NASA/CR–2012-217553

Safety Assurance in NextGen

Cody Harrison Fleming, Melissa Spencer, and Nancy Leveson
Massachusetts Institute of Technology, Cambridge, Massachusetts

Chris Wilkinson
Honeywell Aerospace Advanced Technology, Columbia, Maryland

March 2012

NASA/CR–2012-217553

Safety Assurance in NextGen

Cody Harrison Fleming, Melissa Spencer, and Nancy Leveson
Massachusetts Institute of Technology

Chris Wilkinson
Honeywell Aerospace Advanced Technology, Columbia, Maryland

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

Prepared for Langley Research Center
under Contract NNL10AA13C

March 2012

Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320
443-757-5802

Table of Contents

List of Figures

List of Tables

1 Introduction

This technical report is one of the deliverables for a NASA-sponsored research project where an innovative approach to hazard analysis and safety assurance based on systems and control theory is being demonstrated, evaluated, and compared both to the more traditional approaches from decades past as well as newer certification approaches used by the FAA and EUROCONTROL. The overall goal is to develop more powerful tools for assuring aircraft and airspace safety as changes are made in the National Airspace System.

Traditional approaches to safety analysis assume that accidents are caused by component failures. They therefore focus on reliability analysis techniques, particularly fault tree or event tree analysis. The goal is to determine scenarios of component failures that together will lead to an accident or loss event. Failures may be single or multiple and are usually assumed to be random. After the component failure scenarios are identified, engineers use fault tolerance or fail-safe techniques to protect against hazards caused by the identified failures and to increase individual component integrity. A fly-fix-fly approach augments the design techniques with investigation of accidents in great depth and recommendations made from the results to prevent reoccurrences.

This approach has been very effective in the past because there have been relatively few changes in the basic aircraft or air traffic control design; the systems are relatively simple; technology has changed slowly; engineers have been able to use very conservative design approaches; and the system components can be effectively decoupled so that interactions can be anticipated, simplified, and guarded against. This approach, by itself, is becoming less effective, however, as these assumptions start to be violated.

Software is increasingly an important part of systems and allows enormously more complex systems to be constructed. The potential for accidents arising from unsafe interactions among non-failed components, i.e., unplanned systems and software behavior, is increasing. NextGen components, for example, may involve more than just one aircraft and one onboard system but rather span aircraft, ground controllers, space-based systems, and communication links between aircraft. The traditional hardware-oriented safety engineering techniques focusing on failures do not handle these types of new accident causes.

In addition, humans are changing from direct control to assuming supervisory roles over automation, which requires more cognitively complex human decision-making. Like software, the changing roles of pilots and ground controllers introduces the potential for new causes of accidents that are not well handled by today’s failure-oriented and hardware-oriented approaches.

To deal with these new accident causes, we have developed a more comprehensive accident causality model based on systems theory as well as analysis tools constructed from this new model. The model and tools include the causes of accidents considered in the past, but also consider the new accident causality factors that are increasingly occurring today.

In this report, a comparison is made of the approach and results of our new systems-theoretic approach to safety assurance and certification with the safety analysis and certification approach being used for NextGen procedures. For this case study, we selected a new ATC procedure, called ATSA-ITP (Airborne Traffic Situational Awareness In-Trail Procedures) because the safety analysis had already been performed and safety requirements generated. We then performed our own analysis using our new systems-theoretic approach. We first describe and critique the results of the ITP safety analysis documented in DO-312 (Safety, Performance and Interoperability Requirements Document for the In-Trail Procedure in the Oceanic Airspace (ATSA-ITP) Application) [4]. We then describe our new approach and the results. Finally, we conclude with a summary of the results.

2 Safety and Hazard Analysis Techniques for NextGen

In this section, a brief introduction to the case study is first presented and then the methods used to assure its safety by the FAA and Eurocontrol in DO-312. The next section describes the new approach and its results. The last section of the report provides a formal comparison of the two approaches to certifying the safety of NextGen components.

2.1 Background: NextGen and ATSA-ITP

According to the FAA, NextGen represents the transformation of the National Airspace System through an "evolution from the ground-based systems of air traffic control to a satellite-based system of air traffic management" [9]. The overarching goals of NextGen are to (1) reduce flight delays by improving airport operations; (2) improve aviation's impact on the environment through reduced CO2 emissions and fuel use; and (3) make the airspace safer via more precise tracking, improved information-sharing, and implementing a Safety Management System [10]. Airborne Traffic Situational Awareness In-Trail Procedure (ATSA-ITP, referred to herein as just ITP) is designed to achieve these objectives by enabling "aircraft that desire Flight Level changes in Procedural Airspace to achieve these changes on a more frequent basis, thus improving flight efficiency while maintaining safe seperation [sic] from other aircraft" [4]. ITP, within the larger framework of NextGen and its European counterpart SESAR, provides a real-world case study with which to compare the safety assurance philosophy and analytical techniques being proposed to those of the FAA, EUROCONTROL, and their associated organizations.

2.2 DO-312 Description

The purpose of DO-312 is to provide "the minimum operational, safety, and performance requirements and interoperability requirements for the implementation of enhanced Airborne Traffic Situational Awareness for 'In-Trail Procedure'" [4]. These requirements can be used for approval processes for hardware, software, and operational procedures including aircraft type design, aircraft operator approval, and Air Traffic Services (ATS). It is essentially a performance-based safety assurance document, where the appropriate[1] parts of the NAS must show compliance with minimal, quantitative functional performance levels. Development of the document can be broken into three basic parts: (1) Operational Services and Environment Description, (2) Safety and Performance Requirements, and (3) Interoperability Requirements. Each of theses parts is described below.

[1] Consideration of, and agreement on what is deemed appropriate for this kind of system is not necessarily straightforward, as our comparison and critique in Section 4 suggests.

2.2.1 Operational Services and Environment Description (OSED)

The OSED is concerned with developing and describing the services, functions, and procedures necessary to facilitate the ultimate goal of enabling an increased rate of Flight Level changes in Procedural (in this case transoceanic) Airspace. This part of the document defines the system architecture and the necessary stakeholders involved in operation. Appendix A of [4] provides an informative, detailed description of the ITP design along with several examples and the context in which the procedure should occur. A brief description and example is included here to assist the reader:

> "For a standard Flight Level change, the controller uses standard, procedure-based separation minima and procedures to ensure that separation will exist between an aircraft requesting a Flight Level change and all other aircraft at the initial, intermediate and requested Flight Levels. The ATSA-ITP was developed to enable either leading or following Same Track aircraft to perform a climb or descent to a requested Flight Level through Intervening Flight Levels that might otherwise be disallowed when using current standard separation minima. The ITP Equipment would allow the flight crew to determine if the criteria for an ITP request are met with respect to one or two Reference Aircraft at Intervening Flight Levels……Once these criteria are met, the flight crew may request an ITP, identifying the Reference Aircraft in the request. ATC would verify that the ITP and Reference Aircraft were Same Track and that the maximum Closing Mach Differential was not exceeded……If the controller then determines that separation minima will be met with all Other Aircraft, the climb or descent request may be granted. The controller does not determine or verify the separation distance from the Reference Aircraft." [4]

An example of one the six potential ITP maneuver geometries follows in Figure 1.

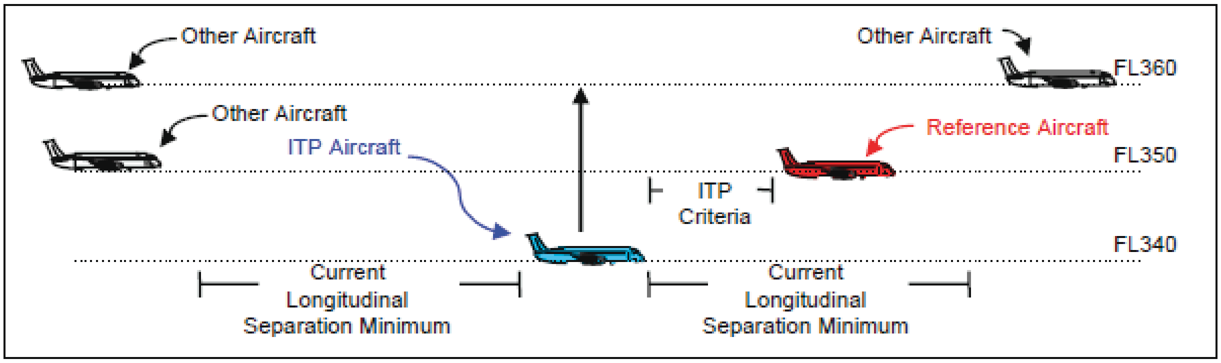


Figure 1: ITP Following-Climb [4]

OSED further defines the procedural means by which ITP must occur. It consists of four phases: the initiation phase, instruction phase, execution phase, and termination phase. From [4]:

1. ITP Initiation phase: The preparation for performing the application consists of realizing the desire and assessing the appropriateness for requesting an ITP maneuver by the flight crew. This includes the identification of the Reference Aircraft in the procedure and transmission of the ITP request to the ground controller.

2. ITP Instruction phase: The ITP clearance is issued by the controller, and reevaluated by the flight crew.
3. ITP Execution phase: The cleared ITP Aircraft performs the ITP maneuver, maintaining the required rate of climb/descent and speed as directed by the ITP clearance. Conducting an ITP maneuver is similar operationally to standard climbing/descending maneuvers.
4. ITP Termination phase: The procedure is terminated once the ITP Aircraft has achieved the requested Flight Level or an abnormal event results in premature termination of the ITP maneuver.

2.2.2 Safety and Performance Requirements (SPR)

Using the operational environment, or OSED, DO-312 derives safety and performance requirements via a Collision Risk Model of the expected state vectors of aircraft in the ATSA-ITP airspace, Operational Performance Assessment of all the surveillance aspects needed to satisfy the assumptions in the Collision Risk Model, and an Operational Safety Assessment of the potential hazards to which the constituents may be exposed.

We briefly reviewed the Collision Risk Model and are assuming that the analysis has been done rigorously and correctly. We also assume the associated Operational Performance Assessment appropriately correlates with the risk model. This report focuses on the safety/hazard analysis.

Figure 2 shows the connectivity between the various elements of the safety analysis, called the Operational Safety Assessment (OSA). The descriptions of these elements are provided from [4]:

- In the center of the model stands the Operational Hazard (OH), both expressed for the detected and undetected case at the boundary of the application. Hazards are identified by operational personnel using the application description and associated phases and actions as a reference, along with a consideration of potential abnormal events.
- On the right-hand side resides the Operational Hazard Assessment (OHA), from the boundary of the application up to the operational effects on the airspace. The OHA objective is to set the Safety Objective for the OH (for both the detected and undetected case). External Mitigation Means, identified in the OHA and used in the determination of the Safety Objectives, are converted into Operational Requirements in the OSED.
- The left-hand side depicts the Allocation of Safety Objectives and Requirements (ASOR) process, located inside the application. The objective of this activity is to allocate safety requirements to the airborne and ground domain in order to meet the safety objectives for each operational hazard. This is achieved by the identification of the Basic Causes leading to each hazard, their combination (shown in a Fault Tree) and the derived requirements. Internal Mitigation Means are identified to ensure the Safety Objectives are met; these become Safety Requirements if they are technical or Operational Requirements if they are procedural.

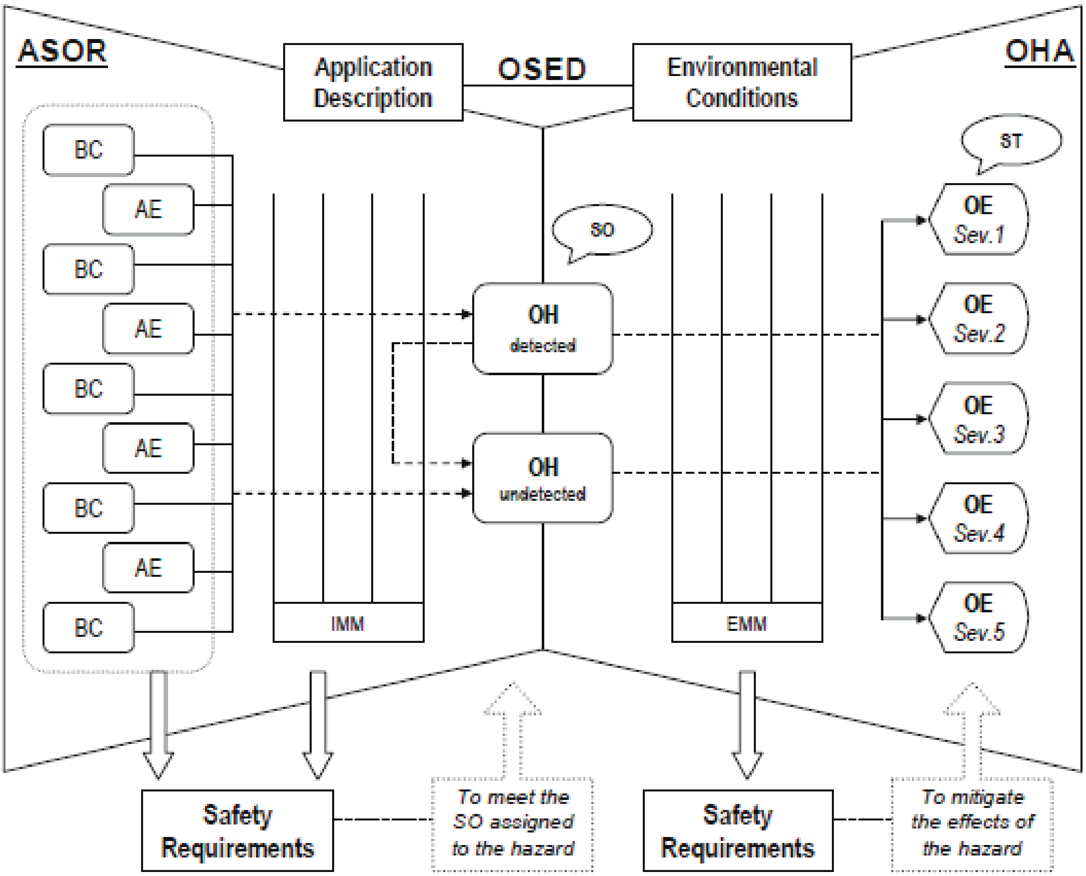


Figure 2: OSA Process Overview [4]

The Operational Hazard Assessment (OHA) on the right side of Figure 2 merits further description, as it provides a basis for comparison with the methods developed by MIT as well as other standards used throughout the aviation industry and other domains. There are four steps to conducting the OHA used in DO-312: (1) identify hazards, (2) allocate severity classes, (3) determine probability of occurrence (Pe), and (4) assign a safety objective. Figure 3 and the outline below describe this process flow along with brief definitions of the terms.

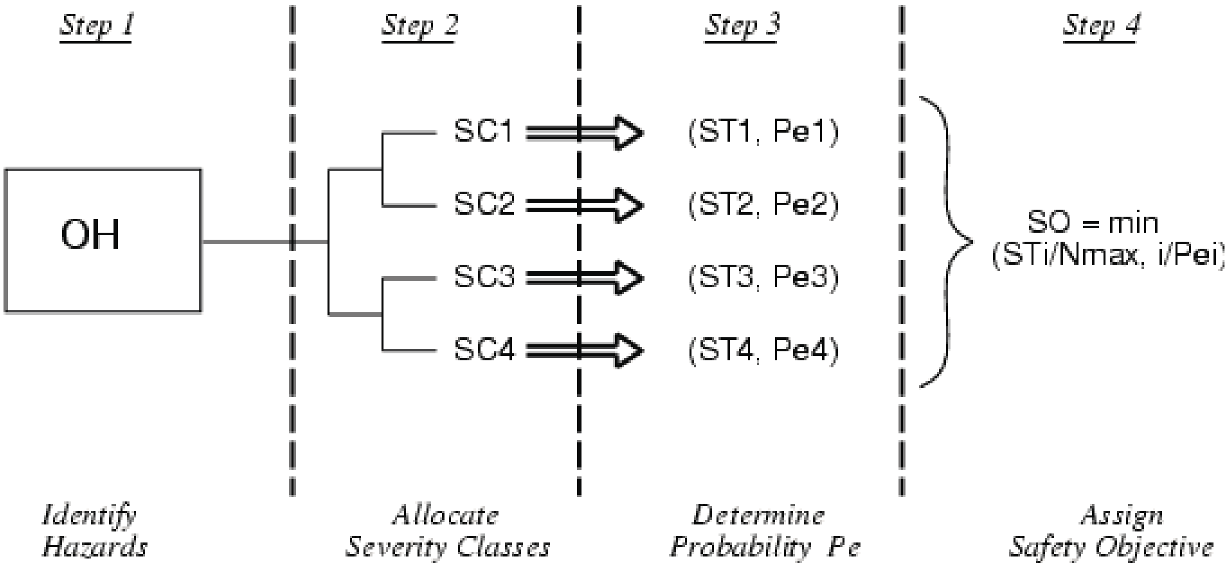


Figure 3: OHA Process Flow [4]

1. Identify Operational Hazards (OH): An OH is defined as an event that may arise when the system is in a faulted mode[2]
    a. Obtain list of Abnormal Events (AE) by applying failure modes
        i. Loss: Action not provided
        ii. Incorrect: Action performed incorrectly
        iii. Others: Action executed in non-suitable conditions or out of sequence
    b. Perform an expert analysis: Brainstorming sessions with air traffic controllers and pilots (used to complete and validate Step 1a)
    c. Identify Basic Causes (BC) and Abnormal Events (AE) that can lead to an OH
        i. System failures, human errors, procedure dysfunctions or failures and conditions external to the application itself (such as GPS constellation failure)
        ii. BCs lead to safety requirements or assumptions
2. Hazard Assessment and Severity Class allocation
    a. Describe the operational environment (OSED)
        i. Environmental Conditions (EC): Characteristics of the environment in which the application is expected to be used
        ii. External Mitigation Means: Mitigation means (mainly procedures) that help to "reduce" the hazard effects
    b. Classify hazards
        i. Effect on operations, occupants, air crew, air traffic service, specific effects

[2] We are unsure exactly what this definition of an OH means as it is not well defined in the report, but it appears to simply be an event that follows some failure. There does not seem to be any tie to an accident or incident, which is the usual definition of a hazard.

        ii. Rate 1 (most severe) to 5 (least severe)

3. Determine probability "Pe" and apportion the ATM risk budget: Define Risk Classification Scheme or Safety Targets. ST1 is assigned to Severity Class 1 and has lowest occurrence rate (1E-08/flt-hr), ST1 is assigned to Severity Class 2, and so on.
4. Assign Safety Objective: SOj = min (STi / Peij), i.e. the minimum of the safety target divided by the probability for each event tree leaf and each OH.

DO-312 derives safety requirements through a process called Allocation of Safety Objectives and Requirements (ASOR), which is a continuation of the above four steps.

5. Fault Tree Development
    a. Use information from OSED
    b. Query operational and system experts
6. Allocate safety objective and ASOR
    a. Validate results from Step 5
    b. Explore risk mitigation strategies
7. Derive Safety Requirements from basic causes (fault trees)

2.2.3 Interoperability Requirements

Interoperability requirements (INTEROP) are intended to ensure that the elements employed for the ATSA-ITP application work together correctly. INTEROP requirements specify the exchange of data between the elements of the airspace system that will be used for ITP, including ADS-B applications between transmitting and receiving aircraft involved in the procedure. These requirements are also intended to specify the exchange of data between aircraft and ground domains but (intentionally) do not contain detailed operational requirements for avionics and ground equipment.

2.3 Critique of DO-312 Methodology

We have identified several problems with this approach. First, the safety assessment is based on the nominal cases outlined in the OSED and then tries to predict a probability of deviation from nominal. Section 3 and [8] describe the potential danger of this type of approach, which is based on expected incorrect behavior (called a "design basis accident" in the nuclear power community) rather than worst case analysis. Starting with a hazard (as usually defined rather than the definition used in DO-312) and assuming worst-case system behavior has the potential of identifying a greater set of contingencies for "off-nominal" behavior.

2.3.1 Hazard Definition

DO-312 begins its analysis with non-traditional definitions for safety-related terms. For example, Operational Hazard is defined in two different ways in the document:

1) An event that may arise when the system is in a faulted mode.[3] Events leading to an OH are called its Basic Causes and Abnormal Events, and can either be system failures,

[3] The term "system faulted mode" is not defined.

human errors, procedure dysfunctions or failures, or conditions external to the application itself.

2) Any condition, event, or circumstance that could induce an operational effect[4] [4]

The process used to identify the ITP safety requirements in DO-312 uses the first "faulted mode" definition and defines abnormal events as arising due to system failures, human errors, procedural issues, and/or external conditions. The severity of the hazard is then determined by the effect it may have on the system. Defining hazards as abnormal events or events that arise when a system is in a faulted mode leads to defining all system failures as hazards, not just those that can lead to a loss (accident or incident). Essentially, safety and reliability are incorrectly equated. For example, one hazard identified in DO-312 is that ATC incorrectly rejects an ITP clearance (and therefore, the ITP is not executed). Although such an event is not desirable, it is not unsafe. Furthermore, this definition leads to important omissions of unsafe states, which will be explained in the following sections. As Figure 4 shows, while some failure scenarios are unsafe, some are safe, and some unsafe scenarios lie outside the realm of a "failure".

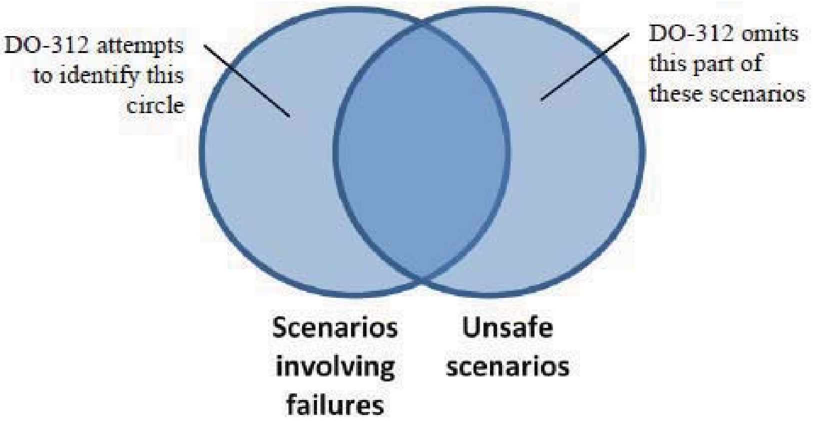

DO-312 attempts to identify this circle
DO-312 omits this part of these scenarios
Scenarios involving failures
Unsafe scenarios

Figure 4: The DO-312 Approach to Hazard Definition

While definitions of standard engineering terms used for decades can be changed, such new definitions that conflict with standard practice and the FAA's own guidelines for safety assessment [3] can lead to serious problems. At the least, communication can be inhibited and, at worst, operational safety can be degraded. A more standard definition of hazard is a system state that, together with a particular set of environment conditions, will result in an unplanned or undesired loss (i.e., an accident). Using the standard hazard definition leads to the identification of more and different hazards and hazard causes for ITP, capturing the unsafe scenarios illustrated in Figure 4.

[4] Definition of operational effect in DO-312: *The potential ultimate result of a hazard. The severity of the effect is reduced by external mitigations when they are available*.

2.3.2 Hazard Identification

Another set of issues with the DO-312 methodology concerns the use of a chain-of-event accident causality model in identifying causes and hazards. This model (and resulting hazard analysis techniques) puts an emphasis on preventing or reducing failures and also tacitly assumes that failure modes are independent. As noted in [5],[6],[7], and elsewhere, components need not fail in order to induce hazardous behavior at the system level. Fault trees do little to capture component interactions or the emergent nature of safety in complex systems.

DO-312 identifies six operational hazards that are used in the ITP safety assurance. To identify the hazards, abnormal events were found by applying failure modes to each expected action throughout the ITP phases. Each abnormal event is then traced forward in time to create a chain of events that leads to an outcome such as an accident or inconvenience. An event from each chain is then selected and labeled as an operational hazard.[5] Note that the same operational hazard may appear in more than one chain of events.

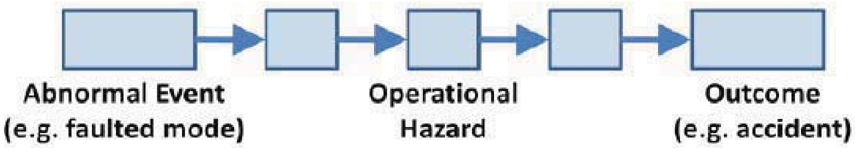


Figure 5: Chain of Events Model Used in DO-312 for Hazard Identification

Figure 5 shows the generic chain of events model used, and Table 1 shows the operational hazards that were identified.

Table 1: Operational Hazards from DO-312 Table C.6

OH-1: Interruption of an ITP maneuver
OH-2: Execution of an ITP clearance not compliant with ITP Criteria
OH-3: ITP request not accepted by ATC. (flight crew requests ITP but the request is denied by ATC.)
OH-4: Rejection by the flight crew of an ITP clearance not compliant with the ITP Criteria
OH-5: Rejection by the flight crew of an ITP clearance compliant with the ITP Criteria.
OH-6: Incorrect execution of an ITP maneuver.

This process identified OH-3, OH-4, and OH-5 in Table 1 as operational hazards, but they are noted to "have no effect on safety" and therefore are not analyzed. In fact, OH-4 is exactly what

[5] These conditions appear to correspond to the "boundary of application" in DO-312.

should happen, so it is difficult to understand why this was identified as a hazard. OH-2 and OH-6 are identified as having the potential for gravest impact, and became the focus of the ITP safety analysis along with OH-1 to a lesser extent.

The process of tracing abnormal events forward in time to identify operational hazards involves an arbitrary choice of which event in the chain is considered the operational hazard. DO-312 states that operational hazards are "identified along the boundary of the application under assessment". Although this criterion is not explicitly defined for ITP, it appears that operational hazards were selected such that one or more attributes in Table 2 were known.[6] Notice that every operational hazard is written as a combination of one or more of these attributes. For example, OH-3 is comprised of the attributes {(ATC evaluation of ITP = Denied), (ITP clearance = compliant)}.

Every operational hazard is written in terms of one or more of these conditions, and each hazard assumes that an ITP request has already been made. For example, OH-3 describes the set of conditions {(ATC evaluation of ITP = Denied), (ITP clearance = compliant)}. Clearly, not every possible combination of attributes is hazardous. However, there are several hazardous combinations that are not covered by the operational hazards in Table 1 and therefore were never analyzed in DO-312. Some examples of operational hazards that fit the narrow definition in DO-312 but were never analyzed include:

- an ITP is executed before ATC approves or denies the request
- an ITP is denied by ATC, but is executed by Flight Crew (FC)
- an ITP is not re-evaluated by FC before being executed
- an ITP clearance is accepted but not executed
- ITP criteria are incorrectly evaluated

Table 2: Conditions Used to Describe Operational Hazards

	A	B	C
1 ATC evaluation of ITP	Approved	Denied	No response
2 FC reevaluation of ITP	Accepted	Rejected	Not reevaluated
3 Compliance of ITP clearance	Compliant	Non-compliant	Not requested
4 ITP maneuver execution	Executed correctly	Executed incorrectly	Not executed
5 ITP maneuver outcome	Maneuver completed	Maneuver abandoned	Maneuver not initiated

In the analysis of each of the ITP hazards in DO-312, additional assumptions are made that further narrow the scope of each operational hazard. For example, OH-1 describes an interruption of an ITP maneuver but the analysis of OH-1 also assumes that {(ATC evaluation = approved), (FC reevaluation=accepted) , (ITP clearance=compliant)} whenever an ITP maneuver

[6] These conditions appear to correspond to the "boundary of application" in DO-312.

is interrupted.[7] These assumptions overlook important scenarios, such as cases where the ITP maneuver is abandoned because it is discovered that ITP criteria are not met. In some cases, the analysis even overlooks the abnormal events that were used to derive the hazard in the first place. For example, OH-1 was identified in part by the possibility of an ACAS (TCAS) resolution advisory (RA) causing the crew to interrupt the maneuver. However, the analysis of OH-1 and the resulting fault tree completely omit that scenario.[8]

Even using the DO-312 definition of an operational hazard, the method for identifying hazards is inadequate because it is considers only known failure modes. Accidents often arise due to unanticipated failures or through normal interactions without any failures. Starting a safety analysis with failures puts the analyst at risk of identifying a very limited set of the potential causes, as opposed to beginning with hazards and identifying the actions and interactions that could potentially lead to hazardous states. Furthermore, it is difficult or impossible to verify the quantitative probabilities of failure prescribed in the fault tree nodes of DO-312. Hardware that has rich heritage can be verified probabilistically, but human operator or software performance cannot be predicted in this way.

2.3.3 Barriers and Event Trees

The approach used in DO-312 is grounded in identifying the effects of all the Operational Hazards and then designing barriers to prevent any adverse effects. Event trees were used to identify the different possible chains of events that can result from each hazard given the barriers in place and to quantify the probabilities of each adverse outcome. Both the barriers and effects were identified through a workshop process of expert interviews. The use of barriers (and indeed event trees themselves) comes from process safety and, in particular, the nuclear power industry. Aviation more commonly uses a fail-safe approach.

The barrier and event tree approach assumes that accidents are a result of linear (or multi-linear) chains-of-events and that accidents can be eliminated by building barriers or "breaking the chain." This approach is inadequate because it does not account for the nonlinear behavior exhibited in tightly coupled, complex systems. It also requires either oversimplified and subjective selection of potential event chains or a list that becomes unwieldy and cumbersome to analyze.[9] To illustrate, one event tree includes the following chain of events:

1) An ITP maneuver is interrupted
2) Another aircraft is less than 10NM away, then less than 5NM away, then less than 1NM away
3) The flight crew visually sees the nearby[10] aircraft and takes appropriate action.

The analysis recognizes that each event may or may not follow from the previous event, but assumes that if all events occur then a Near Mid-Air Collision (NMAC) will NOT occur. In

[7] From DO-312 description of OH-1: —An ITP Aircraft requests and is cleared to perform an ITP operation. The request and clearance are compliant with the procedure and all criteria for ITP are met.

[8] In fact, the fault tree analysis of OH-1 only identifies two basic causes for OH-1: a technical failure (e.g. engine failure) or a misuse of traffic information by the flight crew.

[9] Event trees were created to model the very simple designs of nuclear plant shutdown systems and are rarely used outside that application. Identifying all potential orderings of events is possible only in very simple designs and systems.

[10] "Nearby" means less than 1 NM.

addition to assuming that the probability of each event is known, this oversimplification ignores critical characteristics described above. For example, the conditions that led to the ITP interruption are ignored even though they may have a significant effect on whether the crew is able to visually notice a nearby aircraft. It also ignores critical situations including the possibility of a NMAC despite the crew eventually seeing the other aircraft and taking appropriate action.

The use of event trees also requires assigning probabilistic values to the mitigating effects of the barriers. For example, the aircraft crew detecting an aircraft's proximity during an interrupted ITP maneuver through visual means and taking appropriate action to avoid an NMAC is assigned a probability of success of 0.80, and by means other than unaided visual acquisition and responding properly is assigned the probability of success of 0.90. These numbers seem arbitrary and difficult to support.

2.3.4 Safety Targets

Safety targets are assigned to events based on severity of the hazard. The Safety Objective for each hazard is an upward bound on the allowable probability of occurrence, where the probabilities of the Basic Causes are modeled, assumed, or required such that the likelihood of the associated hazard is less than the Safety Objective [10].

This approach to safety assurance is inappropriate for several reasons. First, not all unsafe states are included in the safety target and many of the probabilities for events seem arbitrarily assigned. Second, the collision risk model used in the report calculates probabilities based on nominal system behavior, where the probability of longitudinal overlap—a potential crash scenario—is the aggregation of errors in aircraft attitude and environmental assumptions. The underlying mathematics is executed flawlessly, but the problem lies in the modeling assumptions, i.e., that ITP and Reference aircraft will always maintain minimum separation requirements and that error propagation is due solely to instrumentation error. The "Collision Risk Model" would perhaps be more aptly named "Collision Risk Model for the *Expected System State*". Accidents rarely happen during expected operations, however: Virtually all occur during off-nominal system behavior.

Finally, the process presented in DO-312 to define event probabilities assumes that all the failure modes are independent. This assumption contradicts the conclusions of many accident investigation reports: it is rarely one basic event that leads to an accident, but multiple events that share common roots [11]. A typical example is that budget restrictions stemming from an increasingly competitive environment takes its toll on maintenance expenditures as well as operators' ability to respond to adverse events, such as increased work hours causing more fatigue and degraded operational performance leading to reduced procedure conformity.

2.3.5 Human Error Analysis

The human-oriented error analyses in DO-312 are based on operational safety workshops with pilots, controllers and operations experts as conducted by EUROCONTROL. A linear chain of human actions is assumed that leads towards a Basic Cause. Then the experts qualitatively assessed the likelihood of occurrence for certain types of errors as very often, often, rare, or very rare. These qualitative measures were mapped to quantitative measures and assessed relative to classifications in EUROCONTROL's ATM standard [12].

The quantitative values used to represent qualitative opinions appear to be arbitrary: An error that may happen “Very Often” is assigned the probability of occurring between 1-10%, while a “Very Rare” is described as occurring less than 0.01% of the time. For example, “The probability that the ITP Aircraft flight crew levels off at an intermediate Flight Level is assumed to occur no more than Very Rare” [4], meaning that this scenario has a probability of occurrence less than 1E-04.

Human errors are identified in DO-312 by constructing a top-down fault tree beginning with each identified hazard and drilling down to identify potential causes. When an identified cause describes a single failure, a human error, or an environmental factor, that event is considered a Basic Cause and the analysis of the branch stops. As noted above, the hazard identification process is inconsistent and incomplete, which results in fault trees that identify and evaluate an incomplete set of human errors.

The problems are not just in completeness. Human error is treated in exactly the same way as a physical failure, that is, as a deviation from a predefined behavior or procedure. Unfortunately, this treatment of human error oversimplifies it as a binary decision between right and wrong. Many of the most important situations involved in accidents are overlooked because they are difficult or impossible to model in this way, including:

- Situations where the correct behavior is not predefined or not clear
- Situations where the prescribed behavior is thought to be incorrect by the person responsible for following it
- Situations where procedures conflict with each other, or it is not clear which procedure applies
- Situations where the person has multiple responsibilities or goals that may conflict
- Situations where the information necessary to carry out a procedure is not available or is incorrect
- Situations where past experiences and current knowledge conflict with a procedure
- Situations where the procedure is misunderstood or the responsibility for the procedure is unclear
- Situations where the procedure is incorrect

For example, the identification of hazards anticipated the basic cause “FC fails to accomplish reassessment” [of the satisfaction of the ITP criteria, which is required]. However, this human error appears to have been overlooked throughout the analysis of every hazard, including OH-2.

The analysis produced a short list of human errors such as “flight crew fails to detect inadequate climb/descent rate”. Because basic causes are the “lowest level of failure,” human errors are not analyzed in further detail. No attempt is made to understand why the human errors may arise or to prevent them. Instead, all errors are assumed to occur randomly at a given probability rate. If necessary, mitigation attempts are made to reduce the chance that human errors will lead to a hazard. Mitigation is done by adding barriers called “mitigation measures”. Interestingly, every mitigation measure is simply a new procedure that is imposed on the humans.

Perhaps because human behavior was treated as random, no attempt was made to explain or understand the potential human errors. The lack of such understanding precludes the possibility of eliminating or reducing errors in the first place, which is typically more effective than managing hazards through mitigation alone. There is also no guarantee that humans will perform better when additional [mitigation] procedures are added, and they may actually perform worse because of the additional workload. Instead, a safety analysis should not only identify *what* humans can do wrong, but also *why* and *how it can be avoided*. Assuming that the flight crew and ATCO are not intentionally malicious, this identification requires understanding the conditions under which each erroneous decision can make sense to them and modifying or adding requirements to help make the correct decisions obvious.

To summarize, the treatment of human actions as independent random events greatly oversimplifies the role of humans and may lead to incorrect conclusions. Human behavior is usually not random, but influenced by the current context, the information observed, and constructed beliefs about the system. Human behavior is also heavily dependent on interactions with other system components and past experiences and is rarely independent of other events.

2.3.6 Summary of Critique

Even if DO-312 safety analysis for ATSA-ITP had been done correctly and completely according to their own methodology, the basic approach used assumes that accidents are caused by a linear chain of events and that the probability of links on the chain contributing to a hazardous scenario can be accurately modeled. Although many electro-mechanical parts have sufficient heritage to yield an accurate probabilistic assessment, such individual physical component statistics may not hold in a complex system and is not useful for new components or old components operating in new environments. Even less can be said with numerical precision about how other types of system components, such as humans, software, or some combination thereof, will behave in a nonlinear and dynamic socio-technical system. Although the analysis laid out in DO-312 may be adequate for some specific components of the system, a comprehensive safety assessment of a complete system requires a different approach.

3 Using STAMP and STPA for NextGen

The significant technical changes envisioned for NextGen creates a necessity for a new, more powerful model of accident causality that better represents today's complex, socio-technical systems. The new model used in our analysis, called STAMP (Systems-Theoretic Accident Model and Processes) [6][13], 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. STPA (System Theoretic Process Analysis) is a hazard analysis technique built on STAMP.

In systems theory, emergent properties associated with a set of components are related to constraints upon the degree of freedom of those components' behavior. 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 dysfunctional interactions among system components are not handled adequately or controlled—where controls may be managerial, organizational, physical, operational, or manufacturing—such that required safety constraints on behavior are violated.

In a systems-theoretic view of safety, the emergent safety properties are controlled or enforced by a set of safety constraints related to the behavior of the system components. Safety constraints specify those relationships among system variables or components that constitute the non-hazardous or safe system states—for example, the power must never be on when the access door to the high-power source is open; two aircraft must never violate minimum separation requirements; pilots in a combat zone must be able to identify targets as hostile or friendly; and the public health system must prevent the exposure of the public to contaminated water and food products. Accidents result from interactions among system components that violate these constraints—in other words, from a lack of appropriate constraints on component and system behavior.

Section 3.1 describes the hazard analysis procedure, called STPA, used to identify the system constraints necessary to ensure safe development and operation of complex socio-technical systems. It also presents a model-based framework, called Intent Specifications, which captures the results of the hazard analysis in a readable, reviewable way by people from multiple disciplines.[11]

3.1 STPA (System Theoretic Process Analysis)

In STAMP, accidents are viewed as resulting from inadequate enforcement of constraints on system behavior. Figure 6 shows a generic (example) safety control structure to enforce safety constraints. Each hierarchical level of the control structure represents a control process and control loop with actions and feedback. Two control structures are shown in Figure 6—system development and system operations—both of which have different responsibilities with respect to enforcing safe system behavior. The reason behind the inadequate enforcement may involve classic component failures, but it may also result from unsafe interactions among components operating as designed or from erroneous control actions by software or humans.

[11] The model-based specification method, Intent Specifications, was partially developed for the certification of TCAS II and later extended.

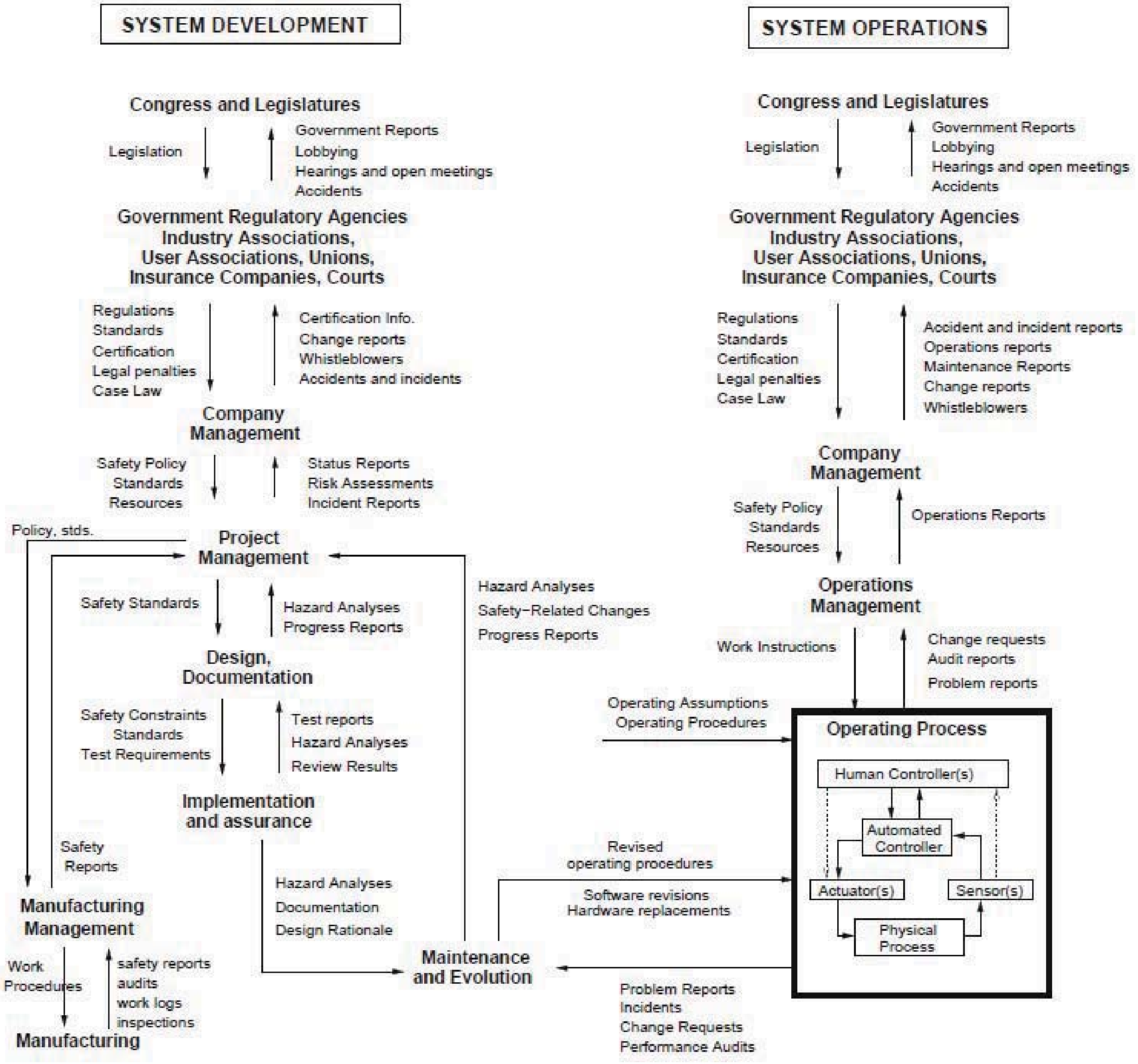


Figure 6: Example Model of a Socio-Technical Safety Control Structure

Human and automated controllers use a process model (usually called a mental model for humans), which they use to determine what control actions are needed. The process model contains the controller's understanding of (1) the current state of the controlled process, (2) the desired state of the controlled process, and (3) the ways the process can change state. Software and human errors often result from incorrect process models, e.g., the software thinks the spacecraft has landed and shuts off the descent engines. Accidents can therefore occur when an incorrect or incomplete process model causes a controller to provide control actions that are hazardous. While process model flaws are not the only causes of accidents involving software and human errors, it is a major contributor.

There are four types of hazardous control actions that need to be eliminated or controlled to prevent accidents:

1) A control action required for safety is not provided or is not followed
2) An unsafe control action is provided that leads to a hazard
3) A potentially safe control action is provided too late, too early, or out of sequence
4) A safe control action is stopped too soon or applied too long.

STPA (System Theoretic Process Analysis) is a hazard analysis technique built on STAMP. Identifying the potentially unsafe control actions for the specific system being considered is the first step in STPA. These unsafe control actions are used to create safety requirements and constraints on the behavior of both the system and its components. Additional analysis can then be performed to identify the detailed scenarios leading to the violation of the safety constraints. As in any hazard analysis, these scenarios are then used to design controls or mitigate mitigation measures for the potential hazards in the system design.

Before beginning an STPA hazard analysis, potential accidents and related system-level hazards are identified along with the corresponding system safety constraints that must be controlled. As an illustrative example for this application, consider a flight crew in oceanic airspace. The fundamental losses or accidents under consideration are human death or injury. The system-level hazards relevant to this definition of an accident include:

- H-1: A pair of controlled aircraft violate minimum separation standards
- H-2: Aircraft enters unsafe atmospheric region
- H-3: Aircraft enters uncontrolled state
- H-4: Aircraft enters unsafe attitude (excessive turbulence or pitch/roll/yaw that causes passenger injury but not necessarily aircraft loss)
- H-5: Aircraft enters a prohibited area

For the application used in this report, we focused on hazard H-1.

STPA is performed on a functional control diagram of the system, which is shown in Figure 7 for the ITP-related parts of the system. The first part of STPA identifies hazardous control actions for each component that could produce a system-level hazard by violating the system safety constraints. Once the set of hazardous control actions has been identified, the second part of STPA analyzes the system to determine the potential scenarios that could lead to providing a hazardous control action. These scenarios can be used to design controls for the hazards or, if the design already exists, to ensure that these scenarios are adequately controlled.

STPA Step One: The first step of STPA identifies control actions for each component that can lead to one or more of the defined system hazards. The four general types of unsafe control actions were shown above. Hazardous control actions can be documented using a table as in Table 3. The hazardous control actions can then be translated into system and component safety requirements and constraints.

Each item in the table should be evaluated to determine whether it is hazardous as defined by the system-level hazards. For instance, in this example the flight crew not executing ITP is not hazardous because it does not lead to H-6 specified above. If this situation is a safety concern, then the hazard list can be updated to include the corresponding hazard. On the other hand, executing the procedure when the criteria are not satisfied could clearly lead to a loss of separation. Each unsafe control action is then translated into a component-level safety constraint (e.g. ITP must not be executed unless it is approved, FC must follow regional procedures when aborting the ITA, etc.).

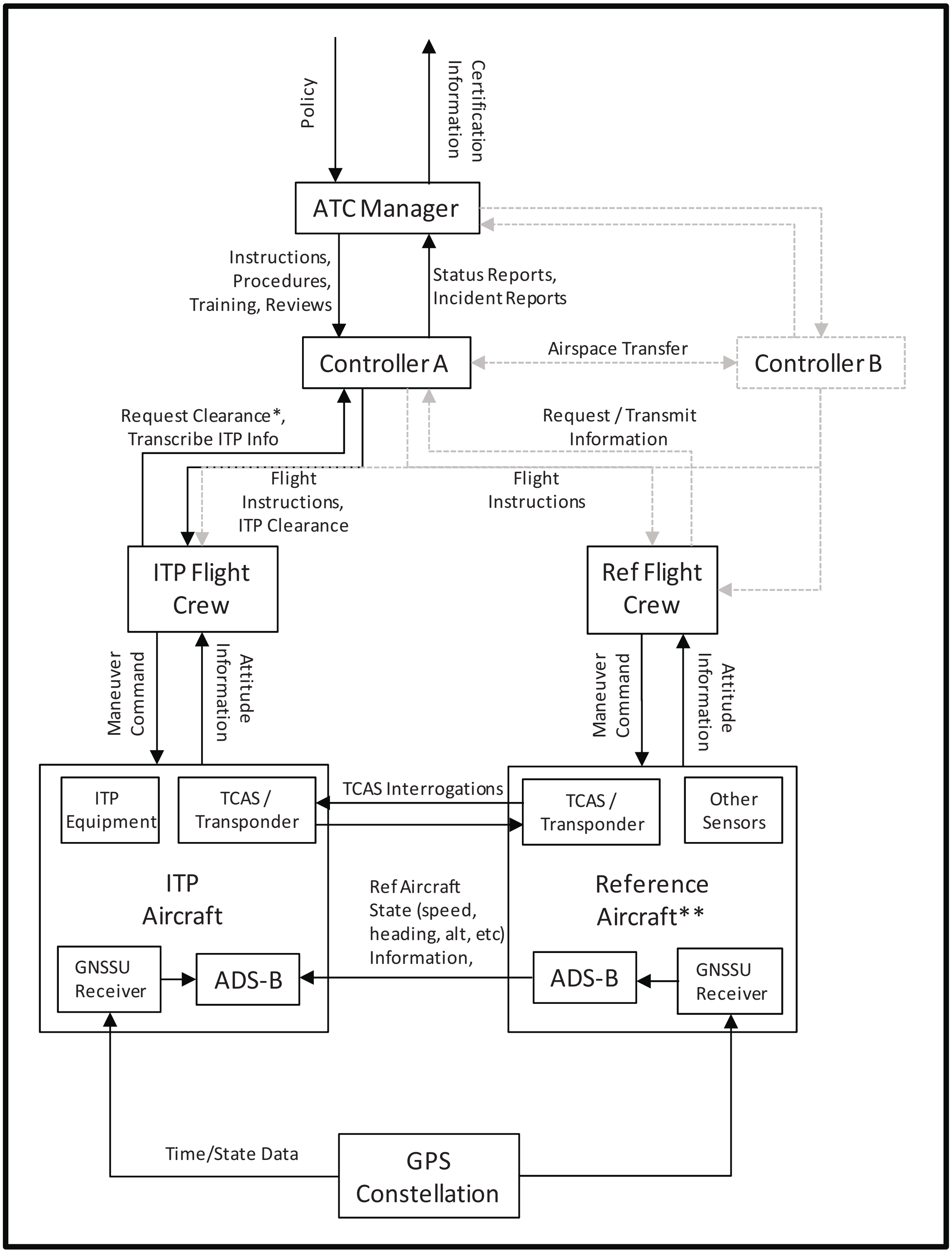


Figure 7: Safety Control Structure for ATSA-ITP

Table 3: Potentially Hazardous Control Actions for Flight Crew (→Hazard H-6)

Control Action	Required Safe Action Not Provided	Unsafe Action is Provided	Incorrect Timing/Order	Stopped Too Soon
Flight Crew executes ITP		ITP executed when not approved. ITP executed when ITP criteria are not satisfied. ITP executed with incorrect climb rate, final altitude, etc.	ITP executed too soon before approval. ITP executed too late.	
Flight Crew performs abnormal termination of ITP	FC continues with maneuver in dangerous situation.	FC aborts unnecessarily. FC does not follow regional procedures while aborting.		

