.3.4.2. IM-related Ground Automation or other tool must monitor FIM aircraft compliance with scheduled Achieve-by point. This requirement assumes that ATC cannot manually monitor compliance to Achieve-by Point with enough precision to support IM operations (Allocated to: IM-related Ground Automation)

STPA-F.20AB.3.5. NAS weather service does not update its surveillance fast enough

STPA-F.20AB.3.5.1. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NWS (AWIPS, WARP, or other))

STPA-F.20AB.3.6. Weather monitoring interface does not update fast enough

STPA-F.20AB.3.6.1. User interface must refresh every TBD seconds or provide

indication that it is not updating (Allocated to: NWS Automation)

STPA-F.20AB.3.6.2. ATC must not give clearance based on a user interface that is not updating (Allocated to: ATC, FAA Procedures)

STPA-F.20AB.4. FIM flight crew takes too long to execute clearance so that expected separation is not achieved when weather changes [Inadequate actuator operation]

STPA-F.20AB.4.1. Flight crew takes too long to enter new speed into FMS

STPA-F.20AB.4.1.1. Flight crew must enter Maintain clearance into FIM automation, target speed into FMS, or manually fly target speed within TBD seconds ATC cancellation of speed advisory (Allocated to: Flight Crew)

STPA-F.20AB.4.2. FIM automation or FMS takes too long to implement change

STPA-F.20AB.4.2.1. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS, FIM automation)

STPA-F.20AB.4.2.2. ATC must verify that new desired speed is reached within TBD seconds of issuing cancellation of IM speed advisory (Allocated to: ATC (Controllers))

STPA-F.20AB.4.3. Aircraft dynamics are different than ATC expectations (takes 60 seconds to reach steady-state Maintain Spacing speed as opposed to 30 sec)

STPA-F.20AB.4.3.1. TFM trajectory modeling must be provided with aircraft performance data on expected time-to-steady-state for completing speed changes. This time should include environmental considerations such as wind, barometric pressure, angle-of-attach, and other relevant factors for flight dynamics (Allocated to: Airline operators, Airframe manufacturers)

STPA-F.20AB.4.4. Aircraft performance is different than expected due to environmental conditions such as headwinds or tailwinds

STPA-F.20AB.4.4.1. Flight crews must verify that Achieve-by then Maintain is feasible given current environmental conditions (Allocated to: Flight crew)

STPA-F.20AB.4.4.2. Flight crews must request an amended clearance if Achieve-by then Maintain is infeasible (Allocated to: Flight crew)

STPA-F.20AB.5. Aircraft / Flight crew executes a clearance prematurely [Inadequate Actuator Operation]

STPA-F.20AB.5.1. FC distraction

STPA-F.20AB.5.1.1. Flight crew must verify that the clearance is safe, including whether the clearance does not violate separation standards, is within aircraft capability, and there is no presence of inclement weather or restricted airspace. (Allocated to: Flight Crews)

STPA-F.20AB.5.1.2. Flight crew must confirm and accept IM clearance after verification (Allocated to: Flight Crews)

STPA-F.20AB.5.1.3. Flight crew must issue a response (acceptance or request of

amended clearance) within TBD seconds of ATC issuing clearance. (Allocated to: Flight Crews)

STPA-F.20AB.5.1.4. ATC must clearly state the starting point criteria as part of clearance (Allocated to: ATC)

STPA-F.20AB.5.1.5. Flight crew must verify that the IM clearance has a delayed starting point (Allocated to: Flight Crews)

STPA-F.20AB.5.2. FC enters clearance into FMS but does not, or forgets to, delay execution

STPA-F.20AB.5.2.1. Flight crew must include starting point (time) in command to FMS, when IM clearance includes starting point (Allocated to: Flight Crews)

STPA-F.20AB.5.2.2. FMS must begin modifying aircraft speed within TBD seconds of receiving updated plan from Flight Crew (Allocated to: FMS)

STPA-F.20AB.5.2.3. Flight crew must enter IM speed into FMS or manually fly IM speed within TBD seconds of starting point (Allocated to: Flight Crew)

STPA-F.20AB.5.3. FC executes clearance early in anticipation of increased workload

STPA-F.20AB.5.3.1. ATC must verify that IM clearance is not being flown until TBD seconds of planned starting point. (Allocated to: ATC (Controllers))

A.2.1.3 IM Turn Analysis

Unsafe Control Action: UCA13.T. IM Turn Clearance not provided when speed-only clearance would not prevent loss of separation with merging or in-**track aircraft ↑[H**-1]

STPA-F.13T.1. ATC does not believe that IM Turn is necessary [Inadequate process model of airspace and procedure]

STPA-F.13T.1.1. Inadequate or incorrect understanding of aircraft states

STPA-F.13T.1.1.1. ATC must have access to closing rates and predicted time/distance to loss of separation (Allocated to: IM-related ground automation, ERAM, other ATC tools)

STPA-F.13T.1.1.2. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.13T.1.1.3. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-F.13T.1.1.4. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.13T.1.1.5. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM,
Radar)

STPA-F.13T.1.2. Aircraft state information is not current

STPA-F.13T.1.2.1. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.13T.1.2.2. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.13T.1.3. ATC using filed flight plan for decision instead of real-time fused track data

STPA-F.13T.1.3.1. ATC and associated IM-S automation must use real-time surveillance data for generating IM clearances

See STPA-F.14.1 for requirement related to flight plans

See STPA-F.14.18-21 for requirements related to surveillance (Allocated to: ATC, IM-related automation)

STPA-F.13T.1.4. Inadequate or incorrect understanding of separation requirements

STPA-F.13T.1.4.1. ATC must issue IM Turn clearance to pair of potential FIM aircraft that will spacing requirements with speed-only clearance (Allocated to: ATC, FAA Procedures)

STPA-F.13T.1.4.2. ATC must use appropriate spacing requirements when issuing Maintain Current Spacing clearance, per JO 7110.65U (Allocated to: ATC, FAA Procedures)

STPA-F.13T.1.5. Automation does not consider spacing regulations or constraints

STPA-F.13T.1.5.1. IM-related ground automation must not generate Maintain Current Spacing clearance to pair of aircraft that are in violation of spacing requirements (Allocated to: IM-related automation)

STPA-F.13T.1.5.2. IM-related ground automation must have access to current surveillance information for all potential FIM and Target aircraft (Allocated to: ADS-B, GNSS, ERAM, Radar)

STPA-F.13T.1.5.3. IM-related ground automation must have access to all spacing regulations for airspace in which the automation generates IM advisories (Allocated to: FAA)

STPA-F.13T.2. ATC attempts to minimize off-track maneuvers [Contextual Factor influences process model]

STPA-F.13T.2.1. Stated policy of (previous) IM operations is to minimize off-track maneuvers, influencing ATC to minimize turns even when they are necessary [IM-S ConOps]

STPA-F.13T.2.1.1. Policy: IM-S Operations are not intended to minimize off-track maneuvers at the expense of spacing requirements (Allocated to: ATC, FAA Procedures)

STPA-F.13T.2.2. ATC is reluctant to issue IM Turn due to relative complexity of IM Turn compared to other IM clearances

STPA-F.13T.2.2.1. ATC must issue IM Turn clearance to pair of potential FIM aircraft that will violate spacing requirements with speed-only clearance (Allocated to: ATC)

STPA-F.13T.3. Flight crew believes a simple IM clearance has been issued and does not execute turn (only speed change)

STPA-F.13T.3.1. ATC neglects to include IM Turn in communication or communicates IM Turn inconsistently (IM clearances are not given in a consistent fashion)

STPA-F.13T.3.1.1. IM Turn clearance must be stated in a clear, consistent, standardized format (Allocated to: ATC, FAA Procedures)

STPA-F.13T.3.1.2. Flight crew must verify that the clearance is an IM Turn and verify the parameters of clearance (Allocated to: Flight Crews)

STPA-F.13T.3.2. IM clearances get confused with other types of clearances

STPA-F.13T.3.2.1. IM Turn clearance must be distinguishable from other types of clearances (Allocated to: ATC, FAA Procedures)

STPA-F.13T.4. Other aircraft merge into or cross flow at an unexpected rate or spacing, saturating the limits of speed-only clearance [Inadequate process model of airspace]

STPA-F.13T.4.1. ATC neglects surge in traffic across or into traffic flow

STPA-F.13T.4.1.1. ATC and/or associated automation must monitor traffic flow to ensure that spacing and sequencing remains consistent with assumptions when Achieve-by then Maintain clearance was originally issued (Allocated to: ATC, IM-S automation, ERAM)

STPA-F.13T.4.2. Weather conditions in adjacent airspace cause increase in traffic within/across IM traffic flow

STPA-F.13T.4.2.1. ATC must be informed of aircraft being diverted into airspace due to inclement weather. This information should include the fact that the reason for the increased traffic is due to weather. (Allocated to: ATC, NWS)

STPA-F.13T.4.3. Airport delays, runway closure cause increase in traffic within/across IM traffic flow

STPA-F.13T.4.3.1. ATC must be informed of aircraft being diverted into airspace due to airport delays. This information should include the fact that the reason for the increased traffic is due to airport delays. (Allocated to: ATC, TRACON, Tower)

STPA-F.13T.4.4. Changes in approach configurations cause increase in traffic within/across IM traffic flow

STPA-F.13T.4.4.1. ATC must be informed of aircraft being diverted into airspace due to changes in airspace configuration. This information should include the fact that the reason for the increased traffic is due to change in airspace configuration. (Allocated to: ATC, TRACON, Tower)

Unsafe Control Action: UCA22.T. IM Turn Clearance not provided when speed-only **clearance would exceed aircraft capability ↑[H-4]**

STPA-F.22T.1. ATC correctly identifies conditions that prevent IM Turn [Adequate process model, contextual factors affect ATC decision to issue IM clearance]

STPA-F.22T.1.1. ATC correctly identifies adjacent aircraft that would prevent safe separation due to turn

STPA-F.22T.1.1.1. ATC must not issue IM clearance if Maintain or Achieve-by exceeds aircraft capability and traffic conflicts with IM Turn (Allocated to: ATC, FAA Procedures, IM Procedures)

STPA-F.22T.1.1.2. Given previous requirement, ATC must issue other clearance or simply maintain current clearances, as necessary. (Allocated to: ATC, FAA Procedures)

STPA-F.22T.1.2. ATC correctly identifies adjacent weather that would cause weather hazard due to turn

STPA-F.22T.1.2.1. ATC must not issue IM clearance if Maintain or Achieve-by exceeds aircraft capability and weather conflicts with IM Turn (Allocated to: ATC, FAA Procedures, IM Procedures)

STPA-F.22T.1.2.2. Given previous requirement, ATC must issue other clearance or simply maintain current clearances, as necessary. (Allocated to: ATC, FAA Procedures)

STPA-F.22T.1.3. ATC correctly identifies restricted airspace adjacent to aircraft that prevents turn

STPA-F.22T.1.3.1. ATC must not issue IM clearance if Maintain or Achieve-by exceeds aircraft capability and restricted airspace conflicts with IM Turn (Allocated to: ATC, FAA Procedures, IM Procedures)

STPA-F.22T.1.3.2. Given previous requirement, ATC must issue other clearance or simply maintain current clearances, as necessary. (Allocated to: ATC, FAA Procedures)

STPA-F.22T.2. ATC does not believe that IM Turn is necessary [Inadequate process model of airspace and procedure]

STPA-F.22T.2.1. Inadequate or incorrect understanding of aircraft states

STPA-F.22T.2.1.1. ATC must have access to closing rates and predicted time/distance to loss of separation (Allocated to: IM-related ground automation, ERAM, other ATC tools)

STPA-F.22T.2.1.2. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to:

ADS-B,
GNSS)

STPA-F.22T.2.1.3. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-F.22T.2.1.4. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.22T.2.1.5. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM,
Radar)

STPA-F.22T.2.2. Aircraft state information is not current

STPA-F.22T.2.2.1. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.22T.2.2.2. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.22T.2.3. ATC using filed flight plan for decision instead of real-time fused track data

STPA-F.22T.2.3.1. ATC and associated IM-S automation must use real-time surveillance data for generating IM clearances