STPA Step Two: The second step of STPA examines each control loop in the safety control structure to identify potential causal factors for each hazardous control action, i.e., the scenarios for causing a hazard. 8 shows a generic control loop that can be used to guide this step. While STPA Step One focused on the provided control actions (the upper left corner of 8), STPA Step Two expands the analysis to consider causal factors along the rest of the control loop.

For example, a safety constraint might be violated because the process model of the controller is incorrect, for example, the FC thinks it is safe to execute the ITP when it is not (an incorrect process model). The incorrect process model, in turn, may be the result of inadequate feedback provided by a failed sensor or the feedback may be delayed or corrupted. Alternatively, the designers may have omitted a feedback signal or the FC may have received incorrect from ATC or from other input devices (such as ADS-B).

Once the second step of STPA has been applied to determine potential causes for each hazardous control action identified in STPA Step One, the causes should be eliminated or controlled in the design. More information about STPA can be found in other publications [6]. Our safety analysis (limited by time and resources) is shown in Appendix B.

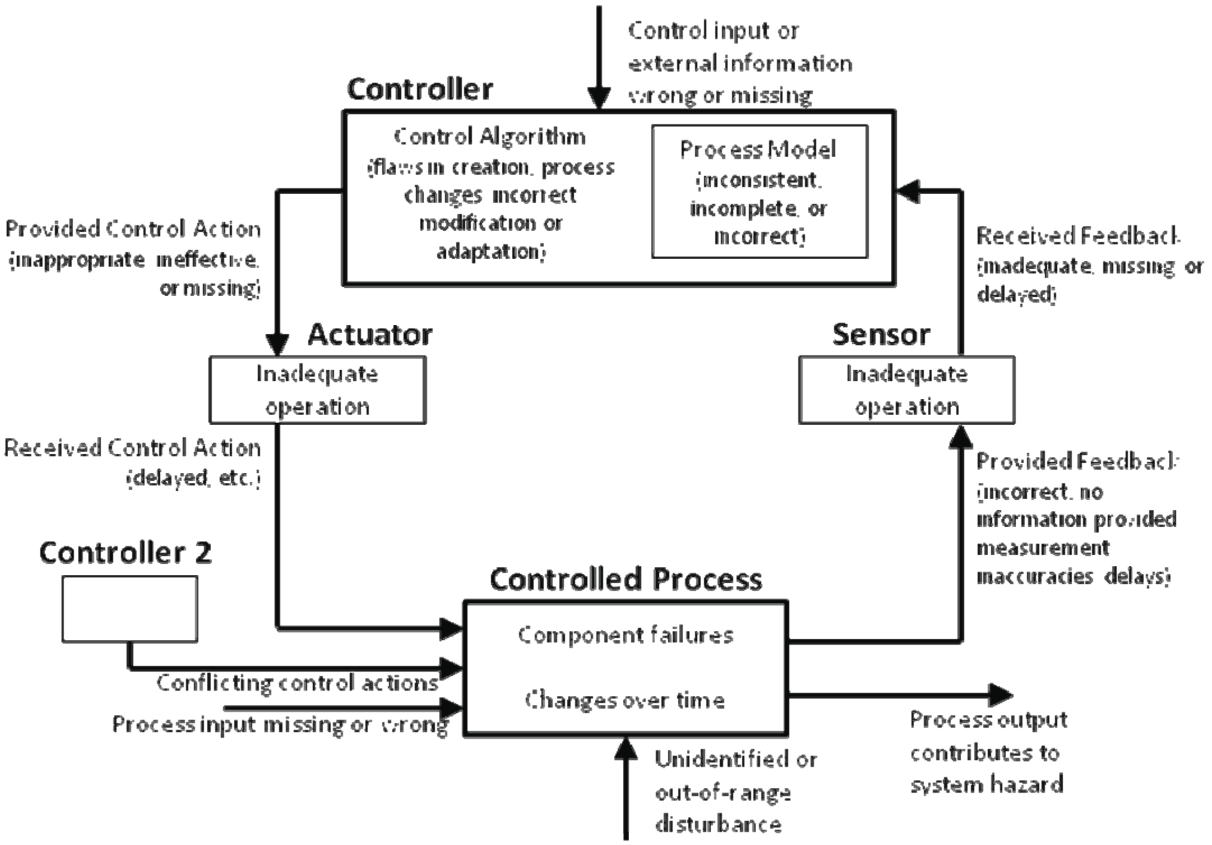

Control input or external information wrong or missing
Controller
Control Algorithm (flaws in creation, process changes incorrect modification or adaptation)
Process Model (inconsistent, incomplete, or incorrect)
Provided Control Action (inappropriate, ineffective, or missing)
Received Feedback (inadequate, missing or delayed)
Actuator
Inadequate operation
Sensor
Inadequate operation
Received Control Action (delayed, etc.)
Provided Feedback (incorrect, no information provided measurement inaccuracies, delays)
Controller 2
Controlled Process
Component failures
Changes over time
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Figure 8: General Control Loop with Causal Factors

3.2 Intent Specifications

An intent specification is a specification and model-based development framework supporting system design and other system engineering activities, intended to assist humans at all organizational levels in dealing with complexity by providing more readable and reviewable specifications. Intent specifications are based on psychological research in human problem solving and on basic principles of system theory and system engineering [6].

Intent specifications do not contain additional information that is not typically found in detailed system engineering specifications. However, an intent specification differs from a standard system engineering specification primarily in its structure, which is designed to (1) facilitate the tracing of system-level requirements and design constraints down into detailed design and implementation and the documentation of design rationale, (2) assist in the assurance of various system properties (such as safety) in the initial design and implementation, and (3) reduce the costs of implementing changes and re-analysis when the system is changed, as it inevitably will be.

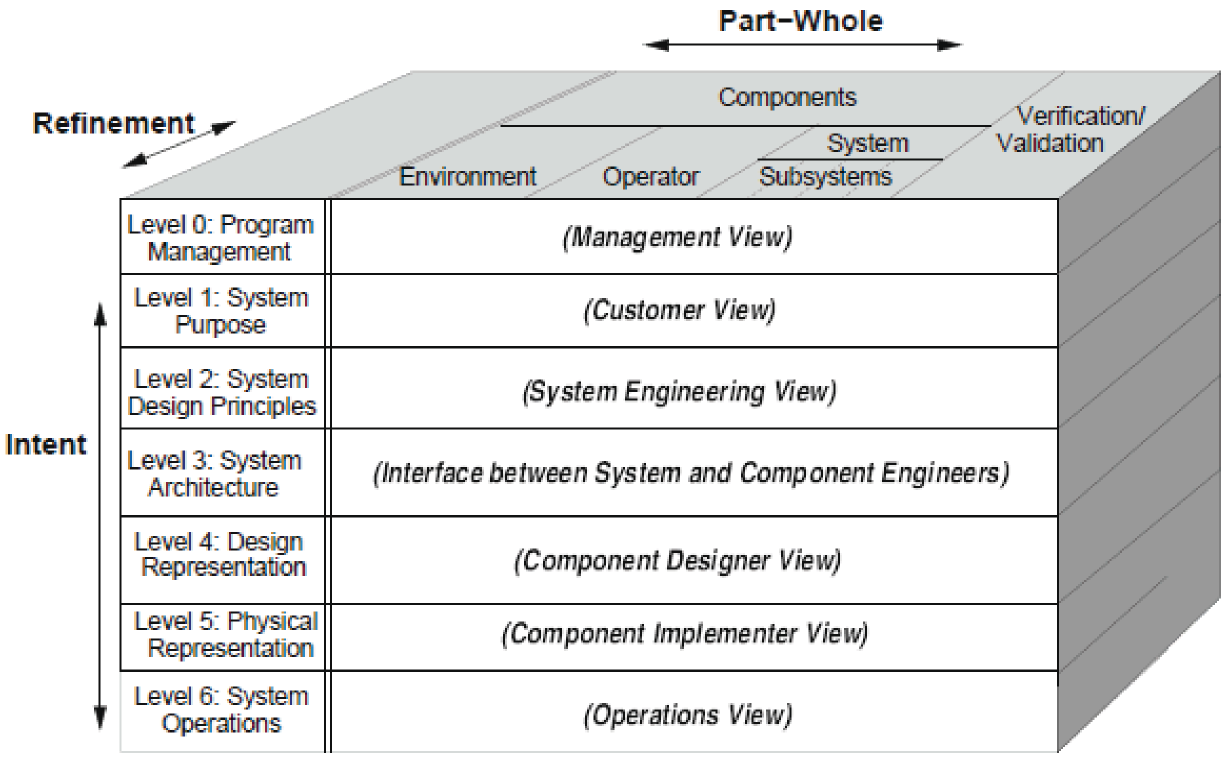

Part−Whole
Refinement
Components
Verification/ Validation
System
Subsystems
Environment
Operator
Intent
Level 0: Program Management
(Management View)
Level 1: System Purpose
(Customer View)
Level 2: System Design Principles
(System Engineering View)
Level 3: System Architecture
(Interface between System and Component Engineers)
Level 4: Design Representation
(Component Designer View)
Level 5: Physical Representation
(Component Implementer View)
Level 6: System Operations
(Operations View)

Figure 9: Intent Specification Hierarchy

There are seven levels in an intent specification, as shown in Figure 9. Levels do not represent refinement, as in other commonly used hierarchical specification frameworks. Instead, each level of an intent specification represents a completely different model of the same system and supports a different type of reasoning about it: each model or level presents a complete view of the system from a different perspective. The model at each level is described in terms of a different set of attributes or language. Refinement and decomposition occurs within each level of the specification. In addition to intra-level refinement, the levels are organized in a "Means/Ends" hierarchy. In such a hierarchy, the information at a level acts as the goals (the ends) with respect to the model at the next lower level [1]. In other words, the next lower level is where the means to the ends of the current level are implemented.

Although this report focuses primarily on Levels 1, 2, and 3, the following bullets briefly describe the content and objectives of each level:

- The top level (Level 0) provides a project management view and insight into the relationship between the plans and project development, with project management plans, safety plan, status information, and other management tools.
- Level 1 of an intent specification is the customer view and assists system engineers and customers in agreeing on what should be built and whether that has been accomplished. It includes system goals, requirements, design constraints, hazards, environmental assumptions, and system limitations.
- Level 2, System Design, is the system engineering level and provides the structure and content needed for engineers to reason about the system in terms of the physical

principles and laws upon which the system design is based. It documents the basic system-level design decisions made to satisfy the requirements and constraints at level 1.

- The third level, or Blackbox Behavior level, enhances reasoning about the logical design of the system as a whole and the interaction among the components as well as the functional state without distractions from implementation issues. This level acts as an unambiguous interface between system engineering and component engineering to assist in communication and review of component blackbox behavioral requirements and to reason about the combined behavior of individual components using informal review, formal analysis, and simulation. The models at this level are formal (rigorously defined) and can be both executed and subjected to formal analysis. These formal models can play an important role in validation by being executed in system simulation environments to identify requirements and design errors (for example, completeness and consistency analyses). The language at this level was created originally to specify TCAS II for the FAA/RTCA [2].
- The next two levels (4 and 5) provide the information necessary to reason about individual component design and implementation issues. Levels 4 and 5 represent the standard component documentation used on most any engineering project.
- Finally, the sixth level provides a view of the operational system. The effort in this task has predominantly focused on levels 0-3 of the intent specification.

Figure 10 shows an example of intent specification traceability between Levels 1 and 2 through partial specification of the ITP Equipment example used for this research. Traceability is captured through hyperlinks denoted by arrows and the specification item tag (for example, ↓H-1). Traceability links denote different relationships between specifications based on their direction. An up arrow (↑) denotes that the current specification item is involved in the implementation of the intent of a specification item at a higher level in the "means-ends" hierarchy denoted by the tag after the arrow. A down arrow (↓) points to a specification item at a lower level in the "means-ends" hierarchy that is involved in the implementation of the intent of the current specification item. Left and right arrows denote relationships between specification items at the same level in the "means-ends" hierarchy that affect the items' relationships to items on other levels. The direction of the arrow for this type of relationship depends on the physical location of the specification item in the intent specification document. A left arrow (←) points to a specification item at the same level that appears earlier in the specification than the current specification item. Conversely, a right arrow (→) points to another specification item at the same level that appears later in the current specification document. Thus, in Figure 10, the hazard H1 is linked to the accident related to this hazard (e.g. ACC1). This relationship shows 'why' the hazard is of concern:. The accident has a link to H1 showing the related hazard(s). Similarly, H1 points across the level to a safety constraint [1.2] derived from the hazard. The safety constraint has downward pointing links to Level 2 where that safety constraint is enforced with system design decisions. Lastly, the relationship between the design decisions is captured through traces across Level 2.

Level 1

Hazard
[H-1] A pair of controlled aircraft violate minimum separation standards (←[A-1],→[1.2])

Causal Analysis
[FC.1] FC believes aircraft climb/descent capability is greater than it is (process model inconsistency)
[FC.2] FC does not receive communication from ATC (inadequate/missing feedback)

Safety Requirements
[1.2] ITP shall provide the flight crews of aircraft operating in procedural airspace the ability to determine if an ITP maneuver is appropriate (←[H-1], ←[FC.1], ↓[2.1])
[1.3.1] ITP training shall include communication protocols (both channels and appropriate syntax) between flight crew and air traffic control (←[H-1], ←[FC.2], ↓[2.5])

…

Level 2

Design Decisions
[2.1] The ITP flight crew must check that the following criteria are fulfilled before requesting an ITP clearance. This requirement does not imply that an individual assessment of each criterion is carried out by the flight crew, but rather that each criterion is assessed by either the flight crew, or by automation (see section 3.5.1). Although not required for all criterion, it is recognized that automation may provide a more predictable solution. (↑[1.2], [1.9],[1.26],[1.27])

[2.1.1] The Ownship climb/descend capability criteria are considered passed if and only if the ITP Aircraft can climb/descend in the desired direction at a rate of 300 fpm or more.

> **Design Rational**: Initiation Distance Criteria and other geometric values ([2.1.2], [2.1.3], [2.1.4]) were selected such that when a Flight Level change at 300 fpm is performed with the related 20 or 30 kts Closing Ground Speed Differential, the distance between the aircraft does not become less than the ITP Separation Minimum (i.e., 10 NM).

[2.5] ATC should include a minimum data set in its clearance, in order to minimize the risk of confusion during communication between the Flight Crew and ATC. This information includes the Reference Aircraft ID and the cleared-to Flight Level in the ITP clearance.(↑[1.3.1])

Figure 10: ITP Equipment Intent Specification Partial Example

Intent information represents the design rationale upon which the specification is based. This design rationale is integrated directly into the specification. For example, “Design Decision.1” in 10, and its related Design Decisions in Level 2, represents a design implementation with the *intent* of preventing “Hazard H-1” and in turn enforcing “Safety Requirement Constraint.1.2”. Each level also contains additional information (such as that labeled “**Design Rational**” in

Figure 10) about underlying assumptions upon which the requirements, design, and safety assessment is based.

Assumptions must also be documented and are especially important in operational safety analyses. When conditions change such that the assumptions are no longer true, then a new safety analysis should be triggered. In the traditional system engineering specification approach, these assumptions may be included in a safety analysis document (or at least should be), but are not usually traced to the parts of the implementation they affect. Therefore, even if the system safety engineer knows that a safety analysis assumption has been changed, it is very difficult and resource-intensive process to figure out which parts of the design used that assumption.

Appendix B shows the intent specification we generated for ATSA-ITP. Because of limitations on time and resources available to us, the specification is necessarily incomplete but provides a good example of the results of using STAMP/STPA.

In summary, intent specifications foster a transition from system to component (including software) specifications and the integration of formal and informal aspects of system and software development. The structure facilitates the tracing of system-level requirements and constraints into the design and the assurance of various system properties (such as safety) in the initial design and implementation. It also reduces the costs of implementing changes and re-analysis by providing traceability and rationale capture. Finally, each level of the intent specification supports a different type of reasoning about the system, from high-level systems engineers working with system-level goals and tradeoffs to the experts who design and implement individual components.

4 Comparison of the Two Approaches and Their Results

The results of any derivation and of a specification is inextricably linked with the overall philosophy and viewpoint of the approach, the models used to understand system behavior, and the definitions that undergird the models. Therefore, in order to compare the results of DO-312 with those of STPA, we must also compare the underlying philosophy of each approach, as well as the definitions and terms used in each analysis. Sections 2 and 2 describe each approach in greater detail, but some of these accounts are reiterated here for succinct comparison. Table 4 summarizes the comparison.

Table 4: General Comparison of Approaches

	DO-312	**STAMP/STPA**
Analysis Philosophy	Success oriented, i.e. it assumes nominal case then tries to predict probability of deviation Provides set of contingencies for off-nominal behavior	Assumes worst-case scenario, i.e. it starts with accident, then hazards, then causal factors and assumes that any of the causal factors can happen
	Emphasis on preventing or reducing failures	Emphasis on enforcing constraints on system (and thus component) behavior
	Assumes most failure modes are independent	Accounts for sub-system interactions and how these influence safety-related behavior

Causal Factors	Considers only hardware failures, or treats operators and software as if they are hardware (e.g. leaves on a fault tree with assigned probabilities of failure)	Assumes that software does not “fail” but can still be hazardous due to *flawed requirements or unsafe interactions* with rest of system Human operators perform within the context of a larger system design and, like software, do not necessarily “fail” but can make unsafe decisions
Certification Method	Assign performance goals or necessary probabilities of failure, then manufacturer attempts to assure compliance	Specify safety constraints derived from STPA, based on safety-related control actions and required component behavior which manufacturer implements.

DO-312 and STPA are fundamentally different in their approach to identifying accident causality. DO-312 is based on the assumption that the system operates nominally and that accidents result due to deviation from nominal behavior at the component or sub-system level. Safe behavior is then imposed by providing contingencies for the identified off-nominal behaviors or conditions. In contrast, STAMP/STPA assumes a worst-case scenario and identifies potential scenarios that could lead to that worst case.

As described earlier, the DO-312 safety analysis is based on a chain-of-events model of causality, where the events represent component failures. Therefore DO-312 relies on preventing or reducing the probability of component failure to prevent accidents. Fault tree analysis (FTA) (at least as used in DO-312) also assumes that most of the component failure modes are independent. In addition, FTA treats human operators and software as if they fail like mechanical hardware, and then assigns probabilities of failure to these components.

Alternatively, STPA and STAMP assume the worst case in identifying accident causality. That is, STPA starts with an accident, identifies hazards that may lead to an accident, and then identifies causal factors. An important distinction with STPA and the FTA performed in DO-312 is the assumption about basic causal factors. DO-312 assumes or prescribes independent probabilities for off-nominal behavior, while STPA assumes that any and all causal factors may occur coincidentally. While the nodes of a fault tree assume independence of causes, STPA accounts for sub-system interaction using control systems theory and in fact assumes that not only can causal factors be dependent but also that the behavior of one component might be highly influential on other aspects of the system.

STPA also recognizes that software does not fail, but merely performs the way it was designed—it can therefore be hazardous due to flawed requirements (or implementation) or unsafe interactions with the rest of the system. Nor do human operators fail in the sense that hardware does nor do they fail randomly (except, perhaps, in the case of a “slip” although that can also be influenced by the design of the control panel). Instead, they are influenced by the design and operation of the overall context of the system and can thus make unsafe decisions due to the factors in Figure 12, such as incorrect mental models of the process they are controlling, possibly due to missing or incorrect feedback. Finally, STPA emphasizes the enforcement of constraints on component behavior (including software and human operators), which then affects the emergent system behavior.

Due to the differences outlined above, the certification method that results is necessarily dissimilar. The DO-312 is performance based; the document specifies performance goals or necessary minimum probabilities of component and system failure in order to meet the assumptions used in the fault or event trees. Manufacturers must then attempt to assure compliance with these performance metrics. On the other hand, the analysis produced by STPA results in a specification of behavioral constraints (requirements), based on safety-related control actions for all the system components.

4.1 Hazard Definitions and Identification

DO-312 and STPA use vastly different definitions of the term "hazard," shown in Table 5, where the DO-312 definition is unconventional. The difference between the definitions renders the task of comparing the ensuing results quite difficult. Consider the hazards identified in the second row of Table 5. There are two general problems with the identified hazards, also discussed earlier: (1) many of the hazards are actually events or causes, and (2) several of the hazards are not actually hazards (and in the case of OH_5, the operational hazard is actually the very behavior required to ensure safety). However, most of the analysis in DO-312 pertains only to OH_2 and OH_6, which are singled out as the only hazards that relate to safety.[12] OH_1, interruption of an ITP maneuver (which is actually a cause that could lead to a hazard), was deemed to have less significant impact on safety, but again this distinction reflects the overarching philosophy of assuming nominal- or best-case behavior. Using STPA, we actually identified interruption of maneuver in later steps as an important potential cause of a hazard and derived requirements to constrain this behavior.

The list for STPA includes general hazards for aircraft safety, which have been used for hazard analysis and equipment specifications for other aspects of the airspace domain [15]. For further refinement of scope and to consider only those aspects that directly relate to ITP, the STPA analysis focused on preventing a violation of minimum separation requirements, hazard H-1.

Table 5: Hazard Analysis Comparison

	DO-312	STPA
Hazard Definition	An event that may arise when the system is in a faulted mode; events leading to an OH are called its Basic Causes and Abnormal Events, and can either be system failures, human errors, procedures dysfunctions or failures and conditions external to the application itself Or, any condition, event, or circumstance which could induce an	A system state or set of conditions that together with a particular set of worst-case environmental conditions, will lead to an accident (loss)

[12] Again, we argue that these should not be called hazards if they do not impact safety.

	operational effect	
Hazard Identification	OH_1 – Interruption of an ITP maneuver (flight crew abandons the maneuver). OH_2 – Execution of an ITP clearance not compliant with ITP Criteria. OH_3 – ITP request not accepted by ATC. OH_4 – Rejection by the flight crew of an ITP clearance not compliant with the ITP Criteria. OH_5 – Rejection by the flight crew of an ITP clearance compliant with the ITP Criteria. OH_6 – Incorrect execution of an ITP maneuver.	H1 – a pair of controlled aircraft violate minimum separation standards H2 – aircraft enters unsafe atmospheric region H3 – aircraft enters uncontrolled state H4 – aircraft enters unsafe attitude (excessive turbulence or pitch/roll/yaw that causes passenger injury but not necessarily aircraft loss) H5 – aircraft enters a prohibited area

4.2 Analysis Process and Results

Chapter 2 and the earlier sections of this chapter describe the differences in the methods used in DO-312 and STPA. This section is intended to further demonstrate those differences by showing a few short examples of results. The example used is instructive because it consists of a cause identified in both the DO-312 and STPA analyses, i.e., execution of a procedure not compliant with ITP criteria. Specifically, the cause in DO-312 is defined as noncompliance with ITP distance and undetected by both the flight crew and air traffic control. A similar type of analysis can be performed for all of the other ITP criteria (mach, closing speed, and others) and our STPA has purposefully used a more general unsafe control action, i.e., execution of ITP when criteria (any of the flight parameters) are not met.

4.2.1 DO-312 Approach

Beginning with the Operational Hazards defined above, DO-312 identifies causal factors by using fault trees. As an example, see Figure 11. The top of the fault tree, “Procedure not compliant with criterion 2…” represents a high level cause of a hazard: improper execution of ITP. According to this analysis, failure to comply can occur either because the FC does not understand the minimum distance or the ATC does not receive data or fails to detect noncompliance (which could also be due to an error in the communication protocol).

Notice first the assigned safety objective at the top of the tree, which fits into a larger system-level safety objective. The lower level causes and associated probabilities are combined, depending on their logical and/or relationships, to yield a higher level probability of occurrence. Two nodes of the fault tree in Figure 11 represent human behavior (a critique of this approach was provided earlier). The probability of a human error cannot be verified, and the fault tree analysis gives no guidance on how to prevent these errors but instead assumes they happen arbitrarily or randomly. The fault tree also assumes independent behavior, however the interaction and behavior of the flight crew and ATC may be coupled, with the parties exerting influence on each other or being influenced by higher-level system constraints. Finally, the analysis asserts that communication errors are due to corruption of data during transport (essentially a hardware or software error), but there are many other reasons for potential errors in communication.

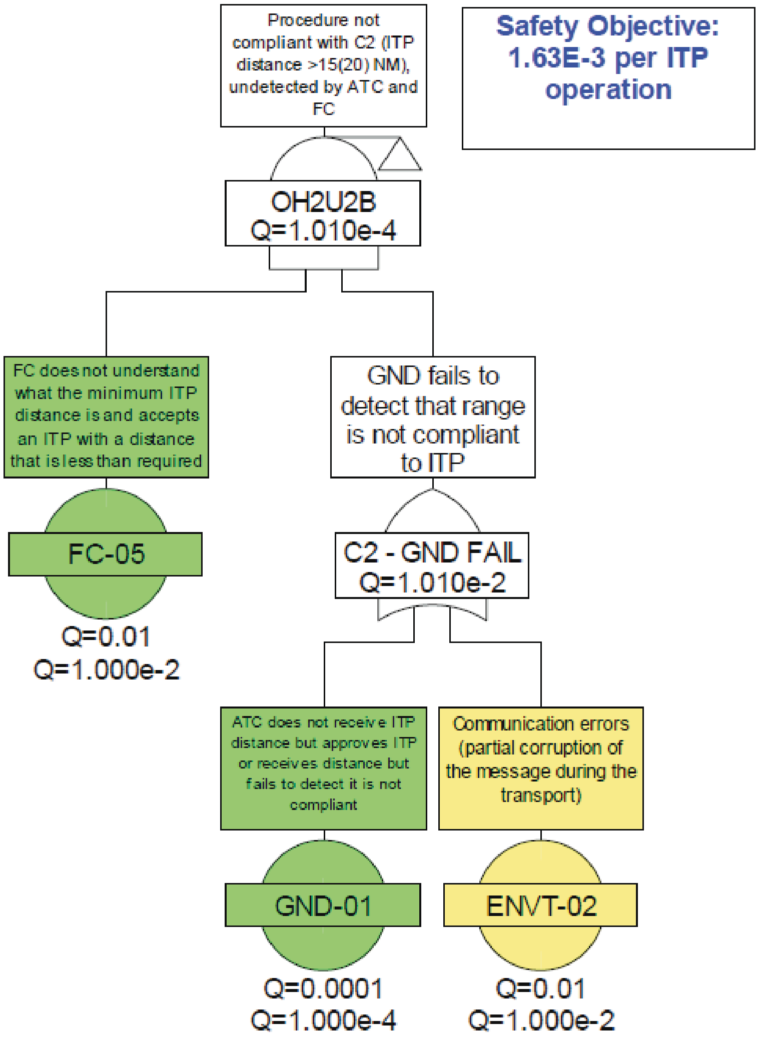
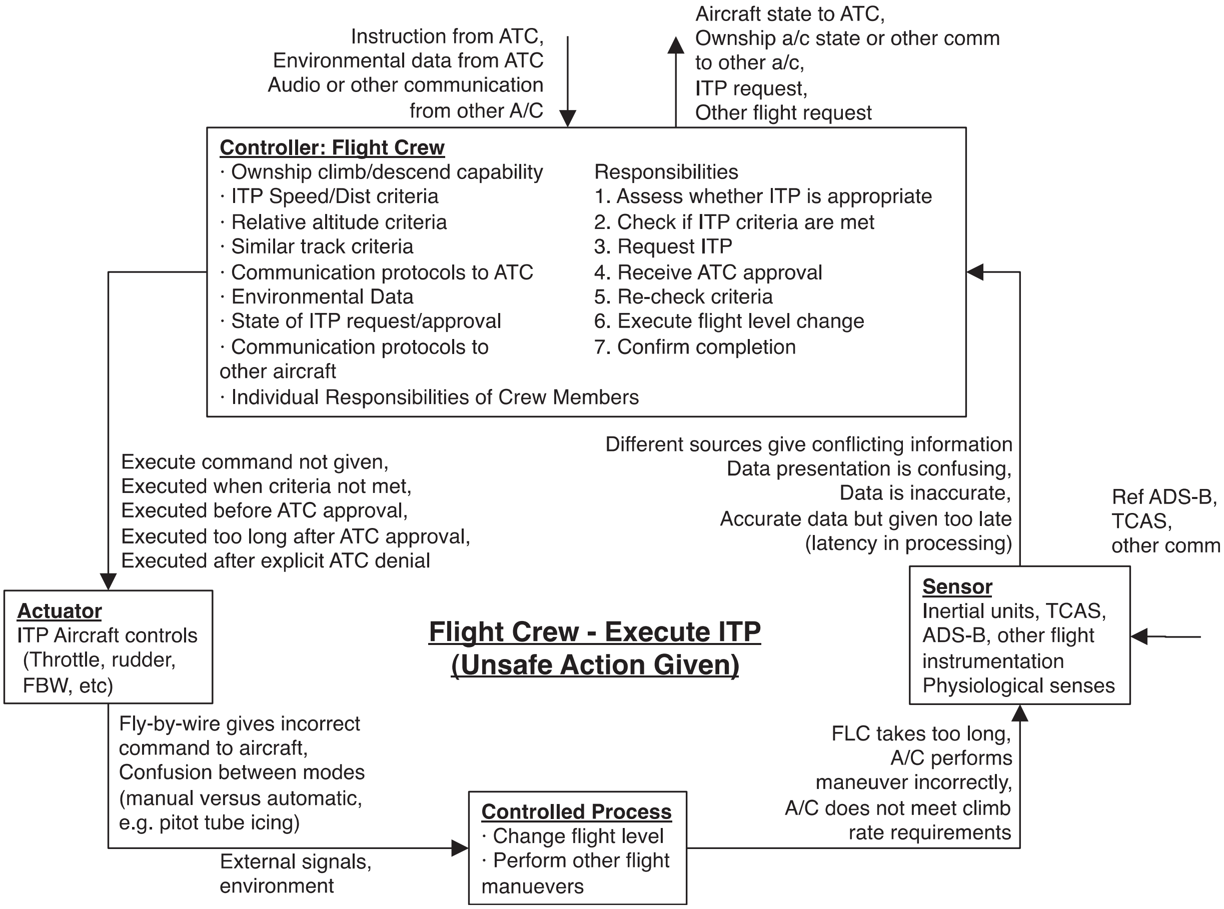

Procedure not compliant with C2 (ITP distance >15(20) NM), undetected by ATC and FC
Safety Objective: 1.63E-3 per ITP operation
OH2U2B
Q=1.010e-4
FC does not understand what the minimum ITP distance is and accepts an ITP with a distance that is less than required
FC-05
Q=0.01
Q=1.000e-2
GND fails to detect that range is not compliant to ITP
C2 - GND FAIL
Q=1.010e-2
ATC does not receive ITP distance but approves ITP or receives distance but fails to detect it is not compliant
GND-01
Q=0.0001
Q=1.000e-4
Communication errors (partial corruption of the message during the transport)
ENVT-02
Q=0.01
Q=1.000e-2

Figure 11: Example Fault Tree from DO-312 [4]

4.2.2 STPA Approach

Figure 12 shows the results of STPA and the various causes identified using controls and systems theory. The STPA example includes the basic communication errors included in FTA, but it also includes additional reasons for communication errors as well as guidance for understanding human error within the context of the system. Communication errors may result because there is confusion about multiple sources of information (for either the flight crew or ATC), confusion about heritage or newly implemented communication protocols, or simple transcription or speaking errors. There is no way to quantify or verify the probabilities of any of these sources of error for many reasons, particularly because the errors are dependent on context and the operator environments are highly dynamic. Instead of assuming that humans will rarely "fail," our analysis assumes they will make mistakes and specifies requirements accordingly.



Instruction from ATC,
Environmental data from ATC
Audio or other communication
from other A/C
Aircraft state to ATC,
Ownship a/c state or other comm
to other a/c,
ITP request,
Other flight request
Controller: Flight Crew
· Ownship climb/descend capability
· ITP Speed/Dist criteria
· Relative altitude criteria
· Similar track criteria
· Communication protocols to ATC
· Environmental Data
· State of ITP request/approval
· Communication protocols to other aircraft
· Individual Responsibilities of Crew Members
Responsibilities
1. Assess whether ITP is appropriate
2. Check if ITP criteria are met
3. Request ITP
4. Receive ATC approval
5. Re-check criteria
6. Execute flight level change
7. Confirm completion
Execute command not given,
Executed when criteria not met,
Executed before ATC approval,
Executed too long after ATC approval,
Executed after explicit ATC denial
Different sources give conflicting information
Data presentation is confusing,
Data is inaccurate,
Accurate data but given too late
(latency in processing)
Ref ADS-B,
TCAS,
other comm
Actuator
ITP Aircraft controls
(Throttle, rudder,
FBW, etc)
Flight Crew - Execute ITP
(Unsafe Action Given)
Sensor
Inertial units, TCAS,
ADS-B, other flight
instrumentation
Physiological senses
Fly-by-wire gives incorrect
command to aircraft,
Confusion between modes
(manual versus automatic,
e.g. pitot tube icing)
FLC takes too long,
A/C performs
maneuver incorrectly,
A/C does not meet climb
rate requirements
Controlled Process
· Change flight level
· Perform other flight
manuevers
External signals,
environment

Figure 12: Example STPA Results

4.2.3 Specifications and Summary of Results

Each analysis results in a specification: either assumptions about the system (DO-312) or requirements on system components or operators (STPA).[13] The approach to human and software behavior in DO-312 leads to assumptions about their performance, while STPA results in requirements that constrain or enforce certain types of behavior. Table 6 shows this difference and maps the analyses shown in Figure 11 and Figure 12. While DO-312 assumes or requires that a communication error (due only to corruption of data) occurs no more than "*often*," STPA specifies requirements to ensure that communication is done correctly and completely and also specifies ways to detect if communication has not been done correctly. Further refinement of the STPA requirements will result in specifications that relate to timing or obsolescence of data and accounts for the processes by which humans make decisions, instead of assuming that ATC error is Very Rare.[14] Table 6 illustrates the difference in specifications, and how these differences necessarily arise from the differences in the philosophical approach to safety assurance; the techniques used to model system behavior; the more powerful treatment of system complexity, human performance, software behavior included in STPA; and the definitions used within these techniques.

Table 6: Comparison of Specifications

	DO-312	**STPA**
Requirements and Assumptions	Assumption **AS.40** The probability that ATC does not receive ITP Distance (as part of the ITP climb/descent request) but approves ITP procedure or fails to detect that ITP Distance received in the request is not compliant, is assumed to occur no more frequently than Very Rare. **AS.12** The corruption of information because of HF occurs no more than Often.	Requirement **[1.1.2]** ITP shall provide the flight crews of aircraft operating in procedural airspace the ability to determine a clear procedure for communicating data about the desired flight level change and necessary state data to the local air traffic controller **[1.2.1.1]** Once ITP request has been made, all communication between ATC and the FC must occur on the same communication channel **[1.2.1.2]** All communication protocols must include definitions of when a communication is complete

[13] Both approaches ultimately include assumptions about behavior or environment, just as both approaches lead to specific requirements about behavior or performance. But this example illustrates how the different approaches yield totally divergent results.

[14] See [4] or Section 3 herein for a further description of what these assumptions mean.

	DO-312	STPA
		[1.10] – [1.17] (see appendix B) **[1.18]** ATC must have access to current* knowledge of the velocity, heading, and location of all aircraft involved in ITP request Assumption: ATC will have this knowledge as part of their overall ability to maintain separation, regardless of ITP clearances.

5 Conclusions

In this report, we compared the safety assurance methodology being used on ATSA-ITP with a more general approach called STAMP/STPA. While the assurance methods used for ITP were based on older, chain-of-events models of accident causation, STPA is based on a systems-theoretic model that captures additional accident causes associated with the complex socio-technical systems of today. STPA is a more powerful hazard analysis technique that not only captures the failure modes identified in event or fault tree analyses but also captures errors due to interaction or inadequate specifications that are prevalent in complex systems.

The type of specification and certification of requirements for ATSA-ITP that arise using STAMP/STPA are much more in line with approaches used traditionally in aircraft system certification (for example, TCAS II [2]) than that being used for NextGen.

This report also illustrates the importance of the philosophical assumptions that undergird any approach to safety assurance as well as the definitions of the approach's constituent parts. One approach is to assume likely or expected system behavior and predict accident causation based on nominal behavior or from deviations off of nominal. However, accidents do not, and should not, occur when a system is behaving normally, but rather accidents happen because of a confluence of events and causes that are often related. By trying to show how or why an accident *can* happen, an analysis can produce a more complete set of potential accident causes. Combining an approach that assumes worst-case system behavior with analytical techniques that capture component interaction and emergent system properties should produce a more comprehensive set of safety-related requirements that apply to the complex, dynamic nature of NextGen and future changes in the NAS.

6 References

[1] Leveson, N.G., "Intent Specifications: An Approach to Building Human-Centered Specifications," *IEEE Transactions on Software Engineering*, SE-26, No. 1, January 2000.

[2] Leveson, N.G., Heimdahl, M.P.E., Hildreth, H., Reese, J.D., "Requirements Specification for Process-Control Systems," *IEEE Transactions on Software Engineering*, SE-20, No. 9, September, 1994.

[3] FAA, "System Safety Handbook: Practices and Guidelines for Conducting System Safety Engineering and Management," FAA, Washington DC, December 30, 2000.

[4] RTCA, "Safety, Performance and Interoperability Requirements Document for the In-Trail Procedure in the Oceanic Airspace (ATSA-ITP) Application," DO-312, Washington DC, June 19, 2008

[5] Leveson, N.G., *Safeware: System Safety and Computers*, Addison Wesley Publishers, 1995.

[6] Leveson, N.G., *Engineering a Safer World*, MIT Press, in production (to appear in print in 2012), available freely at http://sunnyday.mit.edu/safer-world.

[7] Pereira, S.J., Lee, G., and Howard, J.. "A System-Theoretic Hazard Analysis Methodology for a Non-advocate Safety Assessment of the Ballistic Missile Defense System," *AIAA Missile Sciences Conference*, Monterey, CA, Nov. 2006.

[8] Houck, O.A., "Worst Case and the Deepwater Horizon Blowout: There Ought to be a Law," *Environmental Law Reporter*, 40 ELR 11036, Nov., 2010.

[9] FAA, “What is NextGen”, http://www.faa.gov/nextgen/why_nextgen_matters/what/

[10] NextGen Integration and Implementation Office, “FAA’s NextGen Implementation Plan”, FAA, March 2011.

[11] Dekker S.W.A., *Ten Questions About Human Error: A New View of Human Factors and System Safety*, CRC Press, 2004.

[12] EUROCONTROL. Safety Regulatory Requirement — ESARR 4: Risk Assessment and Mitigation in ATM, Edition 1.0.

[13] Leveson, N.G. A New Accident Model for Engineering Safer Systems, *Safety Science*, 42(4):237-270, April 2004.

[14] Leveson, N.G. A Systems-Theoretic Approach to Safety in Software-Intensive Systems, *IEEE Trans. on Dependable and Secure Computing*, Vol. 1, No. 1, January 2005.

[15] Leveson N.G. et al, A Safety and Human-Centered Approach to Developing New Air Traffic Management Tools. *ATM 2001*, Albuquerque NM, December 2001.

Appendix A – Acronyms

Intent Specification Terms:

1 – 5:	Requirements Level
G:	Goal (Level 1)
EA:	Environmental Assumption (Level 1)
EC:	Environmental Constraint (Level 1)
OP:	Operator Behavior (Level 1)
L:	Limitation (Level 1)
C:	Non-safety related Design Constraint (Level 1)
SC:	Safety-related Design Constraint (Level 1)

Other Terms:

ADS-B:	Automatic Dependant Surveillance Broadcast
ASTA:	Airborne Traffic Situational Awareness
ATC:	Air Traffic Controller
FC:	Flight Crew
FL:	Flight Level
ITP:	In Trail Procedure
RA:	Reference Aircraft

Appendix B – Intent Specification

B.1 Preface

The ATSA-ITP requirements are specified as an intent specification in this document. Intent specifications were developed as a result of the efforts to certify TCAS-II [2]. It differs from a standard specification primarily in its structure: Hierarchical abstraction is based on *intent* (“why”) rather than simply the more usual *what* and *how*. Because each level is mapped to the appropriate part of the intent levels above and below it, traceability of design rationale and design decisions is provided from high-level system requirements and constraints down to code (or physical form if the function is implemented in hardware) and vice versa. Only the first three levels of the intent specification are included here because the goal is to provide a requirements specification that can be used by the manufacturers of the ITP boxes.

There are five levels to an intent specification. Each level supports a different type of reasoning about the system and represents a different model of the same system. The model at each level is described in terms of a different set of attributes and perhaps language.

The highest level of an intent specification represents the “contract” between the customer and the system engineers and assists the system engineers in their reasoning about system-level properties such as system goals, requirements, constraints, priorities, and tradeoffs among them. The second level, System Design Principles, allows engineers to reason about the system in terms of the physical principles and laws upon which the design is based. The third, or Component Blackbox Behavior level, provides a formal, executable model of the system and enhances reasoni8ng about the logical design of the system as a whole and the interactions among the components as well as the functional state without being distracted by implementation issues. The lowest two levels provide the information necessary to reason about individual component design and implementation issues. The mappings between levels provide the relational information that allows reasoning across the hierarchical levels and tracing from high-level requirements down to implementation and vice versa.

The intent information represents the design rationale upon which the specification is based and, thus, design rationale is integrated directly into the specification. Each level also contains information about underlying *assumptions* upon which the design and validation is based. Assumptions are especially important in operational safety analyses. When conditions change such that the assumptions are no longer true, then a new safety analysis should be triggered. These assumptions may be included in a safety analysis document (or at least should be), but are not usually traced to the parts of the implementation they affect. Thus the system safety engineer may know that a safety analysis has changed (e.g., the pacemakers are now being used on children rather than the adults for which the device was originally designed and validated), but it is a very difficult and resource-intensive process to figure out what parts of the design used that assumption.

Each of the five intent levels is also organized in terms of the more common part-whole abstractions, i.e., parallel decomposition and refinement. Each level also contains a specification of the requirements and results of verification and validation activities of the information at that specification level.

The specification as a whole allows a seamless transition from system to component (including software) specifications and the integration of formal and informal aspects of system and software development. Because the structuring is based on what is know about human problem solving, we believe this type of specification will enhance human processing and use of specifications and will also enhance our ability to engineer for quality and to build evolvable and changeable systems without degrading quality. The structure is designed to facilitate the tracing of system-level requirements and constraints into the design and the assurance of various system properties (such as safety0 in the initial design and implementation as well as reduce the costs of implementing changes and reanalysis when the system is changed, as it inevitably will be.

In this document, we try to use industry standard terminology where "shall" represents a requirement, "should" denotes an option, "must" represents a constraint and "will" denotes an assumption about the environment. We had to guess at some of these because of incompleteness in the documents we used to describe ATSA-ITP. Mappings are indicated by pointers. The first number or letters of a link tells you where it is located or its type:

Number 1-5: the level on which it is located

G: a goal

EA: environmental assumption

OP: operational behavioral requirement, assumption, or constraint

L: limitation

C: non-safety-related design constraint

SC: safety-related design constraint

STPA-x: the part of the STPA (hazard) analysis involved

B.2 Caveats

This specification and safety analysis is only an example. It was created using the information we have about ITP, which may be incomplete. In addition, it has had no review from anyone outside our research group nor any ITP expert. The underlying assumptions upon which the specification is based are not complete due to our lack of knowledge about ITP.

B.3 Level 1 System-Level Goals, Requirements, Constraints and Hazard Analysis

B.3.1 Introduction

The enhanced Airborne Traffic Situational Awareness (ATSA) for "In Trail Procedure" (ITP) enables either leading or following Same Track aircraft to perform a climb or descent to a Requested Flight Level through Intervening Flight Levels. The application will require the crew to use information derived on the aircraft to determine if the criteria for applying the ITP procedures are met with respect to one or two Reference Aircraft at Intervening Flight Levels.

The proposed format of the ITP will entail three broad phases. First, during the *Initiation Phase*, the flight crew of the ITP craft will use the ITP equipment to check that an ITP maneuver is possible based on the proscribed criteria. Once it is determined that the flight level change is possible, the flight crew will request clearance from sector Air Traffic Control (ATC). During the next phase, the *Instruction Phase*, ATC will verify that all ITP criteria are met and then communicate an approval or denial of the request back to the ITP flight crew. In the case of an approval, the flight crew will then check all ITP criteria once more. After all criteria are re-checked, the flight crew begins the *Execution Phase* by performing the maneuver and concludes it by informing ATC that the maneuver is complete.

ITP maneuvers can fall into six categories based on the relative positions of the aircraft requesting ITP clearance and the aircraft(s) that it uses as a reference aircraft (RA) during the maneuver. Those categories are: a following climb/descent (where the ITP craft is following the RA), a leading climb/descent (where the ITP craft is leading the RA) and a combined leading-following climb/descent (where the ITP craft has a RA both leading and following it).

While the addition of ITP does move some of air traffic controls responsibility (namely, determining initial feasibility of a maneuver) into the cockpit, it is not meant to replace the air traffic controller who will retain ultimate approval authority.

B.3.2 Historical Information

Because of the limited radar coverage in oceanic and other remote airspaces, air traffic controllers have historically relied on procedural separation rules to ensure safe traffic. Aircraft in these sectors generally fly long, pre-defined flight paths, and air traffic controllers have few options for accurately knowing the positions of all aircraft in a sector at the same time or the ability to directly communicate with aircraft. To compensate for these limitations, these sectors of the airspace often have much larger separation requirements than those applied to airspace with more surveillance and communication coverage. These large separation minimum mean, however, that there are severe limits on the capacity of a given track in a remote airspace.

It is often desirable for aircraft to make flight level (FL) changes during long-haul flights. Because of the changes in aircraft weight over the course of the flight (as fuel is burned), different flight levels will allow for greater fuel efficiency. However, because of the large separation requirements, it is often the case that a desired flight level might not be available due to the presence of "blocking" aircraft in intervening flight levels that fall within the minimum longitudinal separation distance.

The new In-Trail Procedure (ITP) described in this document would allow many of these previously blocked flight level changes to occur. The details of the procedure were developed as part of the Enhanced Oceanic Operations (EOO) research done under the NASA Next Generation Air Transportation System (NextGen) Air Traffic Management Airspace project. The primary goal of EOO was the development of the methodologies and procedures necessary to reduce the aforementioned longitudinal separation requirements. Full details of the ITP procedure can be found in the Operational Services and Environment Description Document (DO-312) produced by RTCA.

B.3.3 Environment

This section describes the environment in which the ITP equipment and procedures need to operate, including how the addition of ITP equipment will interact with other aircraft systems already in place. Because ITP is a procedure applied by both the flight crew and air traffic controllers, it affects the work load of these operators.