See STPA-F.14.1 for requirement related to flight plans

See STPA-F.14.18-21 for requirements related to surveillance (Allocated to: ATC, IM-related automation)

STPA-F.22T.3. Inadequate or incorrect understanding of aircraft capability [Inadequate process model of aircraft and airspace]

STPA-F.22T.3.1. Incorrect aircraft type and performance

STPA-F.22T.3.1.1. Aircraft data file must be provided to IM-related ground automation and ATC in standardized format. (Allocated to: Airline operators)

STPA-F.22T.3.1.2. Aircraft data includes certification, airworthiness, and other regulations. (Allocated to: Airframe manufacturers)

STPA-F.22T.3.1.3. Aircraft data file must be updated every flight (Allocated to: Airline operators)

STPA-F.22T.3.1.4. V speeds must be provided to IM-related ground automation in a

standardized format (Allocated to: Airframe manufacturers)

STPA-F.22T.3.1.5. Stall speeds and speed limits must be provided to TFM automation (Allocated to: Airframe manufacturers)

STPA-F.22T.3.2. ATC has incorrect information about current aircraft state, including speed, altitude, heading, configuration

STPA-F.22T.3.2.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.22T.3.2.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: IM-related ground Automation, FIM Automation, ATC, Flight Crew)

STPA-F.22T.3.2.3. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related Ground Automation, FIM Automation)

STPA-F.22T.3.2.4. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM)

STPA-F.22T.3.2.5. ATC must have access to surveillance data (Allocated to: ERAM)

STPA-F.22T.3.2.6. ATC must have access to location of Achieve-by point in format that is consistent with aircraft surveillance and airspace standards (Allocated to: IM-related Ground Automation, ERAM, Radar screen user interface)

STPA-F.22T.3.2.7. IM-related Ground Automation must calculate predicted duration, required airspeed, or other necessary parameters for Achieve-by then Maintain clearance (Allocated to: IM-related Ground Automation)

STPA-F.22T.3.2.8. IM-related Ground Automation must present predicted FIM aircraft trajectory information to ATC (Allocated to: IM-related Ground Automation)

STPA-F.22T.3.3. ATC has incorrect understanding of environmental conditions

STPA-F.22T.3.3.1. IM-related ground automation must have access to real-time wind data for the airspace. (Allocated to: ATC Weather Service)

STPA-F.22T.3.3.2. IM-related ground automation must calculate maximum and minimum allowed speeds for given real-time data. (Allocated to: IM-related Ground Automation, Airframe manufacturers)

STPA-F.22T.3.3.3. IM-related ground automation must not issue Achieve-by points that result in airspeeds outside of maximum and minimum allowed speeds. (Allocated to: IM-related Ground Automation)

STPA-F.22T.3.3.4. Flight crew must verify that clearance is within aircraft capability (Allocated to: Flight crew,
FMS)

STPA-F.22T.3.3.5. Flight crew must request amendment to clearance if required IM speed to meet Achieve-by point exceeds capability. Amendment request should explicitly state that speed exceeds aircraft capability (Allocated to: Flight Crew)

STPA-F.22T.3.4. Automation does not consider aircraft capability

STPA-F.22T.3.4.1. IM-S related ground automation must have access to aircraft capabilities (Allocated to: Airline Operators, Airframe Manufacturers)

STPA-F.22T.3.4.2. IM-S related ground automation must issue IM Turn advisories when available speed advisories exceed aircraft capability (Allocated to: IM-S related Ground Automation)

STPA-F.22T.3.4.3. IM-S related ground automation must have access to current and forecasted environmental conditions that affect aircraft capability (Allocated to: NWS, Airframe Manufacturers)

STPA-F.22T.3.4.4. IM-S related ground automation must include relevant current and forecasted environmental conditions in IM advisories (Allocated to: IM-S related Ground Automation)

STPA-F.22T.4. ATC attempts to minimize off-track maneuvers [Contextual Factor influences process model]

STPA-F.22T.4.1. Stated policy of (previous) IM operations is to minimize off-track maneuvers, influencing ATC to minimize turns even when they are necessary [IM-S ConOps]

STPA-F.22T.4.1.1. Policy: IM-S Operations are not intended to minimize off-track maneuvers at the expense of spacing requirements (Allocated to: ATC, FAA Procedures)

STPA-F.22T.4.2. ATC is reluctant to issue IM Turn due to relative complexity of IM Turn compared to other IM clearances

STPA-F.22T.4.2.1. ATC must issue IM Turn clearance to pair of potential FIM aircraft that will violate spacing requirements with speed-only clearance (Allocated to: ATC)

STPA-F.22T.5. Flight crew believes a simple IM clearance has been issued and does not execute turn (only speed change)

STPA-F.22T.5.1. ATC neglects to include IM Turn in communication or communicates IM Turn inconsistently (IM clearances are not given in a consistent fashion)

STPA-F.22T.5.1.1. IM Turn clearance must be stated in a clear, consistent, standardized format (Allocated to: ATC, FAA Procedures)

STPA-F.22T.5.1.2. Flight crew must verify that the clearance is an IM Turn and verify the parameters of clearance (Allocated to: Flight Crews)

STPA-F.22T.5.2. IM clearances get confused with other types of clearances

STPA-F.22T.5.2.1. IM Turn clearance must be distinguishable from other types of clearances (Allocated to: ATC, FAA Procedures)

STPA-F.22T.6. Other aircraft merge into or cross flow at an unexpected rate or spacing, saturating the limits of speed-only clearance [Inadequate process model of airspace]

STPA-F.22T.6.1. ATC neglects surge in traffic across or into traffic flow

STPA-F.22T.6.1.1. ATC and/or associated automation must monitor traffic flow to ensure that spacing and sequencing remains consistent with assumptions when Achieve-by then Maintain clearance was originally issued (Allocated to: ATC, IM-S automation, ERAM)

STPA-F.22T.6.2. Weather conditions in adjacent airspace cause increase in traffic within/across IM traffic flow

STPA-F.22T.6.2.1. ATC must be informed of aircraft being diverted into airspace due to inclement weather. This information should include the fact that the reason for the increased traffic is due to weather. (Allocated to: ATC, NWS)

STPA-F.22T.6.3. Airport delays, runway closure cause increase in traffic within/across IM traffic flow

STPA-F.22T.6.3.1. ATC must be informed of aircraft being diverted into airspace due to airport delays. This information should include the fact that the reason for the increased traffic is due to airport delays. (Allocated to: ATC, TRACON, Tower)

STPA-F.22T.6.4. Changes in approach configurations cause increase in traffic within/across IM traffic flow

STPA-F.22T.6.4.1. ATC must be informed of aircraft being diverted into airspace due to changes in airspace configuration. This information should include the fact that the reason for the increased traffic is due to change in airspace configuration. (Allocated to: ATC, TRACON, Tower)

Unsafe Control Action: UCA23.T. IM Turn Clearance not provided when IM spacing is **needed and convective weather or restricted airspace is in previous aircraft path ↑[H-2; H-5]**

STPA-F.23T.1. ATC does not believe that IM Turn is necessary [Inadequate process model of airspace and procedure]

STPA-F.23T.1.1. Inadequate or incorrect understanding of aircraft states

STPA-F.23T.1.1.1. ATC must have access to closing rates and predicted time/distance to loss of separation (Allocated to: IM-related ground automation, ERAM, other ATC tools)

STPA-F.23T.1.1.2. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.23T.1.1.3. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-F.23T.1.1.4. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.23T.1.1.5. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM,
Radar)

STPA-F.23T.1.2. Aircraft state information is not current

STPA-F.23T.1.2.1. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.23T.1.2.2. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.23T.1.3. ATC using filed flight plan for decision instead of real-time fused track data

STPA-F.23T.1.3.1. ATC and associated IM-S automation must use real-time surveillance data for generating IM clearances

See STPA-F.14.1 for requirement related to flight plans

See STPA-F.14.18-21 for requirements related to surveillance (Allocated to: ATC, IM-related automation)

STPA-F.23T.2. Inadequate or incorrect understanding of weather conditions [Inadequate process model of airspace]

STPA-F.23T.2.1. Inclement weather forms rapidly, before ATC can be made aware

STPA-F.23T.2.1.1. Flight crews may request an amended clearance due to inclement weather if the crew deams it necessary (Allocated to: Flight Crews)

STPA-F.23T.2.1.2. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NAS Weather Service (NWS))

STPA-F.23T.2.2. NAS weather service surveillance is inaccurate

STPA-F.23T.2.2.1. Precipitation measurements must be within TBD dBZ with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-F.23T.2.2.2. Wind measurements must be within TBD kts with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-F.23T.2.2.3. NAS weather service must notify ATC of accuracy and resolution of weather data, or notify ATC when the above requirements are not met. (Allocated to: NWS)

STPA-F.23T.2.3. ATC misinterprets or misunderstands"Resolution" or accuracy of weather service

STPA-F.23T.2.3.1. The weather service user interface must clearly present the spatial resolution of weather surveillance (Allocated to: NWS User Interface)

STPA-F.23T.2.3.2. The weather service user interface must clearly present the time of applicability of weather surveillance (Allocated to: NWS User Interface)

STPA-F.23T.2.4. NAS weather service does not update its surveillance fast enough

STPA-F.23T.2.4.1. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NWS (AWIPS, WARP, or other))

STPA-F.23T.2.5. Weather monitoring interface does not update fast enough

STPA-F.23T.2.5.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: NWS Automation)

STPA-F.23T.2.5.2. ATC must not give clearance based on a user interface that is not updating (Allocated to: ATC,
FAA Procedures)

STPA-F.23T.2.6. ATC has incorrect understanding of location of weather

STPA-F.23T.2.6.1. The weather service user interface must have the same scale and perspective as aircraft surveillance surveillance screens (Plan position indicator) (Allocated to: NWS Automation)

STPA-F.23T.2.7. Weather data is displayed incorrectly or in a confusing manner

STPA-F.23T.2.7.1. Weather data must be presented in a consistent format, within and across sectors (Allocated to: NWS,
Tower,
TRACON,
ARTCC facilities)

STPA-F.23T.2.8. ATC receives report of inclement weather from flight crew but misinterprets location of aircraft

STPA-F.23T.2.8.1. ATC must verify location of aircraft per FAA standards (Allocated to: ATC,
FAA Procedures)

STPA-F.23T.2.8.2. See surveillance requirements (Allocated to: System Requirement)

STPA-F.23T.2.9. Automation does not consider inclement weather

STPA-F.23T.2.9.1. This is an assumption of FIM operations. ATC must be provided information about FIM's lack of consideration of inclement weather (Allocated to: System Requirement)

STPA-F.23T.3. ATC attempts to minimize off-track maneuvers [Contextual Factor influences process model]

STPA-F.23T.3.1. Stated policy of (previous) IM operations is to minimize off-track maneuvers, influencing ATC to minimize turns even when they are necessary [IM-S ConOps]

STPA-F.23T.3.1.1. Policy: IM-S Operations are not intended to minimize off-track maneuvers at the expense of trajectories that lead to inclement weather (Allocated to: ATC, FAA Procedures)

STPA-F.23T.3.2. ATC is reluctant to issue IM Turn due to relative complexity of IM Turn compared to other IM clearances

STPA-F.23T.3.2.1. ATC may issue IM Turn clearance if IM Turn results in FIM aircraft avoiding inclement weather. NOTE: In general, IM clearances may not be the preferred solution for weather avoidance. (Allocated to: ATC)

STPA-F.23T.4. Flight crew believes a simple IM clearance has been issued and does not

execute turn (only speed change)

STPA-F.23T.4.1. ATC neglects to include IM Turn in communication or communicates IM Turn inconsistently (IM clearances are not given in a consistent fashion)

STPA-F.23T.4.1.1. IM Turn clearance must be stated in a clear, consistent, standardized format (Allocated to: ATC, FAA Procedures)

STPA-F.23T.4.1.2. Flight crew must verify that the clearance is an IM Turn and verify the parameters of clearance (Allocated to: Flight Crews)

STPA-F.23T.4.2. IM clearances get confused with other types of clearances

STPA-F.23T.4.2.1. IM Turn clearance must be distinguishable from other types of clearances (Allocated to: ATC, FAA Procedures)

Unsafe Control Action: UCA14.T. IM Turn Clearance provided where Intercept Point results in loss of separation with traffic that was previous off-**track ↑[H**-1]

STPA-F.14T.1. ATC provides an IM Turn Clearance to aircraft that has different characteristics / capabilities than ATC expectations [Process Model Flaw: Aircraft / FC Model]

STPA-F.14T.1.1. ATC provides incorrect / inadequate direction for turn, requiring a longer or shorter than expected deviation from path

STPA-F.14T.1.1.1. ATC must provide turn clearance (heading) that maintains separation between FIM aircraft and lateral or crossing traffic. (Allocated to: ATC)

STPA-F.14T.1.1.2. ATC must monitor FIM aircraft for conflicts through turn. (Allocated to: ATC,
Conflict detection & resolution tools)

STPA-F.14T.1.2. Incorrect or delayed surveillance

STPA-F.14T.1.2.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.14T.1.2.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: FIM Automation,
ATC Automation,
ATC, Flight Crew)

STPA-F.14T.1.2.3. TFM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.14T.1.2.4. TFM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM)

STPA-F.14T.1.2.5. ATC must have access to surveillance data (Allocated to: ERAM)

STPA-F.14T.1.2.6. ADS-B must be updated and transmitted every 1 second (Allocated to: ADS-B)

STPA-F.14T.1.2.7. Mode S radar surveillance must be updated and transmitted every 12 seconds. (Allocated to: Air traffic control radar beacon system)

STPA-F.14T.1.3. ATC provides IM tolerance that exceeds aircraft capability

STPA-F.14T.1.3.1. ATC must not provide IM tolerance that exceeds aircraft capability (Allocated to: ATC)

STPA-F.14T.1.3.2. ATC must be provided with performance information associated with each aircraft in a FIM clearance (Allocated to: Airline operators,
Airframe manufacturers)

STPA-F.14T.1.3.3. ATC must be provided with real-time performance monitoring information prior to and during FIM clearance (Allocated to: ADS-B, radar, fused-track surveillance

ERAM or other PBN-related monitoring tool)

STPA-F.14T.1.3.4. ATC must modify clearance if FIM aircraft does not meet performance requirement.

Modified clearance could include new FIM clearance with different performance bounds or rejection of FIM clearance and issuance of other clearance. (Allocated to: ATC)

STPA-F.14T.1.3.5. Flight crew must notify ATC of inability to meet performance requirements (Allocated to: Flight crew)

STPA-F.14T.1.4. Aircraft given different clearance immediately prior to or after FIM clearance

STPA-F.14T.1.4.1. All controllers must have access to new clearances and time of applicability. (Allocated to: ARTCC, TRACON, and Tower Control tools, and/or

Inter- and intra-sector communication protocols and procedures)

STPA-F.14T.1.4.2. ATC must not give FIM clearance if a different clearance has been issued within TBD seconds prior (Allocated to: ATC)

STPA-F.14T.1.4.3. FIM clearance becomes invalid if new clearance is issued to either FIM or target aircraft after initiation of FIM. (Allocated to: ATC)

STPA-F.14T.1.4.4. ATC must cancel FIM clearance and issue new clearances accordingly when FIM clearance becomes invalid. (Allocated to: ATC)

STPA-F.14T.2. ATC believes that particular section of airspace is unoccupied, so ATC clears other aircraft into that area. [Process Model Flaw: Airspace]

STPA-F.14T.2.1. Controller clears other (non-IM, or IM aircraft in a different IM scenario) based on incorrect assumptions about location of IM Turn aircraft

STPA-F.14T.2.1.1. ATC must monitor FIM aircraft for conflicts through turn. (Allocated to: ATC,
Conflict detection & resolution tools)

STPA-F.14T.2.2. There are conflicting aircraft in the path of the turn

STPA-F.14T.2.2.1. ATC must not provide IM Turn clearance in the direction of conflicting aircraft. (Allocated to: ATC)

STPA-F.14T.2.2.2. ATC must wait for conflicting aircraft to clear before issuing IM Turn clearance, OR (Allocated to: ATC)

STPA-F.14T.2.2.3. ATC must issue de-conflicting clearances to aircraft in the area of a turn before issuing IM Turn clearance. (Allocated to: ATC)

STPA-F.14T.2.3. Other (non-FIM) aircraft join traffic flow during the time that the FIM aircraft is in the turn

STPA-F.14T.2.3.1. ATC and/or associated tools must monitor original traffic flow during IM Turn Clearance. (Allocated to: ATC)

STPA-F.14T.2.3.2. ATC must modify current IM Turn clearance if predicted spacing of traffic flow has changed (Allocated to: ATC)

STPA-F.14T.2.3.3. ATC must modify spacing of traffic flow so that the spacing matches the assumptions in the original FIM clearance. (Allocated to: ATC)

STPA-F.14T.2.3.4. Spacing modification could be achieved through speed modifications, path stretching, or altitude modifications (removing aircraft from flow). (Allocated to: ATC)

STPA-F.14T.3. ATC incorrectly understands or implements FIM procedure. [Process Model Flaw: FIM Procedure]

STPA-F.14T.3.1. Aircraft starts too soon or too late due to Starting Event

STPA-F.14T.3.1.1. FIM Starting Event must allow for sufficient spacing between all aircraft in airspace (Allocated to: ATC,
FIM Automation)

STPA-F.14T.3.1.2. FIM Starting Event must not start too late when aircraft within a flow are closing (Allocated to: ATC,
FIM Automation)

STPA-F.14T.3.1.3. FIM Starting Event must not cause conflict with crossing or lateral aircraft (Allocated to: ATC,
FIM Automation)

STPA-F.14T.3.2. Planned termination point causes aircraft to exceed capability or execute more aggressive turn trajectory than would otherwise be executed with a different

termination point

STPA-F.14T.3.2.1. FIM Planned Termination Point must allow for sufficient spacing between all aircraft in airspace (Allocated to: ATC,
FIM Automation)

STPA-F.14T.3.2.2. FIM Planned Termination Point must not finish too soon when aircraft within a flow are closing, or when termination would result in closing speeds (Allocated to: ATC,
FIM Automation)

STPA-F.14T.3.2.3. FIM Planned Termination Point must not cause conflict with crossing or lateral aircraft (Allocated to: ATC,
FIM Automation)

STPA-F.14T.3.2.4. FIM Planned Termination Point must result in aircraft speed that is within performance bounds.

Stall and overspeed are function of aircraft state, type, and environment (Allocated to:
FIM Automation,
Airframe Manufacturers,
ADS-B,
Weather Service)

STPA-F.14T.3.2.5. FIM Planned Termination Point must result in turn that is within performance bounds.

Allowed banking are function of aircraft state, type, and environment (Allocated to: FIM Automation,
Airframe Manufacturers,
ADS-B,
Weather Service)

STPA-F.14T.4. ATC misunderstands the algorithm and model of automation (its 'intentions') and issues an incorrect command. [Process Model Flaw: FIM Automation / DST]

STPA-F.14T.4.1. ATC issues clearance based on a certain sequence while FIM automation generates parameters for a different sequence

STPA-F.14T.4.1.1. ATC must have access to FIM sequencing plans (Allocated to: FIM Automation,
IM user interface (ATC interface))

STPA-F.14T.4.1.2. ATC must issue clearances that are consistent with sequencing algorithm, OR (Allocated to: ATC)

STPA-F.14T.4.1.3. ATC must reject IM clearances if ATC believes the IM sequence is inappropriate (Allocated to: ATC)

STPA-F.14T.4.2. FIM automation generates incorrect heading for IM turn

STPA-F.14T.4.2.1. NA (Allocated to: NA)

STPA-F.14T.4.3. FIM calculates turn-back point incorrectly, resulting in a trajectory that conflicts with adjacent or lateral aircraft

STPA-F.14T.4.3.1. FIM aircraft trajectory must not conflict with other aircraft during FIM Turn Clearance (Allocated to: ATC,
FIM Flight Crew)

STPA-F.14T.5. Aircraft does not follow expected trajectory when ATC actions are otherwise correct. [Inadequate Actuator Operation]

STPA-F.14T.5.1. Aircraft takes too long to turn back expected flight path

STPA-F.14T.5.1.1. ATC must be provided information about degraded aircraft performance.

Suggest requirement: Flight crew must notify ATC of degraded aircraft performance (Allocated to: Flight Crews,
FMS, other)

STPA-F.14T.5.1.2. ATC must not issue IM Clearances for degraded aircraft. (Allocated to: ATC)

STPA-F.14T.5.1.3. IM tools must include current environmental characteristics in trajectory model, including winds, pressure, and convective weather. (Allocated to: FIM Automation,)

STPA-F.14T.5.1.4. IM tools include ground-based automation and FIM. (Allocated to: Other IM Tools, ERAM)

STPA-F.14T.5.1.5. FIM aircraft must fly IM trajectory within performance bounds. FIM aircraft altitude must be within TBD feet, vertical speed must be within TBD ft/sec, airspeed must be within TBD mach (or knots), position must be within TBD NM. (Allocated to: Flight Crew,
FMS)

STPA-F.14T.5.2. Aircraft flies an unusual or unexpected trajectory to meet IM Turn clearance parameters

STPA-F.14T.5.2.1. Order of priority for IM clearances should be (increasing to

decreasing priority)
1. Maintain Current Spacing clearance
2. Precise Value spacing
3. Closed Interval spacing
4. No Closer than Interval
5. Achieve-by then Maintain clearance
6. IM Turn Clearance (Allocated to: ATC,
FAA Procedures and Policies)

STPA-F.14T.5.3. Flight crew (or flight deck) fails to identify conflicting aircraft

STPA-F.14T.5.3.1. Conflict detection and resolution takes priority over execution of IM Clearance. (Allocated to: System requirement,
FAA Procedures and Policies)

STPA-F.14T.5.3.2. ATC must issue clearances that maintain separation of aircraft and are within performance bounds of aircraft. (Allocated to: ATC)

STPA-F.14T.5.3.3. Flight crew must deviate from IM Clearance if the IM clearance results in a loss of separation (Allocated to: Flight Crew)

STPA-F.14T.5.3.4. Flight crew must deviate from IM Clearance if the IM clearance exceed aircraft capability (Allocated to: Flight Crew)

STPA-F.14T.5.3.5. Flight crew must notify ATC of deviation from IM clearance and provide reason. (Allocated to: Flight Crew)

Unsafe Control Action: UCA15.T. IM Turn Clearance provided where Intercept Point **exceeds aircraft capability, including turn rate↑[H**-3; H-4]

STPA-F.15T.1. ATC has incorrect understanding of geometry and dynamics required to safely execute IM turn [Inadequate process model of airspace and aircraft capability

STPA-F.15T.1.1. ATC issues turn heading is too sharp or too shallow and requires overly aggressive maneuvers

STPA-F.15T.1.1.1. ATC must issue an IM Turn initial heading that is within aircraft capabilities (Allocated to: ATC, FAA Procedures)

STPA-F.15T.1.1.2. ATC must have access to aircraft turn capabilities (Allocated to: Airline Operators, Airframe Manufacturers)

STPA-F.15T.1.1.3. Flight crew must verify that IM Turn is within aircraft capability (Allocated to: FIM Flight crew)

STPA-F.15T.1.1.4. Flight crew must request amended clearance if IM Turn heading exceeds aircraft capability (Allocated to: FIM Flight crew)

STPA-F.15T.1.2. ATC issues turn point that is too early or too late along original track

STPA-F.15T.1.2.1. ATC must issue turn point that allows sufficient time and space for FIM aircraft to turn and/or modify speed within capability (Allocated to: ATC, IM Procedure)

STPA-F.15T.1.3. ATC issues intercept point that is too close or too deep along original track

STPA-F.15T.1.3.1. ATC must issue intercept point that allows sufficient time and space for FIM aircraft to execute IM Turn clearance within capability (Allocated to: ATC, IM Procedure)

STPA-F.15T.1.4. Turn required to get back to Intercept Point in time exceeds aircraft capabilities