ITP Equipment must function within the broader context of general aircraft operations. Furthermore, in order to function as desired, the equipment depends on other components within and outside of the aircraft. The primary external links to and from ITP equipment consist of the interface with the Flight Crew and the transponder that transmits state data about the ITP and Reference Aircraft. The primary links between the Flight Crew and ATC remain the existing Direct Controller-Pilot Communication (DCPC) modes, or communication channels such as radio and datalink that do not rely on a third party for communication between ATC and the flight crew. Figure B.1 shows how the ITP equipment will interact with other system components in a typical implementation.

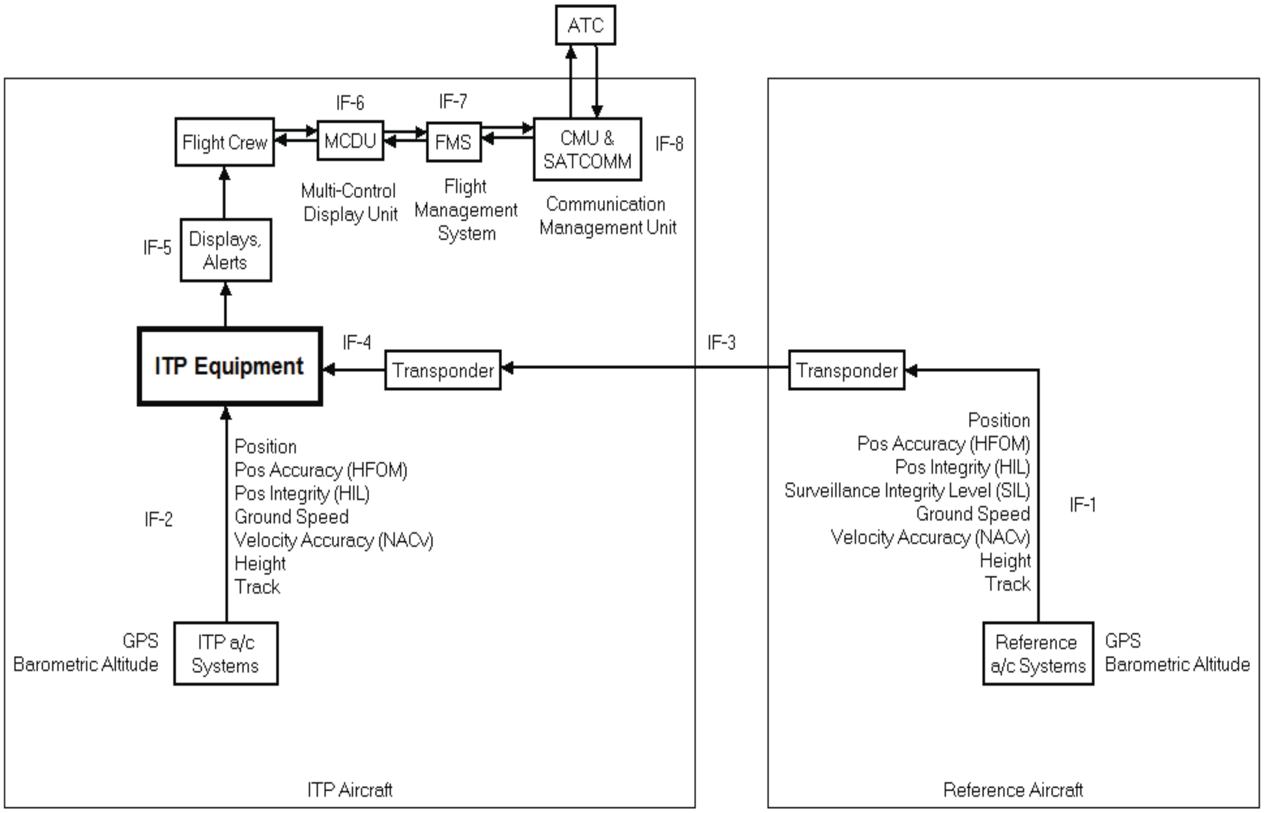


Figure B.1 ITP Equipment Interface

Key to Figure :

- IF-1 = Encompasses the following:

    - Position sensor input interface, e.g., at sensor antenna, for Reference Aircraft
    - Sensor outputs for Reference Aircraft
    - Output from Surveillance Transmit Processing (STP) to the ADS-B Transmit function
- IF-2 = Encompasses the following
    - Position sensor source input interface, e.g., at sensor antenna, for ITP Aircraft
    - Sensor outputs for ITP Aircraft
- IF-3 = ADS-B link environment
- IF-4 = ADS-B receive function, generating ADS-B reports for ITP equipment
- IF-5 through IF-8 are specific to the manufacturer and operator implementation

B.3.3.1 State Data

The data necessary to calculate ITP feasibility consists of position, velocity and time (PVT) information for both the ITP aircraft and all surrounding aircraft, especially potentially blocking aircraft at intervening flight levels that may impact the desirability of a flight level change. This state data may be calculated from reported data or measured directly by the aircraft in question. These describe the items along lines IF-1 and IF-2 in Figure B.1.

- ***ADS-B Transmit Aircraft Data***

  ITP state data for all potentially blocking aircraft will come from ADS-B data for surrounding aircraft, hereafter referred to as 'Transmit Aircraft'. The minimum data required consist of Identity, Horizontal Position, Vertical Position, Horizontal Velocity, and Surveillance Quality Indication (used to determine if the data is of high enough quality to be used for the ITP calculation).

- ***Transmit Aircraft Identity***

  The identity of all transmit aircraft will be the 24 bit aircraft address within the ADS-B message. This identity is defined, as per IAO Doc 444 as 'a group of letters, figures or a combination thereof which is either identical to, or the coded equivalent of, the aircraft call sign to be used in air-ground communications, and which is used to identify the aircraft in ground-ground air traffic services communications.' This identification is further clarified to be either the call sign (e.g. KLM511, AA321, etc) or the registration marking of the aircraft; neither one may exceed 7 characters.

- ***Transmit Aircraft Horizontal Position***

  The transmit aircraft will transmit information that can be used to calculate its horizontal position (i.e. latitude, longitude) along with quality indicators (for accuracy and integrity) for these values. This data will be used to calculate relative track angle to the ITP aircraft (this angle must be less than 45 or more than 315 degrees in order for ITP criteria to be met).

- ***Transmit Aircraft Vertical Position***

  The transmit aircraft will send its barometric altitude to demonstrate its vertical position.

- ***Transmit Aircraft Horizontal Velocity***

  The transmit aircraft will transmit its horizontal velocity (ground velocity) along with a quality indicator.

- ***Receive Aircraft Data***

  The receive aircraft—that is the aircraft that seeks to gain clearance for an ITP must have the same state data for itself. This includes horizontal position, barometric altitude, horizontal velocity, horizontal position accuracy, and horizontal velocity accuracy and integrity indicators.

B.3.3.2 Direct Controller-Pilot Communication

All communication for ITP is accomplished through Direct Controller-Pilot Communication. This may be via a voice communication over radio, or text communication, but there will not be a third party relaying messages between the flight crew and air traffic control.

B.3.3.3 Collision Avoidance Systems

While it is not required that ITP aircraft are equipped with an Airborne Collision Avoidance System (or Traffic Alert and Collision Avoidance System), most aircraft operating within procedural airspace will be so equipped. Although any advisories from an ACAS do not impact the ITP calculation, pilots will have the additional situation awareness that is provided by these systems.

B.3.4 Environmental Assumptions

This section contains the environmental assumptions upon which the ITP Equipment Certification is based. Any changes to these assumptions may require changes to the requirements and therefore the minimum number of assumptions necessary should be made. Any changes to these assumptions should trigger a reevaluation of the requirements, including a reevaluation of the safety analysis and safety design features.

The correct operation of ITP Equipment is based on assumptions about the environment in which the equipment operates and the procedure is applied:

[EA.1] ITP as analyzed in this document will be used only in areas of procedural (non-radar) control—areas of the airspace where procedural separation minima are applied and where the air traffic controller has limited ability to obtain real-time traffic information.

[EA.2] High-integrity communications exist between ITP Flight Crew and ATC, e.g. CPDLC, SatComm

[EA.3] Any aircraft requesting ITP will have up-to-date ITP equipment on board and a crew that is trained in performing ITP.

[EA.4] All other aircraft in the region of the ITP aircraft will be known to the sector ATC.

[EA.5] All aircraft will have legal identification numbers known to ATC.

[EA.6] All data transmitted by ADS-B to the ITP aircraft has the level of accuracy specified in DO-242A.

[EA.7] All ITP aircraft will meet the airworthiness standards set by the FAA.

[EA.8] Pilots in procedural airspace will not make changes to their own flight clearance (such as increasing mach) in order to meet ITP criteria.[15]

[EA.9] FC will continue to have primary responsibility for the operation of their own aircraft and the proper conformance to clearances issued by air traffic control.

[15] This is included in the environmental assumptions because it intends to address actions taken by a pilot prior to requesting clearance for ITP. In F. J. L. Bussink, et al., "PILOT IN-TRAIL PROCEDURE VALIDATION SIMULATION STUDY," (2008), the authors describe an incident when a pilot participating in an ITP simulation study realized prior to requesting ITP that his mach differential would not meet criteria, so increased his mach by .001 in order to request ITP. Because this occurs outside of the ITP process, we are classifying it as an environmental assumption.

[EA.10] ATC will continue to have primary responsibility for the safe separation of aircraft and the issuance of clearances.

B.3.5 Environmental Constraints

[EC.1] The behavior of the ITP equipment must not be degraded by the behavior of or interaction with non-ITP equipment.

[EC.2] The behavior of the non-ITP equipment must not be degraded by the behavior or interaction with ITP equipment.

B.3.6 System Goals

To provide a procedure that will allow pilots operating in Procedural Airspace to make desired Flight Level changes on a more frequent basis, in order to improve both efficiency on these tracks while also maintaining safe separation from other aircraft in the vicinity.

[G.1] Provide flight crews operating in Procedural Airspace the ability to determine if a flight level change is feasible prior to contacting ATC for clearance. (→[SC-FC.2], [1.6], [1.8],↓[2.1],[2.15],[2.32])

[G.2] Provide flight crews the ability to understand the state of nearby traffic in areas not covered by ATC or radar systems. (→[1.7],↓[2.28])

[G.3] Provide flight crews with the necessary information to communicate to sector ATC their intended flight level change and the presence of potentially blocking aircraft. (→[SC-FC.1], [1.3],↓[2.3])

[G.3.1] The ITP procedure must not add to the workload of the FC

[G.4] Ensure that Air Traffic Controllers have the necessary information to issue flight level change clearances in Procedural airspace and continue to ensure aircraft separation. (→[SC-ATC.1], [SC-FC.1], [1.9],↓[2.2])

[G.4.1] The ITP procedure must not add to the workload of the ATC

B.3.7 System Limitations

Some hazards or hazard causes cannot be eliminated or controlled by the system design. Decision makers need to decide whether the risk is acceptable. Such decisions may require a risk assessment beyond the scope of this document or information we do not have available.

[L.1] The ITP equipment provides no information about nearby aircraft that do not transmit ADS-B data. (↓[2.32])

[L.2] ITP depends on the accuracy of the transmit aircraft's data and the ITP aircraft's internal data, including the ADS-B data that is used for clearance calculations. If any of that data is degraded, the separation assurance calculated by ITP will be similarly degraded. (↓[2.1.4],[2.32.4])

Rationale: This limitation holds for existing reliance on aircraft data, and for the safe completion of procedures other than ITP.

[L.3] Some of the data necessary to determine strict ITP feasibility will only be available to the ITP flight crew. ATCs ability to correctly analyze and apply this data relies on the ITP flight crew correctly transmitting it to ATC. (↓[1.3.1],[2.2],[2.3])

[L.4] The correct implementation of ITP relies on the ITP flight crew's ability to determine that an ITP maneuver is correct and feasible. ITP will not "alert" the crew that ITP may be possible. (↓[2.1])

Rationale: This is included here as a limitation, but it essentially a design choice and is covered as such in Level 2.

B.3.8 System Control Structure

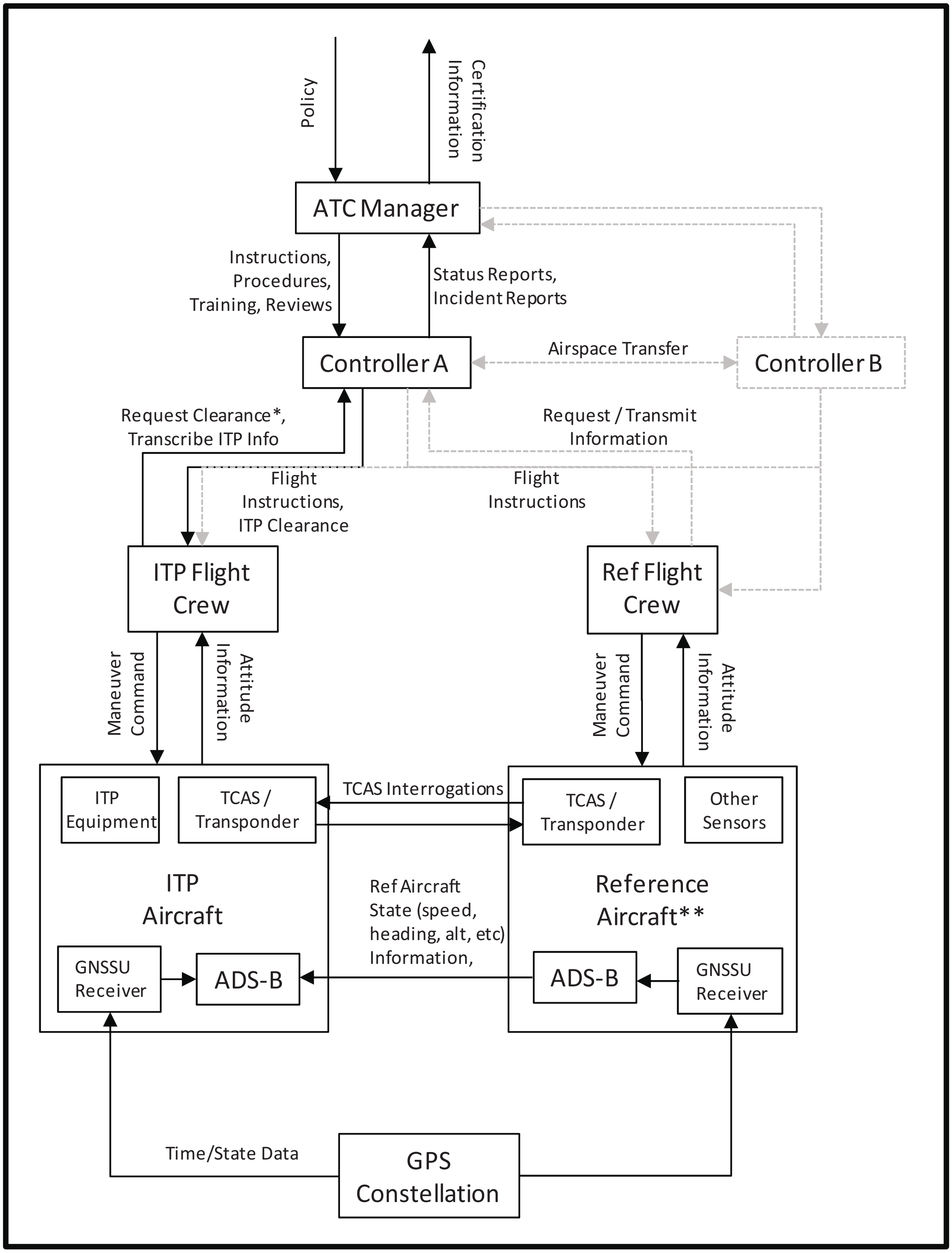


Figure B.2 Control Structure of ASTA-ITP System

FigureB.2 shows the high-level control structure for ASTA-ITP. The primary controllers at the system level are the air traffic controller and the flight crew. We limit our specification and analysis of the system to these two controllers and do not look at higher levels of the socio-technical system.

The flight crew of the ITP aircraft requests clearance from the current controller of the aircraft and sends ITP information to be used in granting the clearance. The air traffic controller provides a clearance and flight instructions. The flight crew in turn gets information about the satisfaction of the ITP criteria from the ITP equipment and uses that and the clearance to execute the maneuver.

The diagram also shows the flight crew of the reference aircraft used during the ASTA-ITP and uses dashed lines to illustrate that while the flow of information, control and feedback between the Reference Aircraft (RA) and ATC is not a direct part of ITP[16], it plays an important role in the implementation and safety of the procedure.

[16] The resulting process model of the controller is certainly important to the analysis, but the mechanisms for informing that model are not directly part of the new ITP.

B.3.9 Hazard Analysis

This section provides an example of a hazard analysis using System-Theoretic Process Analysis (STPA), the details of which can be found in Leveson's upcoming book, "Engineering A Safer World: Systems Thinking Applied to Safety."[17] *A description of the process is included, but would not be part of a normal intent specification.*

The general ICAO safety policy concerned is that the addition of any new protocols or equipment must not affect the aircraft or other aircraft or air traffic control in a way that can adversely affect the safety of the flight. The hazard analysis is used to ensure that the design of the ITP equipment and procedures do not violate this policy.

A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident or loss. Hazards are potentially unsafe states that the system design should eliminate, and if they cannot be eliminated, then they must be controlled. Table B.1 shows the high-level system hazards we considered for ASTA-ITP. Different hazards might be considered depending on decisions by the regulatory agencies and international standards.

B.3.9.1 High-Level System Hazards

Table B.1: Hazards Associated with ASTA-ITP

ID	Description
H-1	A pair of controlled aircraft violate minimum separation standards
H-2	Aircraft enters unsafe atmospheric region
H-3	Aircraft enters uncontrolled state
H-4	Aircraft enters unsafe attitude (excessive turbulence or pitch/roll/yaw that causes passenger injury but not necessarily aircraft loss)
H-5	Aircraft enters a prohibited area

B.3.9.2 Unsafe Control Actions

Next, for the two controllers with which we are concerned, we must determine how those controllers might exert unsafe control on the system—an action that has the potential to result in a hazardous system state or the lack of an action needed to prevent a hazardous system state. In the case of ASTA-ITP, the hazardous state that we are most concerned with is *H-1: a pair of*

[17] To be published by MIT Press in Fall 2011, available online: http://sunnyday.mit.edu/safer-world/safer-world.pdf

controlled aircraft violates minimum separation standards. We considered the other hazards but did not find that introducing ITP over oceanic airspace could lead to them. If ITP is used in other airspace or under other conditions, then the other hazards must be analyzed (see Environmental Assumption EA.1).

A controller can provide unsafe control in four ways

1. An unsafe control action is provided that moves the system into a hazardous state
2. Control actions required for safety are not provided (that is, a hazard occurs due to lack of a control action)
3. Necessary control actions for safety are provided by at the wrong time or in the wrong sequence
4. A control action required for safety is stopped too soon or applied too long.

To assist in identifying the hazardous control actions, we use a table to look at all these possibilities for each of the control actions. Only some of them will turn out to be hazardous but considering all incorrect control actions will identify those that are hazardous under certain conditions.

The responsibilities of the Air Traffic Controller are to process the ITP request of the flight crew, which involves analyzing the ITP data and the traffic in the area and to communicate approval or denial of the request. The control actions provided by the Air Traffic Controller are to approve the ITP request, to deny the ITP request, or to tell the flight crew to abort the procedure.

Table B.2 summarizes the hazardous control actions by ATC.

At this level in the analysis, the control actions are considered at a very high level. Later analysis, if necessary, will break these high-level control actions into their constituent pieces. That is, instead of considering a very specific action (e.g. “pilot uses aircraft elevators to increase flight level”) we have focused specifically on the control actions of the ITP as a process (e.g. “pilot performs ITP”). For the purposes of providing requirements for ITP, the specific details of how to fly an aircraft or how to direct air traffic do not need to be analyzed—we instead focus on the procedure itself as a control action, and not the individual actions of each controller that comprise the procedure at this first high-level analysis.

Table B.2: Unsafe Control Actions for Air Traffic Control

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopped Too Soon or Applied Too Long
Approve ITP request		Approval given when criteria are not met Approval given to incorrect aircraft	Approval given too early Approval given too late	
Deny ITP request				

Abnormal Termination Instruction	Aircraft should abort but instruction not given	Abort instruction given when abort is not necessary	Abort instruction given too late	

Four control actions of the air traffic controller are identified as unsafe in Table B.2 and need to be further analyzed to determine their potential causes. The reasons why these are unsafe should be fairly obvious: an incorrect or out of sequence ITP approval can directly lead to loss of separation, and an unnecessary or incorrect abnormal termination command introduces unnecessary maneuvering under uncertain conditions.

The reason why some of the boxes are empty and thus not considered to be unsafe and subject to further analysis may be less clear. ATC not giving ITP approval is not unsafe because the aircraft will continue on its original flight path (or if it does not, this control action would be an example of the flight crew incorrectly executing ITP, which is captured in the analysis of the flight crew). Likewise, the control action of denying the request may be incorrectly given—that is, ATC may deny a request even though all ITP criteria are met—but because denial of request will mean that the ITP aircraft continues on its flight path, this action will not result in an unsafe scenario. The control actions are discrete so stopped too soon or applied too long are not relevant in this case.

The flight crew can execute the ITP or abort it.

Table B.3: Unsafe Control Actions for ITP Flight Crew

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing/Order Causes Hazard	Stopped Too Soon/Applied Too Long
Execute ITP		ITP executed when not approved ITP executed when ITP criteria are not satisfied ITP executed with incorrect climb rate, final altitude, etc	ITP executed too soon before approval ITP executed too late	
Abnormal Termination of ITP	FC continues with maneuver in dangerous situation	FC aborts unnecessarily FC does not follow regional procedures while aborting		

Four inadequate control actions of the ITP flight crew are identified as potentially unsafe in B.3. Again, these are self-explanatory: when the flight crew incorrectly executes the ITP or does so out of sequence (which we define as prior to receiving approval or not immediately after receiving approval) or does not initiated an abnormal termination or does so incorrectly, this action may very clearly put the ITP aircraft in proximity of a nearby aircraft. The other inadequate control actions are not highlighted as unsafe for one of three reasons. They are either not unsafe, as is the case of the flight crew not executing IT, they are logically identical to other inadequate control actions (e.g., ITP executed beyond final altitude), or they are illogical (ITP cannot be abnormally terminated if it has not begun or has already completed).

The 14 identified unsafe control actions (hazards) can be translated into high-level safety constraints on the air traffic controller and the flight crew:

[SC-ATC.1] Approval of an ITP request must be given only when the ITP criteria are met. (→STPA-ATC.1, [1.14])

Hazard: H1

1) Unsafe Control Action: ATC Approval Given to Incorrect Aircraft

Process Model Link	Cause
(1) Inadequate Control Algorithm	Algorithm does not include a check / verification of aircraft ID
(2) Process Model Inconsistent	Abundance of aircraft in particular area of sector
	Other aircraft (non-requesting a/c) in airspace with similar state data or aircraft ID
	Other simultaneous requests occur within the ATC domain, including ITP or non-ITP requests
	ATC confuses the Reference and ITP aircraft. This could be due to lack of understanding of ITP architecture, or to a simple “slip”
(3) Inadequate actuator operation	Communication channel to flight crew becomes corrupted
(4) Component Failures/ Changes over time	
(5) Inadequate sensor operation	Datalink becomes corrupted
(6) Incorrect or no information provided (by flight crew)	Flight crew incorrectly transcribes data into CPDLC
	Flight crew does not included aircraft ID in ITP request
(7) Inadequate or missing feedback to controller, feedback delays	Incorrect Aircraft (non ITP requesting) confirms or accepts approval
	Incorrect Aircraft does not immediately respond about discrepancy (i.e. flight crew does not indicate to the ATC soon enough that it is incorrect recipient)

[SC-ATC.2] Approval must be given to the requesting aircraft only. (→STPA-ATC.2, [1.12], [1.14])

[SC-ATC.3] Approval must not be given too early or too late (→STPA-ATC.3, [1.17])

[SC-ATC.4] An abnormal termination instruction must be given when continuing the ITP would be unsafe (→STPA-ATC.4, [1.15], [1.16])

[SC-ATC.5] An abnormal termination instruction must not be given when it is not required to maintain safety and would result in a loss of separation. (→STPA-ATC.5, [1.22.3])

[SC-ATC.6] An abnormal termination instruction must be given immediately if an abort is required (→STPA-ATC.6, [1.22])

The constraints on the flight crew are:

[SC-FC.1] The flight crew must not execute the ITP when it has not been approved by ATC. (→B.11: STPA-FC.2, [1.27], [1.28])

[SC-FC.2] The flight crew must not execute an ITP when the ITP criteria are not satisfied (→ **STPA-FC.1**, [1.23], [1.24], [1.27])

[SC-FC.3] The flight crew must execute the ITP with correct climb rate, flight levels, mach number, and other associated performance criteria (→ **STPA-FC.1**, [1.30])

[SC-FC.4] The flight crew must not continue the ITP maneuver when it would be dangerous to do so (→ **STPA-FC.1**, B.12 STPA-FC.3, [1.33])

[SC-FC.5] The flight crew must not abort the ITP unnecessarily. (Rationale: An abort may violate separation minimums) (→ STPA-FC.4, [1.33.5])

[SC-FC.6] When performing an abort, the flight crew must follow regional procedures (→ STPA-FC.4, [1.33])

[SC-FC.7] The flight crew must not execute the ITP before approval by ATC (→B.11: STPA-FC.2)

[SC-FC.8] The flight crew must execute the ITP immediately when approved unless it would be dangerous to do so. (→B.11: STPA-FC.2, [1.29])

B.3.9.2 Causal Analysis

The next step of STPA is to use the control loops of each controller to determine how each of the 14 identified unsafe control actions (6 for the ATC, 7 for the ITP flight crew) could occur.

Figure B.4 and B.5 show the generic control loops for each of these controllers, followed by a table for each of the 13 unsafe control actions, detailing how problems or errors in each part of the control loop might lead to each of the unsafe control actions. STPA uses a generic feedback control loop model in which the controller exerts a control action on an actuator, which then changes the state of the controlled process. Changes to the process may be fed back to the controller via a sensor, and subsequent control actions may be based on this feedback. STPA examines each of these components—the controller (including the control algorithm and the process model it uses), the actuator, the process itself, and the sensor—as well as the connections between these parts to identify reasons why each of the above unsafe control actions may occur. The identification of unsafe control actions (the arrow between the controller and the actuator) was the first step of STPA, and the casual analysis occurs on the remaining pieces of the control loop.

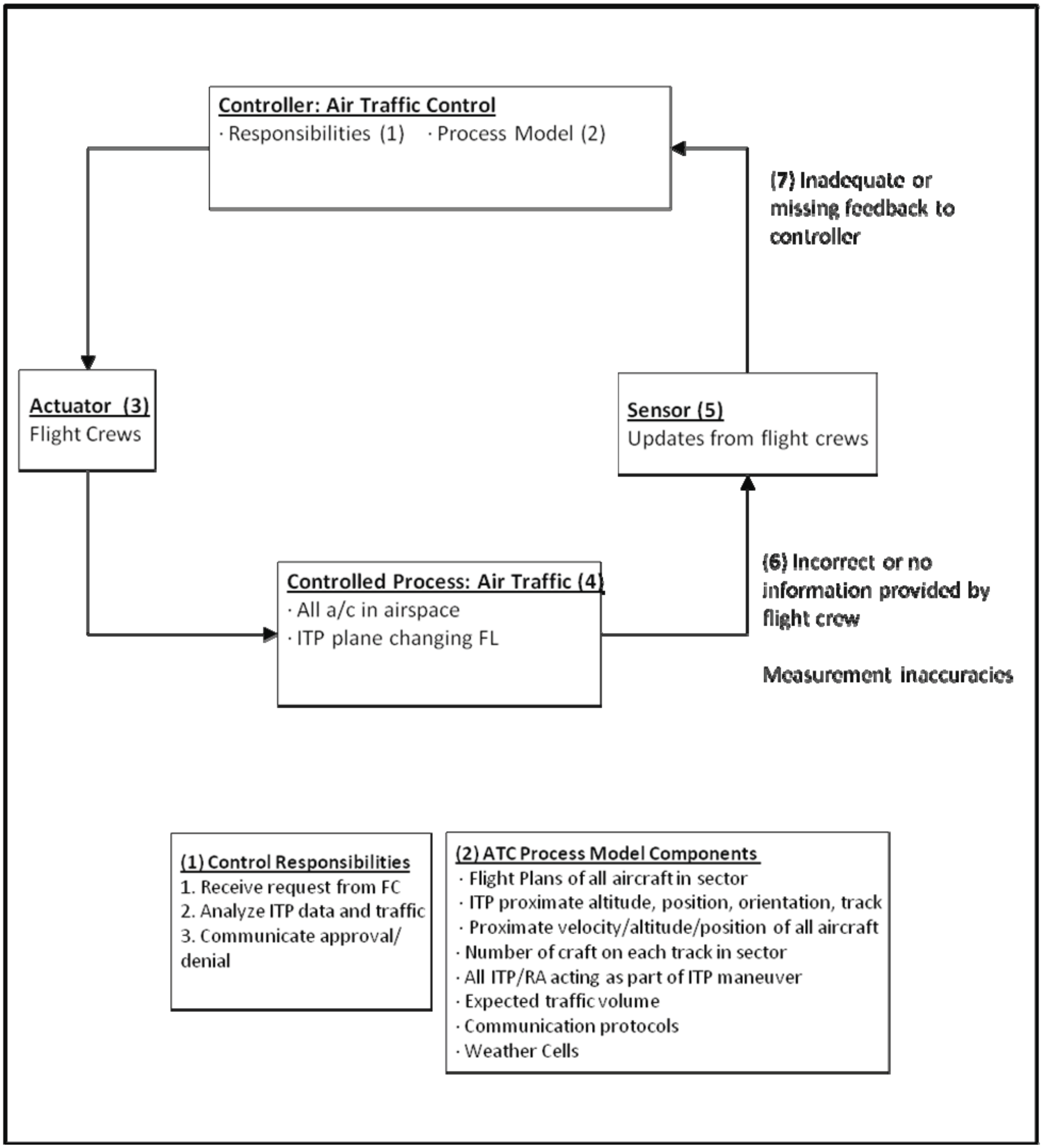

Controller: Air Traffic Control
· Responsibilities (1)
· Process Model (2)
(7) Inadequate or missing feedback to controller
Actuator (3)
Flight Crews
Sensor (5)
Updates from flight crews
Controlled Process: Air Traffic (4)
· All a/c in airspace
· ITP plane changing FL
(6) Incorrect or no information provided by flight crew
Measurement inaccuracies
(1) Control Responsibilities
1. Receive request from FC
2. Analyze ITP data and traffic
3. Communicate approval/ denial
(2) ATC Process Model Components
· Flight Plans of all aircraft in sector
· ITP proximate altitude, position, orientation, track
· Proximate velocity/altitude/position of all aircraft
· Number of craft on each track in sector
· All ITP/RA acting as part of ITP maneuver
· Expected traffic volume
· Communication protocols
· Weather Cells

Figure B.3 Control Loop for ATC during ITP

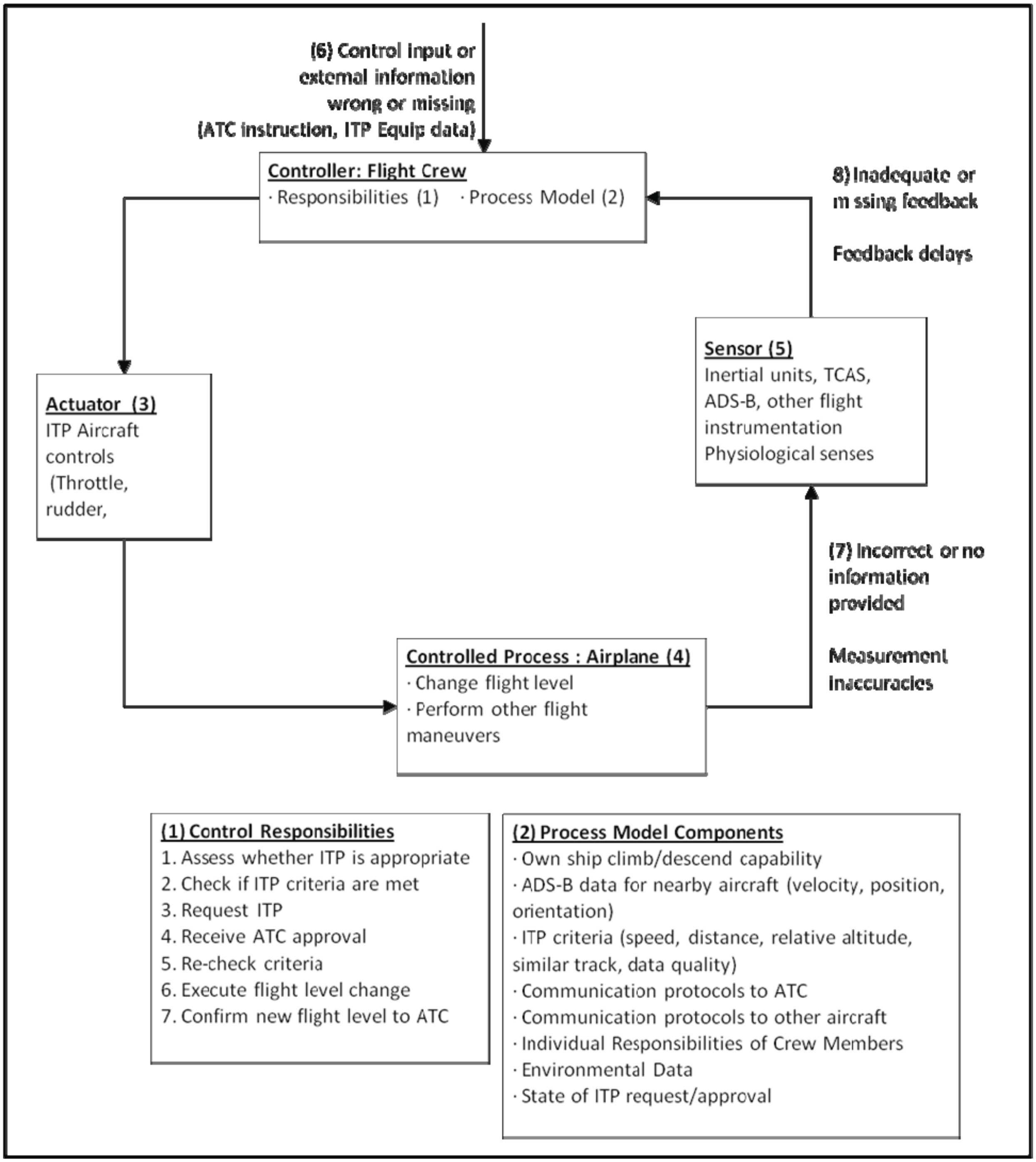

(6) Control input or external information wrong or missing (ATC instruction, ITP Equip data)
Controller: Flight Crew
· Responsibilities (1) · Process Model (2)
8) Inadequate or m ssing feedback
Feedback delays
Sensor (5)
Inertial units, TCAS, ADS-B, other flight instrumentation
Physiological senses
Actuator (3)
ITP Aircraft controls
(Throttle, rudder,
(7) Incorrect or no information provided
Measurement inaccuracies
Controlled Process : Airplane (4)
· Change flight level
· Perform other flight maneuvers
(1) Control Responsibilities
1. Assess whether ITP is appropriate
2. Check if ITP criteria are met
3. Request ITP
4. Receive ATC approval
5. Re-check criteria
6. Execute flight level change
7. Confirm new flight level to ATC
(2) Process Model Components
· Own ship climb/descend capability
· ADS-B data for nearby aircraft (velocity, position, orientation)
· ITP criteria (speed, distance, relative altitude, similar track, data quality)
· Communication protocols to ATC
· Communication protocols to other aircraft
· Individual Responsibilities of Crew Members
· Environmental Data
· State of ITP request/approval

Figure B.4 Control Loop for ITP Flight Crew during ITP

The above diagrams omit any detail on the arrows between the controller and the actuator (upper left-hand portion of diagrams) because the analysis of how the control action may be inappropriate, ineffective or missing is the first step of STPA and can be found in the figures above (Figure B.3 and Figure B.4). Likewise failures in the links between the actuator and the controlled process are captured already: in the case of the ATC control loop: a failure between the actuator (an individual flight crew) and the process (air traffic) applicable to ITP will be captured as a failure of the pilot to exert his own control and in the case of the ITP flight crew, a failure of the actuator implies equipment failure at the component level (e.g. the rudder/throttle/yoke fails).

For both the ATC and the ITP FC, one of the sensors involved in the process is a human operator(s), and the upper-right loop in Figures B.3 and B.4 are the communication channels between ATC and the FC. To examine the lower portion of this feedback, the connection between the process and the sensor, is to examine reasons why the process may not provide feedback. For example, when considering ATC as the controller, this would include reasons why the pilot may not provide feedback (in the case of pilot as controller this would include reasons why the equipment may not provide feedback). Likewise, the upper portion of the feedback, the link between sensor and controller, examines reasons why the controller (ATC) may not *receive* feedback provided by the controlled system or may receive inaccurate feedback.

For each of the unsafe control actions identified above, STPA analyzes each part of this loop to determine the general causes of that unsafe action throughout the loop.[18] At this first-level stage of the analysis these causes are purposefully general—there may be hundreds of reasons *why* the pilot may believe that he or she has received approval when he or she has not, the purpose of this level is not necessarily to identify all of those scenarios, but to ensure that there are appropriate requirements in place to mitigate the effect (potential hazardous scenario) of this situation. Also, some of the links on the control process diagram may not lead to an unsafe control action, and there may not be realistic causes for *all* pieces of the control process for *all* unsafe control actions. Finally, no hazard analysis can ever be complete—there are certainly scenarios and casual factors that any analysis will miss, including STPA. STPA merely provides a more structured framework to complete the analysis and will cast a wider casual net than other, more traditional, methods of hazard analysis because it looks at more than just component failures or faults.

[18] When reading the causal tables, one should interpret the item in the "Cause" column as "a reason for which the unsafe control action in question may arise and lead to the specified hazard." Organizing these causes by their location in the control process loop is merely a way to systemically analyze all of the pieces of the control process—in many cases a particular cause may arguably fit into several pieces of the control loop. The distinction between whether or not, for example, "ATC believes that ITP FC will initiate an abnormal termination when necessary" is best defined as an inadequate control algorithm instead of a process model flaw is not important, as long as the process for defining all the causes is complete enough that they arise at some point during the analysis.

B.3.9.3

Table B.4: STPA-ATC.1

Hazard: H1 **1) Unsafe Control Action: ATC Approval Given When ITP Criteria Not Met**	
Process Model Link	**Cause**
(1) Inadequate Control Algorithm	ATC does not check to see if normal FL change is possible
	ATC does not wait for pertinent updates from nearby aircraft prior to approving ITP
	ATC does not communicate details of ITPs in process between separate controllers or sectors
	ATC does not ask for required information missing from request before approving
	ATC does not check to see if there are other blocking aircraft in the vicinity of the ITP
	ATC does not verify that ITP criteria (distance, same track status) are met
(2) Process Model Inconsistent	Controller believes that aircraft is on a flight path/plan that it is not
	ATC understanding of aircraft velocity is wrong
	ATCs understanding of aircraft location is wrong
	ATC understanding of number of aircraft in sector is wrong
	ATC unaware of another ITP currently in progress
	ATC believes that traffic volume in future will change
	ATC believes that communication channel (radio, datalink) is correct to use when it is not
	ATC believes that the weather to be good when it

	is not
(3) Inadequate actuator operation	Flight Crew does not carry out clearance as specified by ATC
(4) Component Failures/ Changes over time	
(5) Inadequate sensor operation	ATC does not understand or receive information on the state of traffic in the sector
(6) Incorrect or no information provided (by flight crew)	Pilot in sector does not give status to ATC when over fix point
(7) Inadequate or missing feedback to controller, feedback delays	ATC does not receive feedback from flight crew
	Feedback from pilots delayed to ATC

Table B.5: STPA-ATC.2

Hazard: H1

2) Unsafe Control Action: ATC Approval Given to Incorrect Aircraft

Process Model Link	Cause
(1) Inadequate Control Algorithm	Algorithm does not include a check / verification of aircraft ID
(2) Process Model Inconsistent	Abundance of aircraft in particular area of sector
	Other aircraft (non-requesting a/c) in airspace with similar state data or aircraft ID
	Other simultaneous requests occur within the ATC domain, including ITP or non-ITP requests
	ATC confuses the Reference and ITP aircraft. This could be due to lack of understanding of ITP architecture, or to a simple "slip"
(3) Inadequate actuator operation	Communication channel to flight crew becomes corrupted
(4) Component Failures/ Changes over time	
(5) Inadequate sensor operation	Datalink becomes corrupted
(6) Incorrect or no information provided (by flight crew)	Flight crew incorrectly transcribes data into CPDLC
	Flight crew does not included aircraft ID in ITP request
(7) Inadequate or missing feedback to controller, feedback delays	Incorrect Aircraft (non ITP requesting) confirms or accepts approval
	Incorrect Aircraft does not immediately respond about discrepancy (i.e. flight crew does not indicate to the ATC soon enough that it is incorrect recipient)

Table B.6: STPA-ATC.3

Hazard: H1

3) Unsafe Control Action: ATC Approval Given too Early or Late

Process Model Link	Cause
(1) Inadequate Control Algorithm	ATC gives approval before request is complete
	ATC delays in giving approval
(2) Process Model Inconsistent	ATC believes that they have all necessary information to grant approval when they do not
	ATC believes they are answering request promptly when there has been a delay
	ATC believes that request from pilot is complete when it is not
(3) Inadequate actuator operation	Delay in pilot-controller communication
(4) Component Failures/ Changes over time	
(5) Inadequate sensor operation	Missing or dropped messages between FC and ATC
(6) Incorrect or no information provided (by flight crew)	FC does not complete request to ATC
	FC does not ask for clarification from ATC when request received out of order
(7) Inadequate or missing feedback to controller, feedback delays	Request received by ATC is incomplete

Table B.7: STPA-ATC.4

Hazard: H1

4) Unsafe Control Action: ATC does not give abnormal termination instruction

Process Model Link	Cause
(1) Inadequate Control Algorithm	ATC unaware that an abnormal termination is possible
	ATC does not know conditions under which abnormal termination should be issued
	ATC does not continue to monitor ITP flight after granting approval
(2) Process Model Inconsistent	ATC believes that pilot has more situational awareness of nearby traffic and will recognize need to abnormally terminate ITP
	ATC does not know that ITP conditions are dangerous
	ATC attempts to maneuver any non-ITP plane out of dangerous traffic while ITP plane is changing flight level
(3) Inadequate actuator operation	
(4) Component Failures/ Changes over time	
(5) Inadequate sensor operation	
(6) Incorrect or no information provided (by flight crew)	Flight Crew does not alert ATC to potentially hazardous traffic situation
(7) Inadequate or missing feedback to controller, feedback delays	ATC does not recognize or acknowledge information from FC about hazardous traffic situation

Table B.8: STPA-ATC.5

Hazard: H1

5) Unsafe Control Action: ATC gives abnormal termination instruction when it not needed

Process Model Link	Cause
(1) Inadequate Control Algorithm	ATC gives abnormal termination instruction before verifying that it is necessary
	ATC gives abnormal termination instruction after realizing they made a mistake in issuing the original clearance, but without checking to see if the mistake was trivial
(2) Process Model Inconsistent	ATC believes traffic situation to be hazardous for ITP aircraft when it is not
	ATC gets conflicting information about the state of traffic from another source
(3) Inadequate actuator operation	Abnormal termination issued to incorrect aircraft
(4) Component Failures/ Changes over time	
(5) Inadequate sensor operation	
(6) Incorrect or no information provided (by flight crew)	
(7) Inadequate or missing feedback to controller, feedback delays	

Table B.9: STPA-ATC.6

Hazard: H1 **6) Unsafe Control Action: ATC gives abnormal termination instruction too late**	
Process Model Link	**Cause**
(1) Inadequate Control Algorithm	ATC takes too long to observe anomalous air traffic condition
(2) Process Model Inconsistent	
(3) Inadequate actuator operation	Communication delay, e.g. datalink message throughput issue
(4) Component Failures/ Changes over time	
(5) Inadequate sensor operation	Refresh rate on ATM screen or weather data is too slow
(6) Incorrect or no information provided (by flight crew)	
(7) Inadequate or missing feedback to controller, feedback delays	Not all aircraft in air space report, report too late, or at incorrect time

3.9.3.4

Table B.10: STPA-FC.1

Hazard: H1 ***1)*** **Unsafe Control Action: The flight crew executes an ITP when the ITP criteria are not satisfied** ***2)*** **The flight crew executes ITP with incorrect climb rate, flight levels, mach number, and other associated performance criteria**	
Process Model Link	**Cause**
(1) Inadequate Control Algorithm	Flight Crew does not correctly check that ITP is appropriate (that normal FL change could not occur)
	Flight Crew does not check that all ITP criteria are met
	Flight Crew does not re-verify that conditions have not changed from when they were originally checked after receiving approval
	Flight Crew does not confirm the established flight level after finishing the maneuver
(2) Process Model Inconsistent	Flight Crew believes that their climb/descend capability is greater than it is
	Flight Crew believes it has all ADS-B data for local traffic
	Flight Crew believes ADS-B data to be accurate when it is not
	Flight Crew believes ITP criteria (speed, distance, relative altitude, relative angle) to be different than it is
	Flight Crew believes communication protocols with ATC to be different than they are
	Flight Crew believes communication protocols with nearby aircraft to be different than they are
	Individual members of the flight crew of a different understanding of how responsibilities are divided among them

Hazard: H1

1) **Unsafe Control Action: The flight crew executes an ITP when the ITP criteria are not satisfied**
2) **The flight crew executes ITP with incorrect climb rate, flight levels, mach number, and other associated performance criteria**

	Flight Crew believes weather/turbulence to be better than it is
(3) Inadequate actuator operation	
(4) Changes over time (to aircraft)	
(5) Inadequate sensor operation	Flight Crew does not understand ITP data
(6) Control input or external information wrong or missing	Flight Crew lacking information from ATC
	ITP Equipment give incorrect or ambiguous state information
(7) Incorrect or no information provided (to sensor)	Information about other aircraft not received by ADS-B
(8) Inadequate or missing feedback	Change in own velocity/altitude/bearing not displayed to pilot
	Change in the velocity/altitude/bearing of nearby ship not displayed to pilot
	Proper aircraft identifier of nearby aircraft not displayed to pilot

Table B.11: STPA-FC.2

Hazard: H1

3) Unsafe Control Action: ITP FC executes without ATC Approval

4) ITP FC executes ITP out of sequence

Process Model Link	Cause
(1) Inadequate Control Algorithm	Flight Crew begins ITP maneuver prior to receiving approval
	Flight Crew delays in executing ITP after receiving approval
(2) Process Model Inconsistent	Flight Crew believes ITP request to be approved when it is not
	Flight Crew believes approval to be recent when it is old
(3) Inadequate actuator operation	
(4) Changes over time (to aircraft)	
(5) Inadequate sensor operation	Flight Crew does not understand or correctly apply ITP data from ITP equipment
(6) Control input or external information wrong or missing	ATC approval not on communication channel that FC is monitoring
	ITP Equipment provides criteria data too late
(7) Incorrect or no information provided (to sensor)	ADS-B data on other aircrafts is outdated or incomplete
(8) Inadequate or missing feedback	FC does not receive communication from ATC
	FC does not receive local traffic information from ADS-B

Table B.12 STPA-FC.3

Hazard: H1

3) Unsafe Control Action: ITP FC does not perform abnormal termination

Process Model Link	**Cause**
(1) Inadequate Control Algorithm	FC does not know the conditions under which an abnormal termination should be initiated
	FC waits for abnormal termination instruction from ATC
	FC does not monitor local traffic while performing ITP maneuver
(2) Process Model Inconsistent	FC believes that ATC is monitoring traffic conditions
	FC believes that hazardous situation will be resolved by the maneuver of another aircraft
	FC does not realize that they are violating ITP criteria (e.g. unable to maintain minimum climb rate)
(3) Inadequate actuator operation	
(4) Changes over time (to aircraft)	
(5) Inadequate sensor operation	
(6) Control input or external information wrong or missing	FC does not receive or does not heed collision avoidance message (TCAS) during ITP maneuver
(7) Incorrect or no information provided (to sensor)	
(8) Inadequate or missing feedback	

Table B.13: STPA-FC.4

Hazard: H1

5) **Unsafe Control Action: ITP FC performs abnormal termination incorrectly**
6) **When performing an abort, the flight crew must follow regional procedures**

Process Model Link	Cause
(1) Inadequate Control Algorithm	FC does not know procedure for completing abnormal termination (e.g. regional contingency plans)
	FC does not know the conditions under which an abnormal termination should occur
(2) Process Model Inconsistent	FC believes that abnormal termination is necessary when it is not
	FC believes that there is hazardous local traffic when there is not
	FC believes that ATC incorrectly granted ITP clearance
	FC believes that regional contingency procedures are different than they are
(3) Inadequate actuator operation	Equipment failure (e.g. aircraft unable to maintain correct climb/descent rate)
(4) Changes over time (to aircraft)	
(5) Inadequate sensor operation	Change in ITP data displayed to FC during maneuver causes them to initiate abnormal termination
(6) Control input or external information wrong or missing	FC unable to contact ATC during maneuver or to confirm completion
(7) Incorrect or no information provided (to sensor)	Equipment failure in ITP aircraft (e.g. altimeter not registering FL change)
(8) Inadequate or missing feedback	FC loses feedback from own plane
	FC loses external feedback (ADS-B, TCAS)

The causes identified in these tables are used later to refine the safety requirements and constraints.