STPA-F.15T.1.4.1. FIM Equipment must not calculate turn that exceeds aircraft capability (Allocated to: FIM Automation)

STPA-F.15T.1.5. ATC unaware of aircraft turn capabilities or ATC miscalculates turn capabilities

STPA-F.15T.1.5.1. ATC must have access to aircraft turn capabilities (Allocated to: Airline Operators, Airframe Manufacturers)

STPA-F.15T.1.6. Aircraft capability is degrade prior to or during flight

STPA-F.15T.1.6.1. ATC must be notified of degraded aircraft capability within TBD seconds of degradation (Allocated to: Airline Operators, Flight Crews)

STPA-F.15T.1.7. Aircraft flying different speed than expected during turn and therefore requires aggressive maneuver to reach Intercept Point in time

STPA-F.15T.1.7.1. ATC must have access to closing rates and predicted time/distance to turn point and separation point (Allocated to: IM-related ground automation, ERAM, other ATC tools)

STPA-F.15T.1.7.2. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B,
GNSS)

STPA-F.15T.1.7.3. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: TFM Automation)

STPA-F.15T.1.7.4. IM automation must check when surveillance data is outside of 95% requirement. (Allocated to: TFM Automation)

STPA-F.15T.1.7.5. IM must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM,
Radar)

STPA-F.15T.1.7.6. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.15T.1.7.7. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.15T.2. Flight crew and aircraft incorrectly implement geometry of IM Turn clearance [Inadequate actuator operation]

STPA-F.15T.2.1. FIM equipment calculates incorrect turn-back point

STPA-F.15T.2.1.1. FIM Equipment must calculate turn-back point that allows FIM aircraft to reach Intercept Point with TBD seconds of scheduled arrival time (Allocated to: FIM Automation)

STPA-F.15T.2.1.2. FIM Equipment must calculate a turn-back point that allows FIM aircraft to fly within upper and lower speed limits (Allocated to: FIM Automation)

STPA-F.15T.2.1.3. FIM Equipment must calculate a turn-back point that allows FIM aircraft to turn within minimum allowed turn radius (Allocated to: FIM Automation)

STPA-F.15T.2.2. FIM equipment calculates or displays turn-back point too late

STPA-F.15T.2.2.1. FIM Equipment must calculate turn-back point at least TBD seconds prior to aircraft reaching that point (Allocated to: FIM Automation)

STPA-F.15T.2.2.2. FIM Equipment must display turn-back parameters at least TBD seconds prior to aircraft reaching that point (Allocated to: FIM Automation)

Unsafe Control Action: UCA16.T. IM Turn Clearance provided where Turn-back or Intercept Point is in restricted airspace or convective weather ↑[H-2; H-5]

STPA-F.16T.1. Target aircraft enters restricted airspace and ATC unaware [Inadequate process model of airspace]

STPA-F.16T.1.1. Target aircraft is allowed to enter restricted airspace but FIM aircraft is not

STPA-F.16T.1.1.1. ATC should not issue IM turn clearances to FIM aircraft that have restrictions along turn trajectory (Allocated to: ATC, FAA Procedures)

STPA-F.16T.1.1.2. ATC must be provided information about aircraft restrictions for all classes of airspace within and across sectors. (Allocated to: FAA, US Gov't, Airline Operators, Airframe Manufacturers)

STPA-F.16T.1.2. FIM aircraft incorrectly enters restricted airspace during turn

STPA-F.16T.1.2.1. IM clearance becomes invalid if FIM aircraft enters restricted airspace (Allocated to: FAA Procedures)

STPA-F.16T.1.2.2. ATC must terminate IM clearance and vector FIM aircraft away from restricted airspace if aircraft enters restricted airspace (Allocated to: ATC, FAA Procedures)

STPA-F.16T.1.3. Airspace restriction changes and is not updated

STPA-F.16T.1.3.1. ATC must have access to restricted airspace updates within TBD seconds of update (Allocated to: FAA, US Gov't, NWS)

STPA-F.16T.1.3.2. (Allocated to:)

STPA-F.16T.1.4. ATC priortizes IM Turn clearance over weather avoidance

STPA-F.16T.1.4.1. ATC must not issue IM Turn that leads to inclement weather (Allocated to: ATC, FAA Procedures)

STPA-F.16T.1.4.2. ATC must amend or terminate IM Turn that is heading towards are in inclement weather (Allocated to: ATC, IM Procedure)

STPA-F.16T.1.5. Downstream environment changes after initiation of advisory

STPA-F.16T.1.5.1. ATC must monitor downstream and adjacent environment before and during execution of advisory (Allocated to: ATC, NWS)

STPA-F.16T.1.5.2. IM-S speed advisory becomes invalid if weather severity is downgraded before or during execution of advisory (Allocated to: TFM automation,

ATC, NWS)

STPA-F.16T.1.5.3. IM-S trajectory modeling refresh rate must be synchronized with weather forecasting and surveillance refresh rates (Allocated to: TFM automation, NWS)

STPA-F.16T.1.6. Change in environment causes aircraft to be in a different state than expected (e.g. headwinds, tailwinds)

STPA-F.16T.1.6.1. ATC and flight crew must monitor compliance with IM speeds and separation (Allocated to: ATC, Flight Crews)

STPA-F.16T.1.6.2. ATC or automation must monitor aircraft compliance with Maintain Separation and predicted target aircraft speed and provide an alert if discrepancy exceeds TBD (Allocated to: IM-related ground Automation)

STPA-F.16T.1.7. Inclement weather forms rapidly, before ATC can be made aware

STPA-F.16T.1.7.1. Flight crews may request an amended clearance due to inclement weather if the crew deems it necessary (Allocated to: Flight Crews)

STPA-F.16T.1.7.2. The NAS weather service must update its surveillance every TBD seconds (Allocated to: NAS Weather Service (NWS))

STPA-F.16T.1.8. NAS weather service surveillance is inaccurate

STPA-F.16T.1.8.1. Precipitation measurements must be within TBD dBZ with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-F.16T.1.8.2. Wind measurements must be within TBD kts with a resolution of TBD square meters and altitude of TBD m (Allocated to: NWS)

STPA-F.16T.1.8.3. NAS weather service must notify ATC of accuracy and resolution of weather data, or notify ATC when the above requirements are not met. (Allocated to: NWS)

STPA-F.16T.1.9. ATC misinterprets or misunderstands "Resolution" or accuracy of weather service

STPA-F.16T.1.9.1. The weather service user interface must clearly present the spatial resolution of weather surveillance (Allocated to: NWS User Interface)

STPA-F.16T.1.9.2. The weather service user interface must clearly present the time of applicability of weather surveillance (Allocated to: NWS User Interface)

STPA-F.16T.1.10. NAS weather service does not update its surveillance fast enough

STPA-F.16T.1.10.1. The NAS weather service must update its surveillance every TBD

seconds (Allocated to: NWS (AWIPS, WARP, or other))

STPA-F.16T.1.11. Weather monitoring interface does not update fast enough

STPA-F.16T.1.11.1. User interface must refresh every TBD seconds or provide indication that it is not updating (Allocated to: NWS Automation)

STPA-F.16T.1.11.2. ATC must not give clearance based on a user interface that is not updating (Allocated to: ATC, FAA Procedures)

STPA-F.16T.1.12. ATC has incorrect understanding of location of weather

STPA-F.16T.1.12.1. The weather service user interface must have the same scale and perspective as aircraft surveillance screens (Plan position indicator) (Allocated to: NWS Automation)

STPA-F.16T.1.13. Weather data is displayed incorrectly or in a confusing manner

STPA-F.16T.1.13.1. Weather data must be presented in a consistent format, within and across sectors (Allocated to: NWS, Tower, TRACON, ARTCC facilities)

STPA-F.16T.1.14. ATC receives report of inclement weather from flight crew but misinterprets location of aircraft

STPA-F.16T.1.14.1. ATC must verify location of aircraft per FAA standards (Allocated to: ATC, FAA Procedures)

STPA-F.16T.1.15. Incorrect surveillance of aircraft

STPA-F.16T.1.15.1. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.16T.1.15.2. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: ERAM, ADS-B)

STPA-F.16T.1.15.3. IM-related ground automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related ground Automation)

STPA-F.16T.1.15.4. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, ADS-B)

STPA-F.16T.2. ATC does not believe turn will cause them to go into restricted airspace or inclement weather

STPA-F.16T.2.1. Turn direct or Turn-back takes longer than expected

STPA-F.16T.2.1.1. ATC must monitor IM Turn FIM aircraft for compliance with

restricted airspace regulataions (Allocated to: ATC, FAA Procedures)

STPA-F.16T.2.1.2. ATC must monitor IM Turn FIM aircraft for avoidance of inclement weather (Allocated to: ATC, NWS)

STPA-F.16T.3. Flight crew or aircraft neglects turn-back

STPA-F.16T.3.1. FIM Equipment does not consider weather

STPA-F.16T.3.1.1. Flight crew must void FIM equipment in the presence of inclement weather (Allocated to: FIM Flight Crew)

STPA-F.16T.3.1.2. Flight crew must notify ATC of inclement weather and request amended clearance (Allocated to: FIM Flight Crew)

STPA-F.16T.3.2. FIM Equipment does not consider restricted airspace

STPA-F.16T.3.2.1. See above requirement for ATC monitoring compliance with restricted airspace regulations (Allocated to: ATC, FAA Procedures)

STPA-F.16T.3.2.2. ATC must terminate IM clearance and vector aircraft away from restricted airspace (see above requirements) (Allocated to: ATC, FAA Procedures)

STPA-F.16T.3.2.3. Flight crew must void FIM equipment when ATC amends clearance due to restricted airspace (Allocated to: FIM Flight Crew)

Unsafe Control Action: UCA18.T. IM Turn Clearance is given after IM aircraft reaches its IM turn point, resulting in a trajectory t**hat potentially exceeds aircraft capability ↑[H-4]**

STPA-F.18T.1. ATC takes too long to give clearance

STPA-F.18T.1.1. Attention is diverted to other issues in airspace

STPA-F.18T.1.1.1. IM Turn point becomes invalid if issued later than TBD seconds before FIM aircraft reaches point (or within TBD NM of aircraft reach point) (Allocated to: ATC, IM Procedure)

STPA-F.18T.1.1.2. IM-related ground automation must clearly display that IM Turn clearance is no longer valid (Allocated to: IM-related Ground Automation)

STPA-F.18T.1.1.3. ATC must no issue IM turn clearance later than TBD seconds before FIM aircraft reaches point (or within TBD NM of aircraft reach point) (Allocated to: ATC)

STPA-F.18T.1.2. ATC has incorrect assessment of aircraft state

STPA-F.18T.1.2.1. ATC must verify location of aircraft relative to IM Turn points (Allocated to: ATC, FAA Procedures)

STPA-F.18T.1.2.2. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.18T.1.2.3. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: ERAM, ADS-B)

STPA-F.18T.1.2.4. IM-related ground automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related ground Automation)

STPA-F.18T.1.2.5. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, ADS-B)

STPA-F.18T.1.3. ATC has incorrect assessment of IM turn point

STPA-F.18T.1.3.1. IM-related ground automation must clearly display location of IM Turn points (Allocated to: IM-related Ground Automation)

STPA-F.18T.1.3.2. IM Turn points must be presented and formatted in a consistent manner with other ATC surveillance tools (Allocated to: IM-related Ground Automation, FAA Standards, User Interfaces)

STPA-F.18T.1.4. IM Turn point delayed because it is near sector boundary

STPA-F.18T.1.4.1. All sectors must have access to IM Turn parameters, including time of applicability (and/or location of applicability) (Allocated to: IM-related Ground Automation, TRACON, Tower, ARTCC)

STPA-F.18T.1.5. FIM aircraft receives amended clearance from originator of IM clearance

STPA-F.18T.1.5.1. The controller monitoring IM aircraft must provide amended IM clearance if (s)he amends FIM aircraft trajectory (Allocated to: ATC)

STPA-F.18T.1.6. FIM aircraft receives amended clearance from different controller in sector

STPA-F.18T.1.6.1. The controller monitoring IM aircraft must be provided with all clearances being issued to FIM aircraft from within sector (Allocated to: ATC, user interfaces)

STPA-F.18T.1.7. FIM aircraft receives amended clearance from different sector

STPA-F.18T.1.7.1. The controller monitoring IM aircraft must be provided with all clearances being issued to Target aircraft from adjacent sectors (Allocated to: ATC, user interfaces)

STPA-F.18T.1.7.2. The controller monitoring IM aircraft must abort or amend IM clearance if trajectory changes in FIM aircraft cause downstream exceedance of capability due to IM constraints (Allocated to: ATC, user interfaces)

STPA-F.18T.1.7.3. The controller monitoring IM aircraft must abort or amend IM clearance if delayed or modified IM Turn points cause exceedance of aircraft capability (Allocated to: ATC, FAA procedures)

STPA-F.18T.1.8. Shift change affects controller awareness of IM Turn locations

STPA-F.18T.1.8.1. ATC and associated IM automation must have access to predicted IM clearances of all adjacent sectors up to TBD hours. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.18T.1.8.2. ATC and associated IM automation must have access to real-time IM clearances and capacity constraints of all adjacent sectors. (Allocated to: TRACON, Tower, ARTCC)

STPA-F.18T.1.8.3. ATC must not issue clearances that saturate airspace with aircraft under IM clearances (Allocated to: ATC, FAA procedures)

STPA-F.18T.1.8.4. ATC must verify new target and FIM aircraft speeds after termination of IM clearance (Allocated to: ATC, FAA procedures)

STPA-F.18T.2. Flight crew takes too long to execute IM turn

STPA-F.18T.2.1. Delay in transmission of clearance

STPA-F.18T.2.1.1. System must ensure that ATC clearance reaches FIM aircraft within TBD seconds of issuance (Allocated to: Communication network)

STPA-F.18T.2.2. FIM equipment calculates incorrect turn-back point

STPA-F.18T.2.2.1. FIM Equipment must calculate turn-back point within TBD seconds (or TBD NM) of reaching that point (Allocated to: FIM Automation)

STPA-F.18T.2.2.2. FIM Equipment must calculate a turn-back point that allows FIM aircraft to fly within upper and lower speed limits (Allocated to: FIM Automation)

STPA-F.18T.2.2.3. FIM Equipment must calculate a turn-back point that allows FIM aircraft to turn within minimum allowed turn radius (Allocated to: FIM Automation)

STPA-F.18T.2.3. FIM equipment calculates or displays turn-back point too late

STPA-F.18T.2.3.1. FIM Equipment must calculate turn-back point at least TBD seconds prior to aircraft reaching that point (Allocated to: FIM Automation)

STPA-F.18T.2.3.2. FIM Equipment must display turn-back parameters at least TBD seconds prior to aircraft reaching that point (Allocated to: FIM Automation)

STPA-F.18T.2.4. Flight crew delays execution

STPA-F.18T.2.4.1. Flight Crew must execute turn within TBD seconds or TBD NM of reaching turn points (Allocated to: Flight Crew, FIM Aircraft)

STPA-F.18T.2.4.2. FIM Equipment must display or inform Flight Crew of non-compliance with IM Turn parameters (Allocated to: FIM Automation)

STPA-F.18T.2.4.3. Flight Crew must notify ATC of noncompliance (Allocated to: Flight Crew)

A.2.1.4 Flight Crew

Unsafe Control Action: UCA.FC.1. Flight crew does not execute IM clearance, which is necessary to maintain safe separation from other aircraft ↑ [H-1]

STPA-F.FC1.1. Flight crew does not implement IM clearance due to ATC instructions [Inadequate process model of ATC and FAA procedures]

STPA-F.FC1.1.1. Flight crew receives conflicting clearances and therefore does not execute IM clearance (or any clearance)

STPA-F.FC1.1.1.1. The following requirement must be analyzed to ensure that it is consistent with FAA policies (Allocated to: System Requirements)

STPA-F.FC1.1.1.2. Flight crew must request amended clearance or ask for clarification if multiple clearances are granted within TBD seconds (Allocated to: Flight Crew)

STPA-F.FC1.1.2. Flight crew receives ambiguous IM clearance

STPA-F.FC1.1.2.1. ATC must grant IM clearances in clear, concise, and consistent format (Allocated to: ATC, FAA Procedures)

STPA-F.FC1.1.2.2. Flight crew must verify IM clearance and repeat parameters when accepting IM clearances (Allocated to: Flight Crew)

STPA-F.FC1.1.3. ATC does not grant IM clearance

STPA-F.FC1.1.3.1. See ATC UCAs below (Allocated to: System Requirements)

STPA-F.FC1.1.4. ATC does not believe IM clearance is the correct thing to do, e.g. due to past incorrect or detrimental IM clearances, but does not request amended clearance

STPA-F.FC1.1.4.1. Flight crews and ATC must report to relevant authorities when IM clearances are deemed unnecessary or detrimental (Allocated to: ATC, FAA, Auditing bodies)

STPA-F.FC1.1.4.2. False or detrimental IM clearances must occur no more than TBD% of total IM clearances (Allocated to: IM-related ground automation, FIM automation)

STPA-F.FC1.1.4.3. Flight crew must request amended clearance if crew does not want to or plan to execute clearance (Allocated to: Flight Crew)

STPA-F.FC1.2. Flight crew does not implement IM clearance due to flight deck issues [Inadequate process model of flight deck operations]

STPA-F.FC1.2.1. Flight crew is distracted or has diverted resources elsewhere. For example, crew is entering data into FMS, check compliance with route, checking onboard anomalies, or others.

STPA-F.FC1.2.1.1. ATC must only assume IM clearance is being followed when flight crew acknowledges and verifies clearance (Allocated to: ATC)

STPA-F.FC1.2.1.2. ATC must monitor compliance with IM clearances (see ATC

UCA causal analysis and requirements) (Allocated to: System Requirements)

STPA-F.FC1.2.2. Captain believes First Officer is executing or will execute IM clearance (and vice versa)

STPA-F.FC1.2.2.1. All crew members must be able to execute IM clearance (Allocated to: FIM Automation)

STPA-F.FC1.2.2.2. All crew members must have access to status of IM clearance execution (Allocated to: FIM Automation)

STPA-F.FC1.3. FIM equipment does not perform IM clearance [Inadequate actuator operation, crew inadequate model of automation]

STPA-F.FC1.3.1. Flight crew does not input IM clearance into automation

STPA-F.FC1.3.1.1. See above requirements (Allocated to: Flight Crew)

STPA-F.FC1.3.2. FIM equipment does not receive IM clearance from ground via datalink (This does not appear to be part of the current FIM design but could be in the future)

STPA-F.FC1.3.2.1. Protection must be provided against jamming or corruption of the signal between ground centers and flight decks (Allocated to: Flight deck avionics, ground software, receivers, transponders)

STPA-F.FC1.3.2.2. The system must control electromagnetic interference. (Allocated to: Flight deck avionics, Center software, receivers, transponders)

STPA-F.FC1.3.2.3. The FIM system must not interfere with existing avionics systems (Allocated to: FIM automation, FIM user interface)

STPA-F.FC1.3.3. FIM equipment cannot calculate a trajectory and times out

STPA-F.FC1.3.3.1. FIM equipment must provide a notification to flight crew when it cannot compute a trajectory (Allocated to: FIM automation, FIM user interface)

STPA-F.FC1.3.4. FIM equipment does not or cannot send trajectory modification to FMS or other system(s) responsible for controlling aircraft surfaces

STPA-F.FC1.3.4.1. System must provide robust data interface between FIM equipment and FMS and/or other flight control avionics (Allocated to: Aircraft avionics - software architecture requirement)

STPA-F.FC1.3.5. Signal or data-sharing between FIM equipment and FMS or other system becomes corrupted

STPA-F.FC1.3.5.1. System must provide protection against signal corruption or jamming between FIM equipment and other avionics (Allocated to: Aircraft avionics - software architecture requirement)

STPA-F.FC1.3.6. FIM equipment has software or hardware fault and cannot compute or implement trajectory

STPA-F.FC1.3.6.1. FIM equipment must provide a notification of when it is in a faulted mode and cannot compute trajectories (Allocated to: FIM Automation)

STPA-F.FC1.4. See UCA 13.M, UCA 13.AB, UCA 13.T, UCA 22.T, UCA 23.T

STPA-F.FC1.4.1. See UCA 13.M, UCA 13.AB, UCA 13.T, UCA 22.T, UCA 23.T

STPA-F.FC1.4.1.1. See UCA 13.M, UCA 13.AB, UCA 13.T, UCA 22.T, UCA 23.T (Allocated to: System Requirements)

Unsafe Control Action: UCA.FC.2. Flight crew executes different type of IM clearance than was given by ATC (e.g. executes maintain current instead of achieve-by) and causes loss of separation ↑ [H-1]

STPA-F.FC2.1. Flight crew incorrectly implements a potentially safe IM clearance from ATC [Incorrect process model of IM operations]

STPA-F.FC2.1.1. Flight crew enters incorrect IM clearance information

STPA-F.FC2.1.1.1. Flight crew must enter IM parameters into FIM equipment per ATC instruction, OR (Allocated to: Flight Crew)

STPA-F.FC2.1.1.2. Flight crew may reject IM clearance and request amended clearance (Allocated to: Flight Crew)

STPA-F.FC2.1.2. Flight crew incorrectly interprets ATC clearance parameters

STPA-F.FC2.1.2.1. ATC must grant IM clearances in clear, concise, and consistent format (Allocated to: ATC, FAA Procedures)

STPA-F.FC2.1.2.2. Flight crew must verify IM clearance and repeat parameters when accepting IM clearances (Allocated to: Flight Crew)

STPA-F.FC2.1.3. Flight crew receives conflicting clearance. This could be either multiple IM clearances or an IM clearance and other types of clearances

STPA-F.FC2.1.3.1. The following requirement must be analyzed to ensure that it is consistent with FAA policies (Allocated to: System Requirements)

STPA-F.FC2.1.3.2. Flight crew must request amended clearance or ask for clarification if multiple clearances are granted within TBD seconds (Allocated to: Flight Crew)

STPA-F.FC2.1.4. Crew is fixated on certain IM clearances and neglects a different type of IM clearance. For example, crew receives an IM Turn clearance but executes Maintain or Achieve-by clearance due to fixation on minimizing off-track maneuvers

STPA-F.FC2.1.4.1. ATC must use different terminology for the different types of IM clearances (Allocated to: ATC, FAA Procedures)

STPA-F.FC2.1.5. Crew is distracted or "primed" by other clearances. For example, crew just performed a vector clearance and therefore does not expect an IM turn and therefore does not execute it. Alternatively, crew just performed a vector and therefore incorrectly executes a subsequent IM Turn.

STPA-F.FC2.1.5.1. IM clearance terminology must be clearly distinguishable from other types of clearances (Allocated to: ATC, FAA Procedures)

STPA-F.FC2.1.5.2. Different parameters of IM clearance must be distinguishable from one another, including IM clearance types and IM clearance parameters (Allocated to: ATC, FAA Procedures)

STPA-F.FC2.2. FIM Equipment implements an unsafe IM clearance and Flight Crew does

not intervene [Inadequate process model of automation]

STPA-F.FC2.2.1. Flight crew enters incorrect information into FIM equipment due to forgetting or "scrambling" IM parameters between time of accepting IM clearance and actually entering information

STPA-F.FC2.2.1.1. Flight crew must enter IM clearance information into FIM equipment within TBD seconds of receiving (and accepting) clearance (Allocated to: Flight Crew)

STPA-F.FC2.2.2. Flight crew enters incorrect information into FIM equipment because user interface is difficult to navigate or interact with. For example, it is unclear or difficult to distinguish between different types of clearances (Maintain, Achieve-by, Turn) or different IM parameters (starting point, achieve-by point, spacing...)