B.3.10 High-Level Functional Requirements and Constraints

The requirements described in this section focus on the general goals of the ITP process and equipment. Specific requirements on the operators—the ITP flight crew and sector Air Traffic Control—are described in the section, "Operator Requirements." Use of the term "ITP" refers to the procedure, specifically to the methods used to train pilots and controllers and the steps of the procedure itself. "ITP equipment" refers to the display unit that ITP aircraft will be equipped with, which displays all of the relevant and necessary state data and whether the criteria are met.

Requirements that are derived from the STPA hazard analysis described below will refer to the portion of STPA from which they are derived in the format: STPA-x.y.z, where x=controller (ATC or ITP FC), y = the casual analysis table referenced (1, 2, etc), and z=the number of the process model link as specific in the hazard analysis casual tables.

B.3.10.1 Design and Safety Constraints

Design constraints are limitations on how requirements may be achieved, that is, on potential system designs.

B.3.10.1.1 Non-Safety Constraints

[C.1] The design of both the procedure for ITP and the ITP equipment must not preclude future changes or modification to procedures used in procedural airspace. (←[EA.1],[G.1])

[C.2] Both the procedure and the equipment must be compatible with existing methods of separation control in procedural airspace. (←[EA.1],[EC.1])

[C.3] Both the procedure and the equipment used for ITP must meet all applicable FAA, FCC and ICAO policies, rules, and philosophies. (←[EA.7])

[C.4] All ITP certified aircraft must be ADS-B equipped and must make use of the ADS-B data of nearby aircraft for calculating ITP criteria. (←[EA.6],[G.1])

[C.5] The desirability of performing a flight level change under ITP must be acceptable by both the flight crew and the air traffic controllers. (←[EA.4],[G.4])

B.3.10.1.2 Safety Constraints

For a system to be safe the safety constraints (constraints on the states of the system) must not be violated or a hazard will result. The safety constraints must be enforced by the safety control structure of the system. Accidents result when the control actions necessary to enforce the safety constraints are not provided, are provided by at the wrong time or in the wrong time, are stopped too soon or applied too long, or when appropriate control actions are provided but not followed. In designing a safe system, the safety constraints must be identified and then the appropriate controls or mitigation measures implemented (as described in Level 2 of the Intent Specification).

The hazard analysis is used to identify the required safety constraints. These constraints arise from the general ICAO safety policy that the addition of any new ITP-related protocols or equipment will not affect the aircraft or other aircraft or air traffic control in a way that can adversely affect the safety of the flight.

[1.1]
All ITP related protocols must not conflict or interfere with existing protocols

[1.1.1]
Requesting and executing an ITP must not interfere with the FCs ability to monitor and attend to the health of their aircraft (←[G.3])

[1.1.2]
Receiving and providing clearance for ITP must not interfere with ATC ability to monitor and attend to the health of the airspace (←[G.4])

[1.2]
ITP shall provide the flight crews of aircraft operating in procedural airspace the ability to determine if an ITP maneuver is appropriate and the communication protocols (channels, syntax, request formatting) for receiving clearance from ATC and conditions under which the maneuver should be abnormally terminated. (←STPA-ATC.1, **STPA-FC.1**,B.11: STPA-FC.2, ↓[2.1])

[1.3]
ITP training shall be provided for all controllers (flight crew and air traffic) in all ITP procedures. In addition to all of the operational requirements detailed in Level 2, training shall include (←[G.1],↓[2.1]):

[1.3.1]

Communication protocols (both channels and appropriate syntax) between flight crew and air traffic control (←STPA-ATC.1, **STPA-FC.1**,B.11: STPA-FC.2)

[1.3.2]

The expected order of all ITP related communications and methods for both ATC and FC to determine how to treat an out of order or unexpected communication (←STPA-ATC.2)

[1.3.3]

Roles and responsibilities of each member of the ITP FC in executing the ITP procedure **(← STPA-FC.1**)

Assumption: *Roles and responsibilities may be clearly tied to general flight responsibilities (for example, if the co-pilot is responsible for all ATC communication and the pilot is responsible for flying the plane, this will also be the division of duties during ITP), but the ITP procedure needs to clearly indicate these roles in order to avoid confusion, especially during unexpected or abnormal circumstances.*

[1.3.4]

ITP training must include conditions under which an abnormal termination of ITP should be initiated by the FC and by ATC (←STPA-ATC.3,B.12 STPA-FC.3, STPA-FC.4)

[1.4]

The ITP FC must be provided a means of determining their ownship climb / descend capability and clearance data (←[G.2],[G.3], **STPA-FC.1**,↓[2.1],[2.15])

Assumption: *The ITP equipment may display this data, but we assume that if it does not, the pilots should know it or be able to find it anyway, as a general requirement of safe aircraft operation.*

[1.5]

ADS-B transponder on ITP aircraft must be certified and regularly tested (←[EA.6] ,↓[2.32])

Assumption*: The certification authorities in each country will determine the certification requirements for ADS-B or will refer to DO-242A*

B.10.3.2 ITP Equipment

[1.6]
ITP equipment shall display information to the crew in a manner that does not distract or confuse them (←[G.1], **STPA-FC.1**,↓[2.15])

[1.7]
ITP equipment shall display all state data for nearby ADS-B aircraft required for the pilot to determine if the ITP criteria have been met (←[G.1], [G.2], **STPA-FC.1**, ↓[2.15])

[1.7.1] ITP equipment shall display that the ITP criteria are met if and only if the criteria are met. (←[G.2])

[1.7.2] ITP equipment shall display information about all nearby aircraft in a way that is clear and understandable to the flight crew. (←[G.2],[G.3], **STPA-FC.1**)

[1.7.3] ITP equipment shall display data quality indicators for all derived data (← STPA-FC.1)

[1.8]
ITP Equipment shall provide state data necessary to determine ITP feasibility (←[G.1], **STPA-FC.1**,B.11: STPA-FC.2), (↓[2.15][2.16])

B.3.10.3 Operator Requirements and Constraints

This section covers the assumptions, requirements and constraints involving operator behavior. In the case of ASTA-ITP there are two general operators that we are concerned with: the flight crew of the ITP requesting aircraft and the Air Traffic Controller of the sector in which the ITP maneuver is requested. This information is used in the design of the ITP equipment interface, the ITP logic, the procedures followed by the flight crew and air traffic control, and training plans and programs.

B.3.10.4 ATC Requirements and Constraints

[1.9]

If ATC is not receiving status updates (e.g. at fix points) from any aircraft in sector, they must not issue ITP clearance (←[SC-ATC.1], STPA-ATC.1)

[1.10]

Prior to issuing ITP clearance, ATC must verify that a normal flight level change is not possible (←[SC-ATC.1], STPA-ATC.1)

[1.11]

If ATC is receiving data from a RA while ITP request is made (via normal fix point update or otherwise) they must wait for data from other aircraft prior to issuing ITP clearance (←STPA-ATC.1)

[1.12]

Controllers must communicate details of ITP clearances granted (ITP craft and RA involved) in real time to other controllers in the same or nearby sectors (←STPA-ATC.1, STPA-ATC.2)

Rationale*: This is to ensure that multiple ITP maneuvers do not occur in the same portion of the airspace*

[1.13]

ATC must request information missing from ITP request from FC prior to issuing ITP clearance (←STPA-ATC.1, ↓[2.12])

[1.14]

ATC must verify all data prior to issuing an ITP clearance. ATC must “sanity check” other data to ensure that it is realistic (←[SC-ATC.1], ↓[2.14],[2.15])

[1.15]

ATC must monitor aircraft in their sector and know the flight plans for those aircraft, and if ATC believes requests are inconsistent with the ATC's data then they must not grant ITP clearance (←[L.1], STPA-ATC.1)

Assumption: *ATC will have this knowledge as part of their overall ability to maintain separation, regardless of ITP clearances.*

[1.16]

ATC must have access to current[19] knowledge of the state data of all aircraft involved in ITP request, both the requesting aircraft as well as any potentially blocking aircraft, including position, velocity, flight level and other aircraft states (←[SC-ATC.3],STPA-ATC.1, ↓[2.17][2.18])

Assumption: *ATC will monitor air traffic using radar, ADS-B, or other measures have this knowledge as part of their overall ability to maintain separation, regardless of ITP clearances.*

[1.16.1]

ATC must not use any assumptions about the future state of the airspace when granting ITP clearance (←STPA-ATC.1)

Rationale*: The potential exists for the ATC (or flight crews) to anticipate that ITP criteria will be met based on present conditions. This should be avoided and clearances only granted on the current state.*

[1.17]

ATC must grant clearance for ITP within TBD minutes of request (←[SC-ATC.3],STPA-ATC.2)

[1.17.1]

ATC must be provided a mechanism for knowing how much time has elapsed since the ITP request was made (←STPA-ATC.2)

[19] "Current" in procedural airspace may rely on the air traffic controller expertise or consensus of what qualifies as current. It must be much less than 5 minutes, since several of the other requirements pertain to

[1.18]

ATC must be provided with all ITP criteria values (←[SC-ATC.1], STPA-ATC.2, ↓[2.12][2.14][2.15])

Assumption*: This could be a document that can be looked up real-time, or numbers on a screen.*

[1.19]

ATC shall follow a contingency plan if communications with FC fail (←STPA-ATC.2, →[1.35])

Rationale*: ATC depends on flight crew communication to determine the state of aircraft that are not in procedural separation. Therefore a contingency plan is necessary if communication has not been properly verified.*

[1.19.1]

ATC must not approve additional ITP maneuvers until existing ITP has been completed and confirmed through formal communication channel

[1.19.2]

ATC shall request communication with ITP FC if confirmation has not been received within TBD minutes

[1.19.3]

ATC shall request procedural separation for all aircraft domain until communication verification has been received from ITP FC

[1.20]

ATC shall prioritize communication with an aircraft performing an ITP maneuver over other aircraft not maneuvering (←STPA-ATC.3)

[1.20.1]

ATC shall relate all pertinent traffic and safety information promptly to ITP FC (← **STPA-FC.1**)

[1.21]

ATC shall continue to monitor ITP aircraft and surrounding aircraft (such as RA) while ITP maneuver is in progress (←STPA-ATC.3)

[1.22]

If ATC notices a potentially hazardous traffic scenario, they must assess if an abnormal termination of the ITP maneuver is necessary, and initiate it if so (←[SC-ATC.4], STPA-ATC.3)

[1.22.1]

ATC must determine when traffic surrounding an ITP maneuver may enter into a hazardous state such as inclement weather of violation of procedural airspace constraints (←STPA-ATC.4)

[1.22.2]

If ATC is using traffic data from multiple sources to monitor traffic surrounding an ITP maneuver, they must be provided with a clearly defined hierarchy of which data to use (←STPA-ATC.4)

[1.22.3]

ATC must not issue abnormal termination commands without cause (←STPA-ATC.4)

[1.22.4]

If ATC becomes aware of a mistake made during the original ITP clearance, they must assess if the mistake could be hazardous prior to terminating the ITP (←STPA-ATC.4)

[1.22.5]

ATC must not approve an ITP request that will allow the aircraft to enter dangerous weather conditions.

B.10.3.5 ITP FC Requirements

[1.23]

ITP FC shall assess that an ITP is desirable and that a normal FL change is not possible prior to issuing an ITP request (←[C.5], **STPA-FC.1**)

[1.23.1]

ITP FC must be provided a mechanism for obtaining local weather and turbulence information, and must factor this information into the decision to request ITP (← **STPA-FC.1**)

[1.24]

ITP FC shall verify that all ITP criteria are met prior to issuing the request (←[SC-FC.2], **STPA-FC.1**, ↓[2.1])

[1.25]

ITP FC shall verify the local contingency procedures prior to requesting ITP (← STPA-FC.4)

[1.26]

If FC receives a clearance unexpectedly (too quickly or prior to finishing the request), they must not accept clearance and must contact ATC for clarification (←[SC-FC.7], STPA-ATC.2)

[1.27]

ITP FC shall verify that all ITP criteria are met after receiving clearance and immediately prior to initiating FL change (←[SC-FC.8], STPA-FC.1, ↓[2.5])

[1.27.1]

ITP FC must not re-evaluate ITP criteria after beginning the FL change (← STPA-FC.4)

[1.28]

ITP FC must not initiate an ITP FL change before receiving an ATC clearance (←[SC-FC.1], B.11: STPA-FC.2, ↓[2.5])

[1.29]

The window of time between ATC clearance and ITP execution shall be less than TBD[20] minutes (←[SC-FC.8], B.11: STPA-FC.2)

[1.29.1]

ITP FC shall track how much time has passed since clearance was given (←B.11: STPA-FC.2)

[1.30]

ITP FC must complete the maneuver specified in the ATC clearance (←[SC-FC.3], B.11: STPA-FC.2)

[20] DO-312 suggests 5 minutes, but this number should be verified

[1.31]

ITP FC must promptly alert ATC of any abnormal conditions encountered during maneuver (←STPA-ATC.1,STPA-ATC.3)

[1.32]

ITP FC must immediately confirm established FL with ATC upon completion of ITP maneuver (← **STPA-FC.1**, ↓[2.9])

[1.32.1]

After establishing new FL, ITP FC must obtain a new clearance from ATC for any further FL change (← STPA-FC.4)

[1.33]

ITP FC must be trained how to assess local traffic during ITP maneuver,

[1.33.1] ITP must monitor nearby traffic while performing maneuver (←B.11: STPA-FC.2,B.12 STPA-FC.3, ↓[2.7],[2.8],[2.9])

[1.33.2]

ITP FC must only use local traffic information from official sources during maneuver (← STPA-FC.4)

[1.33.3]

ITP FC must use additional situational awareness (such as TCAS) during ITP maneuver, and must act on any alerts (←B.12 STPA-FC.3)

[1.33.4]

ITP FC must initiate an abnormal termination of ITP without delay when they believe they will enter a hazardous situation (←B.12 STPA-FC.3, ↓[2.8])

[1.33.5]

ITP FC must not initiate an abnormal termination of ITP if the FC is not in a hazardous situation (←[SC-FC.5],B.12 STPA-FC.3, [SC-FC.5])

[1.34]

ITP FC must only use ITP equipment to determine if a FL change is feasible and to collect the necessary data to transmit to local ATC (← **STPA-FC.1**)

Rationale*: ITP Equipment is designed for the sole purpose of the InTrail Procedure and should not be used for other requests or maneuvers.*

[1.34.1]

ITP equipment must not be used during the procedure; once the ITP FC begins the FL change, ITP should not be used to assess nearby traffic

Rationale*: The ITP and Reference aircraft will necessarily violate procedural separation requirements (as well as the necessary starting conditions for ITP), and therefore the data should be disregarded.*

[1.35]

ITP FC must follow contingency plan if communication fails. This constitutes either voice (HF) or datalink (CPDLC). (←B.12 STPA-FC.3, [1.19])

[1.35.1]

If using voice, during an ITP maneuver the ITP FC must verify every TBD minutes communication with ATC

[1.35.2]

If using datalink, during an ITP maneuver the ITP FC must verify that the data time stamp is within TBD minutes of request

[1.35.3]

ITP FC must follow regional contingencies if ATC is unresponsive to verification of communication through [1.35.1] or [1.35.2]

B.3.11 Hazard List and Hazard Log

These are the high level hazards associated with ASTA-ITP.

H1: A pair of controlled aircraft violate minimum separation standards

Subsystem: ITP, reference, blocking aircraft; Air Traffic Controller; Flight Crew

Operation/Phase: ITP Execution

High-Level Causal Factors:

ITP FC unaware of nearby traffic;

ATC unaware of traffic surrounding ITP aircraft;

Equipment Failure

Level and Effect: Potential loss of life, equipment

Safety Requirements and Constraints:

System Safety Constraints

- All ITP related protocols must not conflict or interfere with existing protocols [1.1]
- Requesting and executing an ITP must not interfere with the FCs ability to monitor and attend to the health of their plane [1.1.1]
- Receiving and providing clearance for ITP must not interfere with ATC ability to monitor and attend to the health of the airspace [1.1.2]
- ITP shall provide the flight crews of aircraft operating in procedural airspace the ability to determine if an ITP maneuver is appropriate and the communication protocols [1.2]
- ITP training shall be provided and include communication protocols (both channels and appropriate syntax) between flight crew and air traffic control [1.3.1]
- ITP training shall be provided and include the expected order of all ITP related communications and methods for both ATC and FC to determine how to treat an out of order or unexpected communication [1.3.2]
- ITP training shall be provided and include roles and responsibilities of each member of the ITP FC in executing the ITP procedure [1.3.3]
- ITP training shall be provided and include conditions under which an abnormal termination of ITP should be initiated by the FC and by ATC [1.3.4]

- The ITP FC must be provided a means of determining their ownship climb / descend capability and clearance data [1.4]
- ADS-B transponder on ITP aircraft must be certified and regularly tested [1.5]

ITP Equipment

- ITP equipment shall display information to the crew in a manner that does not distract or confuse them [1.6]
- ITP equipment shall display all pertinent state data for nearby ADS-B aircraft [1.7]
- ITP Equipment shall meet minimum reliability requirements when displaying calculated data fields [1.7.1]
- ITP equipment shall display data quality indicators for all derived data
- ITP equipment shall be used by the flight crew only to determine if a FL change is feasible and to collect the necessary data to transmit to local ATC [1.7.3]
- ITP Equipment shall provide state data necessary to determine ITP feasibility to the flight crew in a clear and easy to understand interface [1.8]

ATC

- If ATC is not receiving status updates (e.g. at fix points) from any aircraft in sector, they must not issue ITP clearance [1.9]
- Prior to issuing ITP clearance, ATC must verify that a normal flight level change is not possible [1.10]
- If ATC is receiving data from a RA while ITP request is made (via normal fix point update or otherwise) they must wait for data from other aircraft prior to issuing ITP clearance [1.11]
- Controllers must communicate details of details of ITP clearances granted (ITP aircraft and RA involved) in real time to other controllers in the same or nearby sectors [1.12]
- ATC must request information missing from ITP request from FC prior to issuing ITP clearance [1.13]
- ATC must verify all data prior to issuing an ITP clearance. ATC must "sanity check" other data to ensure that it is realistic [1.14]
- ATC must monitor aircraft in their sector and know the flight plans for those aircraft, and if ATC believes requests are inconsistent with the ATC's data then they must not grant ITP clearance [1.15]
- ATC must have access to current knowledge of the state data of all aircraft involved in ITP request, both the requesting aircraft as

well as any potentially blocking aircraft, including position, velocity, flight level and other aircraft states [1.16]

- ITP must not use any assumptions about the future state of the airspace when granting ITP clearance [1.16.1]
- ATC must grant clearance for ITP within TBD minutes of request [1.17]
- ATC must be provided a mechanism for knowing how much time has elapsed since the ITP request was made [1.17.1]
- ATC must be provided with all ITP criteria values [1.18]
- ATC shall follow a contingency plan if communications with FC fail [1.19]
- ATC must not approve additional ITP maneuvers until existing ITP has been completed and confirmed through formal communication channel [1.19.1]
- ATC shall request communication with ITP FC if confirmation has not been received within TBD minutes [1.19.2]
- ATC shall request procedural separation for all aircraft domain until communication verification has been received from ITP FC [1.19.3]
- ATC shall prioritize communication with an aircraft performing an ITP maneuver over other aircraft not maneuvering [1.20]
- ATC shall relate all pertinent traffic and safety information promptly to ITP FC [1.20.1]
- ATC shall continue to monitor ITP aircraft and surrounding aircraft (such as RA) while ITP maneuver is in progress [1.21]
- If ATC notices a potentially hazardous traffic scenario, they must assess if an abnormal termination of the ITP maneuver is necessary, and initiate it if so [1.22]
- ATC must determine when traffic surrounding an ITP maneuver may enter into a hazardous state such as inclement weather of violation of procedural airspace constraints [1.22.1]
- If ATC is using traffic data from multiple sources to monitor traffic surrounding an ITP maneuver, they must have a clearly defined hierarchy of which data to use [1.22.2]
- ATC must not issue abnormal termination commands without cause [1.22.3]
- If ATC becomes aware of a mistake made during the original ITP clearance, they must assess if the mistake could be hazardous prior to terminating the ITP [1.22.4]

- ATC must not approve an ITP request that will allow the aircraft to enter dangerous weather conditions [1.22.5]

Flight Crew

- ITP FC shall assess that an ITP is desirable and that a normal FL change is not possible prior to issuing ITP request [1.23]
- ITP FC must have a mechanism for obtaining local weather and turbulence information, and must factor this information into the decision to request ITP [1.23.1]
- ITP FC shall verify that all ITP criteria are met prior to issuing the request [1.24]
- ITP FC shall verify the local contingency procedures prior to requesting ITP [1.25]
- If FC receives a clearance unexpectedly (too quickly or prior to finishing request), they must not accept clearance and must contact ATC for clarification [1.26]
- ITP FC shall verify that all ITP criteria are met after receiving clearance and immediately prior to initiating FL change [1.27]
- ITP FC must not re-evaluate ITP criteria after beginning FL change [1.27.1]
- ITP FC must not initiate an ITP FL change before receiving an ATC clearance [1.28]
- The window of time between ATC clearance and ITP execution shall be less than TBD minutes [1.29]
- ITP FC shall track how much time has passed since clearance was given [1.29.1]
- ITP FC must complete the maneuver specified in the ATC clearance [1.30]
- ITP FC must promptly alert ATC of any abnormal conditions encountered during maneuver [1.31]
- ITP FC must immediately confirm established FL with ATC upon completion of ITP maneuver [1.32]
- After establishing new FL, ITP FC must obtain a new clearance from ATC for any further FL change [1.32.1]
- ITP FC must be trained how to assess local traffic during ITP maneuver [1.33]
- ITP must monitor nearby traffic while performing maneuver [1.33.1]
- ITP FC must only use local traffic information from official sources during maneuver [1.33.2]

- ITP FC must use additional situational awareness (such as TCAS) during ITP maneuver, and must act on any alerts [1.33.3]
- ITP FC must initiate an abnormal termination of ITP without delay when they believe they will enter a hazardous situation [1.33.4]
- ITP FC must not initiate an abnormal termination of ITP if the FC is not in a hazardous situation [1.33.5]
- ITP FC must only use ITP equipment to determine if a FL change is feasible and to collect the necessary data to transmit to local ATC [1.34]
- ITP equipment must not be used during the procedure; once the ITP FC begins the FL change, ITP should not be used to assess nearby traffic [1.34.1]
- ITP FC must follow contingency plan if communication fails. This constitutes either voice (HF) or datalink (CPDLC). [1.35]
- If using voice, during an ITP maneuver the ITP FC must verify every TBD minutes communication with ATC [1.35.1]
- If using datalink, during an ITP maneuver the ITP FC must verify that the data time stamp is within TBD minutes of request [1.35.2]
- ITP FC must follow regional contingencies if ATC is unresponsive to verification of communication [1.35.3]

Analyses Performed:

Actions Taken:

Status:

Verification:

Final Disposal (Closeout Status):

Responsible Engineer:

Remarks:

H2: Aircraft enters unsafe atmospheric region

> **Assumption:** This hazard does not need to be considered for ITP because no unsafe control action associated with ITP will lead to it. System constraints to avoid this hazard are designed into basic flight protocol, and operate independently of ITP.

H3: Aircraft enters uncontrolled state

> **Assumption:** This hazard does not need to be considered for ITP because no unsafe control action associated with ITP will lead to it. System constraints to avoid this hazard are designed into basic flight protocol, and operate independently of ITP.

H4: Aircraft enters unsafe attitude

> **Assumption:** This hazard does not need to be considered for ITP because no unsafe control action associated with ITP will lead to it. System constraints to avoid this hazard are designed into basic flight protocol, and operate independently of ITP.

H5: Aircraft enters a prohibited area

> **Assumption:** This hazard does not need to be considered for ITP because no unsafe control action associated with ITP will lead to it. System constraints to avoid this hazard are designed into basic flight protocol, and operate independently of ITP.

B.3.12 Verification and Validation

These requirements and constraints have not been independently verified and validated, which would be needed if they were to be used on the real system (instead of on this demonstration project).

B.4 Level 2: System Design Principles

This level of the intent specification answers the question of "why" for all of the design decisions in level 3 and addresses some of the basic properties of system components that impact system design. Additionally, this level will describe the derived requirements, or how the high level requirements in level 1 will be achieved while enforcing the constraints from level 1.

B.4.1 ASTA-ITP System Components

The components of ASTA-ITP that must be considered during the system design phase can be divided up into two categories: the new procedure for performing ITP and the additional equipment needed for the execution of the procedure.

B.4.1.1 ITP Procedure

The ITP procedure consists of the steps required for a correct ITP maneuver to occur. Broadly speaking, these steps are the initiation of ITP, the evaluation of ITP, the execution of ITP and the completion of ITP. There is also the step of abnormal termination of ITP, which will be the emergency procedure necessary to gracefully exit an ITP maneuver found to be unsafe while maintaining the highest possible level of safety.

The ITP procedure designed in this specification is not merely a checklist of steps for the flight crews and the air traffic controllers to follow. It also encompasses requirements for training both the ITP flight crew and the air traffic controllers in how to perform ITP. These training requirements cover not just the procedure itself but also the communication protocols that should be used for the procedure as well as the aforementioned emergency procedures.

B.4.1.2 ITP Equipment

The ITP equipment will be the equipment on board the ITP aircraft that is used specifically by the pilot to assess the feasibility and desirability of the ITP maneuver under consideration prior to initiating the request. This equipment is passive equipment—that is it only displays information to the ITP flight crew; it does not offer advice or suggestions on a "correct" action to take.

Figure B.5 shows the design of the ITP equipment and all related interfaces, detailed in the accompanying key. All of the ITP equipment design decisions in level 2 reflect decisions made about parts of this functional architecture.

B.4.1.3 Data Environment and Assumptions

ITP equipment depends on external data in order to calculate and display ITP criteria. This includes ADS-B under the aegis of the global navigation constellation, as well as barometric pressure data for altitude. This document is intended to specify requirements for ITP equipment and for the operators in the ITP domain. Therefore, this document does not specify certification requirements for external components but rather lists the expected inputs for the minimum expected ITP functionality.

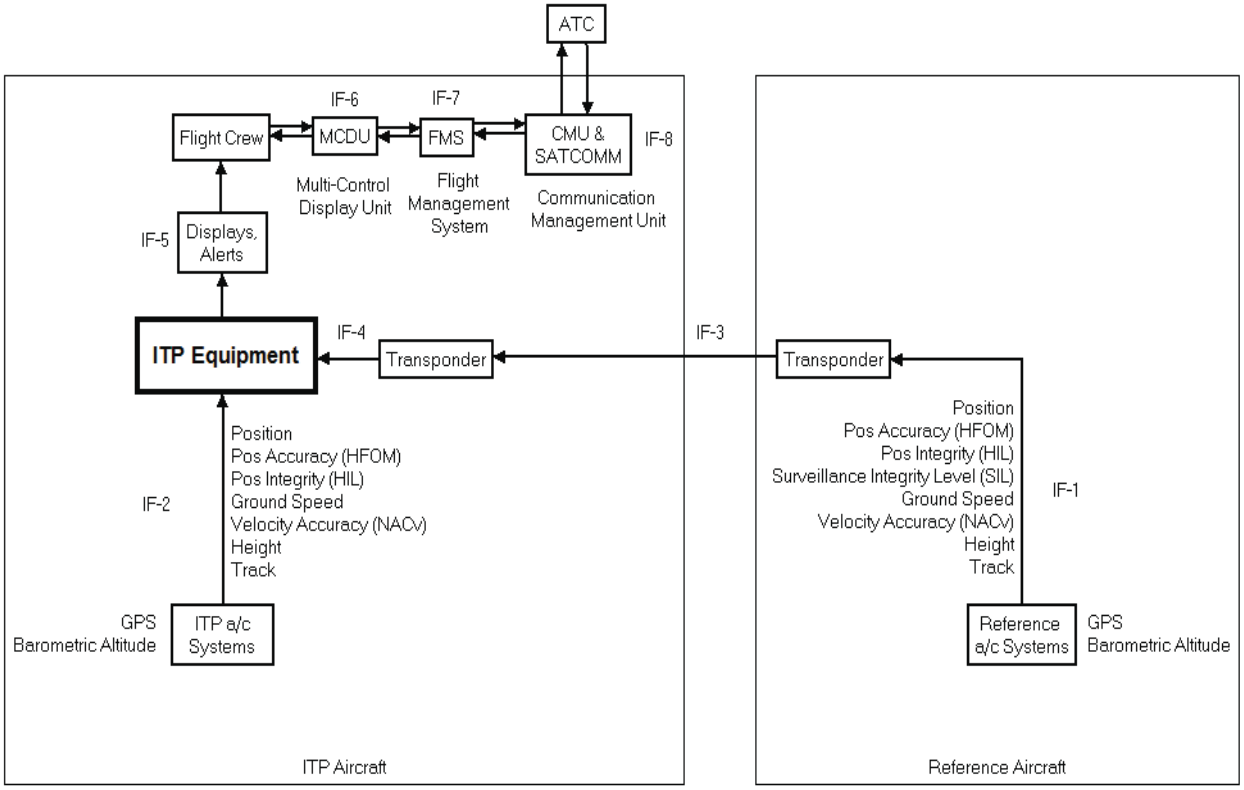


Figure B.5 Surveillance Functional Architecture Scope for ASTA-ITP

Key to Figure B.5**:**

- IF-1 = Encompasses the following:
    - Position sensor input interface, e.g., at sensor antenna, for Reference Aircraft
    - Sensor outputs for Reference Aircraft
    - Output from Surveillance Transmit Processing (STP) to the ADS-B Transmit function
- IF-2 = Encompasses the following
    - Position sensor source input interface, e.g., at sensor antenna, for ITP Aircraft
    - Sensor outputs for ITP Aircraft
- IF-3 = ADS-B link environment
- IF-4 = ADS-B receive function, generating ADS-B reports for ITP equipment
- IF-5 through IF-8 are specific to the manufacturer and operator implementation

B.4.2 System Design Principles

B.4.2.1 Nature of ASTA-ITP Design Needs

When considering how to design ASTA-ITP and what principles to incorporate in that design, it is important to note the unique nature of ASTA-ITP. In essence, ASTA-ITP is the method to reduce separation requirements in a strictly defined scenario. Because ASTA-ITP is essentially a method that must operate within an existing, strictly defined framework (↑SC1) and because the ITP equipment cannot do anything more than calculate and display state data about the system (↑1.3), much of the necessary design principles concern the implementation details as opposed to more traditional "design" issues. Therefore the design consists of three basic categories: 1) Operator Task Design Principles consisting of the steps necessary for the flight crews and air traffic controllers to follow in order to safely execute the procedures; 2) Equipment Design Principles, which include the necessary items to be displayed to the flight crew during operations; and 3) Data Environment Design Principles and Assumptions, which account for inputs, such as ADS-B, that are essential for ITP Equipment to perform its functions.

B.4.2.2 Overview of Concept of Operations

Safe execution depends on situational awareness of the air space by flight crews and air traffic control, recognition of dynamically changing criteria, and coordinated communication between aircraft (flight crews) and air traffic control. Figure B.6B.6 shows the physical relationship between the components of the airspace in an example InTrail Procedure, with the three basic steps required for proper execution. DO-312 describes the purpose and design as follows:

> *For a standard Flight Level change, the controller uses standard, procedure-based separation minima and procedures to ensure that separation will exist between an aircraft requesting a*
>
> *Flight Level change and all other aircraft at the initial, intermediate and requested Flight Levels. The ATSA-ITP was developed to enable either leading or following Same Track aircraft to perform a climb or descent to a requested Flight Level through Intervening Flight Levels that might otherwise be disallowed when using current standard separation minima. The ITP Equipment would allow the flight crew to determine if the criteria for an ITP request are met with respect to one or two Reference Aircraft at Intervening Flight Levels. The ITP Speed/Distance Criteria are designed such that the spacing between the estimated positions of the ITP Aircraft and Reference Aircraft, while the vertical separation is not achieved, is never less than the ITP Separation Minimum until vertical separation between the ITP Aircraft and Reference Aircraft is ensured.*
>
> *The ITP application uses GNSS/GPS/ADS-B data to apply distance based longitudinal separation. The ITP Operational Description can be found in IR.15. The probability of aircraft longitudinal overlap is calculated based on given values of accuracy for GNSS/ADSB, altitude error, latency error, initiation criteria parameters for the ITP, and*

a wind model. A parametric analysis was performed in to determine the sensitivity of collision risk to accuracy, integrity and initiation criteria.

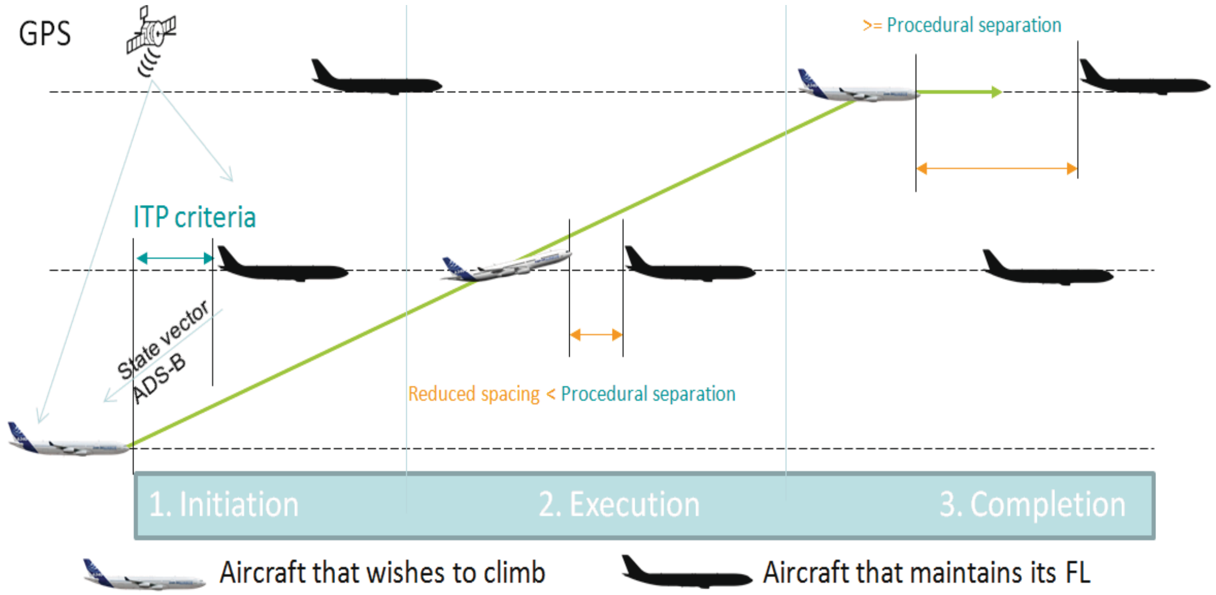
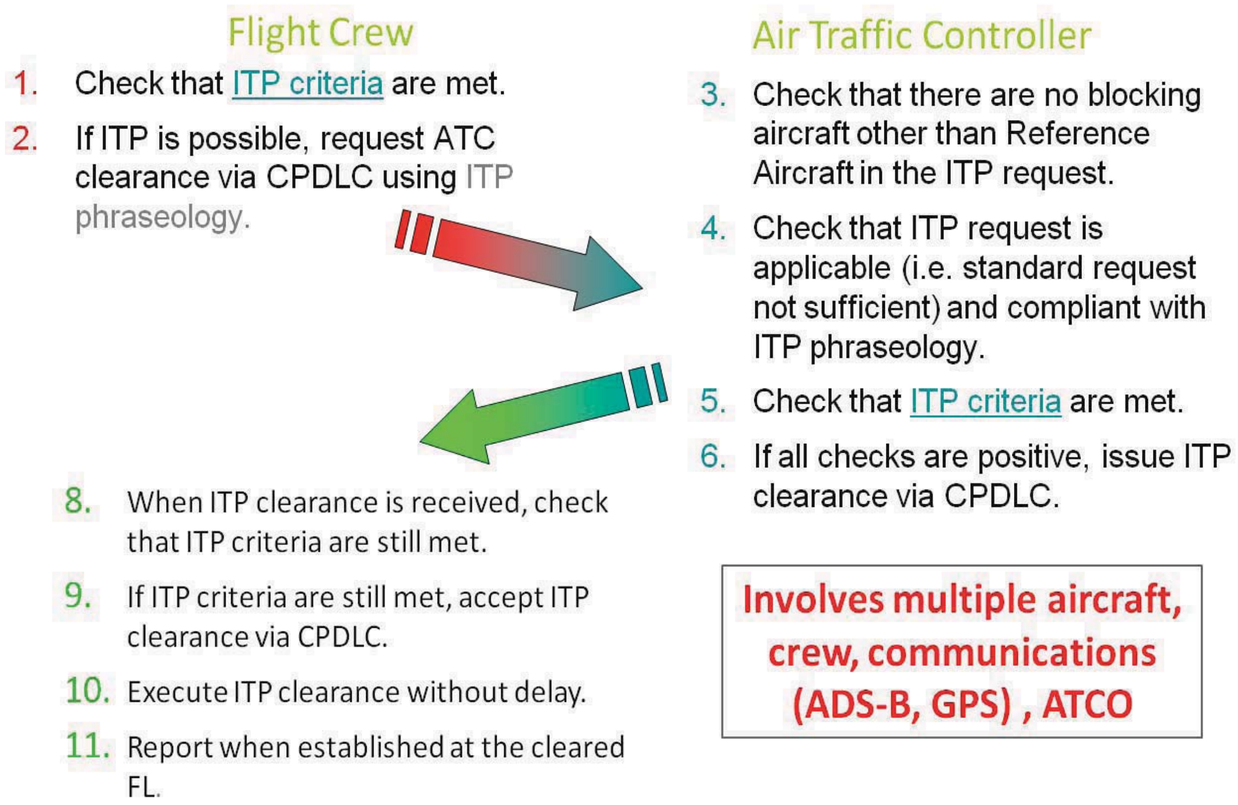

GPS
>= Procedural separation
ITP criteria
State vector
ADS-B
Reduced spacing < Procedural separation
1. Initiation
2. Execution
3. Completion
Aircraft that wishes to climb
Aircraft that maintains its FL

Figure B.6 ATSA-ITP Concept

- Stage 1 Initiation – Before the ITP maneuver, ITP criteria must be met.
- Stage 2 Execution – During an ITP maneuver, the ITP longitudinal separation between aircraft is applied.
- Stage 3 Completion – At final FL, procedural separation must exist with aircraft that are already at that final FL.

Figure B.7 shows the further refinement of these steps. The flight crew initiates ITP by requesting it, the ATC verifies the request and, if the criteria are met, grants clearance, and then the flight re-verifies the criteria and executes



Flight Crew

1. Check that ITP criteria are met.
2. If ITP is possible, request ATC clearance via CPDLC using ITP phraseology.

Air Traffic Controller

3. Check that there are no blocking aircraft other than Reference Aircraft in the ITP request.
4. Check that ITP request is applicable (i.e. standard request not sufficient) and compliant with ITP phraseology.
5. Check that ITP criteria are met.
6. If all checks are positive, issue ITP clearance via CPDLC.

8. When ITP clearance is received, check that ITP criteria are still met.
9. If ITP criteria are still met, accept ITP clearance via CPDLC.
10. Execute ITP clearance without delay.
11. Report when established at the cleared FL.

Involves multiple aircraft, crew, communications (ADS-B, GPS) , ATCO

Figure B.7 Basic Step-by-Step Procedure for ITP Operators

B.4.3 Operator Task Design Principles

This section describes the design principles associated with creating the operator tasks necessary to perform ITP. Because the fundamental tasks (i.e. communication between the FC and ATC, granting clearance, and executing a clearance) are not new, the design principles here focus on the details of the procedures that the flight crew of the ITP aircraft and the air traffic controller will use to perform ITP. All of the modeling and development work used in the design of ITP are based on certain assumptions about operator (i.e. flight crews and air traffic controllers) behavior and order of operations. The design decisions presented below reflect these assumptions, as well as the mathematical modeling techniques used minimum separation.

ITP Flight Crew

[2.1] The ITP flight crew needs to check that the following criteria are fulfilled before requesting an ITP clearance. This requirement does not imply that an individual assessment of each criterion is carried out by the flight crew, but rather that each criterion is assessed by either the flight crew, or by automation (see section 3.5.1) and although not required for all criterion, it is recognized that automation may provide a more predictable solution. (↑[1.2], [1.8],[1.23],[1.24]) See also: DO312-SPR.1

[2.1.1] The Ownship climb/descend capability criteria will be considered passed if and only if the ITP Aircraft can climb/descend in the desired direction at a rate of 300 fpm or more. Initiation Distance Critera and other geometric values ([2.1.2], [2.1.3], [2.1.4]) were selected such that when a Flight Level change at 300 fpm is performed with the related 20 or 30 kts Closing Ground Speed Differential, the distance between the aircraft does not become less than the ITP Separation Minimum (i.e., 10 NM). See also: DO312-SPR.38

[2.1.2] The ITP Speed/Distance Criteria will be considered passed if and only if one of the following are met (See also: DO312-SPR.39):
- (ITP Distance ≥ 15 NM) and (Closing Ground Speed Differential ≤ 20 Kts)
or
- (ITP Distance ≥ 20 NM) and (Closing Ground Speed Differential ≤ 30 Kts)

[2.1.3] The Relative Altitude Criteria will be considered passed if and only if the difference in altitude between the ITP and Reference Aircraft is less than or equal to 3000 feet. Anything greater than this is considered standard, procedural airspace. See also: DO312-SPR.40

Note: *The flight crew/ITP Equipment does not have knowledge of the separation minima. It can only check if the Reference Aircraft is/are vertically 3000 feet or* *less. ATC checks that the vertical distance is 3000 feet or less and that it is 2000 feet or less when the separation minima is 2000 feet.*

[2.1.4] ITP Equipment data accuracy and quality must meet certain minimum requirements in order to ensure that the ITP Separation Minimum is applied within predictable certainty bounds. All of the geometric and aerodynamic calculations used to design the procedure assume a certain level of fidelity in the state data of all aircraft involved in the procedures.

[2.1.4.1] The position accuracy data quality criteria will be considered passed only if the ITP Aircraft data AND Reference Aircraft data each have horizontal position accuracies of at least 0.5 NM at the 95th percentile.

***Note:** To pass the position data quality criteria, both the accuracy and integrity requirements on the data from both ITP and Reference Aircraft must be met. SPR.43 provides the accompanying integrity requirement to pass this criteria.*

[2.1.4.2] The position integrity data quality criteria will be considered passed only if the ITP Aircraft data AND Reference Aircraft data each have horizontal position integrity bounds of 1.0 NM with an integrity level of 1E-5.

***Note:** To pass the position data quality criteria, both the accuracy and integrity requirements on the data from both ITP and Reference Aircraft must be met. SPR.42 provides the accompanying accuracy requirement to pass this criteria.*

[2.1.4.3] The velocity data quality criteria will be considered passed only if the ITP Aircraft data AND Reference Aircraft data each have horizontal velocity accuracies of at least 10 m/s (19.4 kts) at the 95th percentile.

[2.2] The ITP flight crew should include a minimum set of data in its ITP request, including the requested Flight Level and for each Reference Aircraft, its aircraft ID, ITP Distance and relative position (in front or behind). The Air Traffic Controller needs this information in order to have sufficient knowledge of the airspace. (↑[1.3.2],[1.24]) See also: DO312-SPR.20

[2.3] The ITP flight crew will follow normal communication to acknowledge the clearance (via read back if using voice) to ATC to confirm that the clearance has been received and has been received on-board the correct aircraft.(↑[1.3.2]) See also: DO312-SPR.6

[2.4] The ITP flight crew will only perform the ITP maneuver if the specifics provided by ATC in the ITP Clearance are consistent with the information included in the ITP request made by the ITP flight crew.(↑[1.3.2][1.26][1.27][1.28][1.30]) See also: DO312-SPR.7

Note: *Any inconsistencies detected between the ITP Request and the ITP Clearance do not necessarily prohibit execution of an ITP maneuver, but may necessitate a reissue of the ITP request or other means to resolve the discrepancies between the Request and Clearance.*

[2.5] After receiving the ITP clearance the ITP flight crew will check that the following ITP Criteria are fulfilled before commencing an ITP maneuver: (↑[1.27])
- Criteria enumerated in (←[2.1.2],[2.1.3],[2.1.4])
Note: *Again, this design assumption does not imply that an individual assessment of each criterion is carried out by the flight crew, but rather that each criterion is assessed by either the flight crew, or by automation on a selected ADS-B transmitting aircraft (see section 3.5.1) and although not required for all criteria, it is recognised that automation may provide a more predictable solution.*

[2.6] The ITP flight crew will maintain the required Mach number during the ITP maneuver. This is levied based on mathematical calculations so the distance between the aircraft does not become less than the ITP Separation Minimum (i.e., 10 NM). ↑[1.30] See also: DO312-SPR.9

[2.7] During an ITP maneuver, the ITP flight crew should *not* modify the ITP clearance based on the ITP Equipment. This means the flight crew shall conform to the provided clearance and complete the ITP maneuver to the assigned altitude unless there is a flight safety concern detected by the flight crew..(↑[1.27.1][1.30])

Note: *This means the flight crew shall conform to the provided clearance and complete the ITP maneuver to the assigned altitude unless there is a flight safety concern detected by the flight crew.*

[2.8] The ITP flight crew must maintain a compliant climb/descent rate. This is again a mathematical consideration designed to ensure minimum separation distance during ITP.

[2.8.1] If during an ITP maneuver the ITP flight crew detects that the climb/descent rate is not compliant, the crew should attempt to rectify the deficiency. (↑[1.30]) See also: DO312-SPR.11

[2.8.2] If during an ITP maneuver, it is not possible to perform the ITP climb/descent, the ITP flight crew should follow regional contingency procedures. (↑[1.3.4],[1.33.4]) See also: DO312-SPR.12

[2.9] If the ITP flight crew detects a condition where the distance between the ITP and Reference Aircraft is reduced such that a significant reduction in safety or potential mid air collision is possible, the ITP flight crew will follow regional contingency procedures. (↑[1.3.4],[1.33.4]) See also: DO312-SPR.13

Note: *Although not required, automation could be used to improve the FC awareness of any significant reduction in ITP Distance as discussed in B.5.2.*

[2.10] If a confirmation message has not been received by ATC for an ITP clearance or a report for reaching a Flight Level, ATC will contact the flight crew. (↑[1.32.1], [1.35]) See also: DO312-SPR.14

[2.11] If during the "reaching Flight Level" report ATC detects that the ITP Aircraft has leveled off at the wrong Flight Level or if at a position reporting point, ATC detects the aircraft at the wrong Flight Level, ATC will contact the aircraft immediately. (↑[1.32.1], [1.35]) See also: DO312-SPR.15

Air Traffic Control

[2.12] ATC should check the ITP request for compliance with the following criteria before granting an ITP clearance. These mathematical constraints on the system are intended to ensure a desired minimum separation between aircraft, and these are the same criteria that the flight crew must verify (↑[1.9],[1.10],[1.13],[1.15],[1.16], ←[2.1])

- ITP Distance sent in the ITP request equal or greater than 15 nautical miles.
- Closing Mach Differential equal or less than 0.04 Mach.
- Reference Aircraft not maneuvering and not expected to maneuver during ITP.
- Maximum vertical distance between the ITP and Reference Aircraft of:
    - 3000 ft if the required vertical separation minima is 1000 ft, or
    - 2000 ft if the required vertical separation minima is 2000 ft
- ITP and Reference Aircraft are Same Track aircraft.
- ITP Request message format is correct, i.e., proper phraseology and information is included.