STPA-F.FC2.2.2.1. Flight crew must be able to enter IM clearance information in a minimal amount of time and with minimal errors. (Allocated to: Flight Crew, FIM User interface)

STPA-F.FC2.2.2.2. FIM Equipment must provide clear, distinguishable alternative among different clearance types (Allocated to: FIM User interface)

STPA-F.FC2.2.2.3. FIM Equipment must clearly demark IM parameters, including initiation point, termination point, spacing type, and others. (Allocated to: FIM User interface)

STPA-F.FC2.2.3. FIM equipment has incorrect mapping between data input and output to FMS

STPA-F.FC2.2.3.1. FIM Equipment must ensure accurate translation from flight crew inputs to FMS (or other control surface avionics) output (Allocated to: FIM Automation)

STPA-F.FC2.2.3.2. FIM Equipment must ensure accurate translation from datalink inputs to FMS (or other control surface avionics) output. Datalink is not currently part of FIM design but may be in the future (Allocated to: FIM Automation)

STPA-F.FC2.3. ATC delivers incorrect IM clearance

STPA-F.FC2.3.1. See UCA 14.M-17.M, UCA 14.AB, UCA15.AB, UCA14.T-16.T

STPA-F.FC2.3.1.1. See UCA 14.M-17.M, UCA 14.AB, UCA15.AB, UCA14.T-16.T (Allocated to: System Requirements)

Unsafe Control Action: UCA.FC.3. Flight crew executes IM clearance with incorrect parameters (e.g. wrong speed, incorrect turn, incorrect Spacing Goal Type) ↑[H-1]

STPA-F.FC3.1. Flight crew incorrectly implements IM parameters [Inadequate process model of IM operations]

STPA-F.FC3.1.1. Flight crew incorrectly interprets IM parameters. For example, ATC requests "Precisely 60 second spacing" but crew interprets "no less than 60 second spacing"

STPA-F.FC3.1.1.1. ATC must grant IM clearances in clear, concise, and consistent format (Allocated to: ATC, FAA Procedures)

STPA-F.FC3.1.1.2. Flight crew must verify IM clearance and repeat parameters when accepting IM clearances (Allocated to: Flight Crew)

STPA-F.FC3.1.2. Flight crew incorrectly inputs IM parameters into FIM equipment. For example, the different between precise, bounded, and no-less-than spacing is unclear in FIM user interface

STPA-F.FC3.1.2.1. Flight crew must be able to enter IM clearance information in a minimal amount of time and with minimal errors. (Allocated to: Flight Crew, FIM User interface)

STPA-F.FC3.1.2.2. FIM Equipment must provide clear, distinguishable alternative among different clearance types (Allocated to: FIM User interface)

STPA-F.FC3.1.2.3. FIM Equipment must clearly demark IM parameters, including initiation point, termination point, spacing type, and others. (Allocated to: FIM User interface)

STPA-F.FC3.2. Aircraft cannot achieve the desired IM parameters [Inadequate actuator operation]

STPA-F.FC3.2.1. Aircraft cannot achieve IM points in inadequate time due to environmental conditions

STPA-F.FC3.2.1.1. See ATC and Flight Crew monitoring and surveillance requirements for environmental conditions in UCA analysis list below. (Allocated to: System Requirements)

STPA-F.FC3.2.2. Aircraft cannot achieve IM points in inadequate time due to degraded performance

STPA-F.FC3.2.2.1. See ATC and Flight Crew monitoring and surveillance requirements for degraded performance in UCA analysis list below. (Allocated to: System Requirements)

STPA-F.FC3.2.3. Precision or accuracy of surveillance is worse than required navigation performance necessary to achieve IM points at desired time.

STPA-F.FC3.2.3.1. Accuracy of surveillance must be commensurate with required navigation performance in IM clearance points. (Allocated to: ADS-B, GNSS, Radar)

STPA-F.FC3.2.3.2. See ATC and Flight Crew monitoring and surveillance requirements for aircraft states and navigation in UCA analysis list below. (Allocated to: System Requirements)

STPA-F.FC3.3. ATC gives incorrect IM parameters

STPA-F.FC3.3.1. See UCA 14.M-17.M, UCA 14.AB, UCA15.AB, UCA14.T-16.T

STPA-F.FC3.3.1.1. See UCA 14.M-17.M, UCA 14.AB, UCA15.AB, UCA14.T-16.T (Allocated to: System Requirements)

Unsafe Control Action: UCA.FC.4. Flight crew executes IM clearance instead of other maneuver, where other maneuver is necessary to maintain separation ↑[H-1]

STPA-F.FC4.1. Timing of different clearances leads to Flight Crew executing IM in lieu of other clearance [Inadequate process model of airspace and procedures]

STPA-F.FC4.1.1. IM clearance comes immediately before (or after) other clearance and flight crew elects to execute IM clearance

STPA-F.FC4.1.1.1. The following requirement must be analyzed to ensure that it is consistent with FAA policies (Allocated to: System Requirements)

STPA-F.FC4.1.1.2. Flight crew must request amended clearance or ask for clarification if multiple clearances are granted within TBD seconds (Allocated to: Flight Crew)

STPA-F.FC4.1.2. FIM equipment is more prominent than other equipment, visually or aurally. Thus crew executes IM clearance when it should execute other maneuver

STPA-F.FC4.1.2.1. FIM equipment must not interfere with flight crew ability to resolve conflict (Allocated to: FIM Automation, System requirement)

STPA-F.FC4.1.2.2. Conflict resolution tools take precedence over FIM equipment on flight deck. This requirement may include visual or aural prominence (Allocated to: FIM user interface, Other system user interfaces)

STPA-F.FC4.1.3. ATC or flight crew fixation on spacing and sequencing goals at the expense of conflict detection and resolution

STPA-F.FC4.1.3.1. Conflict detection and resolution takes precedence over IM sequencing and spacing (Allocated to: ATC, Flight Crews, FAA Procedures)

STPA-F.FC4.1.4. ATC or flight crew fixation on specific type(s) of IM clearance over other type(s) of IM clearances

STPA-F.FC4.1.4.1. See FC UCA F.2 (Allocated to: See FC UCA F.2)

STPA-F.FC4.2. FIM equipment overrides other flight instruction

STPA-F.FC4.2.1. For example, flight crew enters new flight plan into FMS to prevent/avoid conflict after an IM clearance has started, but FIM equipment continues flying IM

STPA-F.FC4.2.1.1. Updated FMS flight plans override IM clearances (Allocated to: Software or hardware architecture, Software I/O)

STPA-F.FC4.2.1.2. FIM equipment must notify the flight crew that its IM trajectory has been cancelled (Allocated to: FIM Automation)

STPA-F.FC4.2.2. FIM equipment overrides a flight crew that begins to manually fly aircraft maneuver

STPA-F.FC4.2.2.1. FIM equipment must not override manual flight crew inputs to control systems. This includes yoke, side stick, or other features of the aircraft.

(Allocated to: FIM Automation, FMS, Software system architecture)

STPA-F.FC4.2.3. FIM equipment overrides aircraft automation flying a resolution alert maneuver (this is generally not part of current aircraft designs but may be in the future)

STPA-F.FC4.2.3.1. If the aircraft has automated conflict resolution control capability, FIM equipment must not override automatic conflict resolution maneuvers. (Allocated to: FIM Automation, FMS, Software system architecture)

STPA-F.FC4.3. ATC issues IM clearance instead of other necessary maneuver

STPA-F.FC4.3.1. See ATC UCA 17.M

STPA-F.FC4.3.1.1. See ATC UCA 17.M (Allocated to: System Requirements)

Unsafe Control Action: UCA.FC.5. Flight crew executes IM clearance outside of performance bounds or at extrema of performance bounds ↑[H-3; H-4]

STPA-F.FC5.1. Flight crew incorrectly interprets an otherwise correct ATC-issued clearance (see below for ATC unsafe actions) [Inadequate model of aircraft, FIM and other automation]

STPA-F.FC5.1.1. Flight crew rotely accepts IM clearance without checking against aircraft performance. This could be due to many past IM clearances without a problem, in addition to lack of a procedure or automated check

STPA-F.FC5.1.1.1. Flight crew must verify that ATC-issued IM clearance is within allowed aircraft performance envelope (Allocated to: Flight Crew)

STPA-F.FC5.1.2. Flight crew enters incorrect parameter that causes exceedance of performance

STPA-F.FC5.1.2.1. FIM equipment (or FMS or other control system) must reject flight crew-input of IM parameters that exceed aircraft capability (Allocated to: FIM, FMS, software architecture)

STPA-F.FC5.1.2.2. FIM equipment (or FMS or other control system) must reject datalink-input of IM parameters that exceed aircraft capability. Current FIM design does not include datalink capability but may in the future. (Allocated to: FIM, FMS, software architecture)

STPA-F.FC5.1.2.3. FIM equipment (or FMS or other control systems) must notify flight crew of exceedance due to flight crew or datalink input (Allocated to: FIM, FMS, software architecture)

STPA-F.FC5.1.3. IM clearances are given in different terms than normal safety/performance bounds. For example, overspeed and stall are given in terms of airspace, while IM clearances are given in separation times, achievement points, etc.

STPA-F.FC5.1.3.1. System must provide a means for converting IM clearance parameters into variables that are consistent with standard aircraft performance envelope(s). This includes mapping spacing requirements, initiation and termination points into aircraft speeds, required turn radius, etc. (Allocated to: System Requirement)

STPA-F.FC5.1.4. Flight crew or ATC has difficulty "converting" IM clearance parameters into aircraft performance

STPA-F.FC5.1.4.1. Flight crew must verify that IM clearance parameters result in an aircraft trajectory that is within allowed aircraft performance envelope (Allocated to: Flight Crew)

STPA-F.FC5.2. FIM equipment incorrectly suggests or implements IM clearance and flight crew or other systems do not check it [Inadequate process model of automation]

STPA-F.FC5.2.1. FIM equipment instructs aircraft to achieve separation without

consideration of stall, overspeed, turn radius, or other limits.

STPA-F.FC5.2.1.1. FIM equipment must not suggest or implement IM clearance parameters that exceed aircraft performance or safety limits (Allocated to: FIM Automation)

STPA-F.FC5.2.2. FMS or other systems do not check or cannot override FIM instructions

STPA-F.FC5.2.2.1. FMS (or other control systems) may override FIM instructions when FIM instructions exceed allowed aircraft performance (Allocated to: FMS, software architecture)

STPA-F.FC5.2.2.2. FMS (or other control systems) must notify flight crew of exceedance due to FIM instruction (Allocated to: FMS, software architecture)

STPA-F.FC5.3. ATC grants IM clearance that is outside bounds of aircraft performance

STPA-F.FC5.3.1. See UCA 16.M, UCA 15.AB, UCA 15.T

STPA-F.FC5.3.1.1. See UCA 16.M, UCA 15.AB, UCA 15.T (Allocated to: System Requirements)

Unsafe Control Action: UCA.FC.6. Flight crew executes IM clearance instead of other maneuver, where other maneuver is necessary to avoid inclement weather, terrain, or restricted airspace ↑[H-2; H-5]

STPA-F.FC6.1. Flight crew maintains incorrect process model of airspace and objectives and therefore makes incorrect decision regarding IM

STPA-F.FC6.1.1. Flight crew is unaware of inclement weather in or adjacent to trajectory path

STPA-F.FC6.1.1.1. Flight crew must remain vigilant of inclement weather per regular airmanship standards (Allocated to: Flight Crew)

STPA-F.FC6.1.1.2. ATC must notify flight crews of inclement weather (Allocated to: ATC, NWS)

STPA-F.FC6.1.1.3. Flight crew must inform ATC of encounter with inclement weather. This requirement is to ensure that ATC and other flight crews have current and accurate process models of airspace (Allocated to: Flight Crew)

STPA-F.FC6.1.2. Flight crew is unaware of restricted airspace in trajectory path

STPA-F.FC6.1.2.1. ATC must notify flight crews of restricted airspace (Allocated to: ATC, US Government, FAA Procedures)

STPA-F.FC6.1.2.2. ATC must vector aircraft away from or around restricted airspace, according to classification of airspace and aircraft. ATC may include rationale for clearance to ensure that crews are aware of restricted airspace. (Allocated to: ATC, FAA Procedures)

STPA-F.FC6.1.3. Flight crew prioritizes IM separation and sequencing over avoiding inclement weather

STPA-F.FC6.1.3.1. Avoidance of inclement weather takes precedence over IM sequencing and spacing (Allocated to: System requirement)

STPA-F.FC6.1.3.2. See ATC requirements for NWS and alerting requirements relative to IM-related automation (Allocated to: ATC, NWS)

STPA-F.FC6.1.3.3. To the extent that weather alerting systems exist on the flight deck, weather alerting systems should be more prominent than FIM equipment (Allocated to: FIM User Interface, Other flight deck user interfaces)

STPA-F.FC6.1.3.4. Flight deck weather alerting systems should provide false alerts no more than TBD% of total alerts. This requirement is intended to ensure that flight crews heed weather alert systems (Allocated to: Flight deck requirement)

STPA-F.FC6.1.4. Flight crew prioritizes IM separation and sequencing over avoiding restricted airspace

STPA-F.FC6.1.4.1. Avoidance of restricted airspace takes precedence over IM

sequencing and spacing (Allocated to: System requirement)

STPA-F.FC6.1.4.2. See ATC requirements for airspace requirements relative to IM-related automation (Allocated to: ATC, FAA)

STPA-F.FC6.1.4.3. To the extent that restricted airspace alerting systems exist on the flight deck, restricted airspace alerting systems should be more prominent than FIM equipment (Allocated to: FIM User Interface, Other flight deck user interfaces)

STPA-F.FC6.2. FIM equipment does not account for airspace hazards but flight crew does not recognize this limitation in design [Inadequate process model of automation]

STPA-F.FC6.2.1. FIM Equipment does not "see" inclement weather. That is, FIM Equipment is not programmed to account for inclement weather when calculating IM trajectory parameters

STPA-F.FC6.2.1.1. Flight crew is responsible for identifying and avoiding weather that could cause loss of control or damage to aircraft. (Allocated to: Flight Crew)

STPA-F.FC6.2.1.2. System must allow flight crew to override FIM equipment instructions in the presence of inclement weather (Allocated to: FIM Automation, FMS, Software system architecture)

STPA-F.FC6.2.1.3. ATC and weather service have additional requirements for surveillance and forecasting weather. See requirements in UCA 17.M and elsewhere. (Allocated to: System Requirements)

STPA-F.FC6.2.2. FIM Equipment does not "see" restricted airspace. That is, FIM Equipment is not programmed to account for restricted airspace when calculating IM trajectory parameters

STPA-F.FC6.2.2.1. Flight crew (and ATC) is responsible for identifying and avoiding restricted airspace. (Allocated to: Flight Crew)

STPA-F.FC6.2.2.2. System must allow flight crew to override FIM equipment instructions in the presence of inclement weather (Allocated to: FIM Automation, FMS, Software system architecture)

STPA-F.FC6.2.2.3. ATC and weather service have additional requirements for surveillance and forecasting weather. See requirements in UCA 17.M and elsewhere. (Allocated to: System Requirements)

STPA-F.FC6.3. ATC issues IM clearance instead of other necessary maneuver

STPA-F.FC6.3.1. See ATC UCA 17.M

STPA-F.FC6.3.1.1. See ATC UCA 17.M (Allocated to: System Requirements)

Unsafe Control Action: UCA.FC.7. Flight crew executes IM clearance too long after it has been requested/accepted and traffic pattern has changed ↑[H-1]

STPA-F.FC7.1. Flight crew takes too long to implement ATC request, either manually or using FIM automation

STPA-F.FC7.1.1. Flight crew is involved in other tasks between accepting IM clearance and actually implementing it

STPA-F.FC7.1.1.1. See ATC requirements for monitoring compliance with IM clearances (Allocated to: System Requirements)

STPA-F.FC7.1.2. Flight crew has incorrect understanding of conditional clearance. That is, crew believes starting point is supposed to be delayed or is later than ATC expectations

STPA-F.FC7.1.2.1. ATC must grant IM clearances in clear, concise, and consistent format (Allocated to: ATC, FAA Procedures)

STPA-F.FC7.1.2.2. Flight crew must verify IM clearance and repeat parameters when accepting IM clearances (Allocated to: Flight Crew)

STPA-F.FC7.1.2.3. ATC must use different terminology for the different types of IM clearances (Allocated to: ATC, FAA Procedures)

STPA-F.FC7.1.2.4. IM clearance terminology must be clearly distinguishable from other types of clearances (Allocated to: ATC, FAA Procedures)

STPA-F.FC7.1.2.5. Different parameters of IM clearance must be distinguishable from one another, including IM clearance types and IM clearance parameters (Allocated to: ATC, FAA Procedures)

STPA-F.FC7.1.3. Entering data into FIM Equipment takes too long

STPA-F.FC7.1.3.1. Flight crew must enter IM clearance information into FIM equipment within TBD seconds of receiving (and accepting) clearance (Allocated to: Flight Crew)

STPA-F.FC7.1.3.2. Flight crew must be able to enter IM clearance information in a minimal amount of time and with minimal errors. (Allocated to: Flight Crew, FIM User interface)

STPA-F.FC7.1.3.3. FIM Equipment must provide clear, distinguishable alternative among different clearance types (Allocated to: FIM User interface)

STPA-F.FC7.1.3.4. FIM Equipment must clearly demark IM parameters, including initiation point, termination point, spacing type, and others. (Allocated to: FIM User interface)

STPA-F.FC7.2. FIM Equipment takes longer than expected to implement trajectory modifications, and flight crew (and/or ATC) fails to monitor compliance [Inadequate process model of automation]

STPA-F.FC7.2.1. FIM Equipment takes too long to calculate trajectory modifications

STPA-F.FC7.2.1.1. FIM Equipment must calculate trajectory modifications within TBD seconds of receiving input or request for FIM trajectory (Allocated to: FIM Automation)

STPA-F.FC7.2.1.2. FIM Equipment must notify flight crew of delay or inability to calculate trajectory within time constraints. (Allocated to: FIM Automation)

STPA-F.FC7.2.2. FIM Equipment receives direct datalink clearance too late due to delayed transmission (This assumes that future implementations of FIM use CPDLC or similar technology)

STPA-F.FC7.2.2.1. Transmission of datalink must take no longer than TBD seconds from ground center to FIM equipment. (This requirement is for potential future implementations of FIM that use direct data communication between ground and flight deck automation) (Allocated to: Ground center, FIM equipment, communication networks)

STPA-F.FC7.2.2.2. Datalink system must protect against jamming, interference, and latency (Allocated to: Datalink)

STPA-F.FC7.3. ATC delays request of IM clearance

STPA-F.FC7.3.1. See ATC UCA analyses 18.M, 19.M, 18.AB, 18.T

STPA-F.FC7.3.1.1. See ATC UCA analyses 18.M, 19.M, 18.AB, 18.T (Allocated to: System Requirements)

Unsafe Control Action: UCA.FC.8. Flight crew executes IM clearance too long after it has been requested/accepted and environment has changed ↑[H-1; H-2]

STPA-F.FC8.1. Flight crew takes too long to implement ATC request, either manually or using FIM automation

STPA-F.FC8.1.1. Flight crew is involved in other tasks between accepting IM clearance and actually implementing it

STPA-F.FC8.1.1.1. See ATC requirements for monitoring compliance with IM clearances (Allocated to: System Requirements)

STPA-F.FC8.1.2. Flight crew has incorrect understanding of conditional clearance. That is, crew believes starting point is supposed to be delayed or is later than ATC expectations

STPA-F.FC8.1.2.1. ATC must grant IM clearances in clear, concise, and consistent format (Allocated to: ATC, FAA Procedures)

STPA-F.FC8.1.2.2. Flight crew must verify IM clearance and repeat parameters when accepting IM clearances (Allocated to: Flight Crew)

STPA-F.FC8.1.2.3. ATC must use different terminology for the different types of IM clearances (Allocated to: ATC, FAA Procedures)

STPA-F.FC8.1.2.4. IM clearance terminology must be clearly distinguishable from other types of clearances (Allocated to: ATC, FAA Procedures)

STPA-F.FC8.1.2.5. Different parameters of IM clearance must be distinguishable from one another, including IM clearance types and IM clearance parameters (Allocated to: ATC, FAA Procedures)

STPA-F.FC8.1.3. Entering data into FIM Equipment takes too long

STPA-F.FC8.1.3.1. Flight crew must enter IM clearance information into FIM equipment within TBD seconds of receiving (and accepting) clearance (Allocated to: Flight Crew)

STPA-F.FC8.1.3.2. Flight crew must be able to enter IM clearance information in a minimal amount of time and with minimal errors. (Allocated to: Flight Crew, FIM User interface)

STPA-F.FC8.1.3.3. FIM Equipment must provide clear, distinguishable alternative among different clearance types (Allocated to: FIM User interface)

STPA-F.FC8.1.3.4. FIM Equipment must clearly demark IM parameters, including initiation point, termination point, spacing type, and others. (Allocated to: FIM User interface)

STPA-F.FC8.2. FIM Equipment takes longer than expected to implement trajectory modifications, and flight crew (and/or ATC) fails to monitor compliance [Inadequate process model of automation]

STPA-F.FC8.2.1. FIM Equipment takes too long to calculate trajectory modifications

STPA-F.FC8.2.1.1. FIM Equipment must calculate trajectory modifications within TBD seconds of receiving input or request for FIM trajectory (Allocated to: FIM Automation)

STPA-F.FC8.2.1.2. FIM Equipment must notify flight crew of delay or inability to calculate trajectory within time constraints. (Allocated to: FIM Automation)

STPA-F.FC8.2.2. FIM Equipment receives direct datalink clearance too late due to delayed transmission (This assumes that future implementations of FIM use CPDLC or similar technology)

STPA-F.FC8.2.2.1. Transmission of datalink must take no longer than TBD seconds from ground center to FIM equipment. (This requirement is for potential future implementations of FIM that use direct data communication between ground and flight deck automation) (Allocated to: Ground center, FIM equipment, communication networks)

STPA-F.FC8.2.2.2. Datalink system must protect against jamming, interference, and latency (Allocated to: Datalink)

STPA-F.FC8.3. Flight crew unaware of environment change and executes IM clearance anyway [Inadequate process model of airspace]

STPA-F.FC8.3.1. Flight crew and ATC have different understanding of environment

STPA-F.FC8.3.1.1. ATC must notify flight crew of inclement weather in, or adjacent to, its predicted path (Allocated to: ATC)

STPA-F.FC8.3.1.2. ATC must notify flight crew of predicted inclement weather from NWS forecasts (Allocated to: ATC)

STPA-F.FC8.4. Flight crew intentionally delays IM execution due to weather, but ATC is unaware [Inadequate process model of FAA procedures]

STPA-F.FC8.4.1. Flight crew "sees" weather, while ATC only has access to surveillance and models

STPA-F.FC8.4.1.1. Flight crew must notify ATC of inclement weather (Allocated to: Flight Crew)

STPA-F.FC8.4.2. Flight crew and ATC may have access to different weather surveillance and forecasting

STPA-F.FC8.4.2.1. Flight crew may have access to NWS weather surveillance and forecasts. This might not be feasible but is a suggested mitigation for ensuring that ATC and flight crews have consistent understanding of the airspace. This might be too resource-intensive for flight crews (Allocated to: NWS)

STPA-F.FC8.5. ATC delays request of IM clearance

STPA-F.FC8.5.1. See ATC UCA analyses 22.M

STPA-F.FC8.5.1.1. See ATC UCA analyses 22.M (Allocated to: System Requirements)

Unsafe Control Action: UCA.FC.9. Flight crew executes IM clearance too soon before it is actually accepted or expected by ATC ↑[H-1]

STPA-F.FC9.1. Flight crew anticipation of IM clearance [Inadequate control algorithm or model of IM procedure]

STPA-F.FC9.1.1. IM operations become so common that flight crews believe they will always be issued

STPA-F.FC9.1.1.1. Flight crew must only modify aircraft trajectories per ATC clearances, resolution advisories/alerts, or due to inclement weather, or severely degraded aircraft capability. This requirement is per standard FAA policies (JO 7110.65U) and assumes that FIM equipment only implements IM clearances when it receives input from flight crew. (Allocated to: Flight Crew, FAA Procedures)