Note: *The Same Track criterion is not the same as the Similar Track criterion that is checked by the ITP Aircraft flight crew. Same Track includes the concept of Similar Track but also includes a check on whether or not the aircraft track protection areas overlap (which can only be known by the controller). For more information see the definitions list in 3.2 or Annex A.*
Note: *The controller is still responsible for ensuring there are no other aircraft involved.*

[2.13] ATC should not permit an aircraft to be an ITP Aircraft and a Reference Aircraft for another ITP operation at the same time. ATC may allow an aircraft to be a Reference Aircraft for two distinct ITP operations if this aircraft is at the same time leading for one ITP operation and following for another. One of the assumptions in the design of this procedure is that the Reference Aircraft is not maneuvering during an ITP (↑[1.15],[1.16]) See DO312-SPR.4

[2.14] ATC should include a minimum data set in its clearance, in order to minimize the risk of confusion during communication between the Flight Crew and ATC. This information includes the Reference Aircraft ID and the cleared-to Flight Level in the ITP clearance.(↑[1.3.1]) See also: DO312-SPR.5

B.4.3 Equipment Design Principles

This section describes the design principles that will be incorporated in the design of the on board ITP equipment. These principles are also enumerated with more detail in DO-312, with the additional traceability to level 1 and 3 principals added here. This section includes the minimum set of data required to safely execute the ITP, i.e. maintain a minimum separation distance, based on a mathematical model produced in DO-312. This performance model and its associated collision risk model assume certain initial conditions and aerodynamic performance characteristics necessary to achieve a desired flight geometry. These assumptions are captured as design decisions below.

[2.15] The values of the following information elements will be displayed to the ITP flight crew. These are the components of the ownship/reference relative state vector necessary to ensure minimum separation during ITP. These data are based on the Collision Risk Model and associated design laid out in DO-312. (↑[1.8]) See also DO312-SPR.18

Note: *Although not required from the safety and performance analyses, there is a strong preference amongst regulatory and certification authorities that Ground Speed and Relative Track Angle are also displayed to the flight crew.*

- Aircraft ID of Reference Aircraft
- ITP Distance
- Reference Aircraft Relative Altitude
- Leading or Following climb or descent information with respect to the Reference Aircraft

[2.15.1] The ITP Distance will be calculated by the ITP Equipment. (↑[1.8]) See also DO312-SPR.17

[2.15.2] The Ground Speed Differential will be calculated by the ITP Equipment. (↑[1.6],[1.7]) See also DO312-SPR.17

[2.15.3] The relative track angle between the tracks of the Reference Aircraft and the ITP Aircraft will be calculated by the ITP Equipment. (↑[1.6],[1.7]) See also DO312-SPR.27

[2.15.4] When Ground Speed Differential is displayed it must be with an unambiguous indication of whether or not it represents a situation where the aircraft are closing on each other (the distance is being reduced). (↑[1.1.1],[1.6],[1.7]) See also DO312-SPR.20

[2.16] The capability to assess whether the values of the following information elements pass the ITP Initiation Criteria will be provided to the ITP flight crew: (↑[1.7])

- Criteria enumerated in (←[2.1.2],[2.1.3],[2.1.4]) See also DO312-SPR.19

Note: *This assessment could be carried out by ITP Equipment automation functions (leading to a pass/fail being passed to the flight crew), or by the flight crew (leading to the information element values being passed to the flight crew).*

[2.16.1] The ITP Distance displayed to the flight crew must indicate a passed Initiation Criteria only when the calculated distance also passes the criteria (i.e., rounding or other means do not cause displayed data to indicate a passed criteria when it was calculated to fail). (↑[1.6],[1.7]) See also DO312-SPR.17

[2.16.2] The ITP Equipment will provide the ability to assess whether the accuracy and integrity of the surveillance data provided by the Reference Aircraft as well as the position and velocity data of the ITP Aircraft are of a sufficient level for the execution of an ITP maneuver. (↑[1.6],[1.7]) See DO312-SPR.26

[2.16.3] Ground Speed Differential, if displayed to the flight crew, will indicate a passed Initiation Criteria only when the calculated differential also passes the criteria (i.e., rounding or other means do not cause displayed data to indicate a passed criteria when it was calculated to fail). (↑[1.6],[1.7]) See also DO312-SPR.25

[2.16.4] For implementations that indicate whether or not the ITP initiation criteria (ITP Distance, Ground Speed Differential, and Similar Track status) are satisfied, such indication(s) must **shall** be clear and unambiguous. (↑[1.1.1],[1.6],[1.7]) See also DO312-SPR.21

Note: *In the requirement above, the term "Clear and Unambiguous" refers to the perception of the user, e.g., as verified in line with CS/FAR25-1309 [35], [36] or similar assessments.*

[2.17] The Total Receive Aircraft Domain Uncompensated Latency of Received position (from interface D to the input of the ITP Distance calculation) shall not exceed 1.575 seconds. (↑[1.7.3]) See also DO312-SPR.36

[2.18] The Total Receive Aircraft Domain Uncompensated Latency of ownship position (from interface A2 to the input of the ITP Distance calculation) shall not exceed 4.575 seconds. (↑[1.7.3]) See also DO312-SPR.37

[2.19] The Ownship climb/descend capability criteria will be considered passed if and only if the ITP Aircraft can climb/descend in the desired direction at a rate of 300 fpm or more. (↑[1.2], ←[2.1]) See also DO312-SPR.38

[2.20] The ITP Speed/Distance Criteria will be considered passed if and only if one of the following are met: (↑[1.2], ←[2.1]) See also DO312-SPR.39
- (ITP Distance ≥ 15 NM) and (Closing Ground Speed Differential ≤ 20 Kts)
or
- (ITP Distance ≥ 20 NM) and (Closing Ground Speed Differential ≤ 30 Kts)

[2.21] The Relative Altitude Criteria will be considered passed if and only if the difference in altitude between the ITP and Reference Aircraft is less than or equal to 3000 feet. (↑[1.2], ←[2.1]) See also DO312-SPR.40
Note: *The flight crew/ITP Equipment does not have knowledge of the separation minima. It can only check if the Reference Aircraft is/are vertically 3000 feet or less. ATC checks that the vertical distance is 3000 feet or less and that it is 2000 feet or less when the separation minima is 2000 feet.*

[2.22] The Similar Track Criteria will be considered passed if and only if the difference in track angles between the ITP and Reference Aircraft is less than ±45°. : (↑[1.2], ←[2.1]) See also DO312-SPR.41

[2.23] The position accuracy data quality criteria shall be considered passed only if the ITP Aircraft data AND Reference Aircraft data each have horizontal position accuracies of at least 0.5 NM at the 95th percentile. : (↑[1.2], ←[2.1]) See also DO312-SPR.42
Note: To pass the position data quality criteria, both the accuracy and integrity requirements on the data from both ITP and Reference Aircraft must be met. SPR.43 provides the accompanying integrity requirement to pass this criteria.

[2.24] The position integrity data quality criteria shall be considered passed only if the ITP Aircraft data AND Reference Aircraft data each have horizontal position integrity bounds of 1.0 NM with an integrity level of 1E-5. : (↑[1.2], [1.7.1], ←[2.1]) See also DO312-SPR.43
Note: To pass the position data quality criteria, both the accuracy and integrity requirements on the data from both ITP and Reference Aircraft must be met. SPR.42 provides the accompanying accuracy requirement to pass this criteria.

[2.25] The velocity data quality criteria shall be considered passed only if the ITP Aircraft data AND Reference Aircraft data each have horizontal velocity accuracies of at least 10 m/s (19.4 kts) at the 95th percentile. (↑[1.2], ←[2.1]) See also DO312-SPR.44

B.4.4 Data Environment Design Principles and Assumptions

This section describes the principles associated with the interoperability between the ATSA-ITP application ADS-B data. This section does <u>*not*</u> *specify anything pertaining to the certification of ADS-B and other surveillance equipment. Rather, it specifies the types of data that are expected in order for all of the elements of ATSA-ITP to operate effectively and safely.*

[2.26] The following ownship data items will be provided to the ITP Equipment. These are the components of the ownship state vector necessary to ensure minimum separation during ITP. These data are based on the Collision Risk Model and associated design laid out in DO-312. (↑[1.8], ←[2.15]) See also: DO312-SPR.16

- Horizontal Velocity
- Horizontal Velocity Accuracy
- Horizontal Position
- Horizontal Position Accuracy
- Horizontal Position Integrity Containment Bound
- Barometric Altitude

[2.27] The following ownship data items will also be available to the ITP flight crew for the reason outlined above: (↑[1.8], ←[2.15]) See also DO312-SPR.17

Note: *This information could be provided to the flight crew by either the ITP Equipment or through other means.*

- Vertical speed
- Information to determine available climb/descent performance at the current cruise Mach number
- Mach number

[2.28] The following ADS-B parameters will be sent from the Transmit Aircraft Domain: (↑[1.2], ←[2.1]) See also DO312-IR.1

- Identity
- Horizontal Position
- Vertical Position
- Horizontal
- Velocity
- Surveillance Quality Indication (of whether the surveillance quality of a particular aircraft is acceptable for the various functions of ATSA-ITP)

More specific requirements on each data parameter are specified in the following subsections.
Upon receipt of the transmitted data, the Receive Aircraft Domain must properly associate the data and present it to the ITP Equipment for processing.

[2.29] The Receive Aircraft Domain will be able to receive, from an eligible Transmit

Aircraft Domain, ADS-B messages containing at least the elements which enable the avionics to format the required ADS-B Surveillance Reports and associate the surveillance data with ownship surveillance data. See also DO312-IR.2

[2.30] The Transmit Aircraft Domain will transmit the 24 bit aircraft address within each ADS-B message. See also DO312-IR.3

[2.31] The Transmit Aircraft Domain will transmit an ADS-B message containing the aircraft identification. See also DO312-IR.4

[2.32] In order to maintain consistency and interoperability with existing aircraft and other aircraft in the domain, the definitions will align with international standards. As per ICAO Doc. 4444, the following definitions will be applied by the Transmit Aircraft Domain: (←[2.28] see also DO312-IR.5)
- (Chapter 1, Definitions) Aircraft Identification is 'a group of letters, figures or a combination thereof which is either identical to, or the coded equivalent of, the aircraft call sign to be used in air-ground communications, and which is used to identify the aircraft in ground-ground air traffic services communications',
- (Appendix 2, 2.2) one of the following aircraft identifications, not exceeding 7 characters:
-- the ICAO designator for the aircraft operating agency followed by the flight identification (e.g., KLM511, NGA213, JTR25) when in radiotelephony the call sign to be used by the aircraft will consist of the ICAO telephony designator for the operating agency followed by the flight identification (e.g., KLM511, NIGERIA 213, HERBIE 25); or
-- the registration marking of the aircraft (e.g., EIAKO, 4XBCD, N2567GA).

[2.32.1] The Transmit Aircraft Domain will transmit horizontal position information (i.e., latitude, longitude) referenced to WGS-84.

[2.32.2] The Receive Aircraft Domain will interpret received horizontal position information (i.e., latitude, longitude) as referenced to WGS-84.

[2.32.3] The Transmit Aircraft Domain will transmit an indication of quality for the horizontal position information.

[2.32.4] The indicators used will be either Navigation Integrity Category (NIC), Navigation Accuracy Category for Position (NACP) and Surveillance Integrity Level (SIL) as specified in DO-242A or Navigation Uncertainty Category for Position (NUCP) as specified in DO-242.

[2.32.4.1] As opposed to a single quality parameter, the Transmit Aircraft Domain should send accuracy and integrity as independent items (as defined per DO-242A).

[2.32.5] When NACP and NIC are transmitted, the Transmit Aircraft Domain function will determine NACP based upon Horizontal Figure of Merit (HFOM) (or equivalent) and NIC based upon on Horizontal Protection Limit (HPL) (or equivalent)

[2.32.6] When NUCP is transmitted, the Transmit Aircraft Domain function will determine NUCP based upon HPL or equivalent

[2.32.6.1] When the position data source is Global Navigation Satellite System (GNSS), then use of DO-208 RAIM calculations to determine HPL is acceptable as a minimum. However, NUCP/NIC values should be determined using HPL values based on DO- 229D, DO-253B, or DO-310 GNSS receivers RAIM methodology or equivalent when feasible.

[2.32.6.2] When the position data source is GNSS, the NACP values should be determined using the HFOM output from DO-208 or a DO-229D, DO-253B, or DO-310 GNSS receivers or equivalent.

[2.32.7] When the Transmit Aircraft Domain cannot calculate SIL, the value of SIL will reflect the minimum integrity of the measurement integrity and the system integrity.

[2.32.8] For position sources with software design assurance of at least Level C per DO- 178B/ED-12B and hardware design assurance of at least Level C per DO-254/ED-80 or equivalent a system integrity corresponding to SIL 2 is accepted, for others SIL will be set to ZERO (0).

[2.32.9] A distinction between NUCP and NIC/NACP/SIL airborne implementations will be provided by the Transmit Aircraft Domain (e.g., a link-specific defined version number).

[2.32.10] The Transmit Aircraft Domain will transmit pressure altitude

[2.32.10.1] Neither Gilham altitude encoders nor altitude sources with a resolution less than or equal to 7.62 m (25 ft) should be used by aircraft implementations.

[2.32.11] The Receive Aircraft Domain will interpret received Ground Velocity information as referenced to WGS-84.

[2.32.12] The Transmit Aircraft Domain will transmit Ground Velocity information as referenced to WGS-84.

B.5 Level 3: Blackbox Behavior

This level describes the simple blackbox behavior of each component of the system. "Blackbox behavior" means that each component is considered to be a blackbox: we will describe the inputs into the component, and the outputs produced by the component, but do nothing to describe the inner workings of the component—those details are held inside of the blackbox and out of scope of this level.

B.5.1 ITP Equipment

The blackbox behavior of the ITP equipment will be described further in the final document, using the parameters below for the SpecTRM model. The tables represent the limited set of ITP Distance only, as compared to the full set of ITP parameters (velocity, closing velocity, data quality, etc) laid out in DO-312.

Fundamental Goals of ITP equipment

1. Display ITP data – (↑[G.1],[G.2],[G.3]) (required)
2. Display other flight data (optional)

Outputs

1. ITP Distance Display – (↑[1.8][2.15])
2. Ground Speed Differential Display
3. Data Quality Passes Display
4. Data Quality Fails Display
5. Relative Track Angle Similar Track Status Display
6. Reference AC ID Display
7. Data Input Error Display
8. ITP Criteria Display Output (↑[1.7][2.15])

Modes

1. ITP Supervisor
2. ITP Display Mode

States

1. Reference AC Data State
2. ITP AC Data State
3. Data Quality State

Functions

1. ITP Distance Function
2. Ground Speed Differential Function
3. Relative Track Angle Function
4. Intersection Point Function

Inputs

1. Display Mode Input
2. Reference AC Horizontal Position (↑[2.32])

3. Reference AC Horizontal Position Accuracy
4. Reference AC Horizontal Position Integrity
5. Reference AC Surveillance Integrity Level
6. Reference AC Ground Speed
7. Reference AC Ground Speed Accuracy
8. Reference AC Barometric Altitude
9. Reference AC Track
10. Reference AC ID
11. ITP AC Horizontal Position
12. ITPAC Horizontal Position Accuracy
13. ITP AC Horizontal Position Integrity
14. ITP AC Ground Speed
15. ITP AC Ground Speed Accuracy
16. ITP AC Barometric Altitude
17. ITP AC Track

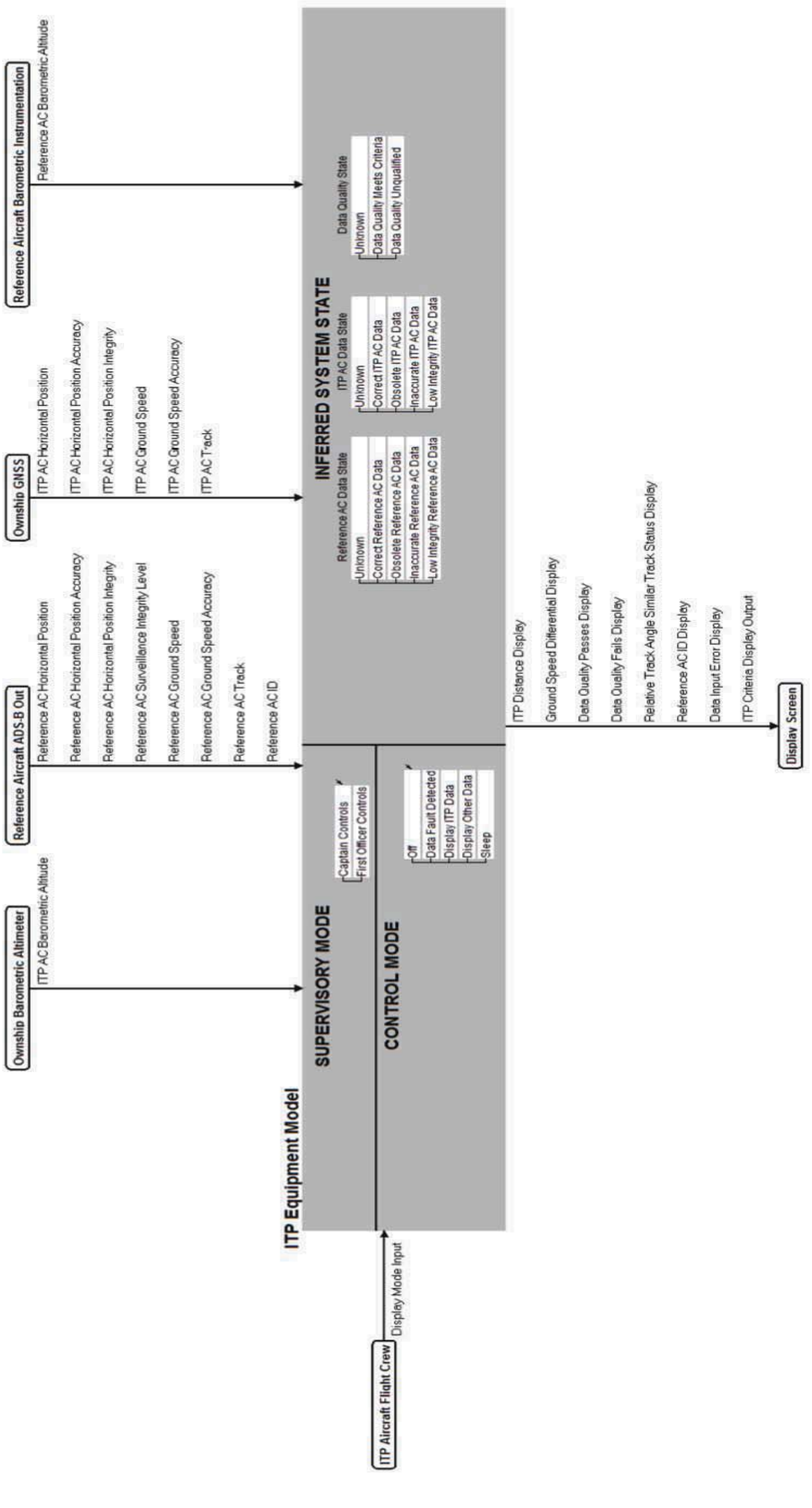
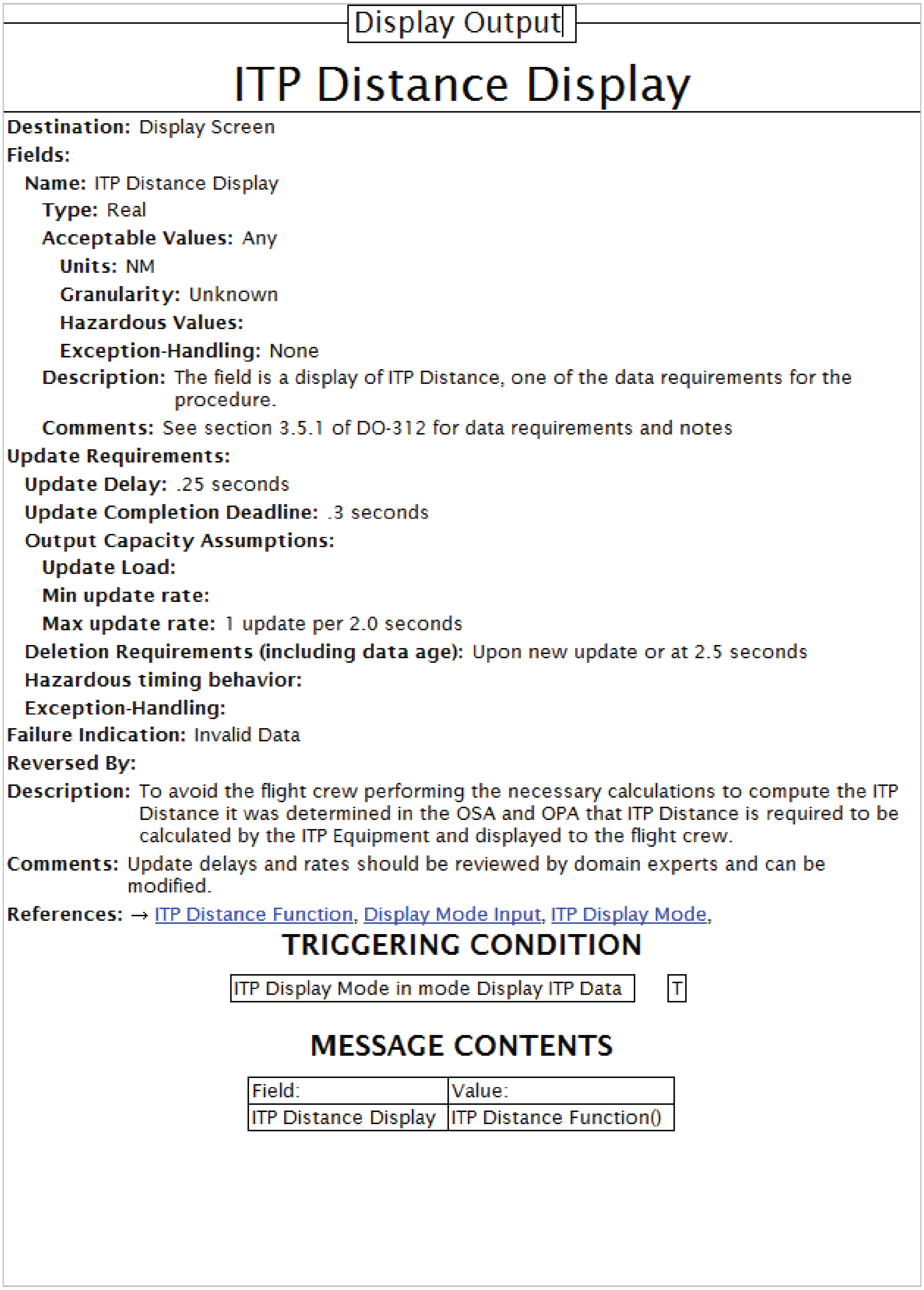

ITP Equipment Model
SUPERVISORY MODE
Captain Controls
First Officer Controls
CONTROL MODE
Off
Data Fault Detected
Display ITP Data
Display Other Data
Sleep
INFERRED SYSTEM STATE
Reference AC Data State
Unknown
Correct Reference AC Data
Obsolete Reference AC Data
Inaccurate Reference AC Data
Low Integrity Reference AC Data
ITP AC Data State
Unknown
Correct ITP AC Data
Obsolete ITP AC Data
Inaccurate ITP AC Data
Low Integrity ITP AC Data
Data Quality State
Unknown
Data Quality Meets Criteria
Data Quality Unqualified
Ownship Barometric Altimeter
ITP AC Barometric Altitude
Reference Aircraft ADS-B Out
Reference AC Horizontal Position
Reference AC Horizontal Position Accuracy
Reference AC Horizontal Position Integrity
Reference AC Surveillance Integrity Level
Reference AC Ground Speed
Reference AC Ground Speed Accuracy
Reference AC Track
Reference AC ID
Ownship GNSS
ITP AC Horizontal Position
ITP AC Horizontal Position Accuracy
ITP AC Horizontal Position Integrity
ITP AC Ground Speed
ITP AC Ground Speed Accuracy
ITP AC Track
Reference Aircraft Barometric Instrumentation
Reference AC Barometric Altitude
ITP Aircraft Flight Crew
Display Mode Input
ITP Distance Display
Ground Speed Differential Display
Data Quality Passes Display
Data Quality Fails Display
Relative Track Angle Similar Track Status Display
Reference AC ID Display
Data Input Error Display
ITP Criteria Display Output
Display Screen

Figure B.8 ITP Equipment Model Visualization

OUTPUTS



Display Output

ITP Distance Display

Destination: Display Screen

Fields:

Name: ITP Distance Display

Type: Real

Acceptable Values: Any

Units: NM

Granularity: Unknown

Hazardous Values:

Exception-Handling: None

Description: The field is a display of ITP Distance, one of the data requirements for the procedure.

Comments: See section 3.5.1 of DO-312 for data requirements and notes

Update Requirements:

Update Delay: .25 seconds

Update Completion Deadline: .3 seconds

Output Capacity Assumptions:

Update Load:

Min update rate:

Max update rate: 1 update per 2.0 seconds

Deletion Requirements (including data age): Upon new update or at 2.5 seconds

Hazardous timing behavior:

Exception-Handling:

Failure Indication: Invalid Data

Reversed By:

Description: To avoid the flight crew performing the necessary calculations to compute the ITP Distance it was determined in the OSA and OPA that ITP Distance is required to be calculated by the ITP Equipment and displayed to the flight crew.

Comments: Update delays and rates should be reviewed by domain experts and can be modified.

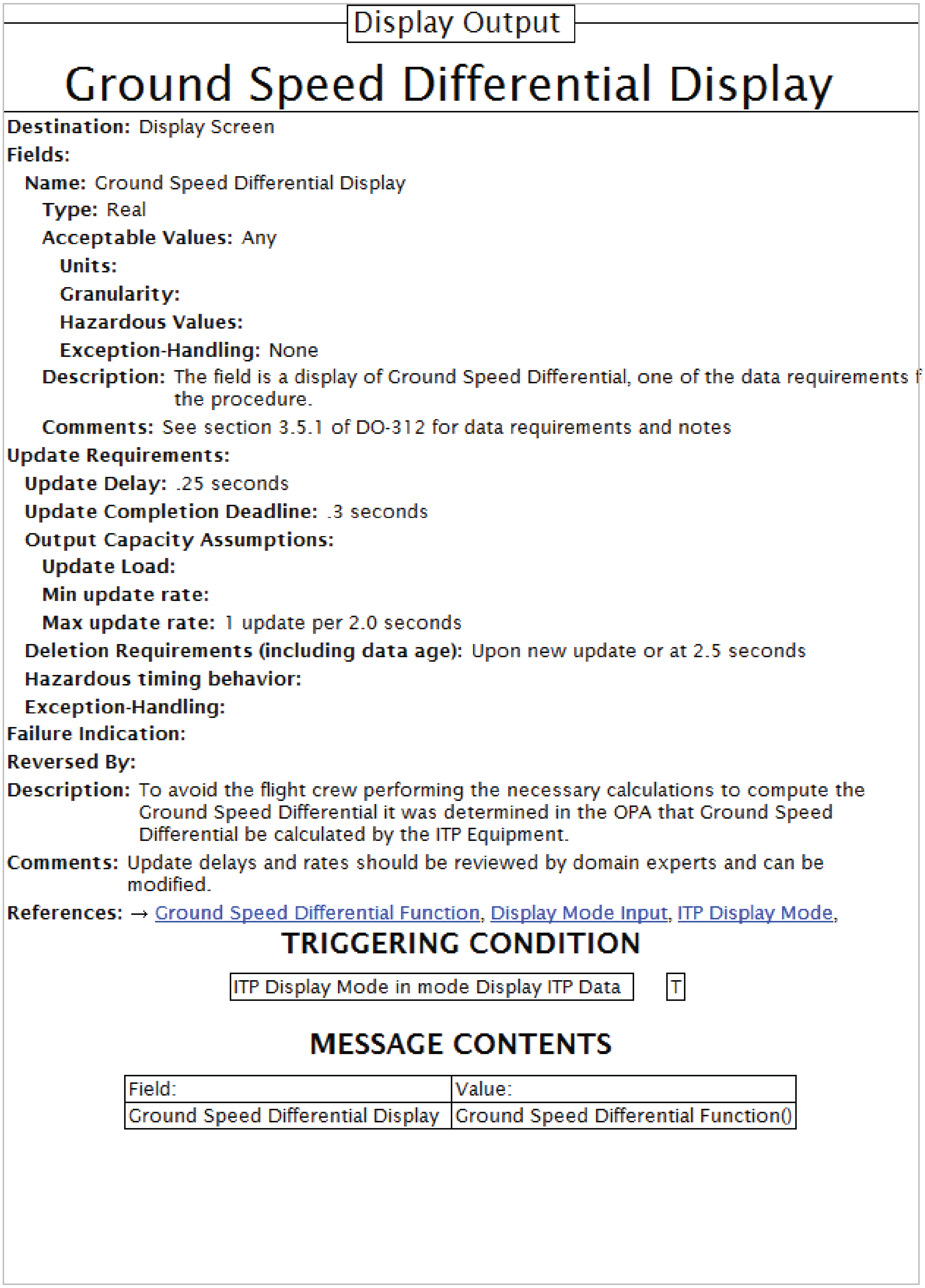
References: → ITP Distance Function, Display Mode Input, ITP Display Mode,

TRIGGERING CONDITION

ITP Display Mode in mode Display ITP Data	T

MESSAGE CONTENTS

Field:	Value:
ITP Distance Display	ITP Distance Function()



Display Output

Ground Speed Differential Display

Destination: Display Screen

Fields:

Name: Ground Speed Differential Display

Type: Real

Acceptable Values: Any

Units:

Granularity:

Hazardous Values:

Exception-Handling: None

Description: The field is a display of Ground Speed Differential, one of the data requirements f the procedure.

Comments: See section 3.5.1 of DO-312 for data requirements and notes

Update Requirements:

Update Delay: .25 seconds

Update Completion Deadline: .3 seconds

Output Capacity Assumptions:

Update Load:

Min update rate:

Max update rate: 1 update per 2.0 seconds

Deletion Requirements (including data age): Upon new update or at 2.5 seconds

Hazardous timing behavior:

Exception-Handling:

Failure Indication:

Reversed By:

Description: To avoid the flight crew performing the necessary calculations to compute the Ground Speed Differential it was determined in the OPA that Ground Speed Differential be calculated by the ITP Equipment.

Comments: Update delays and rates should be reviewed by domain experts and can be modified.

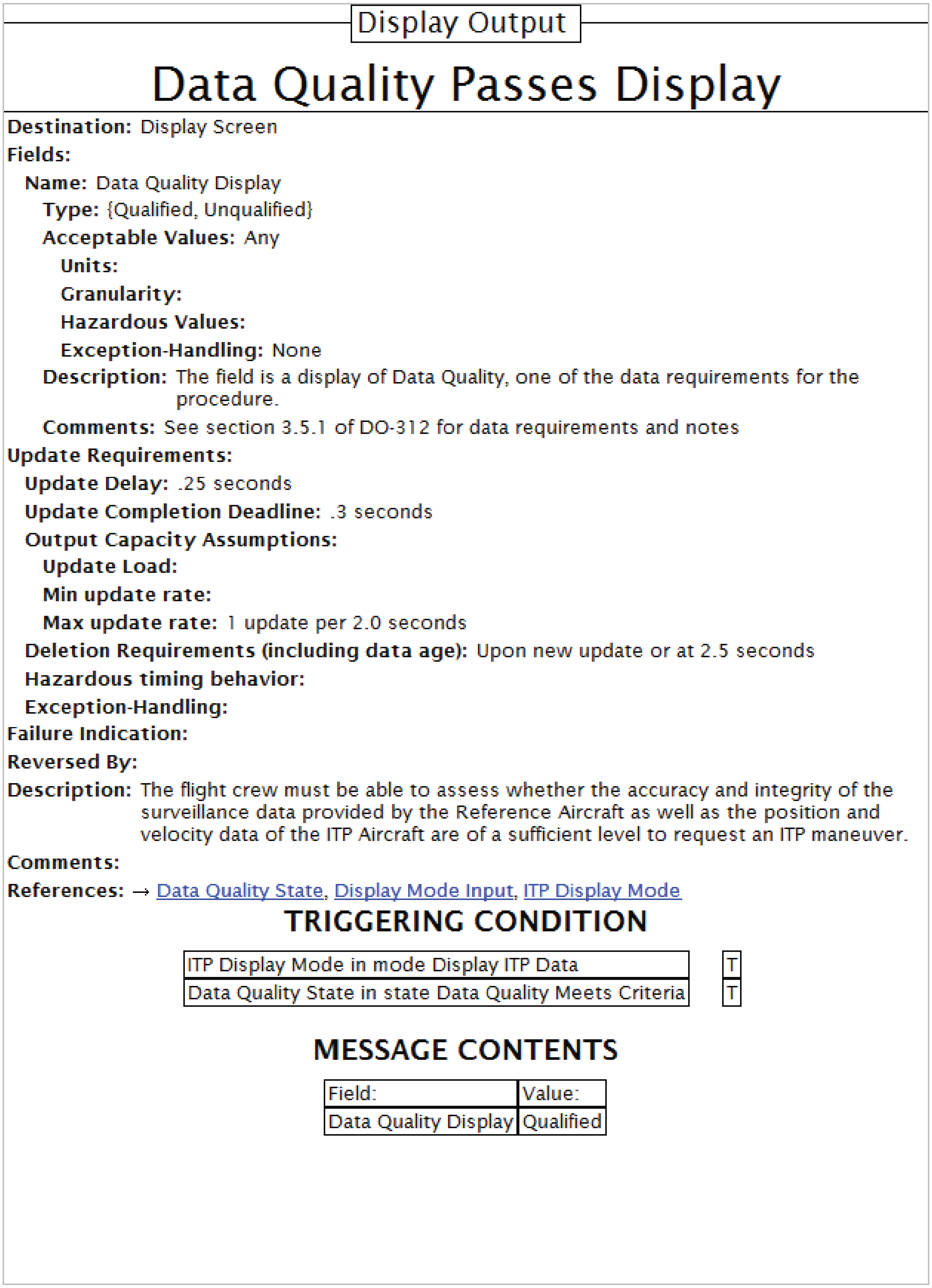
References: → Ground Speed Differential Function, Display Mode Input, ITP Display Mode,

TRIGGERING CONDITION

ITP Display Mode in mode Display ITP Data	T

MESSAGE CONTENTS

Field:	Value:
Ground Speed Differential Display	Ground Speed Differential Function()



Display Output

Data Quality Passes Display

Destination: Display Screen

Fields:

Name: Data Quality Display

Type: {Qualified, Unqualified}

Acceptable Values: Any

Units:

Granularity:

Hazardous Values:

Exception-Handling: None

Description: The field is a display of Data Quality, one of the data requirements for the procedure.

Comments: See section 3.5.1 of DO-312 for data requirements and notes

Update Requirements:

Update Delay: .25 seconds

Update Completion Deadline: .3 seconds

Output Capacity Assumptions:

Update Load:

Min update rate:

Max update rate: 1 update per 2.0 seconds

Deletion Requirements (including data age): Upon new update or at 2.5 seconds

Hazardous timing behavior:

Exception-Handling:

Failure Indication:

Reversed By:

Description: The flight crew must be able to assess whether the accuracy and integrity of the surveillance data provided by the Reference Aircraft as well as the position and velocity data of the ITP Aircraft are of a sufficient level to request an ITP maneuver.

Comments:

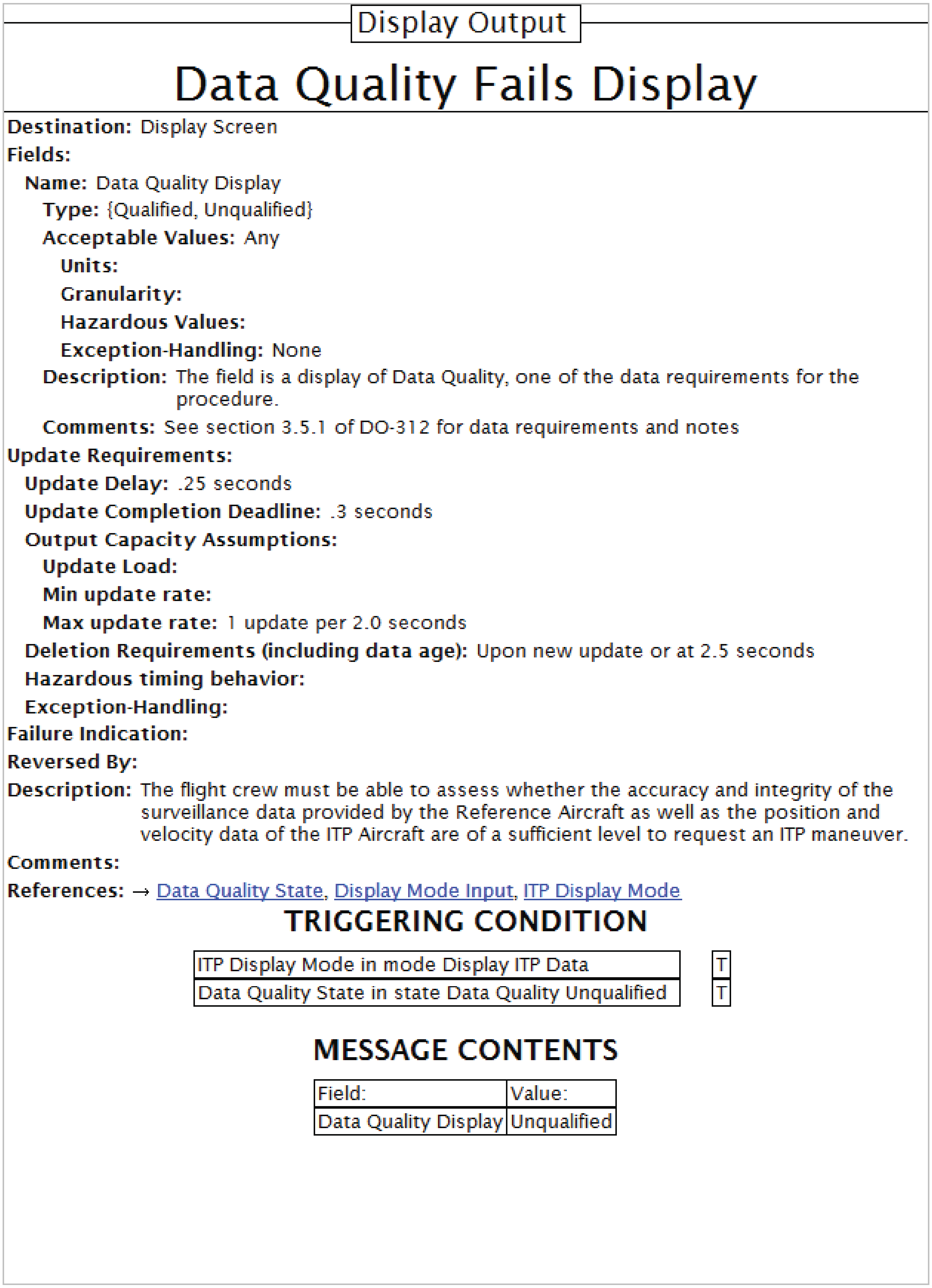
References: → Data Quality State, Display Mode Input, ITP Display Mode

TRIGGERING CONDITION

ITP Display Mode in mode Display ITP Data	T
Data Quality State in state Data Quality Meets Criteria	T

MESSAGE CONTENTS

Field:	Value:
Data Quality Display	Qualified



Display Output

Data Quality Fails Display

Destination: Display Screen

Fields:

Name: Data Quality Display

Type: {Qualified, Unqualified}

Acceptable Values: Any

Units:

Granularity:

Hazardous Values:

Exception-Handling: None

Description: The field is a display of Data Quality, one of the data requirements for the procedure.

Comments: See section 3.5.1 of DO-312 for data requirements and notes

Update Requirements:

Update Delay: .25 seconds

Update Completion Deadline: .3 seconds

Output Capacity Assumptions:

Update Load:

Min update rate:

Max update rate: 1 update per 2.0 seconds

Deletion Requirements (including data age): Upon new update or at 2.5 seconds

Hazardous timing behavior:

Exception-Handling:

Failure Indication:

Reversed By:

Description: The flight crew must be able to assess whether the accuracy and integrity of the surveillance data provided by the Reference Aircraft as well as the position and velocity data of the ITP Aircraft are of a sufficient level to request an ITP maneuver.

Comments:

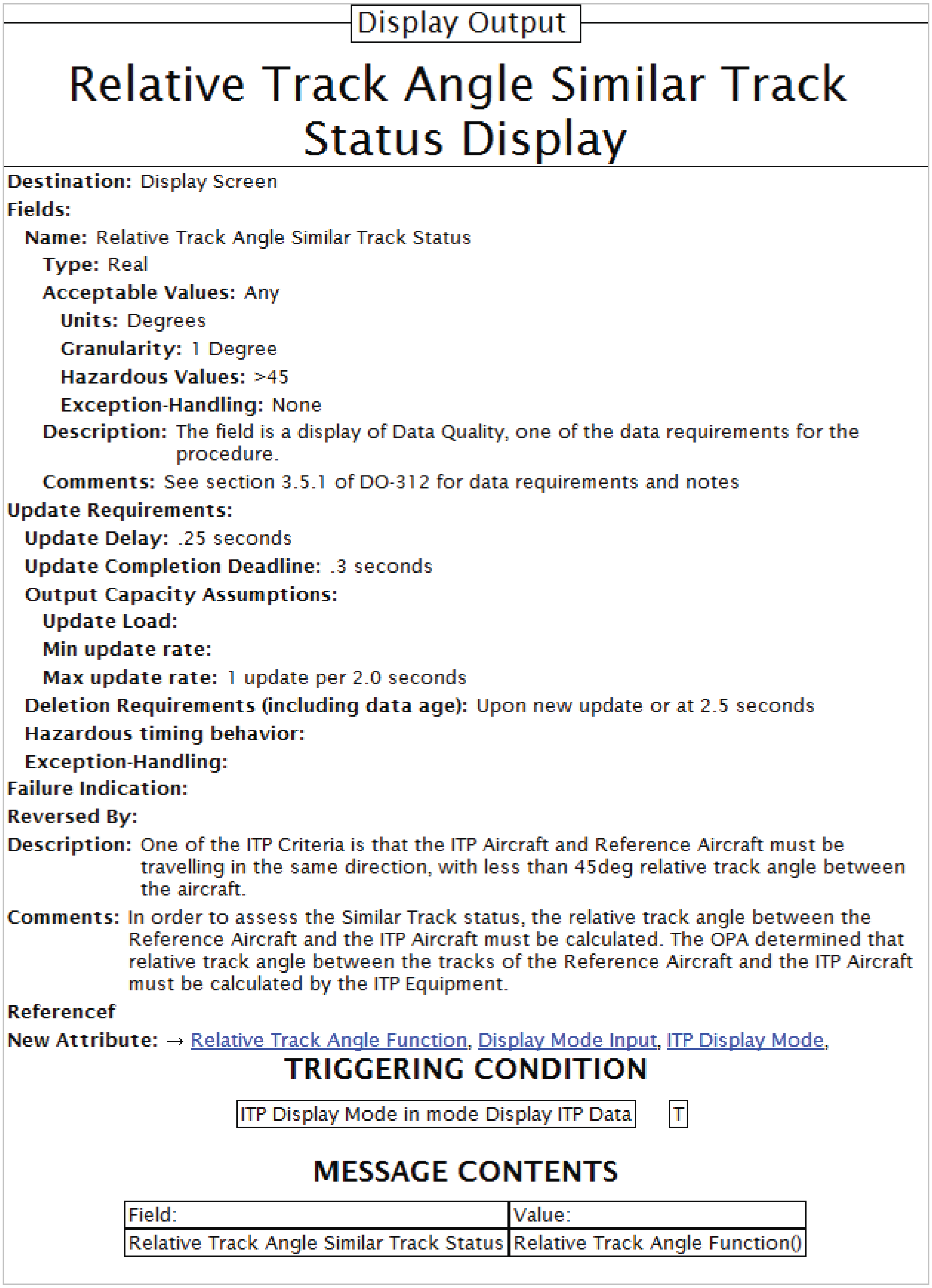
References: → Data Quality State, Display Mode Input, ITP Display Mode

TRIGGERING CONDITION

ITP Display Mode in mode Display ITP Data	T
Data Quality State in state Data Quality Unqualified	T

MESSAGE CONTENTS

Field:	Value:
Data Quality Display	Unqualified



Display Output

Relative Track Angle Similar Track Status Display

Destination: Display Screen

Fields:

Name: Relative Track Angle Similar Track Status

Type: Real

Acceptable Values: Any

Units: Degrees

Granularity: 1 Degree

Hazardous Values: >45

Exception-Handling: None

Description: The field is a display of Data Quality, one of the data requirements for the procedure.

Comments: See section 3.5.1 of DO-312 for data requirements and notes

Update Requirements:

Update Delay: .25 seconds

Update Completion Deadline: .3 seconds

Output Capacity Assumptions:

Update Load:

Min update rate:

Max update rate: 1 update per 2.0 seconds

Deletion Requirements (including data age): Upon new update or at 2.5 seconds

Hazardous timing behavior:

Exception-Handling:

Failure Indication:

Reversed By:

Description: One of the ITP Criteria is that the ITP Aircraft and Reference Aircraft must be travelling in the same direction, with less than 45deg relative track angle between the aircraft.

Comments: In order to assess the Similar Track status, the relative track angle between the Reference Aircraft and the ITP Aircraft must be calculated. The OPA determined that relative track angle between the tracks of the Reference Aircraft and the ITP Aircraft must be calculated by the ITP Equipment.

Referencef

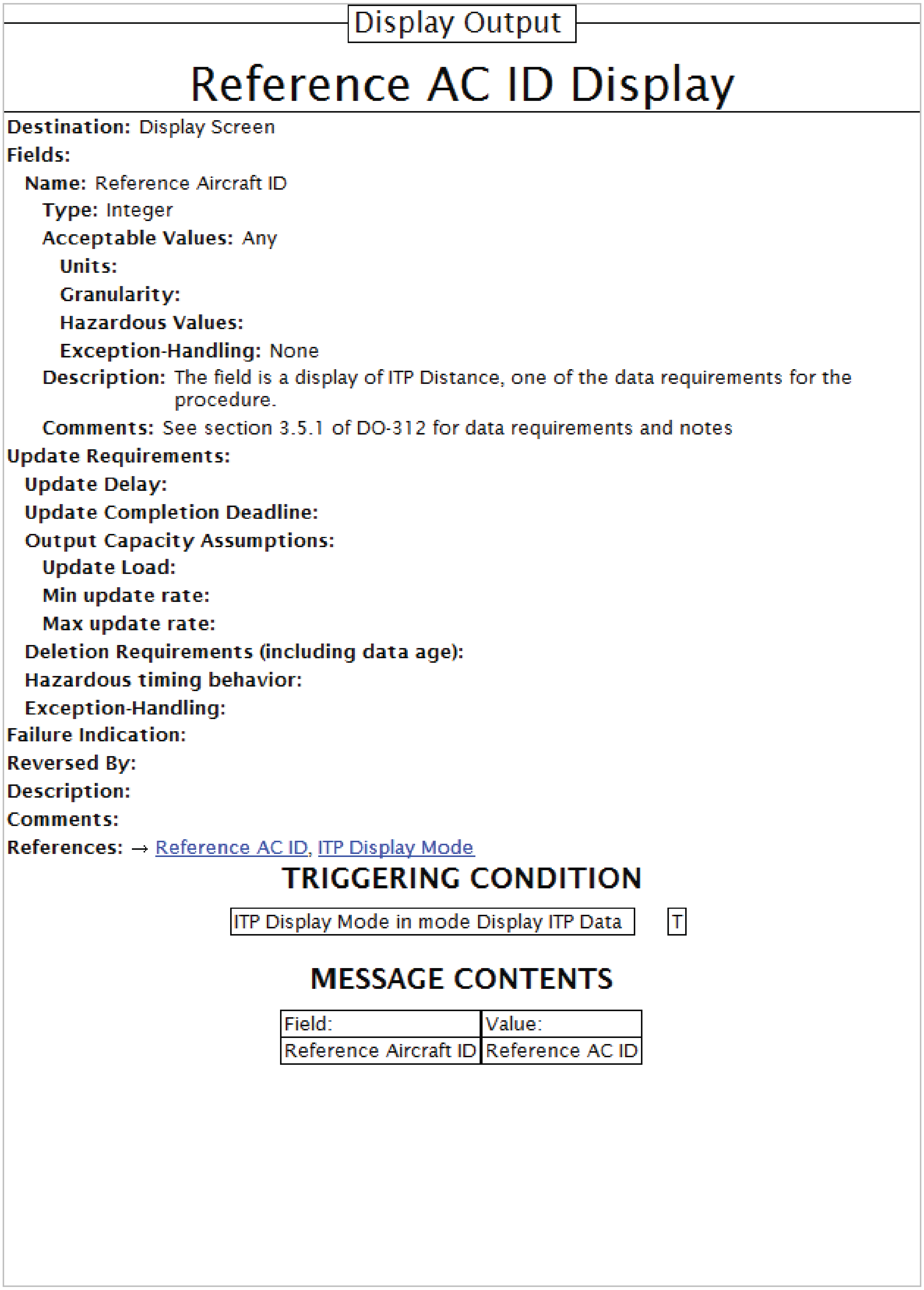
New Attribute: → Relative Track Angle Function, Display Mode Input, ITP Display Mode,

TRIGGERING CONDITION

ITP Display Mode in mode Display ITP Data	T

MESSAGE CONTENTS

Field:	Value:
Relative Track Angle Similar Track Status	Relative Track Angle Function()



Display Output

Reference AC ID Display

Destination: Display Screen

Fields:

Name: Reference Aircraft ID

Type: Integer

Acceptable Values: Any

Units:

Granularity:

Hazardous Values:

Exception-Handling: None

Description: The field is a display of ITP Distance, one of the data requirements for the procedure.