STPA-F.FC9.1.1.2. Flight crew must confirm ATC clearances, OR (Allocated to: Flight Crew)

STPA-F.FC9.1.1.3. Flight crew must notify ATC of resolution advisory (or alert), OR (Allocated to: Flight Crew)

STPA-F.FC9.1.1.4. Flight crew must request amended clearance (Allocated to: Flight Crew)

STPA-F.FC9.1.2. Flight crew anticipation of workload

STPA-F.FC9.1.2.1. FIM flight crew must request amended clearance when the crew feels it cannot or should not reach termination point (Allocated to: Flight Crew)

STPA-F.FC9.1.2.2. See ATC UCA analysis for monitoring and surveillance requirements (Allocated to: System Requirements)

STPA-F.FC9.2. Flight crew simply executes clearance without verifying and confirming, and ATC assumes that aircraft is not flying IM operation [Inadequate process model of IM operations]

STPA-F.FC9.2.1. Flight crew does not understand IM procedures or policies, or assumes IM procedure is different than typical ATC clearances (or typical FAA policy)

STPA-F.FC9.2.1.1. Flight crew must verify feasibility of IM clearance (Allocated to: Flight Crew)

STPA-F.FC9.2.1.2. Flight crew must confirm execution of IM clearance to ATC (Allocated to: Flight Crew)

STPA-F.FC9.2.2. Datalink sends IM clearance message to FIM automation before ATC confirms clearance. Datalink is not part of the current implementation of FIM (to the authors' knowledge) but may be in future implementations

STPA-F.FC9.2.2.1. Datalink messages for requesting IM clearances must not be sent until ATC approval, OR (Allocated to: ATC, Datalink)

STPA-F.FC9.2.2.2. Datalink system must provide notification to ATC that IM clearance

has been issued (Allocated to: Datalink user interface)

STPA-F.FC9.3. FIM autonomously calculates and implements IM clearance [Inadequate process model of automation]

STPA-F.FC9.3.1. Note: Current implementation of FIM requires flight crew input to initialize and execute IM

STPA-F.FC9.3.1.1. To the extent that FIM equipment autonomously generates IM parameters, IM execution requires flight crew approval, OR (Allocated to: Flight Crew, FIM Automation)

STPA-F.FC9.3.1.2. FIM equipment must provide notification to Flight crew that IM clearance is being executed (Allocated to: FIM user interface)

STPA-F.FC9.3.1.3. Flight crew must notify ATC of IM execution (Allocated to: Flight Crew)

Unsafe Control Action: UCA.FC.10. Flight crew continues IM clearance after termination point and other aircraft trajectories' separation(s) are based on IM aircraft stopping at termination point ↑[H-1]

STPA-F.FC10.1. Flight crew does not implement or correctly understand termination point [Inadequate process model of aircraft, airspace, and IM procedure]

STPA-F.FC10.1.1. Flight crew does not input termination point because ATC does not include it in IM clearance

STPA-F.FC10.1.1.1. ATC must clearly state termination parameters as part of original IM clearance, OR (Allocated to: ATC, FAA Procedures)

STPA-F.FC10.1.1.2. ATC must instruct flight crew to terminate IM clearance once objectives are achieved (Allocated to: ATC, FAA Procedures)

STPA-F.FC10.1.2. Flight crew believes IM spacing objectives are indefinite

STPA-F.FC10.1.2.1. Flight crew must verify that IM clearance has a termination point during acceptance communication with ATC (Allocated to: Flight Crew)

STPA-F.FC10.1.3. There is difficulty or lack of clarity in entering termination point (or other IM points) into FIM interface

STPA-F.FC10.1.3.1. FIM Equipment must provide clear, distinguishable alternative among different clearance types (Allocated to: FIM User interface)

STPA-F.FC10.1.3.2. FIM Equipment must clearly demark IM parameters, including initiation point, termination point, spacing type, and others. (Allocated to: FIM User interface)

STPA-F.FC10.1.3.3. FIM Equipment must notify flight crew of impending termination at least TBD seconds prior to termination point. (Allocated to: FIM Automation)

STPA-F.FC10.1.4. Flight crew continues IM clearance because it is unclear what the aircraft is supposed to do upon termination of IM clearance

STPA-F.FC10.1.4.1. ATC must be ready with follow-up clearances at least TBD seconds prior to termination of IM clearance (Allocated to: ATC)

STPA-F.FC10.1.4.2. ATC must communicate follow-up clearances with sufficient time to allow flight crew to implement new trajectory following termination of IM clearance (Allocated to: ATC)

STPA-F.FC10.2. FIM equipment does not calculate that aircraft has finished FIM clearance and flight crew does not understand that clearance should have been terminated [Inadequate process model of FIM automation]

STPA-F.FC10.2.1. FIM equipment received incorrect termination point from flight crew

STPA-F.FC10.2.1.1. See above requirements for flight crew and FIM user interface (Allocated to: FIM Automation, Flight crew)

STPA-F.FC10.2.2. FIM equipment received incorrect termination point directly from ground via datalink. This is not part of current implementation of FIM but may be in the future.

STPA-F.FC10.2.2.1. IM message in datalink must be formatted in a consistent manner that matches FIM equipment inputs (Allocated to: Ground automation, FIM Automation)

STPA-F.FC10.2.2.2. System must protect against jamming, electromagnetic interference, and latency (Allocated to: Receivers, transponders, communication network)

STPA-F.FC10.2.3. FIM equipment has incorrect location of aircraft and therefore does not calculate that aircraft has finished IM clearance

STPA-F.FC10.2.3.1. Termination point tolerances must be commensurate with available surveillance accuracy (Allocated to: FIM Automation, surveillance systems)

STPA-F.FC10.2.4. Aircraft reaches termination point quicker than expected

STPA-F.FC10.2.4.1. Termination point tolerances must be commensurate with available navigation accuracy (Allocated to: FIM Automation, FMS)

STPA-F.FC10.2.4.2. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.FC10.2.4.3. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: ERAM, ADS-B)

STPA-F.FC10.2.4.4. IM-related ground automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related ground Automation)

STPA-F.FC10.2.4.5. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, ADS-B)

STPA-F.FC10.2.5. Surveillance is delayed or FIM equipment updates much faster (or slower) than surveillance updates

STPA-F.FC10.2.5.1. FIM equipment update rate must be synchronized with surveillance update rate, OR (Allocated to: ADS-B, Radar, FIM Automation)

STPA-F.FC10.2.5.2. FIM equipment must account for update rates in its trajectory modeling algorithm (Allocated to: FIM Automation)

STPA-F.FC10.2.5.3. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.FC10.2.5.4. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.FC10.3. ATC delivery of clearances is timed incorrectly

STPA-F.FC10.3.1. See UCA 18.M, UCA 18.AB, UCA 18.T and others

STPA-F.FC10.3.1.1. See UCA 18.M, UCA 18.AB, UCA 18.T and others (Allocated to: System Requirements)

Unsafe Control Action: UCA.FC.11. Flight crew terminates IM clearance before termination point and other aircraft trajectories' separation(s) are based on IM aircraft continuing to termination point ↑[H-1]

STPA-F.FC11.1. Flight crew does not implement or correctly understand termination point [Inadequate process model of aircraft, airspace, and IM procedure]

STPA-F.FC11.1.1. Flight crew does not input termination point because ATC does not include it in IM clearance

STPA-F.FC11.1.1.1. ATC must clearly state termination parameters as part of original IM clearance, OR (Allocated to: ATC, FAA Procedures)

STPA-F.FC11.1.1.2. ATC must instruct flight crew to terminate IM clearance once objectives are achieved (Allocated to: ATC, FAA Procedures)

STPA-F.FC11.1.2. Flight crew believes IM spacing objectives are indefinite

STPA-F.FC11.1.2.1. Flight crew must verify that IM clearance has a termination point during acceptance communication with ATC (Allocated to: Flight Crew)

STPA-F.FC11.1.3. There is difficulty or lack of clarity in entering termination point (or other IM points) into FIM interface

STPA-F.FC11.1.3.1. FIM Equipment must provide clear, distinguishable alternative among different clearance types (Allocated to: FIM User interface)

STPA-F.FC11.1.3.2. FIM Equipment must clearly demark IM parameters, including initiation point, termination point, spacing type, and others. (Allocated to: FIM User interface)

STPA-F.FC11.1.3.3. FIM Equipment must notify flight crew of impending termination at least TBD seconds prior to termination point. (Allocated to: FIM Automation)

STPA-F.FC11.1.4. Flight crew anticipates increased workload, clearance, or environmental factor and modifies FIM prematurely [Inadequate process model of IM operations, contextual factors]

STPA-F.FC11.1.4.1. FIM flight crew must request amended clearance when the crew feels it cannot or should not reach termination point (Allocated to: Flight Crew)

STPA-F.FC11.1.4.2. See ATC UCA analysis for monitoring and surveillance requirements (Allocated to: System Requirements)

STPA-F.FC11.1.5. Flight crew (correctly) reacts to other clearance or resolution advisory but fails to notify ATC

STPA-F.FC11.1.5.1. Flight crew must notify ATC of deviation from IM clearance and include rationale for deviation. Including rationale for deviation is intended to ensure that ATC has accurate model of aircraft and airspace conditions (Allocated to: Flight Crew)

STPA-F.FC11.2. FIM equipment incorrectly calculates that aircraft has finished FIM clearance and flight crew does not understand that clearance should have been terminated [Inadequate process model of FIM automation]

STPA-F.FC11.2.1. FIM equipment received incorrect termination point from flight crew

STPA-F.FC11.2.1.1. See above requirements for flight crew and FIM user interface (Allocated to: FIM Automation, Flight crew)

STPA-F.FC11.2.2. FIM equipment received incorrect termination point directly from ground via datalink. This is not part of current implementation of FIM but may be in the future.

STPA-F.FC11.2.2.1. IM message in datalink must be formatted in a consistent manner that matches FIM equipment inputs (Allocated to: Ground automation, FIM Automation)

STPA-F.FC11.2.2.2. System must protect against jamming, electromagnetic interference, and latency (Allocated to: Receivers, transponders, communication network)

STPA-F.FC11.2.3. FIM equipment has incorrect location of aircraft and therefore does not calculate that aircraft has finished IM clearance

STPA-F.FC11.2.3.1. Termination point tolerances must be commensurate with available surveillance accuracy (Allocated to: FIM Automation, surveillance systems)

STPA-F.FC11.2.4. Aircraft reaches termination point quicker than expected

STPA-F.FC11.2.4.1. Termination point tolerances must be commensurate with available navigation accuracy (Allocated to: FIM Automation, FMS)

STPA-F.FC11.2.4.2. ADS-B must provide 0.1/0.3 NM (95%) accuracy. (Allocated to: ADS-B, GNSS)

STPA-F.FC11.2.4.3. The design must protect against use of data that is not in the 95% accuracy range. (Allocated to: ERAM, ADS-B)

STPA-F.FC11.2.4.4. IM-related ground automation must check when surveillance data is outside of 95% requirement. (Allocated to: IM-related ground Automation)

STPA-F.FC11.2.4.5. System must have access to fused track data that includes sources other than ADS-B (Allocated to: ERAM, ADS-B)

STPA-F.FC11.2.5. Surveillance is delayed or FIM equipment updates much faster (or slower) than surveillance updates

STPA-F.FC11.2.5.1. FIM equipment update rate must be synchronized with surveillance update rate, OR (Allocated to: ADS-B, Radar, FIM Automation)

STPA-F.FC11.2.5.2. FIM equipment must account for update rates in its trajectory modeling algorithm (Allocated to: FIM Automation)

STPA-F.FC11.2.5.3. ADS-B surveillance must be updated every 1 second (Allocated to: ADS-B, GNSS)

STPA-F.FC11.2.5.4. Primary radar surveillance must be updated at least every 12 seconds (Allocated to: Radar, beacons)

STPA-F.FC11.3. ATC delivery of clearances is timed incorrectly

STPA-F.FC11.3.1. See UCA 18.M, UCA 18.AB, UCA 18.T and others

STPA-F.FC11.3.1.1. See UCA 18.M, UCA 18.AB, UCA 18.T and others (Allocated to: System Requirements)