Comments: See section 3.5.1 of DO-312 for data requirements and notes

Update Requirements:

Update Delay:

Update Completion Deadline:

Output Capacity Assumptions:

Update Load:

Min update rate:

Max update rate:

Deletion Requirements (including data age):

Hazardous timing behavior:

Exception-Handling:

Failure Indication:

Reversed By:

Description:

Comments:

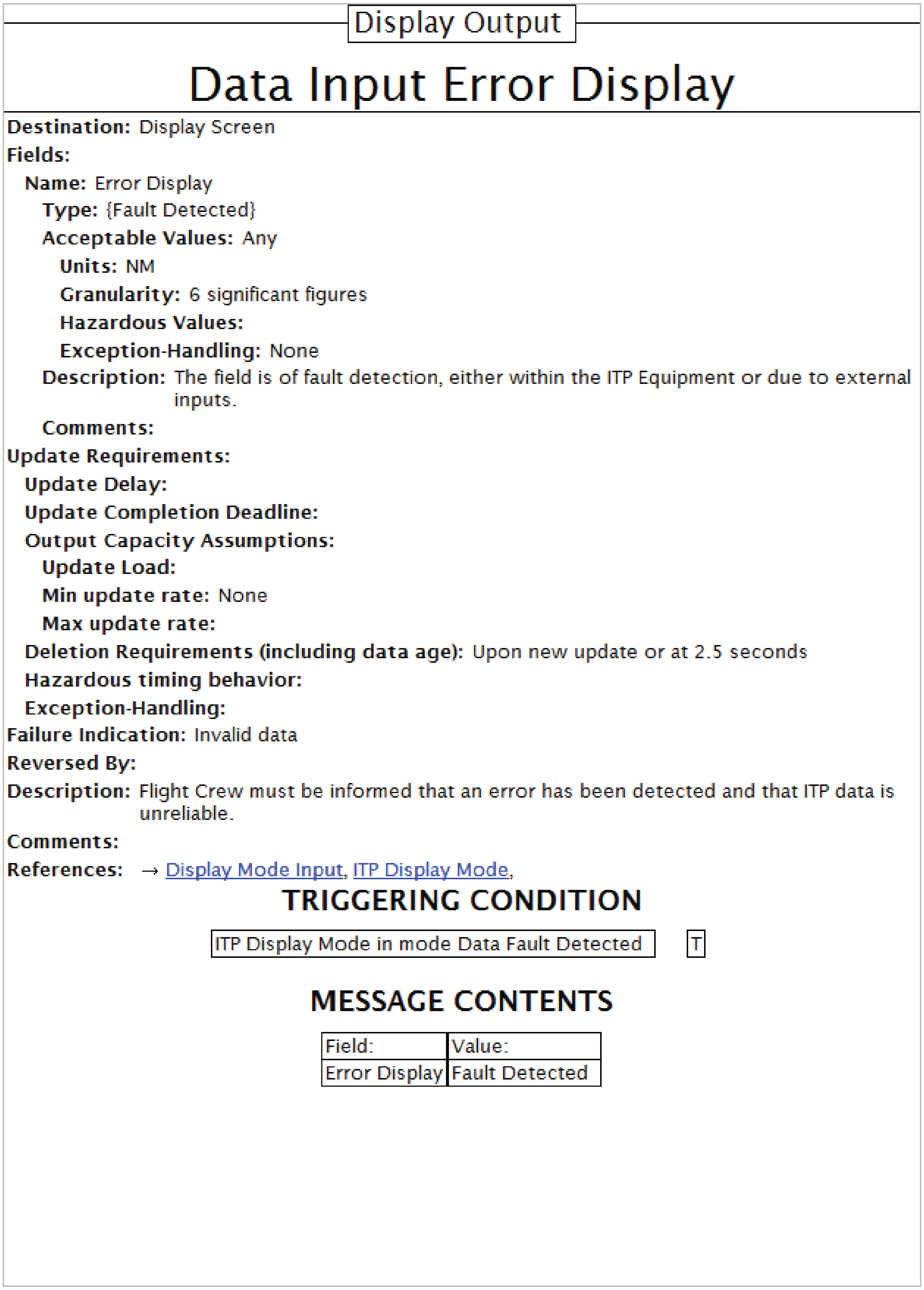
References: → Reference AC ID, ITP Display Mode

TRIGGERING CONDITION

ITP Display Mode in mode Display ITP Data	T

MESSAGE CONTENTS

Field:	Value:
Reference Aircraft ID	Reference AC ID



Display Output

Data Input Error Display

Destination: Display Screen

Fields:

- **Name:** Error Display
  - **Type:** {Fault Detected}
  - **Acceptable Values:** Any
    - **Units:** NM
    - **Granularity:** 6 significant figures
    - **Hazardous Values:**
    - **Exception-Handling:** None
  - **Description:** The field is of fault detection, either within the ITP Equipment or due to external inputs.
  - **Comments:**

Update Requirements:

- **Update Delay:**
- **Update Completion Deadline:**
- **Output Capacity Assumptions:**
  - **Update Load:**
  - **Min update rate:** None
  - **Max update rate:**
- **Deletion Requirements (including data age):** Upon new update or at 2.5 seconds
- **Hazardous timing behavior:**
- **Exception-Handling:**

Failure Indication: Invalid data

Reversed By:

Description: Flight Crew must be informed that an error has been detected and that ITP data is unreliable.

Comments:

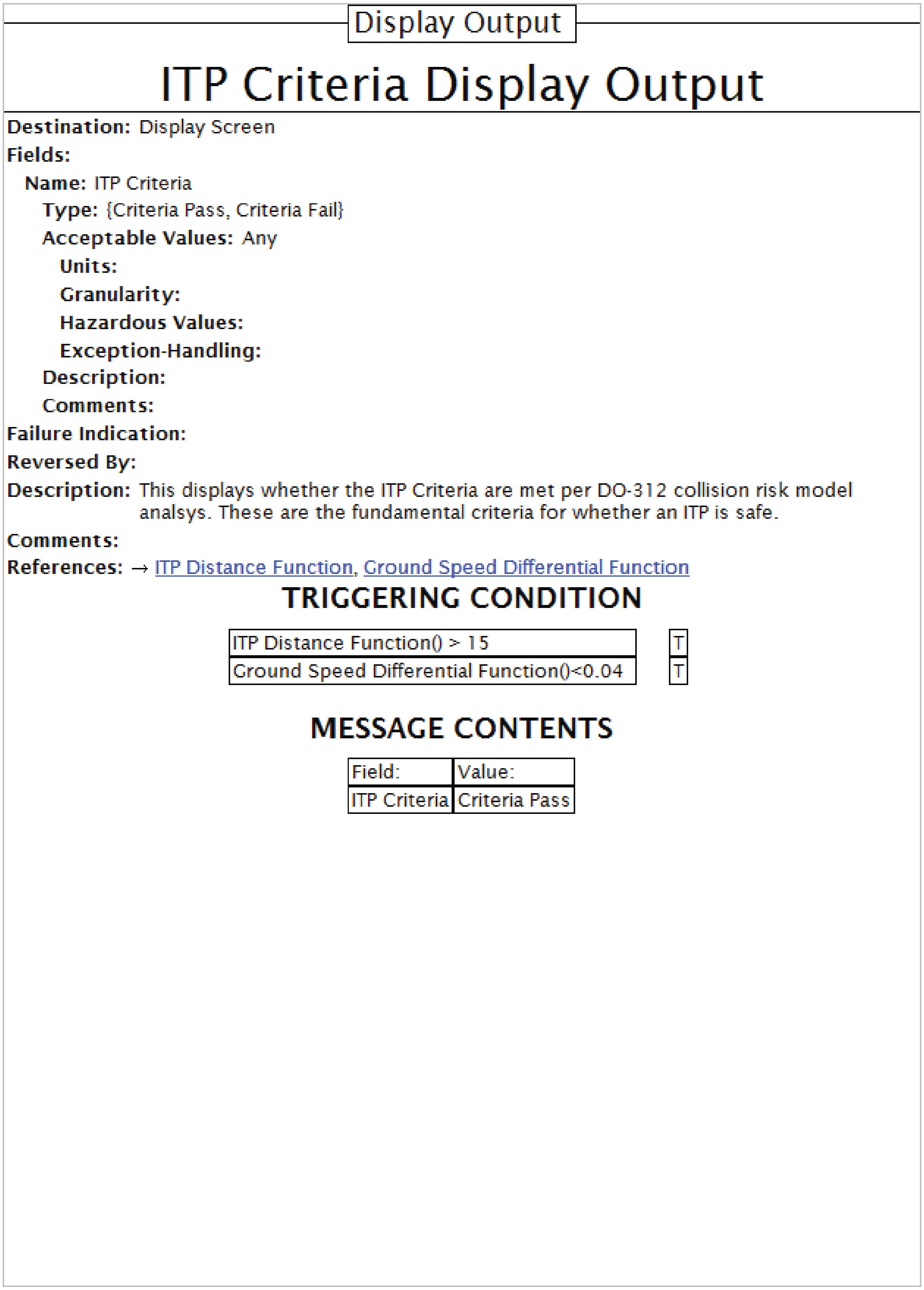
References: → Display Mode Input, ITP Display Mode,

TRIGGERING CONDITION

ITP Display Mode in mode Data Fault Detected	T

MESSAGE CONTENTS

Field:	Value:
Error Display	Fault Detected



Display Output

ITP Criteria Display Output

Destination: Display Screen

Fields:

Name: ITP Criteria

Type: {Criteria Pass, Criteria Fail}

Acceptable Values: Any

Units:

Granularity:

Hazardous Values:

Exception-Handling:

Description:

Comments:

Failure Indication:

Reversed By:

Description: This displays whether the ITP Criteria are met per DO-312 collision risk model analsys. These are the fundamental criteria for whether an ITP is safe.

Comments:

References: → ITP Distance Function, Ground Speed Differential Function

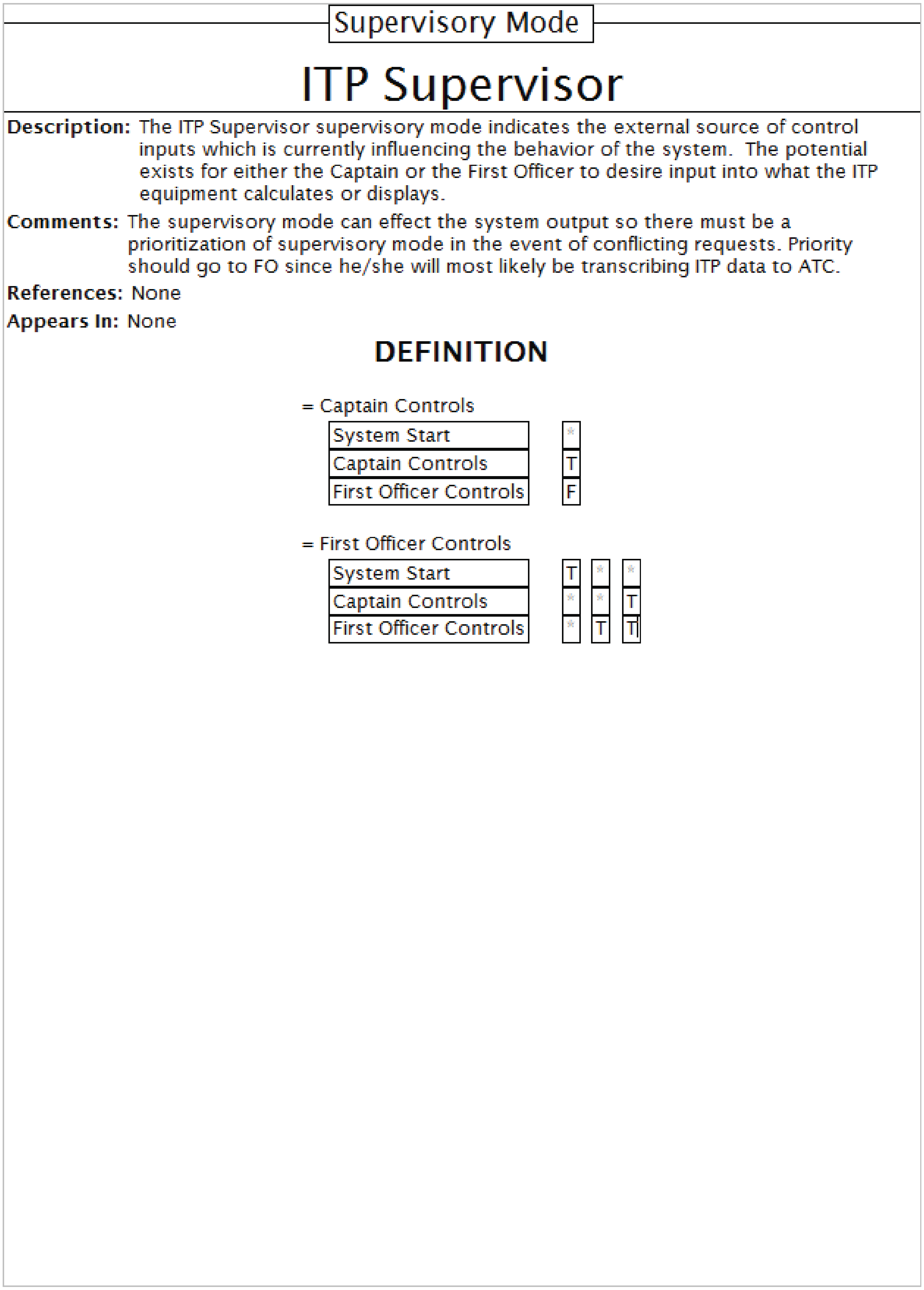
TRIGGERING CONDITION

ITP Distance Function() > 15	T
Ground Speed Differential Function()<0.04	T

MESSAGE CONTENTS

Field:	Value:
ITP Criteria	Criteria Pass

MODES



Supervisory Mode

ITP Supervisor

Description: The ITP Supervisor supervisory mode indicates the external source of control inputs which is currently influencing the behavior of the system. The potential exists for either the Captain or the First Officer to desire input into what the ITP equipment calculates or displays.

Comments: The supervisory mode can effect the system output so there must be a prioritization of supervisory mode in the event of conflicting requests. Priority should go to FO since he/she will most likely be transcribing ITP data to ATC.

References: None

Appears In: None

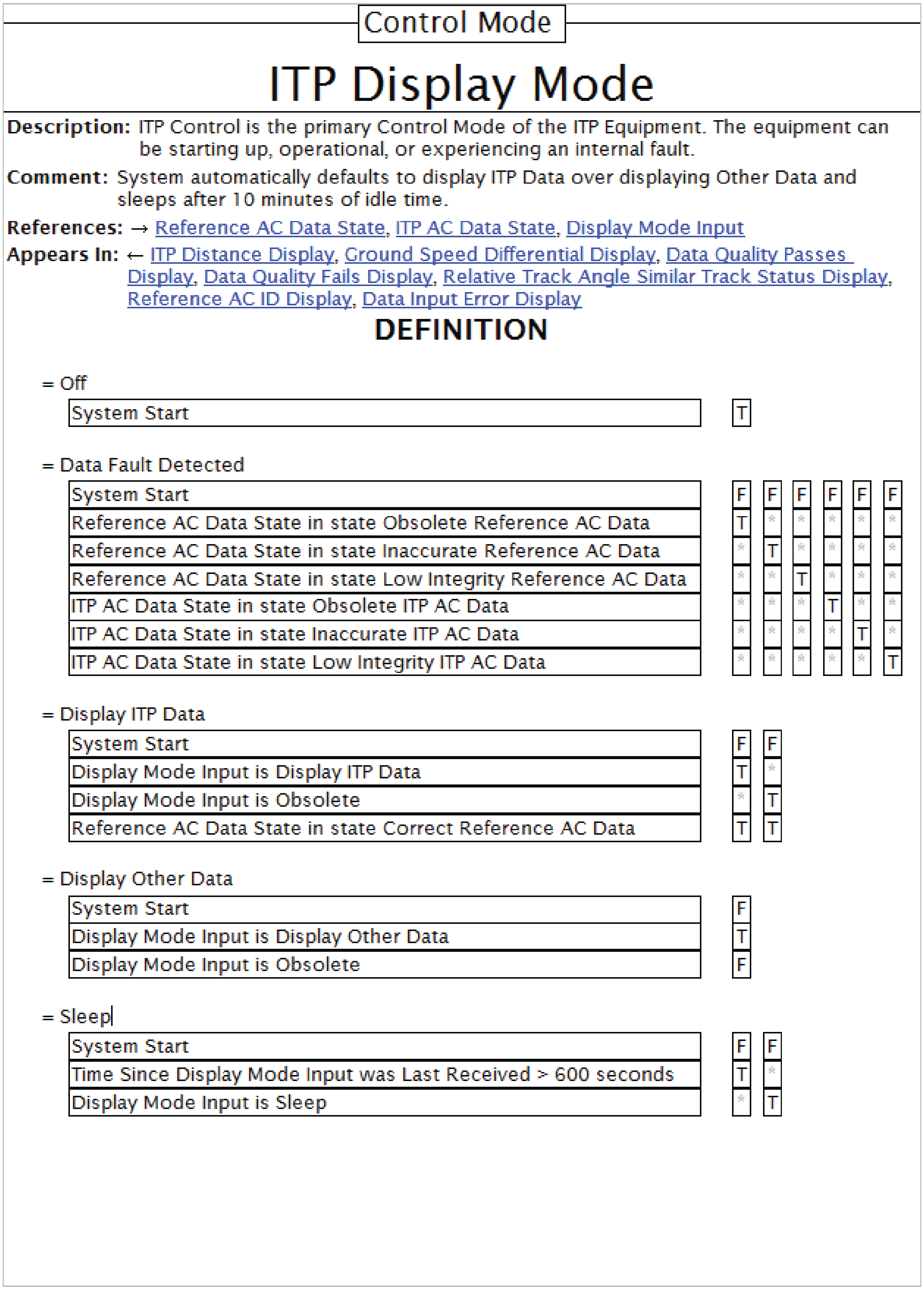
DEFINITION

= Captain Controls

System Start	*
Captain Controls	T
First Officer Controls	F

= First Officer Controls

System Start	T	*	*
Captain Controls	*	*	T
First Officer Controls	*	T	T



Control Mode

ITP Display Mode

Description: ITP Control is the primary Control Mode of the ITP Equipment. The equipment can be starting up, operational, or experiencing an internal fault.

Comment: System automatically defaults to display ITP Data over displaying Other Data and sleeps after 10 minutes of idle time.

References: → Reference AC Data State, ITP AC Data State, Display Mode Input

Appears In: ← ITP Distance Display, Ground Speed Differential Display, Data Quality Passes Display, Data Quality Fails Display, Relative Track Angle Similar Track Status Display, Reference AC ID Display, Data Input Error Display

DEFINITION

= Off

System Start	T

= Data Fault Detected

System Start	F	F	F	F	F	F
Reference AC Data State in state Obsolete Reference AC Data	T	*	*	*	*	*
Reference AC Data State in state Inaccurate Reference AC Data	*	T	*	*	*	*
Reference AC Data State in state Low Integrity Reference AC Data	*	*	T	*	*	*
ITP AC Data State in state Obsolete ITP AC Data	*	*	*	T	*	*
ITP AC Data State in state Inaccurate ITP AC Data	*	*	*	*	T	*
ITP AC Data State in state Low Integrity ITP AC Data	*	*	*	*	*	T

= Display ITP Data

System Start	F	F
Display Mode Input is Display ITP Data	T	*
Display Mode Input is Obsolete	*	T
Reference AC Data State in state Correct Reference AC Data	T	T

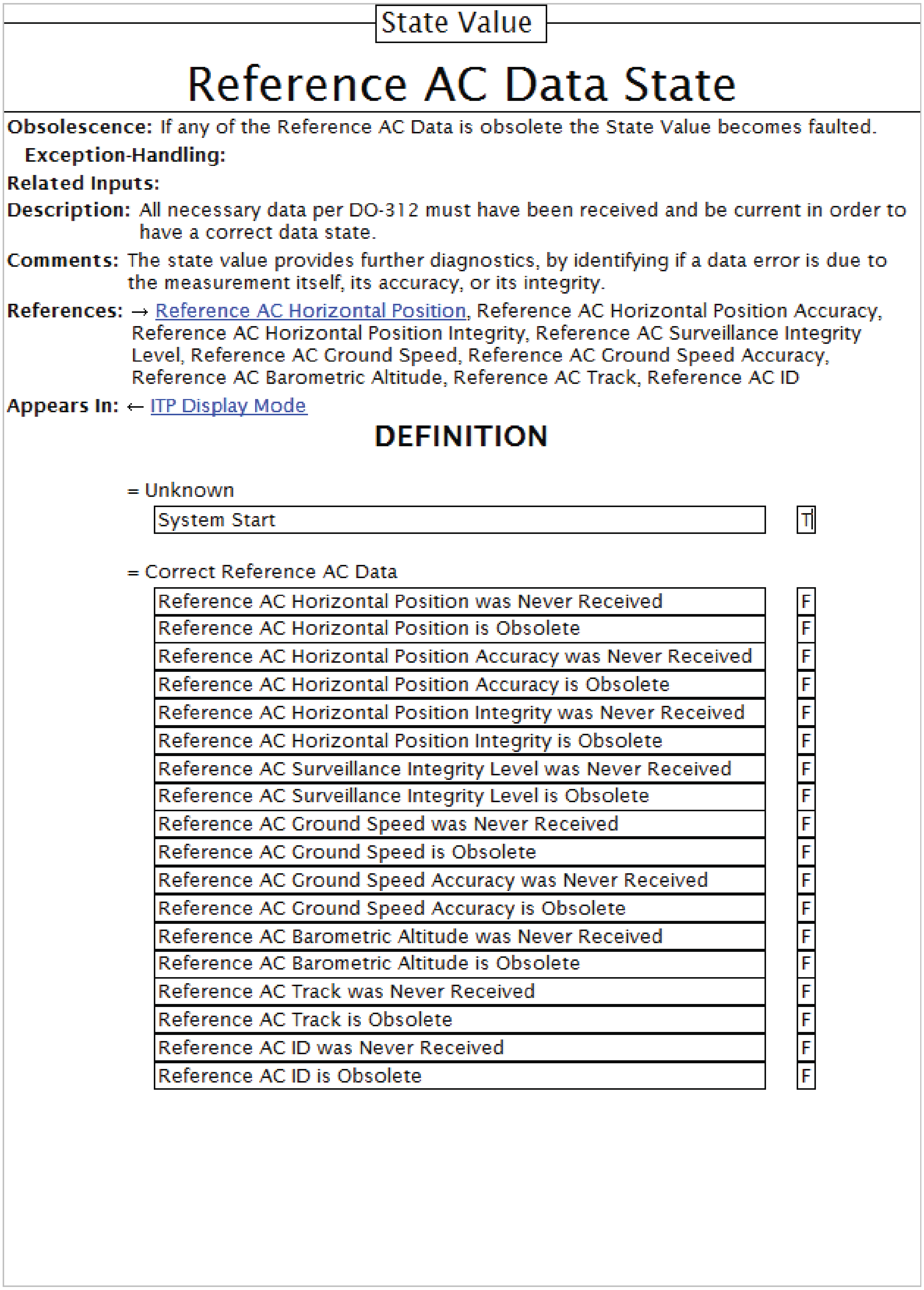
= Display Other Data

System Start	F
Display Mode Input is Display Other Data	T
Display Mode Input is Obsolete	F

= Sleep

System Start	F	F
Time Since Display Mode Input was Last Received > 600 seconds	T	*
Display Mode Input is Sleep	*	T

STATES



State Value

Reference AC Data State

Obsolescence: If any of the Reference AC Data is obsolete the State Value becomes faulted.

Exception-Handling:

Related Inputs:

Description: All necessary data per DO-312 must have been received and be current in order to have a correct data state.

Comments: The state value provides further diagnostics, by identifying if a data error is due to the measurement itself, its accuracy, or its integrity.

References: → Reference AC Horizontal Position, Reference AC Horizontal Position Accuracy, Reference AC Horizontal Position Integrity, Reference AC Surveillance Integrity Level, Reference AC Ground Speed, Reference AC Ground Speed Accuracy, Reference AC Barometric Altitude, Reference AC Track, Reference AC ID

Appears In: ← ITP Display Mode

DEFINITION

= Unknown

System Start	T

= Correct Reference AC Data

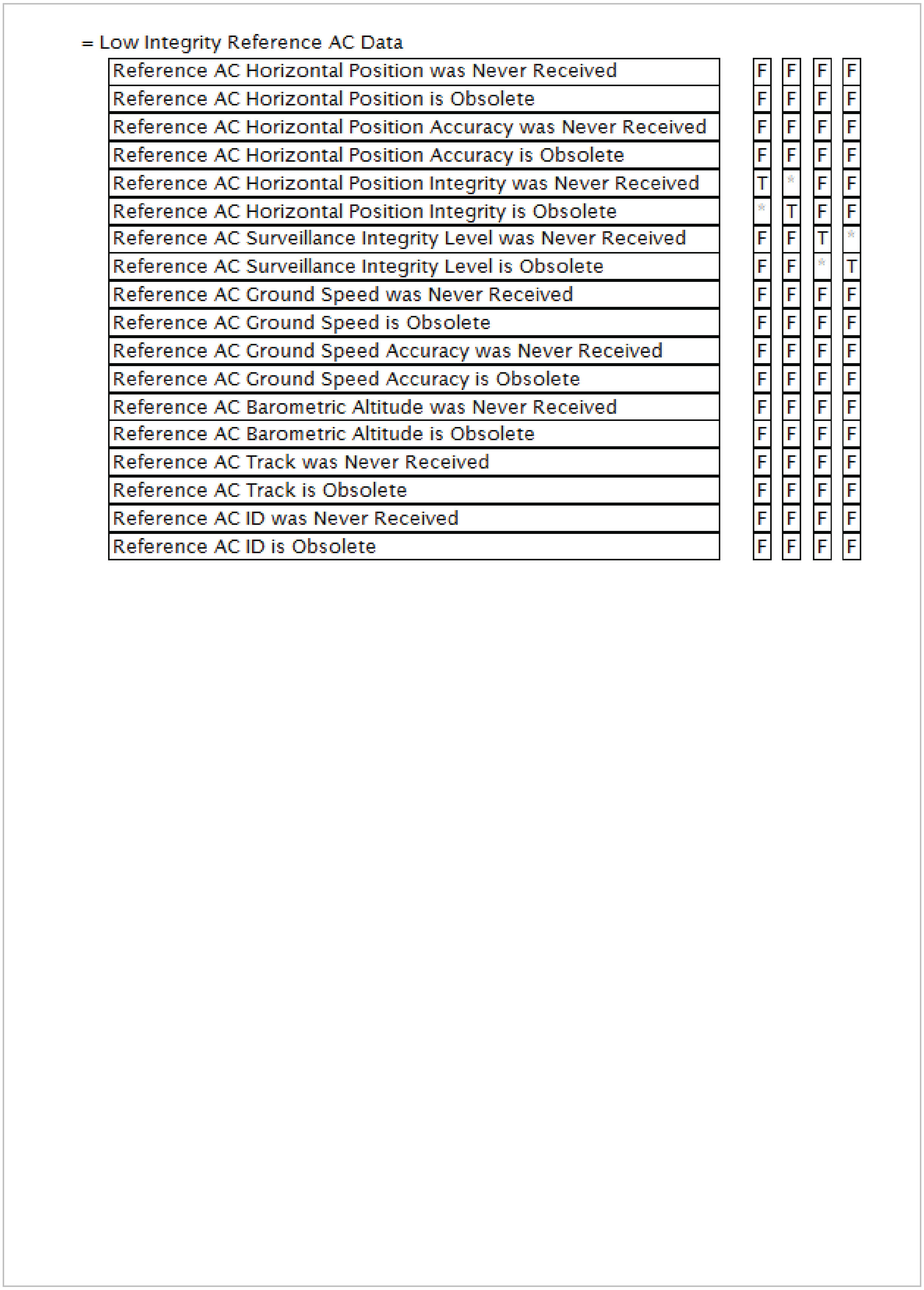
Reference AC Horizontal Position was Never Received	F
Reference AC Horizontal Position is Obsolete	F
Reference AC Horizontal Position Accuracy was Never Received	F
Reference AC Horizontal Position Accuracy is Obsolete	F
Reference AC Horizontal Position Integrity was Never Received	F
Reference AC Horizontal Position Integrity is Obsolete	F
Reference AC Surveillance Integrity Level was Never Received	F
Reference AC Surveillance Integrity Level is Obsolete	F
Reference AC Ground Speed was Never Received	F
Reference AC Ground Speed is Obsolete	F
Reference AC Ground Speed Accuracy was Never Received	F
Reference AC Ground Speed Accuracy is Obsolete	F
Reference AC Barometric Altitude was Never Received	F
Reference AC Barometric Altitude is Obsolete	F
Reference AC Track was Never Received	F
Reference AC Track is Obsolete	F
Reference AC ID was Never Received	F
Reference AC ID is Obsolete	F

= Obsolete Reference AC Data

Reference AC Horizontal Position was Never Received	T	*	F	F	F	F	F	F	F	F
Reference AC Horizontal Position is Obsolete	*	T	F	F	F	F	F	F	F	F
Reference AC Horizontal Position Accuracy was Never Received	F	F	F	F	F	F	F	F	F	F
Reference AC Horizontal Position Accuracy is Obsolete	F	F	F	F	F	F	F	F	F	F
Reference AC Horizontal Position Integrity was Never Received	F	F	F	F	F	F	F	F	F	F
Reference AC Horizontal Position Integrity is Obsolete	F	F	F	F	F	F	F	F	F	F
Reference AC Surveillance Integrity Level was Never Received	F	F	F	F	F	F	F	F	F	F
Reference AC Surveillance Integrity Level is Obsolete	F	F	F	F	F	F	F	F	F	F
Reference AC Ground Speed was Never Received	F	F	T	*	F	F	F	F	F	F
Reference AC Ground Speed is Obsolete	F	F	*	T	F	F	F	F	F	F
Reference AC Ground Speed Accuracy was Never Received	F	F	F	F	F	F	F	F	F	F
Reference AC Ground Speed Accuracy is Obsolete	F	F	F	F	F	F	F	F	F	F
Reference AC Barometric Altitude was Never Received	F	F	F	F	T	*	F	F	F	F
Reference AC Barometric Altitude is Obsolete	F	F	F	F	*	T	F	F	F	F
Reference AC Track was Never Received	F	F	F	F	F	F	T	*	F	F
Reference AC Track is Obsolete	F	F	F	F	F	F	*	T	F	F
Reference AC ID was Never Received	F	F	F	F	F	F	F	F	T	*
Reference AC ID is Obsolete	F	F	F	F	F	F	F	F	*	T

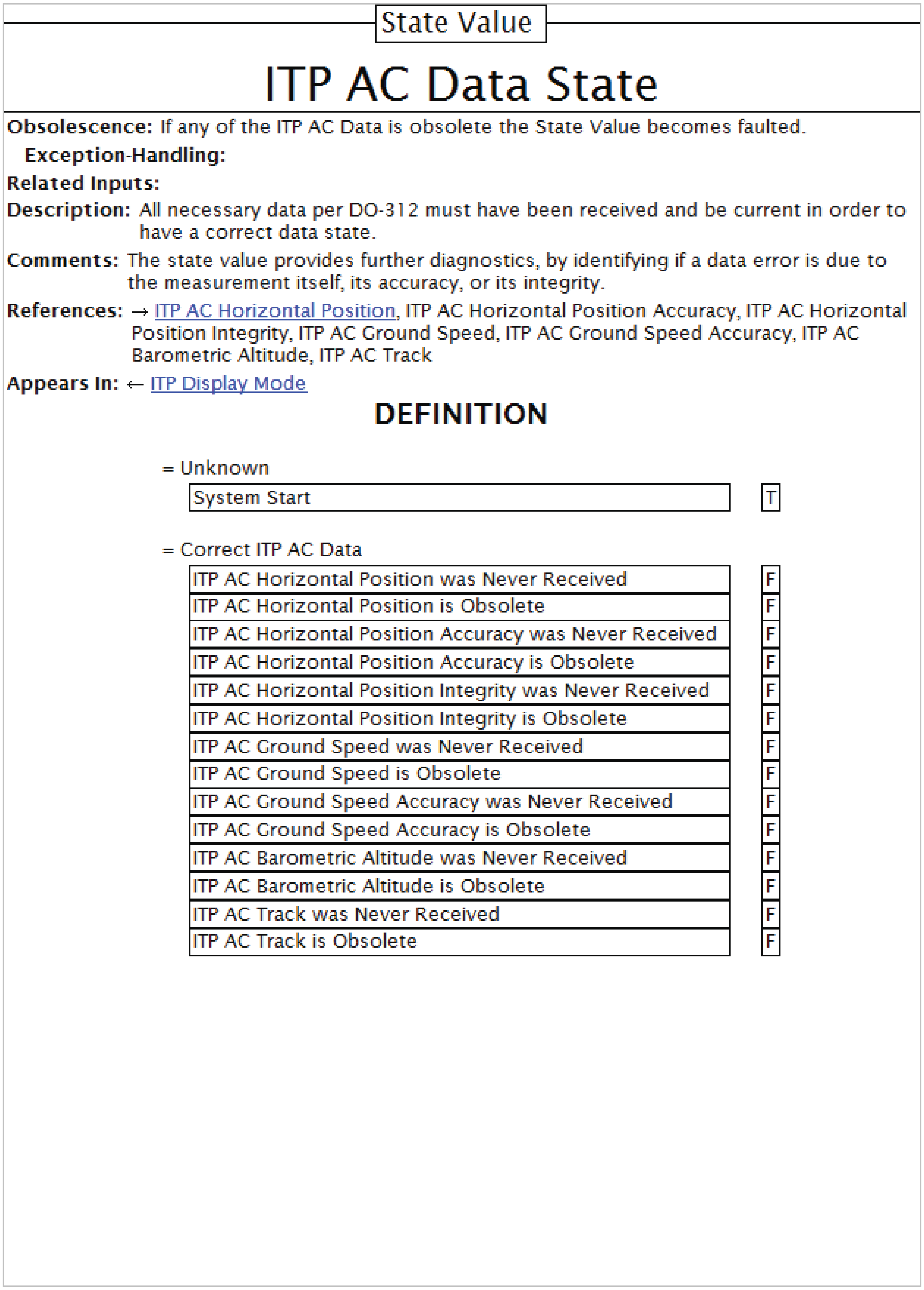
= Inaccurate Reference AC Data

Reference AC Horizontal Position was Never Received	F	F	F	F
Reference AC Horizontal Position is Obsolete	F	F	F	F
Reference AC Horizontal Position Accuracy was Never Received	T	*	F	F
Reference AC Horizontal Position Accuracy is Obsolete	*	T	F	F
Reference AC Horizontal Position Integrity was Never Received	F	F	F	F
Reference AC Horizontal Position Integrity is Obsolete	F	F	F	F
Reference AC Surveillance Integrity Level was Never Received	F	F	F	F
Reference AC Surveillance Integrity Level is Obsolete	F	F	F	F
Reference AC Ground Speed was Never Received	F	F	F	F
Reference AC Ground Speed is Obsolete	F	F	F	F
Reference AC Ground Speed Accuracy was Never Received	F	F	T	*
Reference AC Ground Speed Accuracy is Obsolete	F	F	*	T
Reference AC Barometric Altitude was Never Received	F	F	F	F
Reference AC Barometric Altitude is Obsolete	F	F	F	F
Reference AC Track was Never Received	F	F	F	F
Reference AC Track is Obsolete	F	F	F	F
Reference AC ID was Never Received	F	F	F	F
Reference AC ID is Obsolete	F	F	F	F



= Low Integrity Reference AC Data

Reference AC Horizontal Position was Never Received	F	F	F	F
Reference AC Horizontal Position is Obsolete	F	F	F	F
Reference AC Horizontal Position Accuracy was Never Received	F	F	F	F
Reference AC Horizontal Position Accuracy is Obsolete	F	F	F	F
Reference AC Horizontal Position Integrity was Never Received	T	*	F	F
Reference AC Horizontal Position Integrity is Obsolete	*	T	F	F
Reference AC Surveillance Integrity Level was Never Received	F	F	T	*
Reference AC Surveillance Integrity Level is Obsolete	F	F	*	T
Reference AC Ground Speed was Never Received	F	F	F	F
Reference AC Ground Speed is Obsolete	F	F	F	F
Reference AC Ground Speed Accuracy was Never Received	F	F	F	F
Reference AC Ground Speed Accuracy is Obsolete	F	F	F	F
Reference AC Barometric Altitude was Never Received	F	F	F	F
Reference AC Barometric Altitude is Obsolete	F	F	F	F
Reference AC Track was Never Received	F	F	F	F
Reference AC Track is Obsolete	F	F	F	F
Reference AC ID was Never Received	F	F	F	F
Reference AC ID is Obsolete	F	F	F	F



State Value

ITP AC Data State

Obsolescence: If any of the ITP AC Data is obsolete the State Value becomes faulted.

Exception-Handling:

Related Inputs:

Description: All necessary data per DO-312 must have been received and be current in order to have a correct data state.

Comments: The state value provides further diagnostics, by identifying if a data error is due to the measurement itself, its accuracy, or its integrity.

References: → ITP AC Horizontal Position, ITP AC Horizontal Position Accuracy, ITP AC Horizontal Position Integrity, ITP AC Ground Speed, ITP AC Ground Speed Accuracy, ITP AC Barometric Altitude, ITP AC Track

Appears In: ← ITP Display Mode

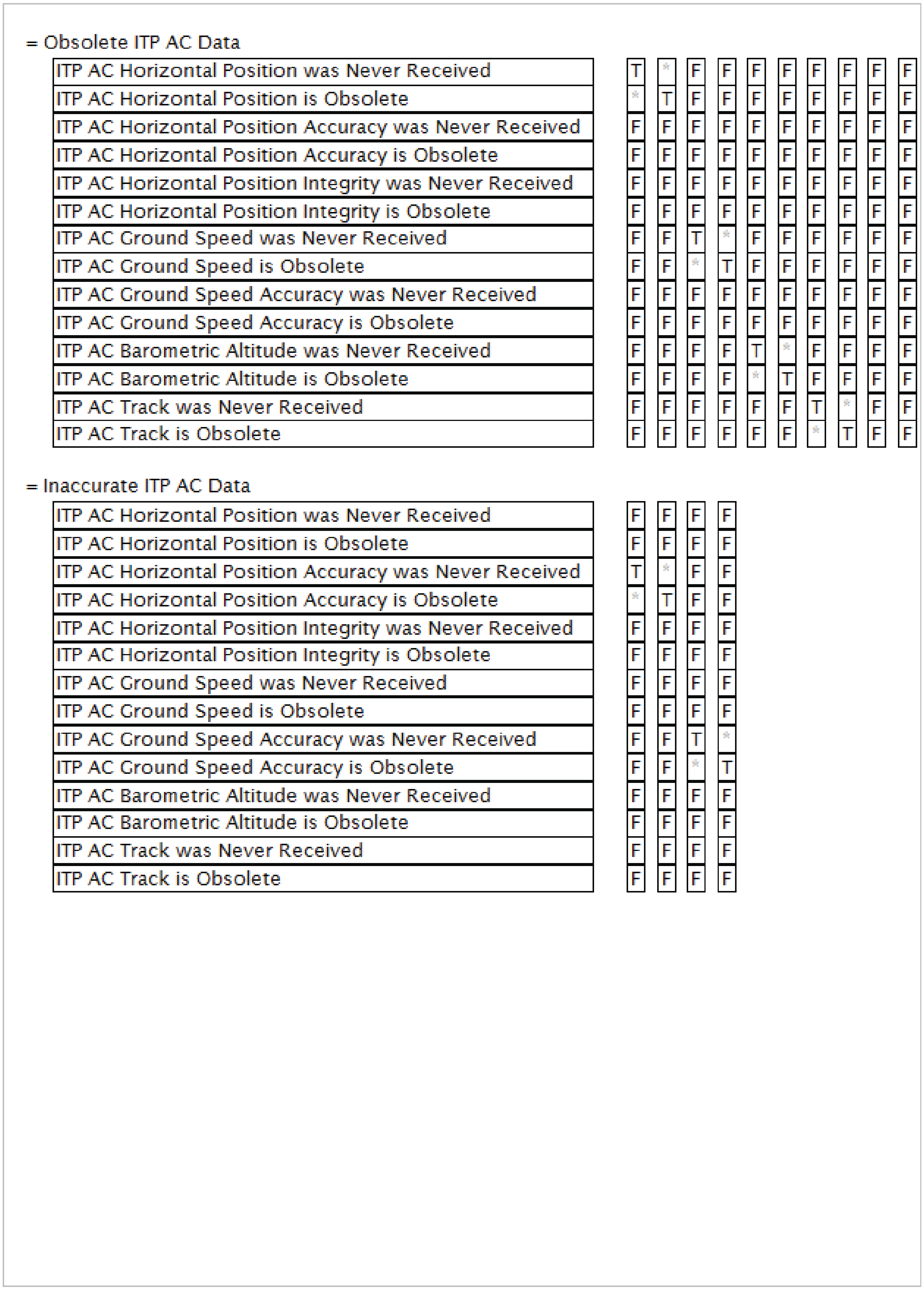
DEFINITION

= Unknown

System Start	T

= Correct ITP AC Data

ITP AC Horizontal Position was Never Received	F
ITP AC Horizontal Position is Obsolete	F
ITP AC Horizontal Position Accuracy was Never Received	F
ITP AC Horizontal Position Accuracy is Obsolete	F
ITP AC Horizontal Position Integrity was Never Received	F
ITP AC Horizontal Position Integrity is Obsolete	F
ITP AC Ground Speed was Never Received	F
ITP AC Ground Speed is Obsolete	F
ITP AC Ground Speed Accuracy was Never Received	F
ITP AC Ground Speed Accuracy is Obsolete	F
ITP AC Barometric Altitude was Never Received	F
ITP AC Barometric Altitude is Obsolete	F
ITP AC Track was Never Received	F
ITP AC Track is Obsolete	F

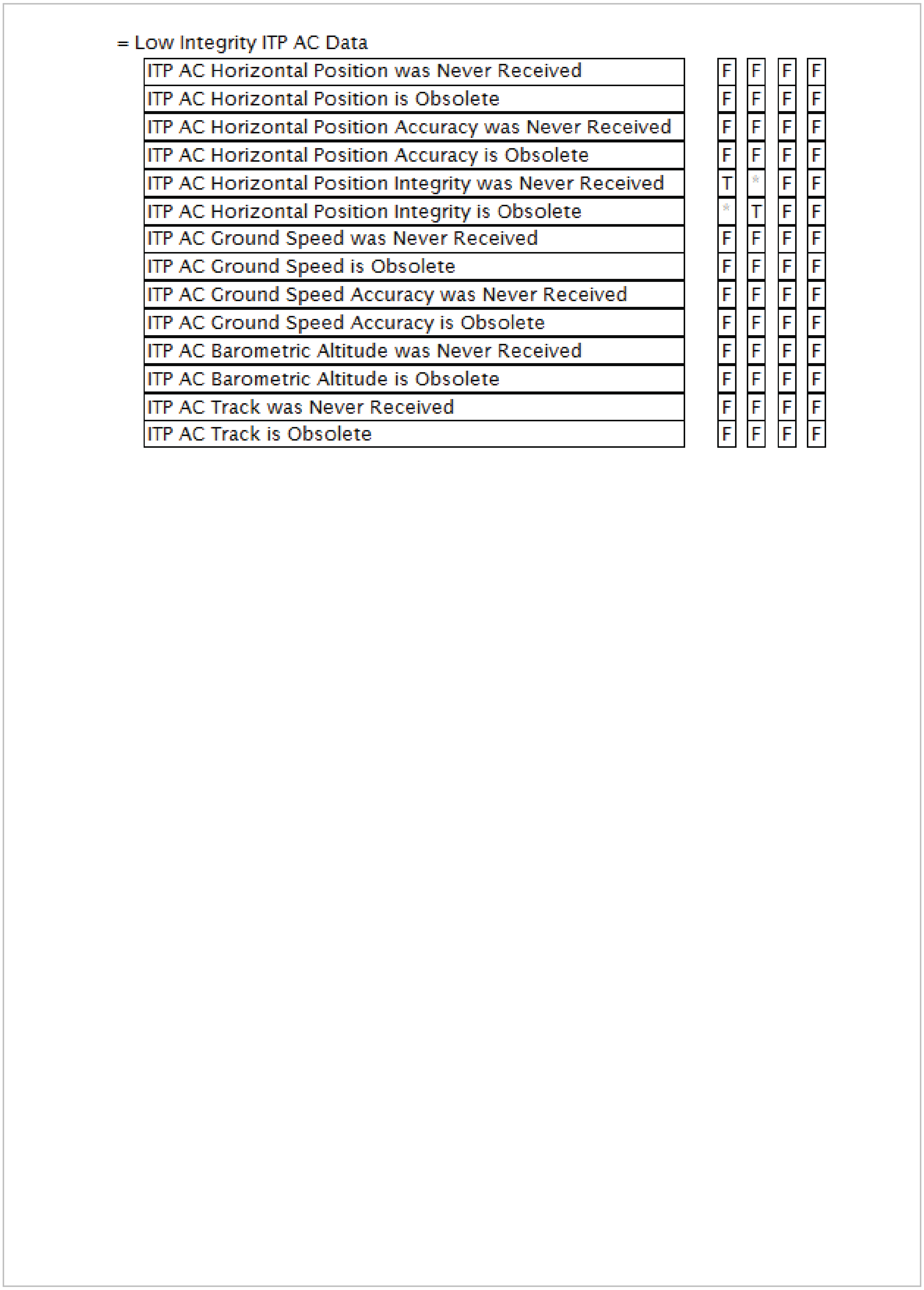


= Obsolete ITP AC Data

ITP AC Horizontal Position was Never Received	T	*	F	F	F	F	F	F	F	F
ITP AC Horizontal Position is Obsolete	*	T	F	F	F	F	F	F	F	F
ITP AC Horizontal Position Accuracy was Never Received	F	F	F	F	F	F	F	F	F	F
ITP AC Horizontal Position Accuracy is Obsolete	F	F	F	F	F	F	F	F	F	F
ITP AC Horizontal Position Integrity was Never Received	F	F	F	F	F	F	F	F	F	F
ITP AC Horizontal Position Integrity is Obsolete	F	F	F	F	F	F	F	F	F	F
ITP AC Ground Speed was Never Received	F	F	T	*	F	F	F	F	F	F
ITP AC Ground Speed is Obsolete	F	F	*	T	F	F	F	F	F	F
ITP AC Ground Speed Accuracy was Never Received	F	F	F	F	F	F	F	F	F	F
ITP AC Ground Speed Accuracy is Obsolete	F	F	F	F	F	F	F	F	F	F
ITP AC Barometric Altitude was Never Received	F	F	F	F	T	*	F	F	F	F
ITP AC Barometric Altitude is Obsolete	F	F	F	F	*	T	F	F	F	F
ITP AC Track was Never Received	F	F	F	F	F	F	T	*	F	F
ITP AC Track is Obsolete	F	F	F	F	F	F	*	T	F	F

= Inaccurate ITP AC Data

ITP AC Horizontal Position was Never Received	F	F	F	F
ITP AC Horizontal Position is Obsolete	F	F	F	F
ITP AC Horizontal Position Accuracy was Never Received	T	*	F	F
ITP AC Horizontal Position Accuracy is Obsolete	*	T	F	F
ITP AC Horizontal Position Integrity was Never Received	F	F	F	F
ITP AC Horizontal Position Integrity is Obsolete	F	F	F	F
ITP AC Ground Speed was Never Received	F	F	F	F
ITP AC Ground Speed is Obsolete	F	F	F	F
ITP AC Ground Speed Accuracy was Never Received	F	F	T	*
ITP AC Ground Speed Accuracy is Obsolete	F	F	*	T
ITP AC Barometric Altitude was Never Received	F	F	F	F
ITP AC Barometric Altitude is Obsolete	F	F	F	F
ITP AC Track was Never Received	F	F	F	F
ITP AC Track is Obsolete	F	F	F	F



= Low Integrity ITP AC Data

ITP AC Horizontal Position was Never Received	F	F	F	F
ITP AC Horizontal Position is Obsolete	F	F	F	F
ITP AC Horizontal Position Accuracy was Never Received	F	F	F	F
ITP AC Horizontal Position Accuracy is Obsolete	F	F	F	F
ITP AC Horizontal Position Integrity was Never Received	T	*	F	F
ITP AC Horizontal Position Integrity is Obsolete	*	T	F	F
ITP AC Ground Speed was Never Received	F	F	F	F
ITP AC Ground Speed is Obsolete	F	F	F	F
ITP AC Ground Speed Accuracy was Never Received	F	F	F	F
ITP AC Ground Speed Accuracy is Obsolete	F	F	F	F
ITP AC Barometric Altitude was Never Received	F	F	F	F
ITP AC Barometric Altitude is Obsolete	F	F	F	F
ITP AC Track was Never Received	F	F	F	F
ITP AC Track is Obsolete	F	F	F	F

State Value

Data Quality State

Obsolescence:

Exception-Handling:

Related Inputs:

Description: Data quality (accuracy, position integrity, and surveillance integrity) must meet certain minimum criteria.

Comments: All positions in NM and speeds in m/s/ per SPR.42 through SPR.44 of DO-312

References: → Reference AC Horizontal Position Accuracy, Reference AC Horizontal Position Integrity, Reference AC Surveillance Integrity Level, Reference AC Ground Speed Accuracy, ITP AC Horizontal Position Accuracy, ITP AC Horizontal Position Integrity, ITP AC Ground Speed Accuracy

Appears In: ← Data Quality Passes Display, Data Quality Fails Display

DEFINITION

= Unknown

System Start	T

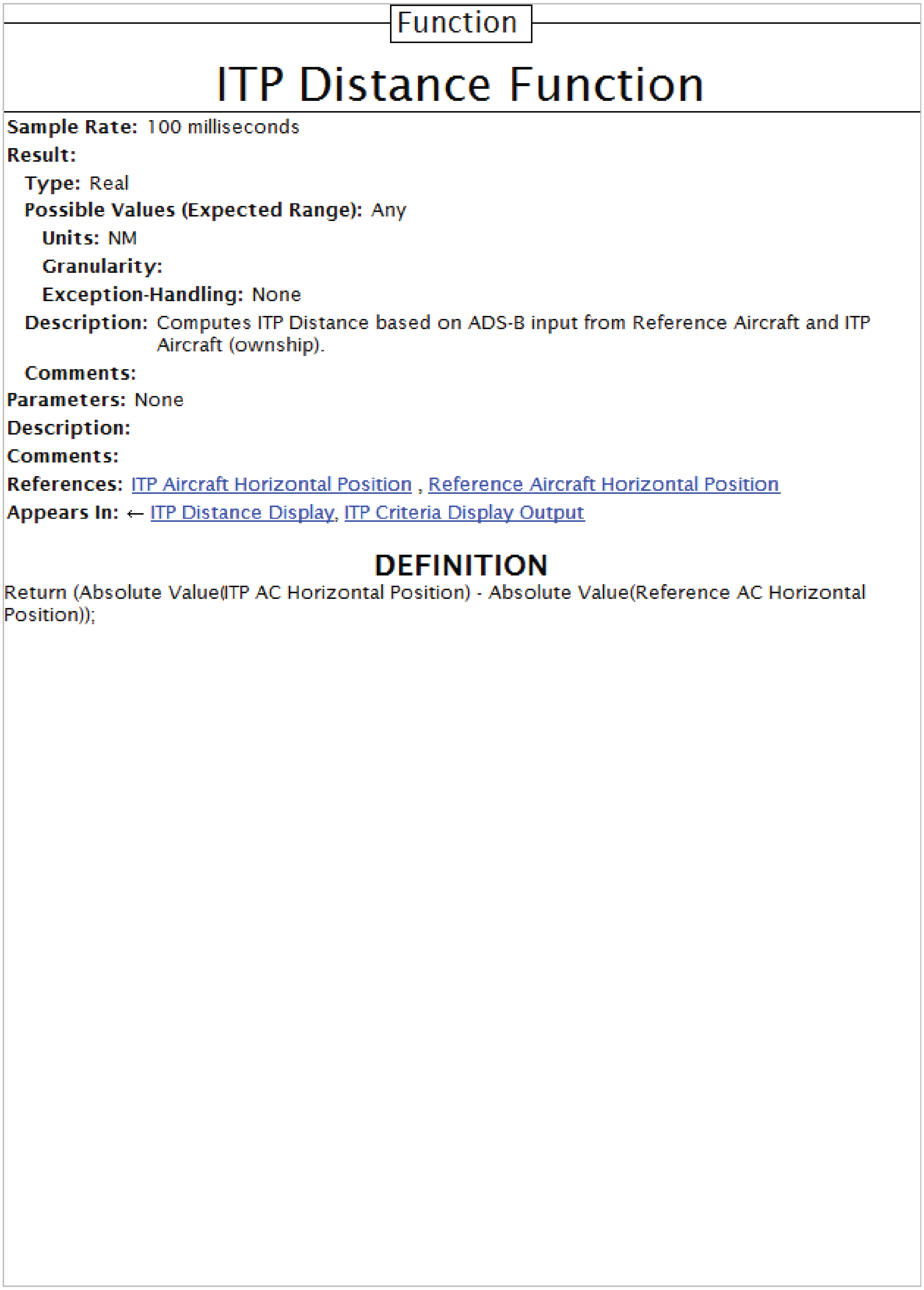
= Data Quality Meets Criteria

System Start	F
Reference AC Horizontal Position Accuracy < 0.5	T
Reference AC Horizontal Position Integrity < 1.0	T
Reference AC Surveillance Integrity Level is Qualified	T
Reference AC Ground Speed Accuracy < 10	T
ITP AC Horizontal Position Accuracy < 0.5	T
ITP AC Horizontal Position Integrity < 1.0	T
ITP AC Ground Speed Accuracy < 10	T

= Data Quality Unqualified

System Start	F	F	F	F	F	F	F
Reference AC Horizontal Position Accuracy >= 0.5	T	*	*	*	*	*	*
Reference AC Horizontal Position Integrity >= 1.0	*	T	*	*	*	*	*
Reference AC Surveillance Integrity Level is Unqualified	*	*	T	*	*	*	*
Reference AC Ground Speed Accuracy >= 10	*	*	*	T	*	*	*
ITP AC Horizontal Position Accuracy >= 0.5	*	*	*	*	T	*	*
ITP AC Horizontal Position Integrity >= 1.0	*	*	*	*	*	T	*
ITP AC Ground Speed Accuracy >= 10	*	*	*	*	*	*	T

FUNCTIONS



Function

ITP Distance Function

Sample Rate: 100 milliseconds

Result:

Type: Real

Possible Values (Expected Range): Any

Units: NM

Granularity:

Exception-Handling: None

Description: Computes ITP Distance based on ADS-B input from Reference Aircraft and ITP Aircraft (ownship).

Comments:

Parameters: None

Description:

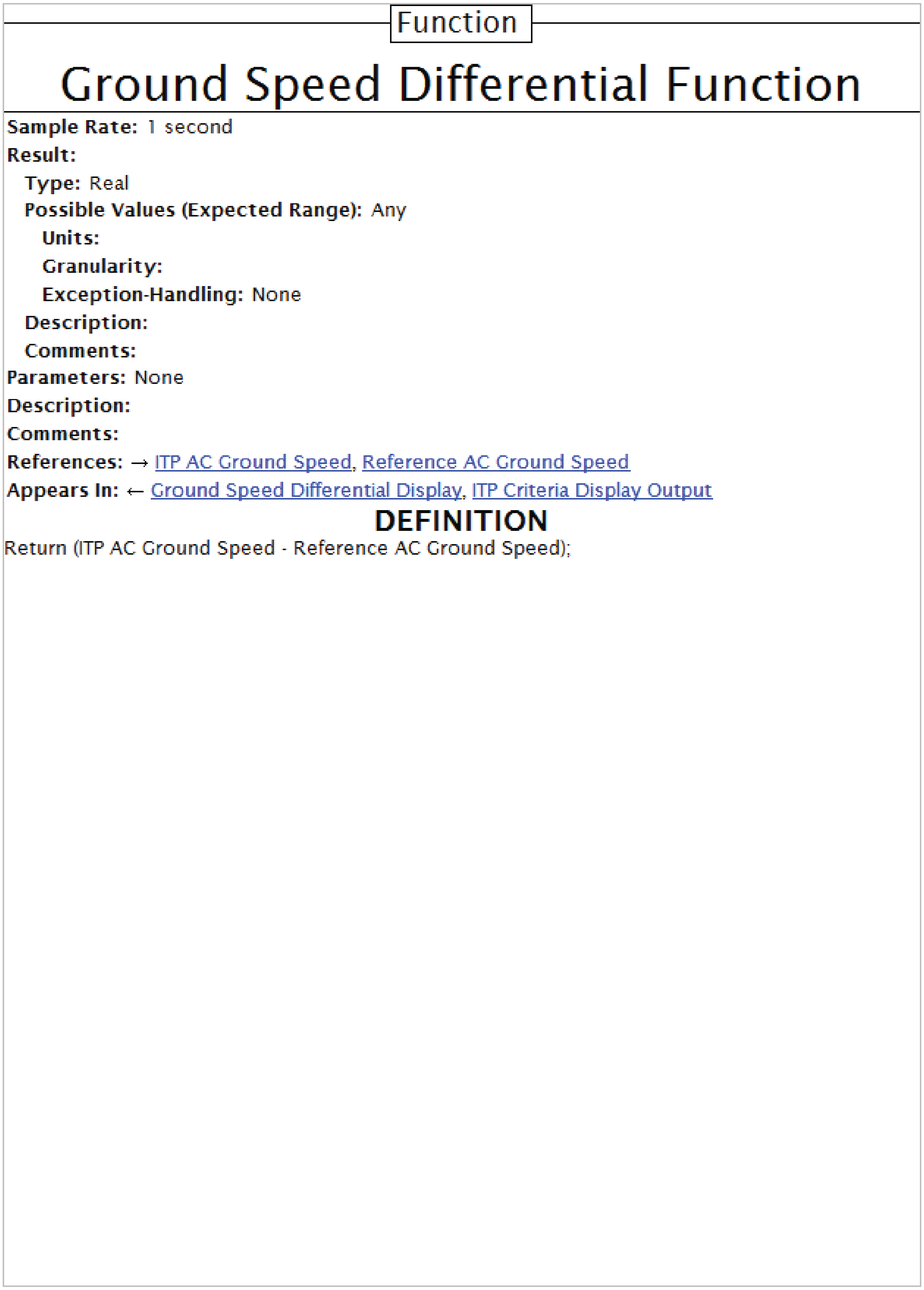
Comments:

References: ITP Aircraft Horizontal Position , Reference Aircraft Horizontal Position

Appears In: ← ITP Distance Display, ITP Criteria Display Output

DEFINITION

Return (Absolute Value(ITP AC Horizontal Position) - Absolute Value(Reference AC Horizontal Position));



Function

Ground Speed Differential Function

Sample Rate: 1 second

Result:

- **Type:** Real
- **Possible Values (Expected Range):** Any
  - **Units:**
  - **Granularity:**
  - **Exception-Handling:** None
- **Description:**
- **Comments:**

Parameters: None

Description:

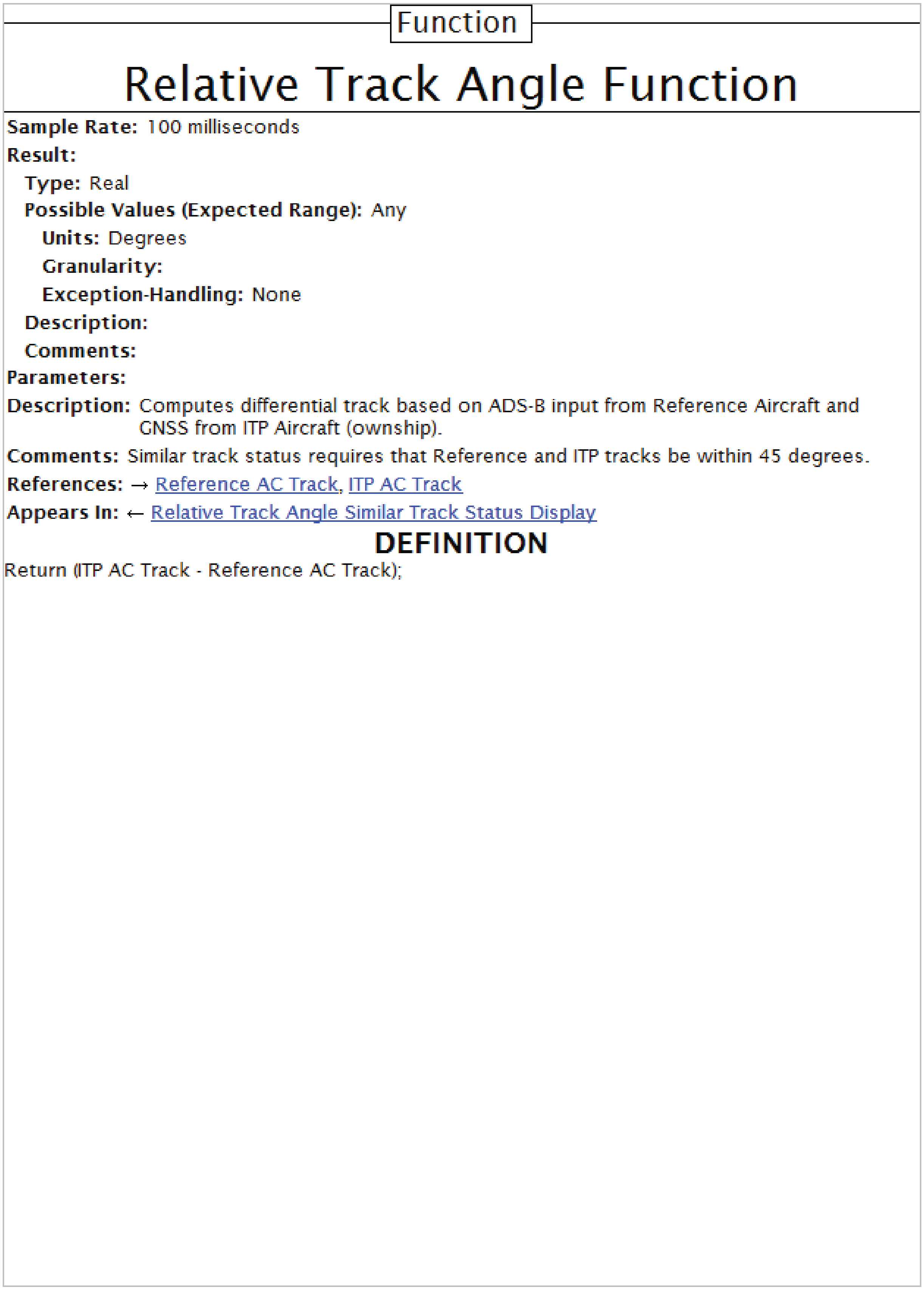
Comments:

References: → ITP AC Ground Speed, Reference AC Ground Speed

Appears In: ← Ground Speed Differential Display, ITP Criteria Display Output

DEFINITION

Return (ITP AC Ground Speed - Reference AC Ground Speed);



Function

Relative Track Angle Function

Sample Rate: 100 milliseconds

Result:

- **Type:** Real
- **Possible Values (Expected Range):** Any
  - **Units:** Degrees
  - **Granularity:**
  - **Exception-Handling:** None
- **Description:**
- **Comments:**

Parameters:

Description: Computes differential track based on ADS-B input from Reference Aircraft and GNSS from ITP Aircraft (ownship).

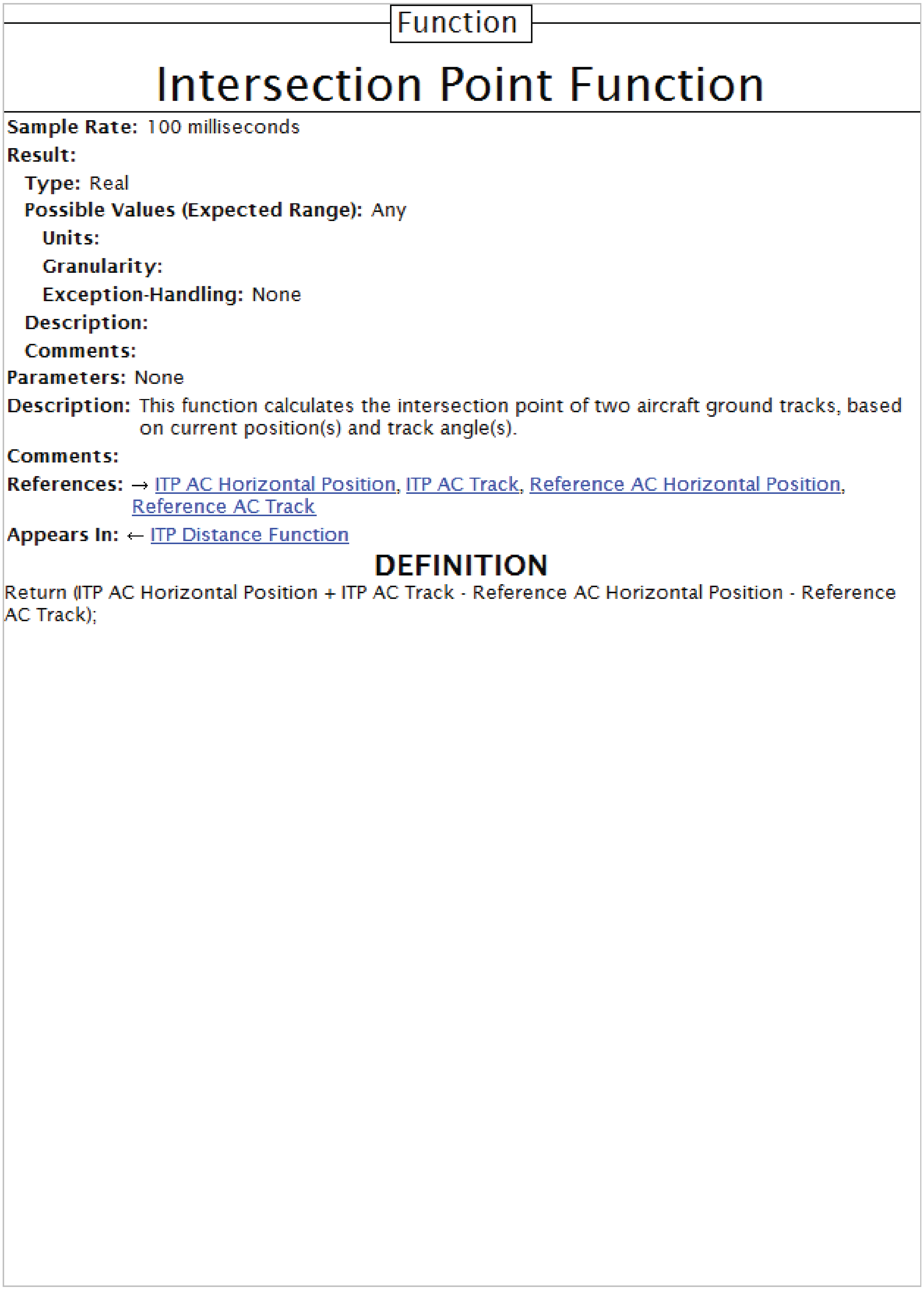
Comments: Similar track status requires that Reference and ITP tracks be within 45 degrees.

References: → Reference AC Track, ITP AC Track

Appears In: ← Relative Track Angle Similar Track Status Display

DEFINITION

```
Return (ITP AC Track - Reference AC Track);
```



Function

Intersection Point Function

Sample Rate: 100 milliseconds

Result:

- **Type:** Real
- **Possible Values (Expected Range):** Any
  - **Units:**
  - **Granularity:**
  - **Exception-Handling:** None
- **Description:**
- **Comments:**

Parameters: None

Description: This function calculates the intersection point of two aircraft ground tracks, based on current position(s) and track angle(s).

Comments:

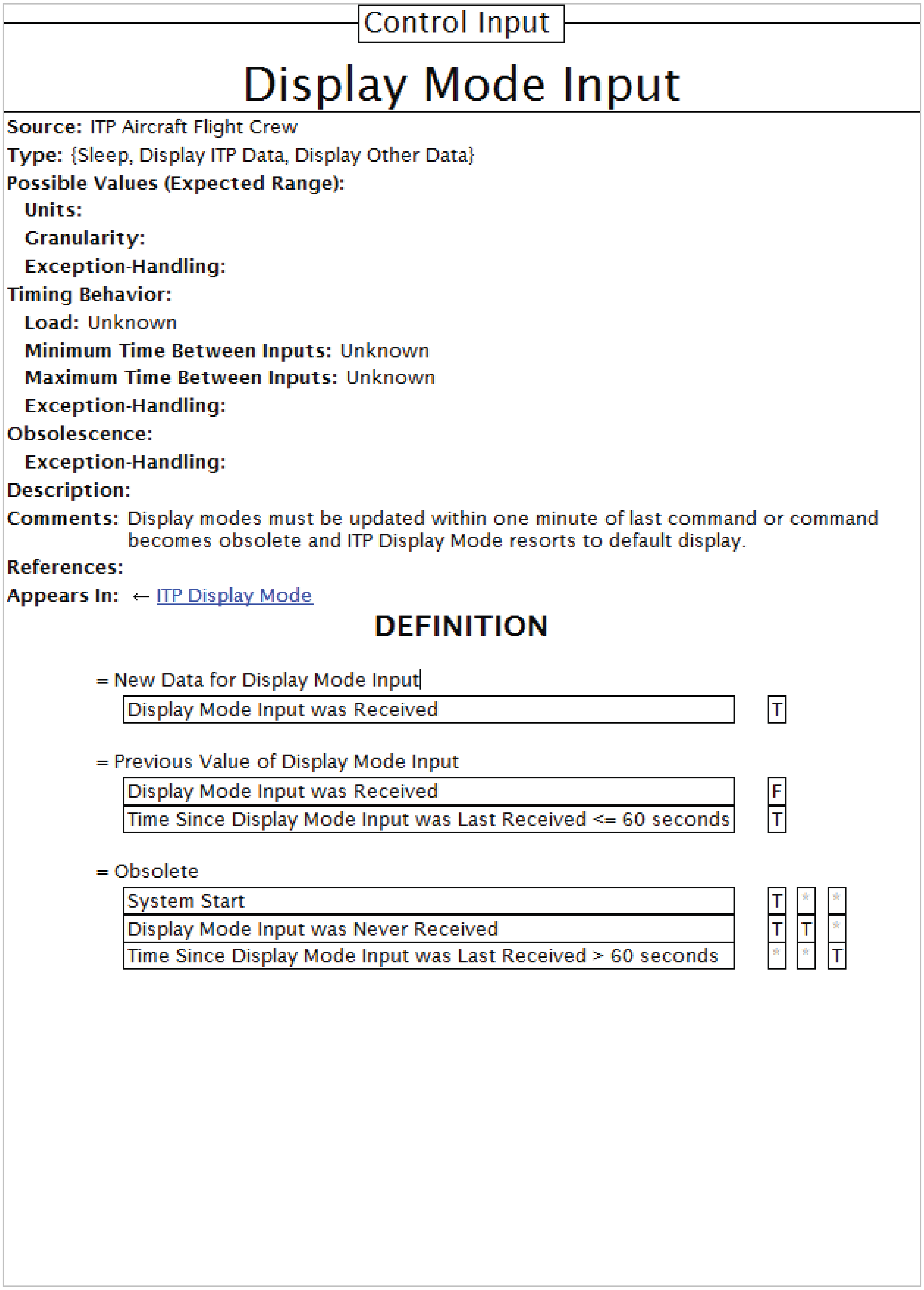
References: → ITP AC Horizontal Position, ITP AC Track, Reference AC Horizontal Position, Reference AC Track

Appears In: ← ITP Distance Function

DEFINITION

Return (ITP AC Horizontal Position + ITP AC Track - Reference AC Horizontal Position - Reference AC Track);

INPUTS



Control Input

Display Mode Input

Source: ITP Aircraft Flight Crew

Type: {Sleep, Display ITP Data, Display Other Data}

Possible Values (Expected Range):

Units:

Granularity:

Exception-Handling:

Timing Behavior:

Load: Unknown

Minimum Time Between Inputs: Unknown

Maximum Time Between Inputs: Unknown

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments: Display modes must be updated within one minute of last command or command becomes obsolete and ITP Display Mode resorts to default display.

References:

Appears In: ← ITP Display Mode

DEFINITION

= New Data for Display Mode Input

Display Mode Input was Received	T

= Previous Value of Display Mode Input

Display Mode Input was Received	F
Time Since Display Mode Input was Last Received <= 60 seconds	T

= Obsolete

System Start	T	*	*
Display Mode Input was Never Received	T	T	*
Time Since Display Mode Input was Last Received > 60 seconds	*	*	T

Input Value

Reference AC Horizontal Position

Source: Reference Aircraft ADS-B Out

Type: Real

Possible Values (Expected Range): Any

Units: NM

Granularity: Unknown

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments:

References:

Appears In: ← Reference AC Data State, ITP Distance Function

DEFINITION

= New Data for Reference AC Horizontal Position

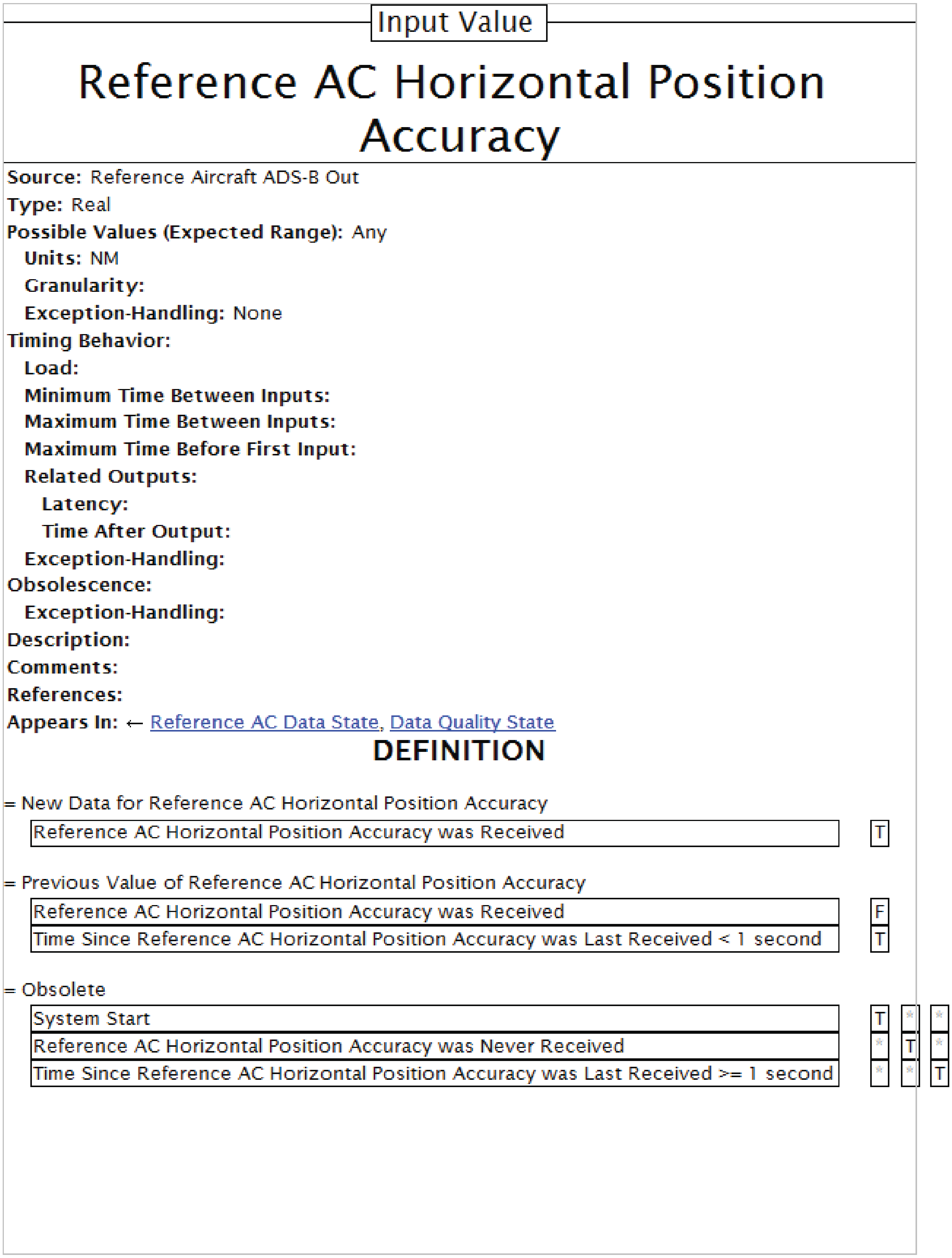
Reference AC Horizontal Position was Received	T

= Previous Value of Reference AC Horizontal Position

Reference AC Horizontal Position was Received	F
Time Since Reference AC Horizontal Position was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
Reference AC Horizontal Position was Never Received	*	T	*
Time Since Reference AC Horizontal Position was Last Received >= 1 second	*	*	T



Input Value

Reference AC Horizontal Position Accuracy

Source: Reference Aircraft ADS-B Out

Type: Real

Possible Values (Expected Range): Any

Units: NM

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments:

References:

Appears In: ← Reference AC Data State, Data Quality State

DEFINITION

= New Data for Reference AC Horizontal Position Accuracy

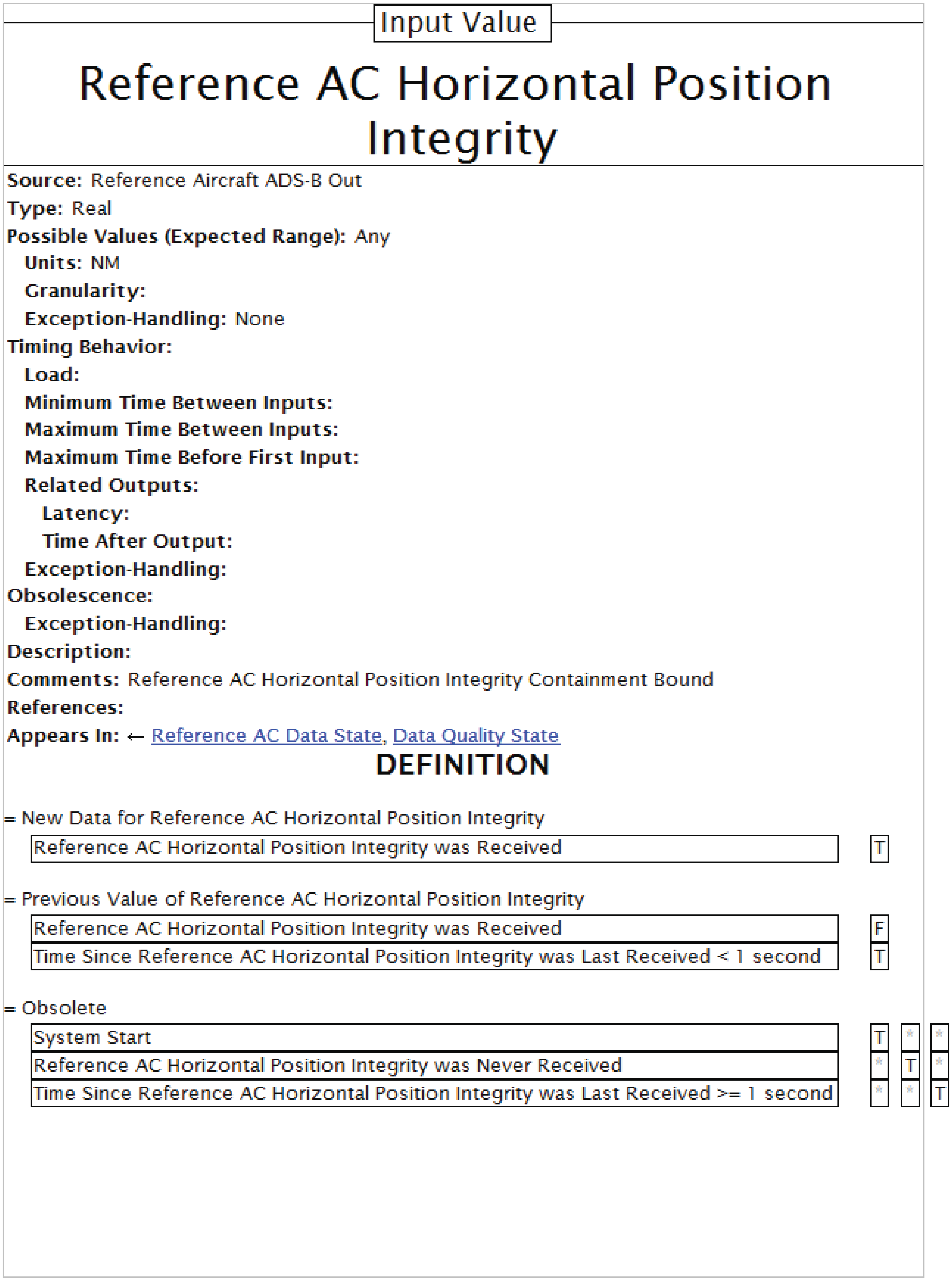
Reference AC Horizontal Position Accuracy was Received	T

= Previous Value of Reference AC Horizontal Position Accuracy

Reference AC Horizontal Position Accuracy was Received	F
Time Since Reference AC Horizontal Position Accuracy was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
Reference AC Horizontal Position Accuracy was Never Received	*	T	*
Time Since Reference AC Horizontal Position Accuracy was Last Received >= 1 second	*	*	T



Input Value

Reference AC Horizontal Position Integrity

Source: Reference Aircraft ADS-B Out

Type: Real

Possible Values (Expected Range): Any

Units: NM

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments: Reference AC Horizontal Position Integrity Containment Bound

References:

Appears In: ← Reference AC Data State, Data Quality State

DEFINITION

= New Data for Reference AC Horizontal Position Integrity

Reference AC Horizontal Position Integrity was Received	T

= Previous Value of Reference AC Horizontal Position Integrity

Reference AC Horizontal Position Integrity was Received	F
Time Since Reference AC Horizontal Position Integrity was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
Reference AC Horizontal Position Integrity was Never Received	*	T	*
Time Since Reference AC Horizontal Position Integrity was Last Received >= 1 second	*	*	T

Input Value

Reference AC Surveillance Integrity Level

Source: Reference Aircraft ADS-B Out
Type: {Qualified, Unqualified}
Possible Values (Expected Range): Any
Units:
Granularity:
Exception-Handling: None
Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence: 1 second
Exception-Handling:
Description:
Comments:
References:
Appears In: ← Reference AC Data State, Data Quality State

DEFINITION

= New Data for Reference AC Surveillance Integrity Level

Reference AC Surveillance Integrity Level was Received	T

= Previous Value of Reference AC Surveillance Integrity Level

Reference AC Surveillance Integrity Level was Received	F
Time Since Reference AC Surveillance Integrity Level was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
Reference AC Surveillance Integrity Level was Never Received	*	T	*
Time Since Reference AC Surveillance Integrity Level was Last Received >= 1 second	*	*	T

Input Value

Reference AC Ground Speed

Source: Reference Aircraft ADS-B Out
Type: Real
Possible Values (Expected Range): Any
Units: m/s
Granularity:
Exception-Handling: None
Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence:
Exception-Handling: None
Description:
Comments:
References:
Appears In: ← Reference AC Data State, Ground Speed Differential Function

DEFINITION

= New Data for Reference AC Ground Speed

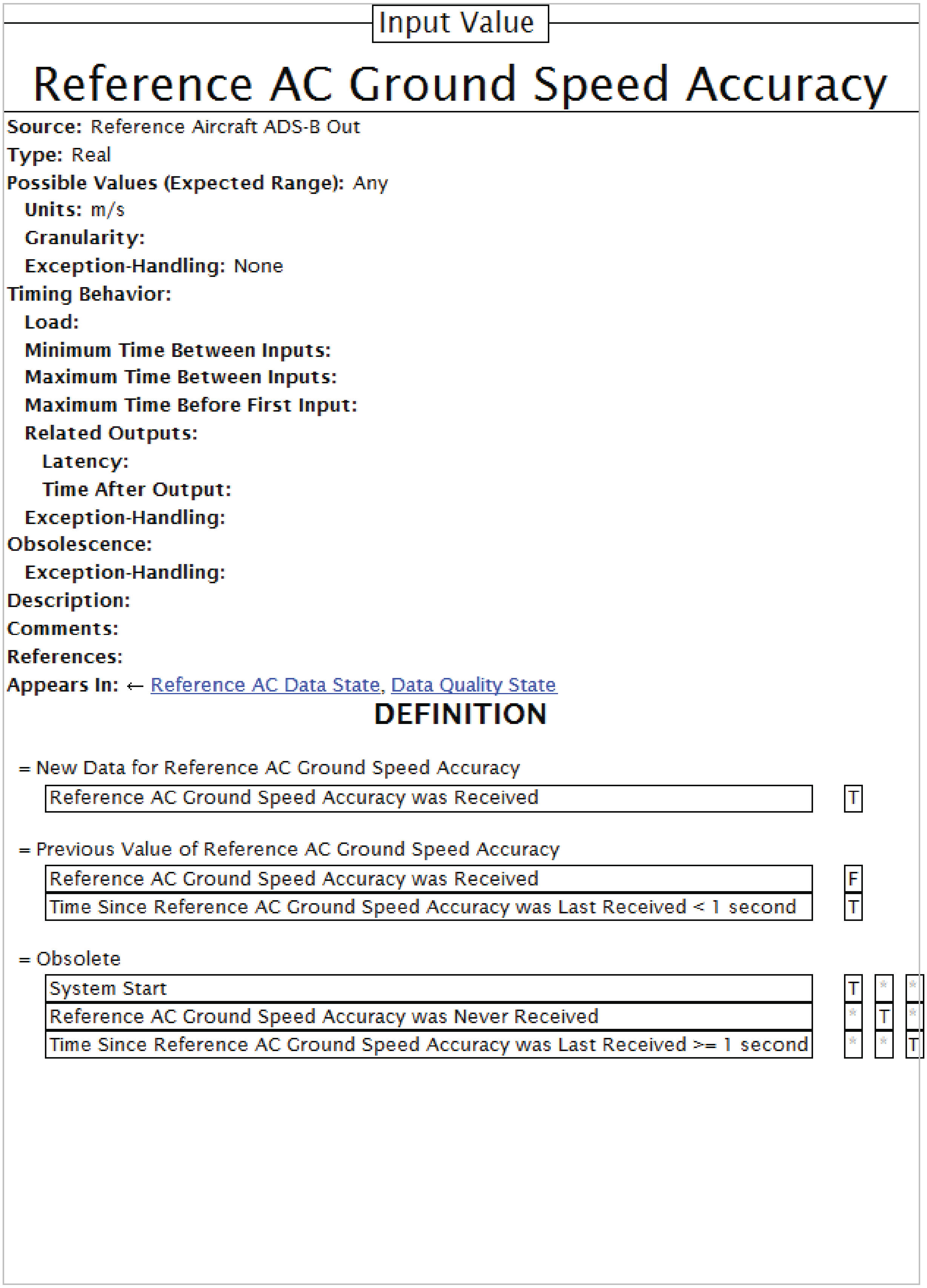
Reference AC Ground Speed was Received	T

= Previous Value of Reference AC Ground Speed

Reference AC Ground Speed was Received	F
Time Since Reference AC Ground Speed was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
Reference AC Ground Speed was Never Received	*	T	*
Time Since Reference AC Ground Speed was Last Received >= 1 second	*	*	T



Input Value

Reference AC Ground Speed Accuracy

Source: Reference Aircraft ADS-B Out

Type: Real

Possible Values (Expected Range): Any

Units: m/s

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments:

References:

Appears In: ← Reference AC Data State, Data Quality State

DEFINITION

= New Data for Reference AC Ground Speed Accuracy

Reference AC Ground Speed Accuracy was Received	T

= Previous Value of Reference AC Ground Speed Accuracy

Reference AC Ground Speed Accuracy was Received	F
Time Since Reference AC Ground Speed Accuracy was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
Reference AC Ground Speed Accuracy was Never Received	*	T	*
Time Since Reference AC Ground Speed Accuracy was Last Received >= 1 second	*	*	T

Input Value

Reference AC Barometric Altitude

Source: Reference Aircraft Barometric Instrumentation

Type: Real

Possible Values (Expected Range): Any

Units:

Granularity: Unknown

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence: 1 second

Exception-Handling:

Description:

Comments:

References:

Appears In:

DEFINITION

= New Data for Reference AC Barometric Altitude

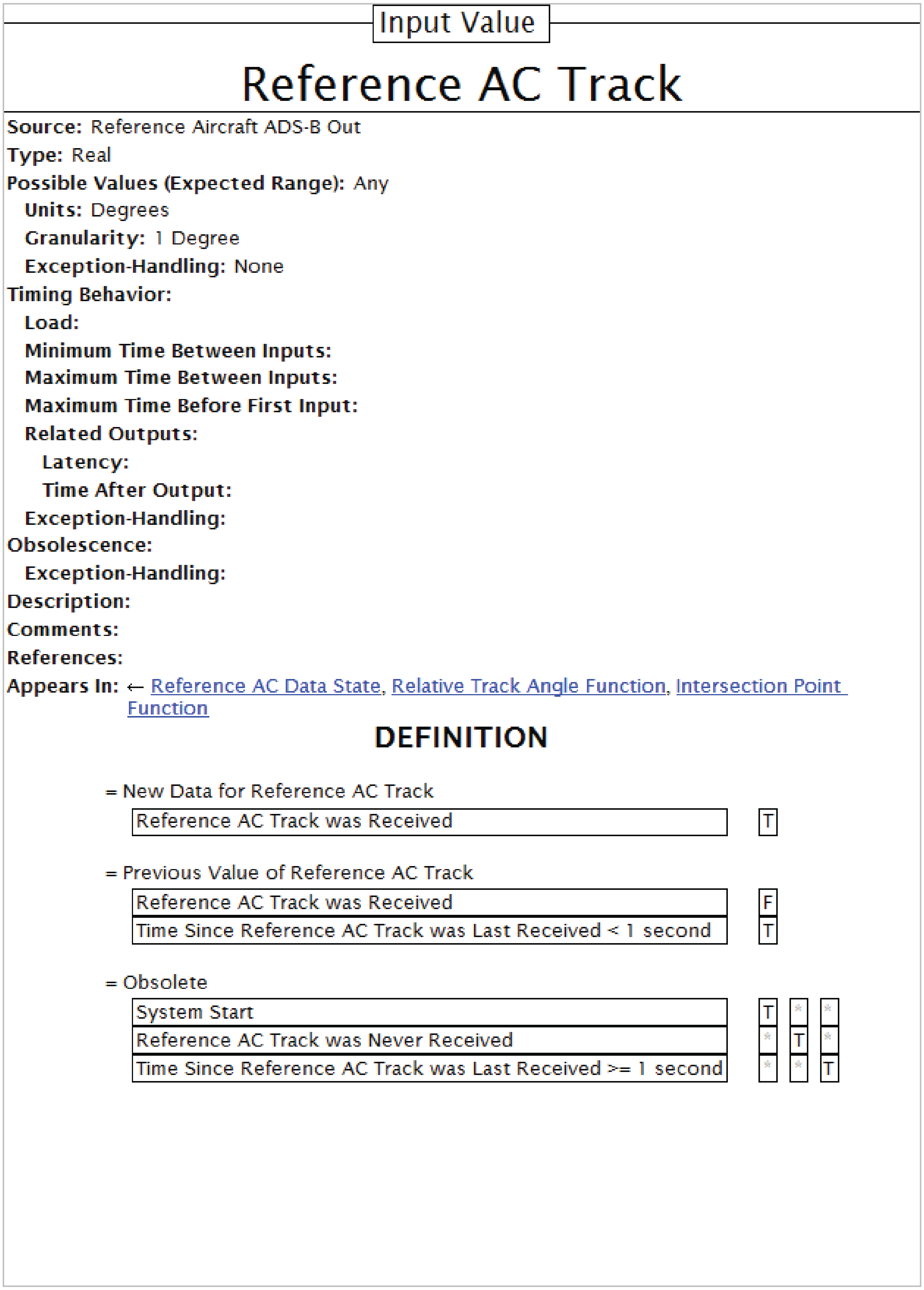
Reference AC Barometric Altitude was Received	T

= Previous Value of Reference AC Barometric Altitude

Reference AC Barometric Altitude was Received	F
Time Since Reference AC Barometric Altitude was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
Reference AC Barometric Altitude was Never Received	*	T	*
Time Since Reference AC Barometric Altitude was Last Received >= 1 second	*	*	T



Input Value

Reference AC Track

Source: Reference Aircraft ADS-B Out

Type: Real

Possible Values (Expected Range): Any

Units: Degrees

Granularity: 1 Degree

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments:

References:

Appears In: ← Reference AC Data State, Relative Track Angle Function, Intersection Point Function

DEFINITION

= New Data for Reference AC Track

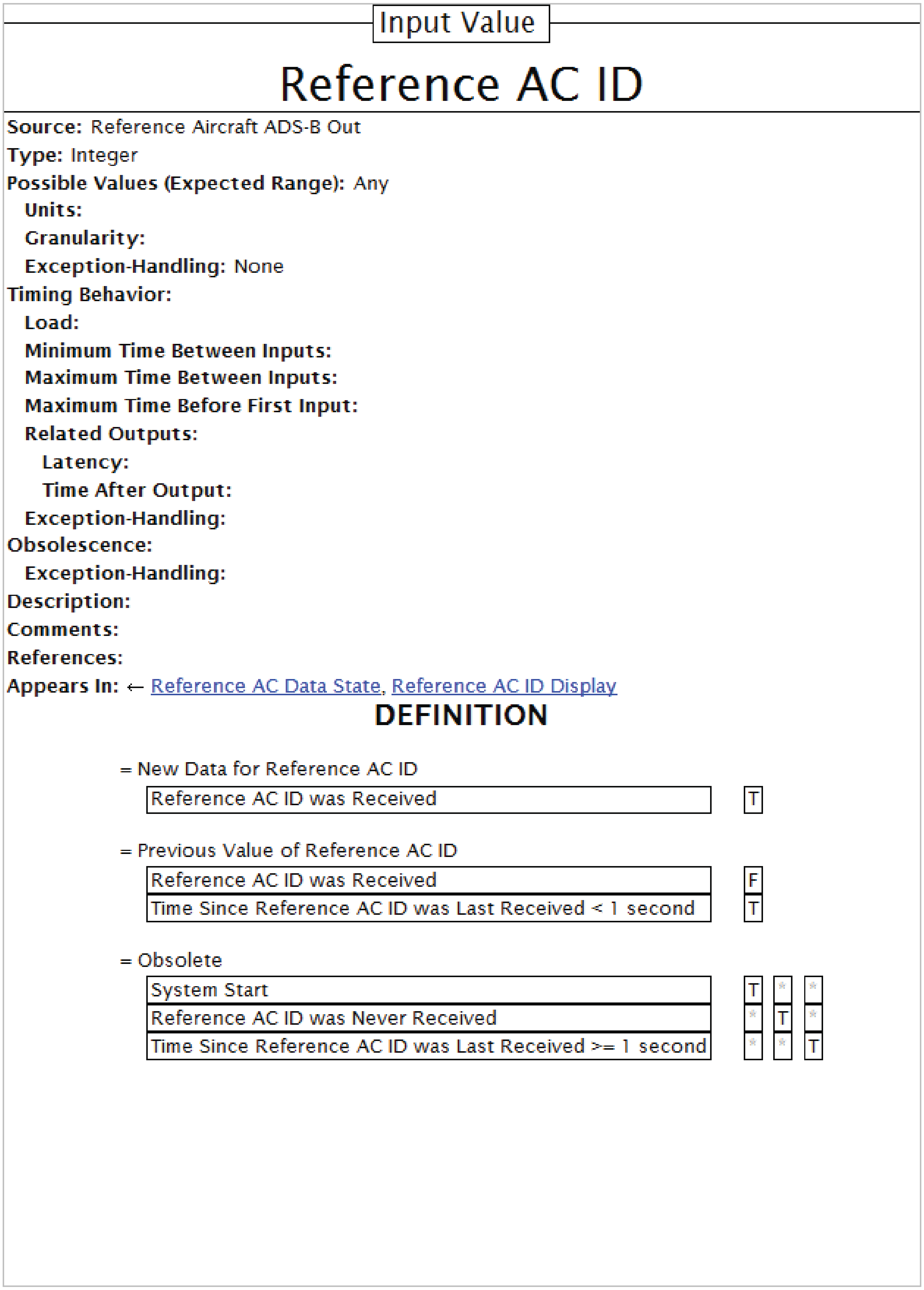
Reference AC Track was Received	T

= Previous Value of Reference AC Track

Reference AC Track was Received	F
Time Since Reference AC Track was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
Reference AC Track was Never Received	*	T	*
Time Since Reference AC Track was Last Received >= 1 second	*	*	T



Input Value

Reference AC ID

Source: Reference Aircraft ADS-B Out

Type: Integer

Possible Values (Expected Range): Any

Units:

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments:

References:

Appears In: ← Reference AC Data State, Reference AC ID Display

DEFINITION

= New Data for Reference AC ID

Reference AC ID was Received	T

= Previous Value of Reference AC ID

Reference AC ID was Received	F
Time Since Reference AC ID was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
Reference AC ID was Never Received	*	T	*
Time Since Reference AC ID was Last Received >= 1 second	*	*	T

Input Value

ITP AC Horizontal Position

Source: Ownship GNSS
Type: Real
Possible Values (Expected Range): Any
  Units: NM
  Granularity:
  Exception-Handling: None
Timing Behavior:
  Load:
  Minimum Time Between Inputs:
  Maximum Time Between Inputs:
  Maximum Time Before First Input:
  Related Outputs:
    Latency:
    Time After Output:
  Exception-Handling:
Obsolescence:
  Exception-Handling:
Description:
Comments:
References:
Appears In: ← ITP AC Data State, ITP Distance Function

DEFINITION

= New Data for ITP AC Horizontal Position

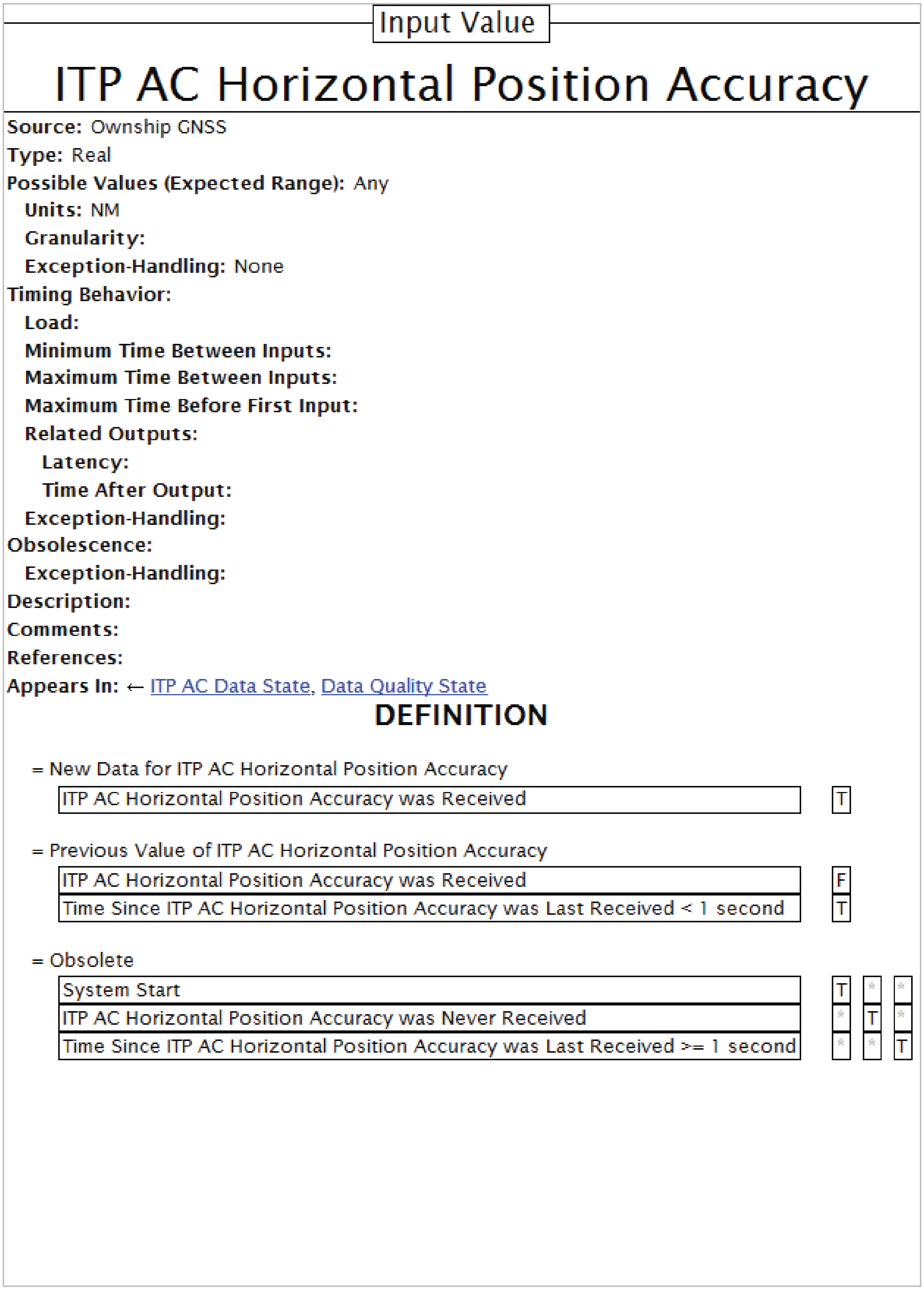
ITP AC Horizontal Position was Received	T

= Previous Value of ITP AC Horizontal Position

ITP AC Horizontal Position was Received	F
Time Since ITP AC Horizontal Position was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
ITP AC Horizontal Position was Never Received	*	T	*
Time Since ITP AC Horizontal Position was Last Received >= 1 second	*	*	T



Input Value

ITP AC Horizontal Position Accuracy

Source: Ownship GNSS

Type: Real

Possible Values (Expected Range): Any

Units: NM

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments:

References:

Appears In: ← ITP AC Data State, Data Quality State

DEFINITION

= New Data for ITP AC Horizontal Position Accuracy

ITP AC Horizontal Position Accuracy was Received	T

= Previous Value of ITP AC Horizontal Position Accuracy

ITP AC Horizontal Position Accuracy was Received	F
Time Since ITP AC Horizontal Position Accuracy was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
ITP AC Horizontal Position Accuracy was Never Received	*	T	*
Time Since ITP AC Horizontal Position Accuracy was Last Received >= 1 second	*	*	T

Input Value

ITP AC Horizontal Position Integrity

Source: Ownship GNSS

Type: Real

Possible Values (Expected Range): Any

Units: NM

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments:

References:

Appears In: ← ITP AC Data State, Data Quality State

DEFINITION

= New Data for ITP AC Horizontal Position Integrity

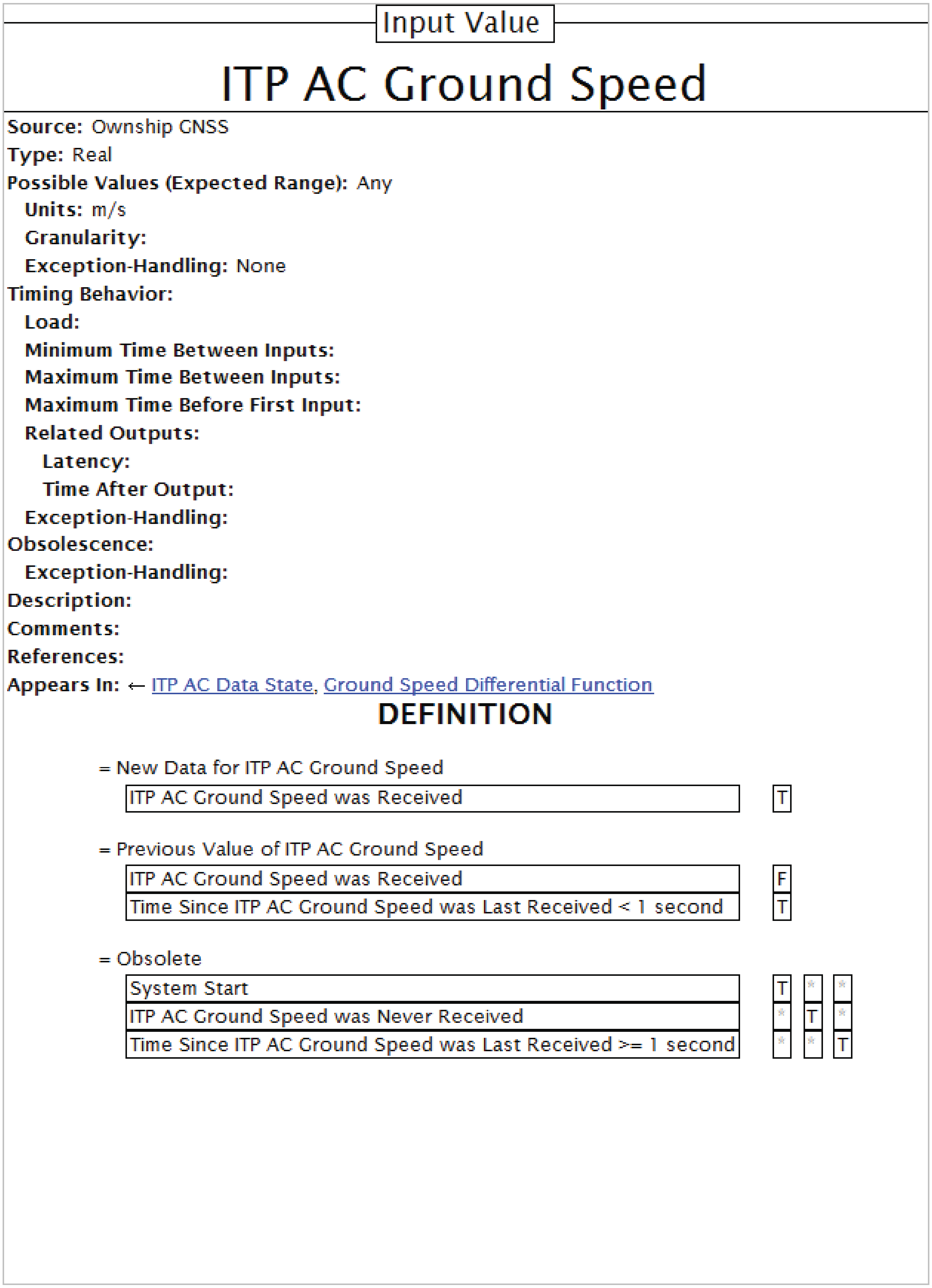
ITP AC Horizontal Position Integrity was Received	T

= Previous Value of ITP AC Horizontal Position Integrity

ITP AC Horizontal Position Integrity was Received	F
Time Since ITP AC Horizontal Position Integrity was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
ITP AC Horizontal Position Integrity was Never Received	*	T	*
Time Since ITP AC Horizontal Position Integrity was Last Received >= 1 second	*	*	T



Input Value

ITP AC Ground Speed

Source: Ownship GNSS

Type: Real

Possible Values (Expected Range): Any

Units: m/s

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments:

References:

Appears In: ← ITP AC Data State, Ground Speed Differential Function

DEFINITION

= New Data for ITP AC Ground Speed

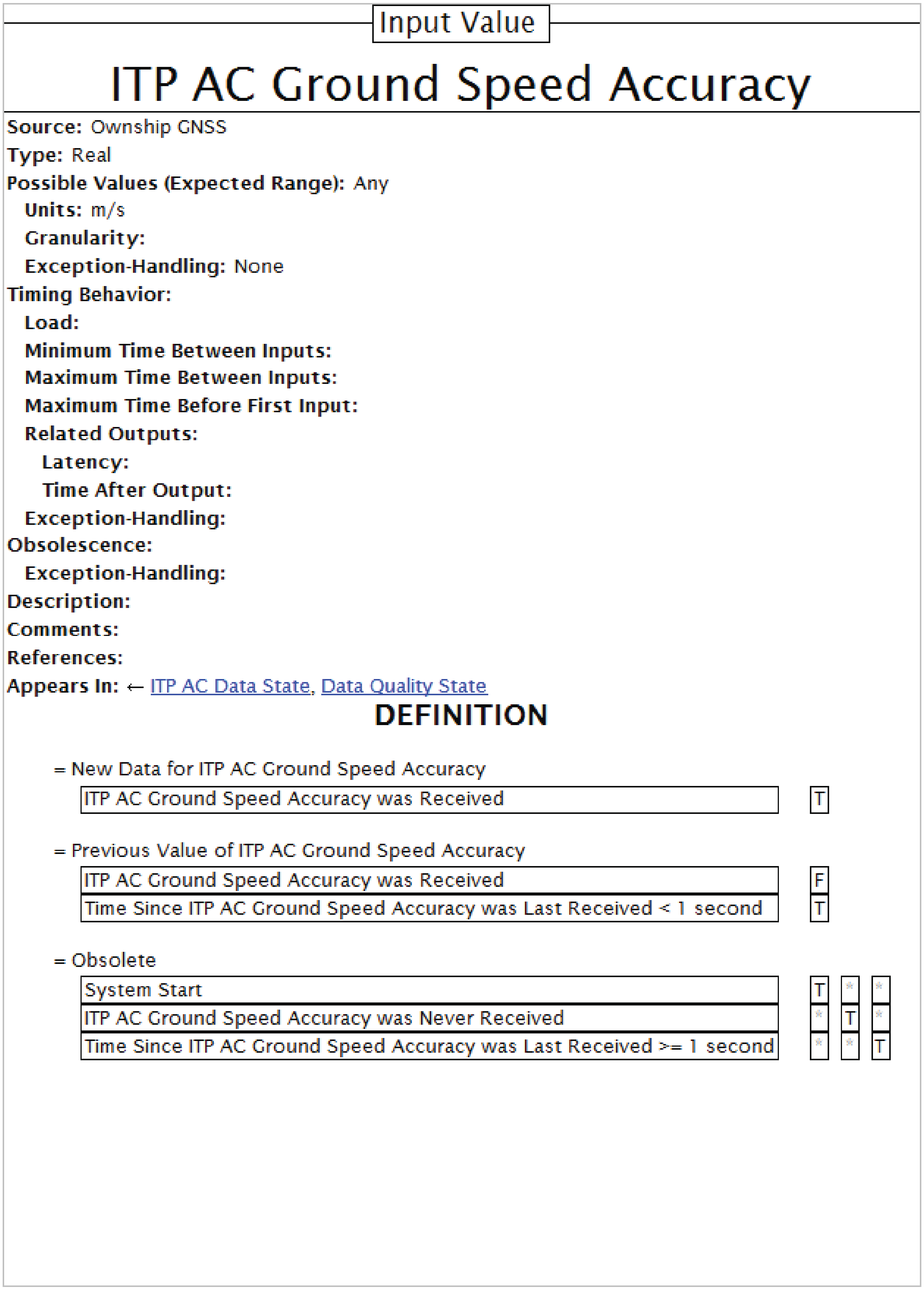
ITP AC Ground Speed was Received	T

= Previous Value of ITP AC Ground Speed

ITP AC Ground Speed was Received	F
Time Since ITP AC Ground Speed was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
ITP AC Ground Speed was Never Received	*	T	*
Time Since ITP AC Ground Speed was Last Received >= 1 second	*	*	T



Input Value

ITP AC Ground Speed Accuracy

Source: Ownship GNSS

Type: Real

Possible Values (Expected Range): Any

Units: m/s

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments:

References:

Appears In: ← ITP AC Data State, Data Quality State

DEFINITION

= New Data for ITP AC Ground Speed Accuracy

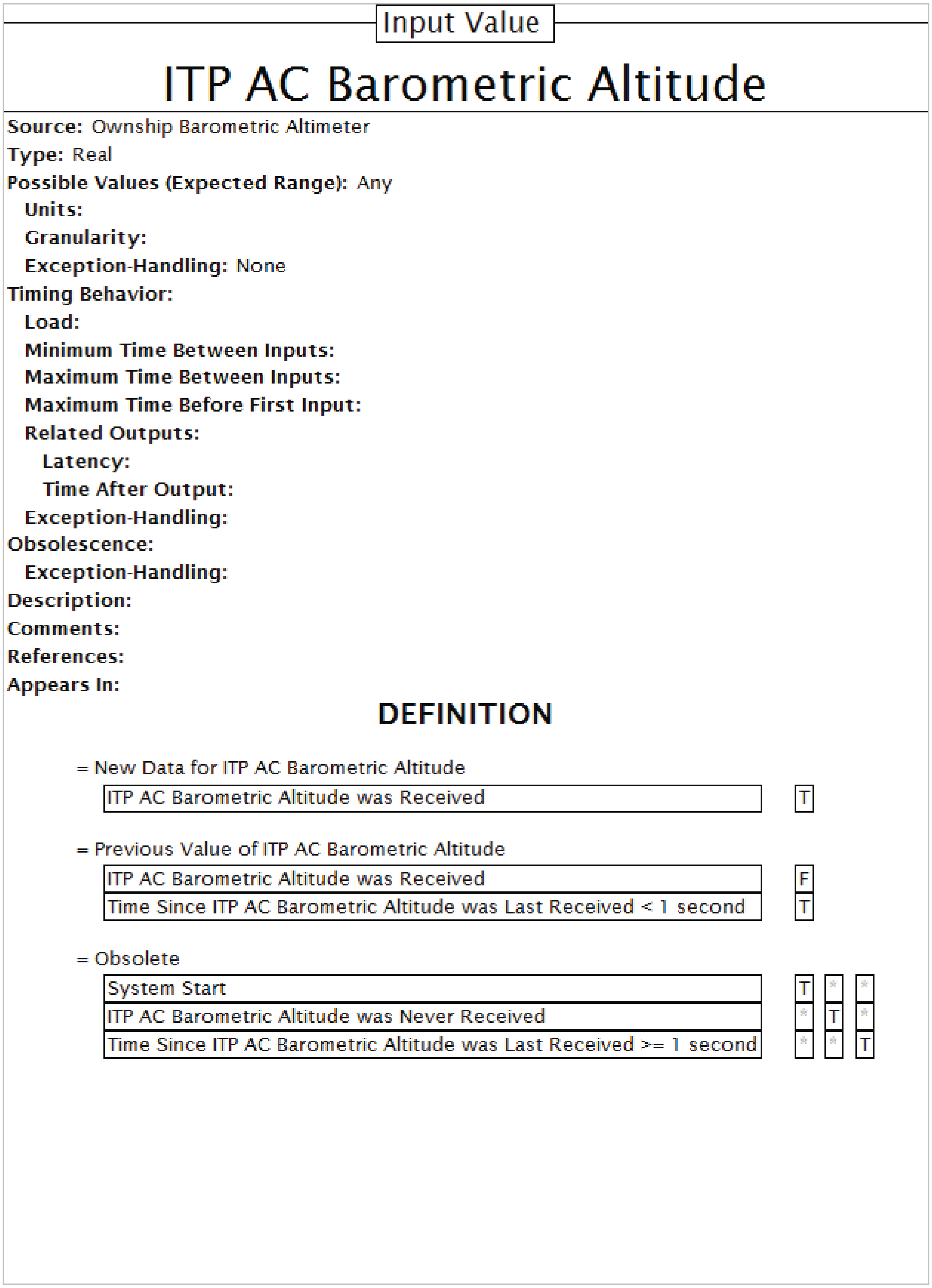
ITP AC Ground Speed Accuracy was Received	T

= Previous Value of ITP AC Ground Speed Accuracy

ITP AC Ground Speed Accuracy was Received	F
Time Since ITP AC Ground Speed Accuracy was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
ITP AC Ground Speed Accuracy was Never Received	*	T	*
Time Since ITP AC Ground Speed Accuracy was Last Received >= 1 second	*	*	T



Input Value

ITP AC Barometric Altitude

Source: Ownship Barometric Altimeter

Type: Real

Possible Values (Expected Range): Any

Units:

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description:

Comments:

References:

Appears In:

DEFINITION

= New Data for ITP AC Barometric Altitude

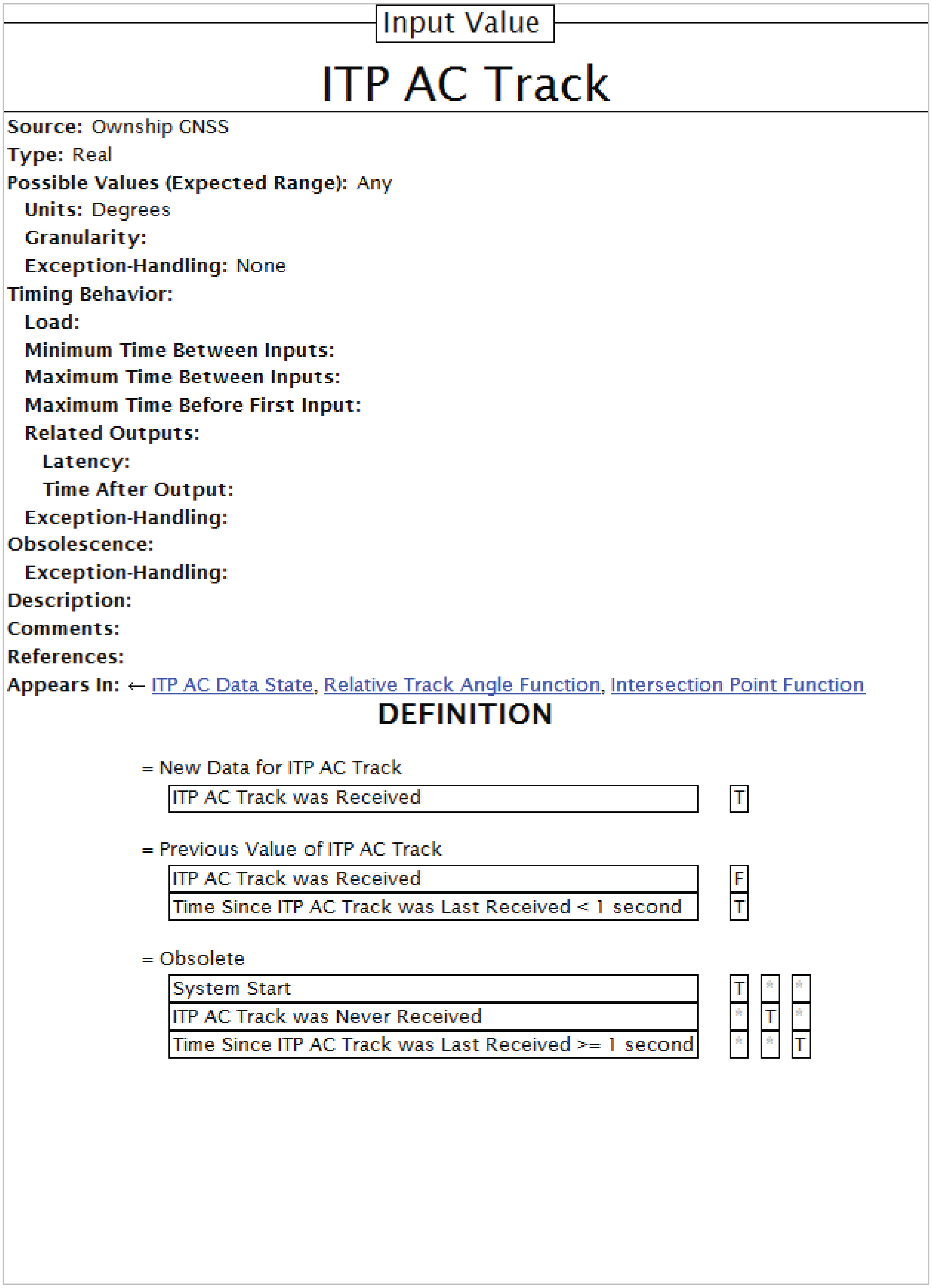
ITP AC Barometric Altitude was Received	T

= Previous Value of ITP AC Barometric Altitude

ITP AC Barometric Altitude was Received	F
Time Since ITP AC Barometric Altitude was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
ITP AC Barometric Altitude was Never Received	*	T	*
Time Since ITP AC Barometric Altitude was Last Received >= 1 second	*	*	T



Input Value

ITP AC Track

Source: Ownship GNSS
Type: Real
Possible Values (Expected Range): Any
Units: Degrees
Granularity:
Exception-Handling: None
Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence:
Exception-Handling:
Description:
Comments:
References:
Appears In: ← ITP AC Data State, Relative Track Angle Function, Intersection Point Function

DEFINITION

= New Data for ITP AC Track

ITP AC Track was Received	T

= Previous Value of ITP AC Track

ITP AC Track was Received	F
Time Since ITP AC Track was Last Received < 1 second	T

= Obsolete

System Start	T	*	*
ITP AC Track was Never Received	*	T	*
Time Since ITP AC Track was Last Received >= 1 second	*	*	T

B.5.2 Air Traffic Controller

The blackbox behavior of the Air Traffic Controller is described herein. This models the expected behavior of human operators given certain conditions, and represents a formal means for validating the procedural steps detailed in Levels 1 and 2.

Fundamental Goals of Air Traffic Controller

1. Approve ITP if criteria are met – (↑[SC-ATC.1])
2. Deny ITP if criteria are not met

Outputs

1. Approve ITP
2. Deny ITP

States

1. ITP Criteria State
2. Flight Crew Request State

Inputs (from user: ITP Flight Crew)

1. ITP Criteria Input
2. Flight Crew Request
3. Blocking Aircraft and Environment

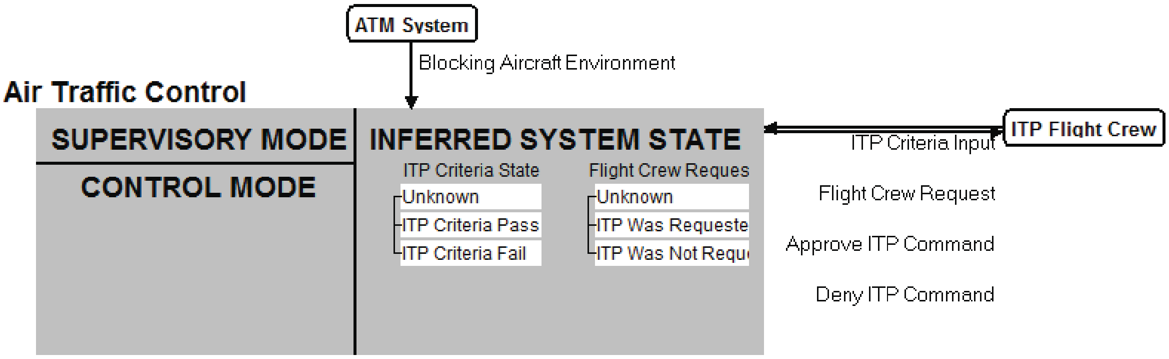


Figure B.9 Air Traffic Control Model Visualization

OUTPUTS

Output Command

Approve ITP Command

Destination: ITP Flight Crew

Fields:

Name: Approve ITP

Type: {Approve, Deny}

Acceptable Values:

Units:

Granularity:

Hazardous Values:

Exception-Handling:

Description:

Comments:

Reversed By:

Description: In order for Air Traffic Control to approve an In Trail Procedure, there must necessarily be 4 (simultaneous) true conditions, shown in the table below.

Comments: Unknown conditions are taken care of in the Deny ITP Command module on the next page.

References: → ITP Criteria State, Flight Crew Request State, Blocking Aircraft Environment

TRIGGERING CONDITION

ITP Criteria State in state ITP Criteria Pass	T
Flight Crew Request State in state ITP Was Requested	T
Time Since Flight Crew Request was Last Received < 300 seconds	T
Blocking Aircraft Environment is Not Present	T

MESSAGE CONTENTS

Field:	Value:
Approve ITP	Approve

Output Command

Deny ITP Command

Destination: ITP Flight Crew

Fields:

- **Name:** Deny ITP
  - **Type:** {Approve, Deny}
  - **Acceptable Values:**
    - **Units:**
    - **Granularity:**
    - **Hazardous Values:**
    - **Exception-Handling:**
  - **Description:**
  - **Comments:**

Reversed By:

Description: In order for Air Traffic Control to approve an In Trail Procedure, there must necessarily be 4 (simultaneous) true conditions, shown in the table below.

Comments: If any of the conditions are false, the ATC must deny ITP clearance.

References: → ITP Criteria State, Flight Crew Request State, Blocking Aircraft Environment

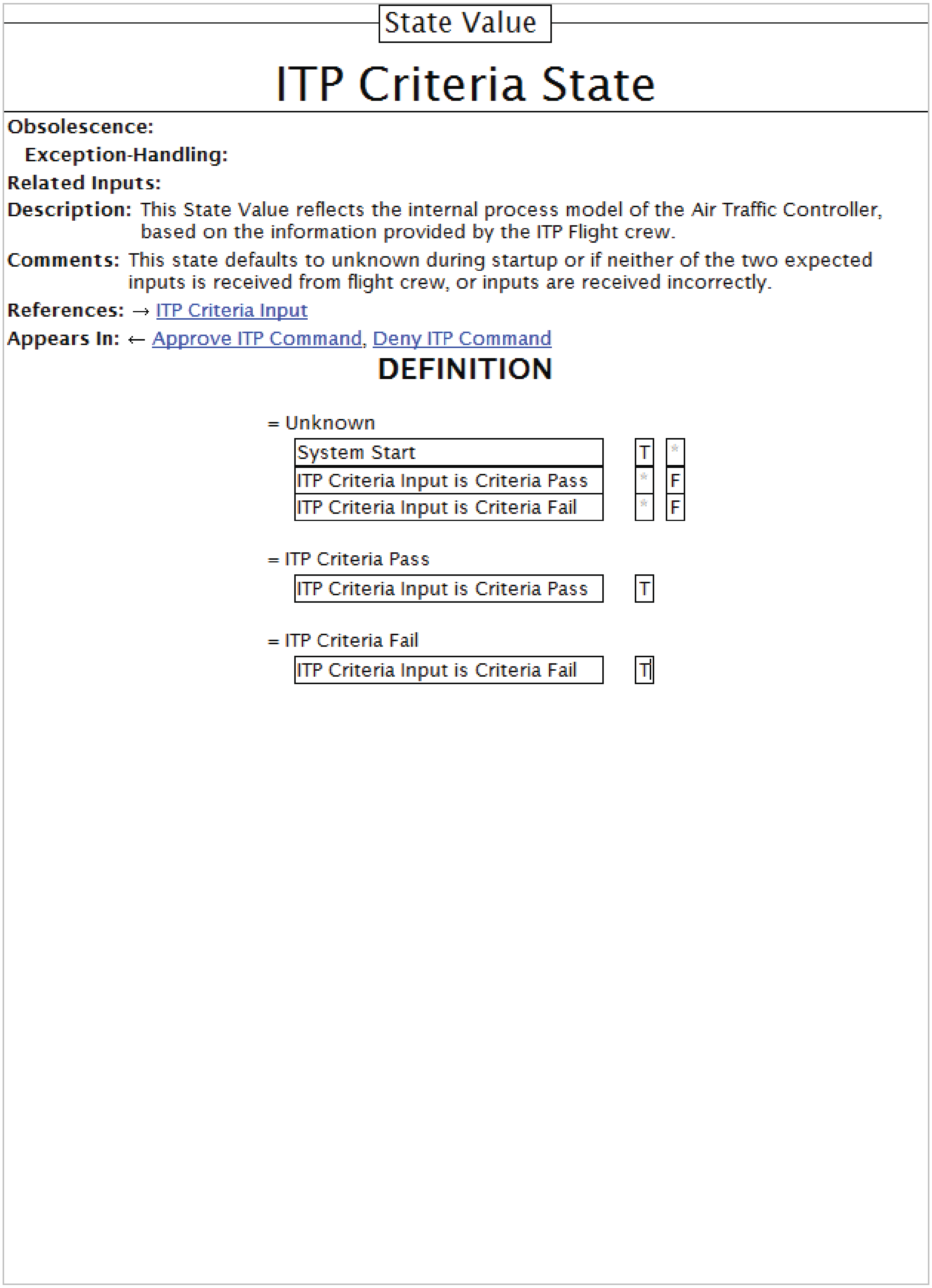
TRIGGERING CONDITION

ITP Criteria State in state ITP Criteria Pass	F	*	*	*
Flight Crew Request State in state ITP Was Requested	*	F	*	*
Time Since Flight Crew Request was Last Received < 300 seconds	*	*	F	*
Blocking Aircraft Environment is Not Present	*	*	*	F

MESSAGE CONTENTS

Field:	Value:
Deny ITP	Deny

STATES



State Value

ITP Criteria State

Obsolescence:

Exception-Handling:

Related Inputs:

Description: This State Value reflects the internal process model of the Air Traffic Controller, based on the information provided by the ITP Flight crew.

Comments: This state defaults to unknown during startup or if neither of the two expected inputs is received from flight crew, or inputs are received incorrectly.

References: → ITP Criteria Input

Appears In: ← Approve ITP Command, Deny ITP Command

DEFINITION

= Unknown

System Start	T	*
ITP Criteria Input is Criteria Pass	*	F
ITP Criteria Input is Criteria Fail	*	F

= ITP Criteria Pass

ITP Criteria Input is Criteria Pass	T

= ITP Criteria Fail

ITP Criteria Input is Criteria Fail	T

State Value

Flight Crew Request State

Obsolescence:

Exception-Handling:

Related Inputs:

Description: This State Value reflects the internal process model of the Air Traffic Controller, based on the request (or lack thereof) provided by the ITP Flight crew.

Comments: This state defaults to unknown during startup or if neither of the two expected inputs is received from flight crew, or inputs are received incorrectly.

References: → Flight Crew Request

Appears In: ← Approve ITP Command, Deny ITP Command

DEFINITION

= Unknown

System Start	T	*
Flight Crew Request is Requested	*	F
Flight Crew Request is Not Requested	*	F

= ITP Was Requested

Flight Crew Request is Requested	T

= ITP Was Not Requested

Flight Crew Request is Not Requested	T

INPUTS

Input Value

ITP Criteria Input

Source: ITP Flight Crew

Type: {Criteria Pass, Criteria Fail}

Possible Values (Expected Range):

Units:

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description: ITP Criteria input from ITP Flight Crew. At this level of analysis this is a binary Pass/Fail but could also include the actual quantities associated with ITP, e.g. closing speed and distance between ITP and Reference Aircraft.

Comments:

References: ↑ Transmit ITP Criteria (ITP Flight Crew)

Appears In: ← ITP Criteria State

DEFINITION

= New Data for ITP Criteria Input

ITP Criteria Input was Received	T

= Previous Value of ITP Criteria Input

ITP Criteria Input was Received	F
Time Since ITP Criteria Input was Last Received < 300 seconds	T

= Obsolete

System Start	T	*	*
ITP Criteria Input was Never Received	*	T	*
Time Since ITP Criteria Input was Last Received >= 300 seconds	*	*	T

Input Value

Flight Crew Request

Source: ITP Flight Crew

Type: {Requested, Not Requested}

Possible Values (Expected Range):

Units:

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description: ITP Request from Flight Crew.

Comments: This analysis does not included the nature of nomenclature of the request, only that it is transmitted in a mutually understood way or not transmitted/received at all.

References: ↑ Request ITP to ATC (ITP Flight Crew)

Appears In: ← Flight Crew Request State

DEFINITION

= New Data for Flight Crew Request

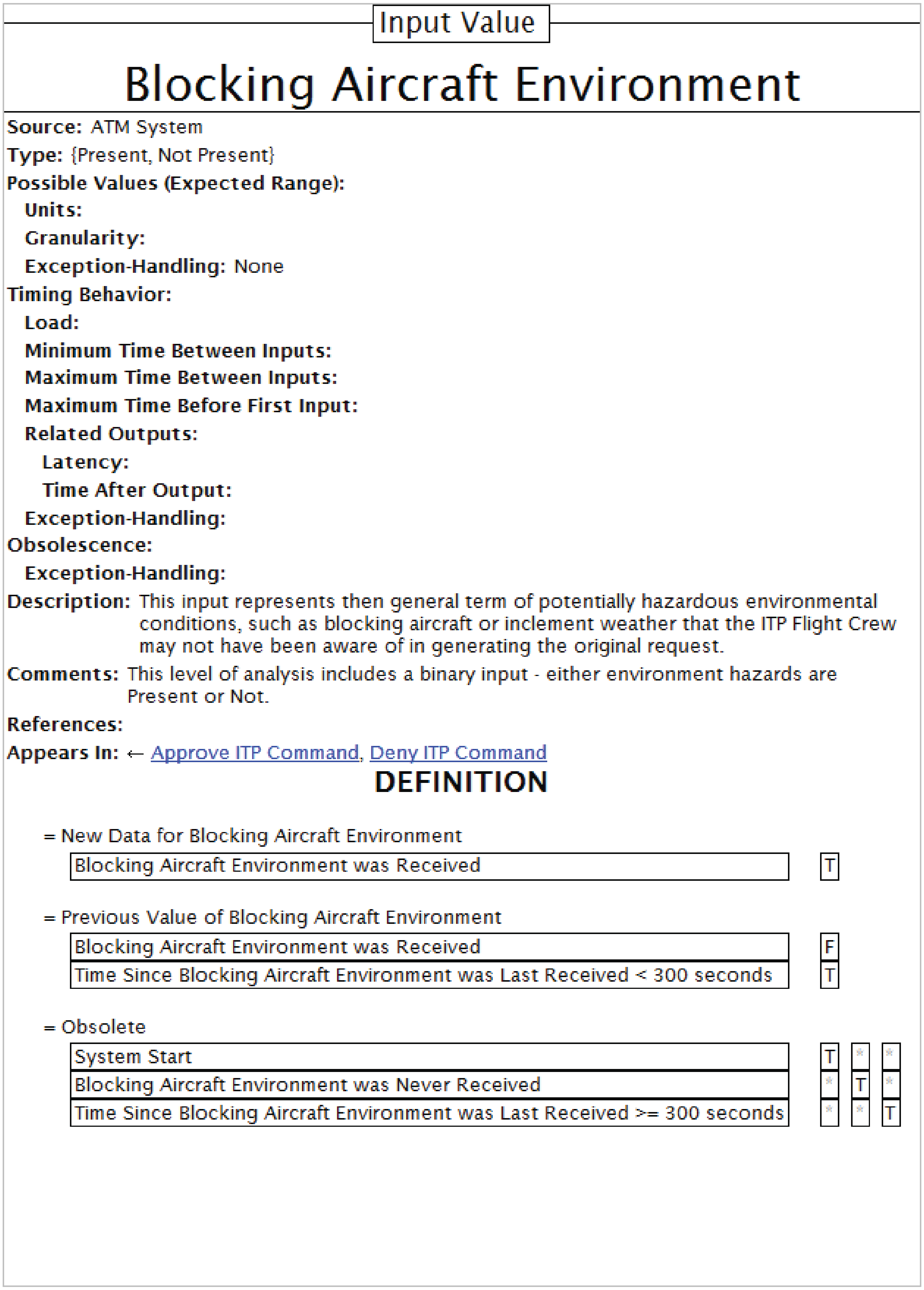
Flight Crew Request was Received	T

= Previous Value of Flight Crew Request

Flight Crew Request was Received	F
Time Since Flight Crew Request was Last Received < 300 seconds	T

= Obsolete

System Start	T	*	*
Flight Crew Request was Never Received	*	T	*
Time Since Flight Crew Request was Last Received >= 300 seconds	*	*	T



Input Value

Blocking Aircraft Environment

Source: ATM System

Type: {Present, Not Present}

Possible Values (Expected Range):

Units:

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description: This input represents then general term of potentially hazardous environmental conditions, such as blocking aircraft or inclement weather that the ITP Flight Crew may not have been aware of in generating the original request.

Comments: This level of analysis includes a binary input - either environment hazards are Present or Not.

References:

Appears In: ← Approve ITP Command, Deny ITP Command

DEFINITION

= New Data for Blocking Aircraft Environment

Blocking Aircraft Environment was Received	T

= Previous Value of Blocking Aircraft Environment

Blocking Aircraft Environment was Received	F
Time Since Blocking Aircraft Environment was Last Received < 300 seconds	T

= Obsolete

System Start	T	*	*
Blocking Aircraft Environment was Never Received	*	T	*
Time Since Blocking Aircraft Environment was Last Received >= 300 seconds	*	*	T

B.5.3 ITP Flight Crew

The blackbox behavior of the ITP Flight Crew is described herein. This models the expected behavior of human operators given certain conditions, and represents a formal means for validating the procedural steps detailed in Levels 1 and 2.

Fundamental Goals of Air Traffic Controller

1. Perform ITP when criteria are met – (↑[SC-FC.2],[SC-FC.3])
2. Execute normal flight operations safely

____

Outputs

1. Execute ITP Command
2. Request ITP to ATC
3. Transmit ITP Criteria

Modes

1. ITP Supervisor Mode
2. ITP Control Mode

States

1. ITP Criteria State
2. ATC Response State

Inputs

1. ITP Criteria Input
2. ATC Response

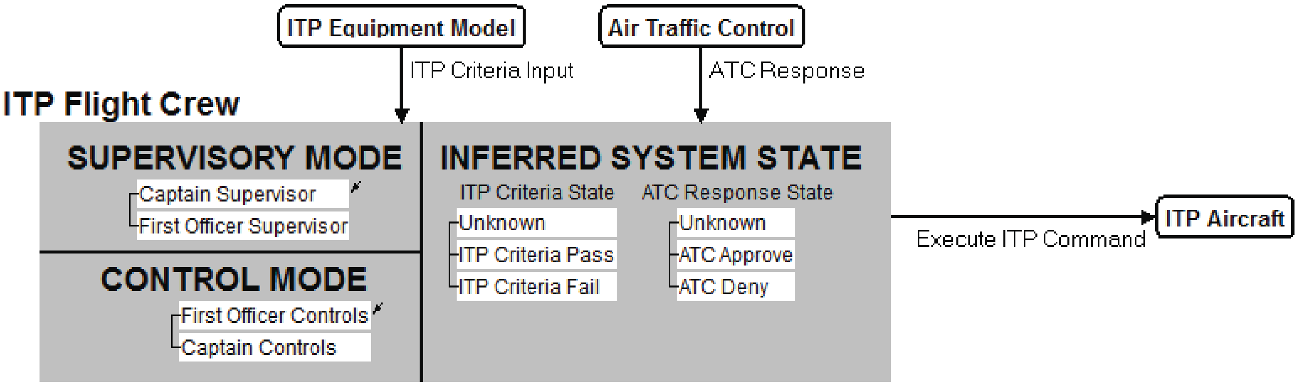
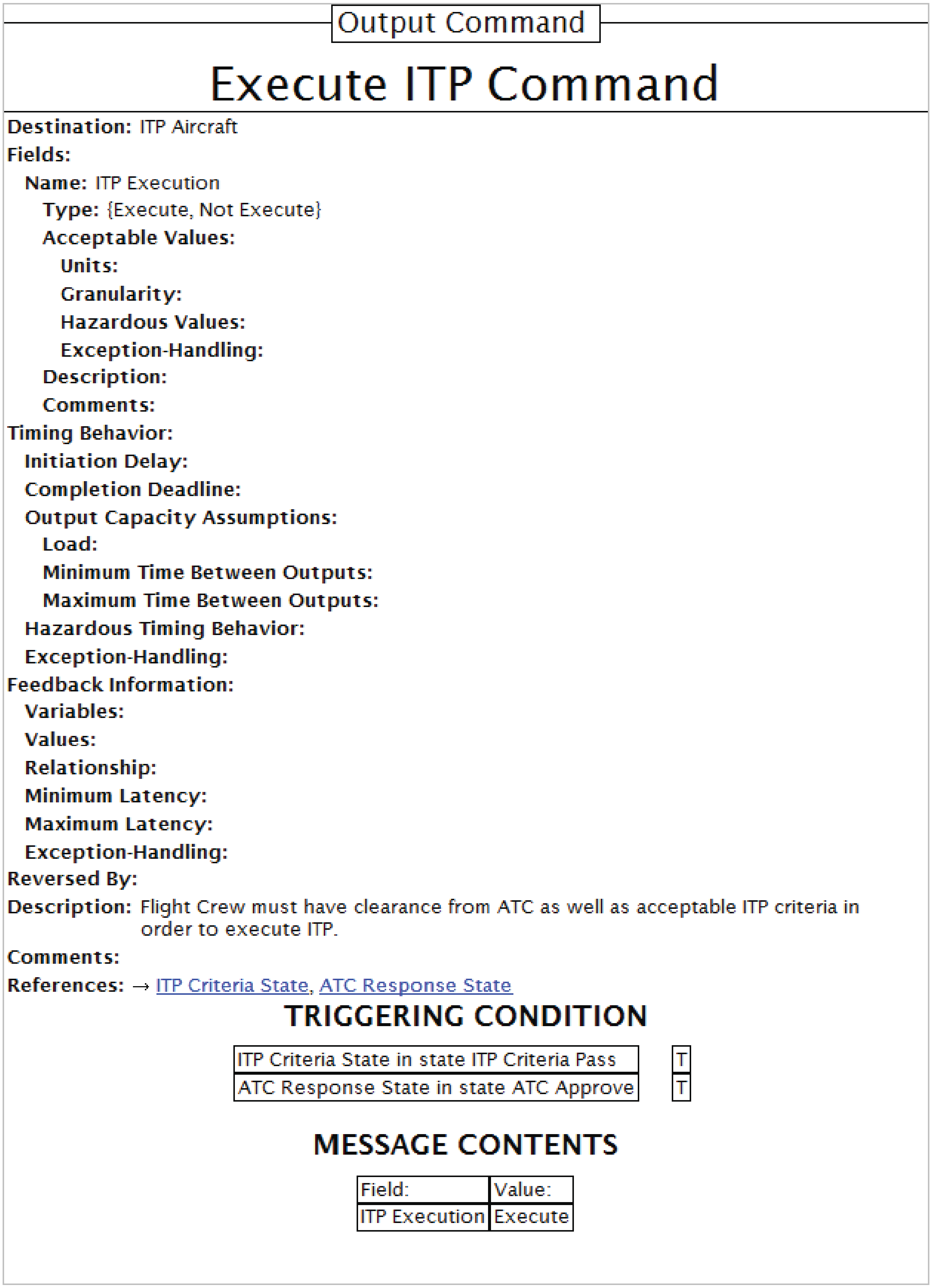


Figure B.10 ITP Flight Crew Model Visualization

OUTPUTS



Output Command

Execute ITP Command

Destination: ITP Aircraft

Fields:

- **Name:** ITP Execution
  - **Type:** {Execute, Not Execute}
  - **Acceptable Values:**
    - **Units:**
    - **Granularity:**
    - **Hazardous Values:**
    - **Exception-Handling:**
  - **Description:**
  - **Comments:**

Timing Behavior:

- **Initiation Delay:**
- **Completion Deadline:**
- **Output Capacity Assumptions:**
  - **Load:**
  - **Minimum Time Between Outputs:**
  - **Maximum Time Between Outputs:**
- **Hazardous Timing Behavior:**
- **Exception-Handling:**

Feedback Information:

- **Variables:**
- **Values:**
- **Relationship:**
- **Minimum Latency:**
- **Maximum Latency:**
- **Exception-Handling:**

Reversed By:

Description: Flight Crew must have clearance from ATC as well as acceptable ITP criteria in order to execute ITP.

Comments:

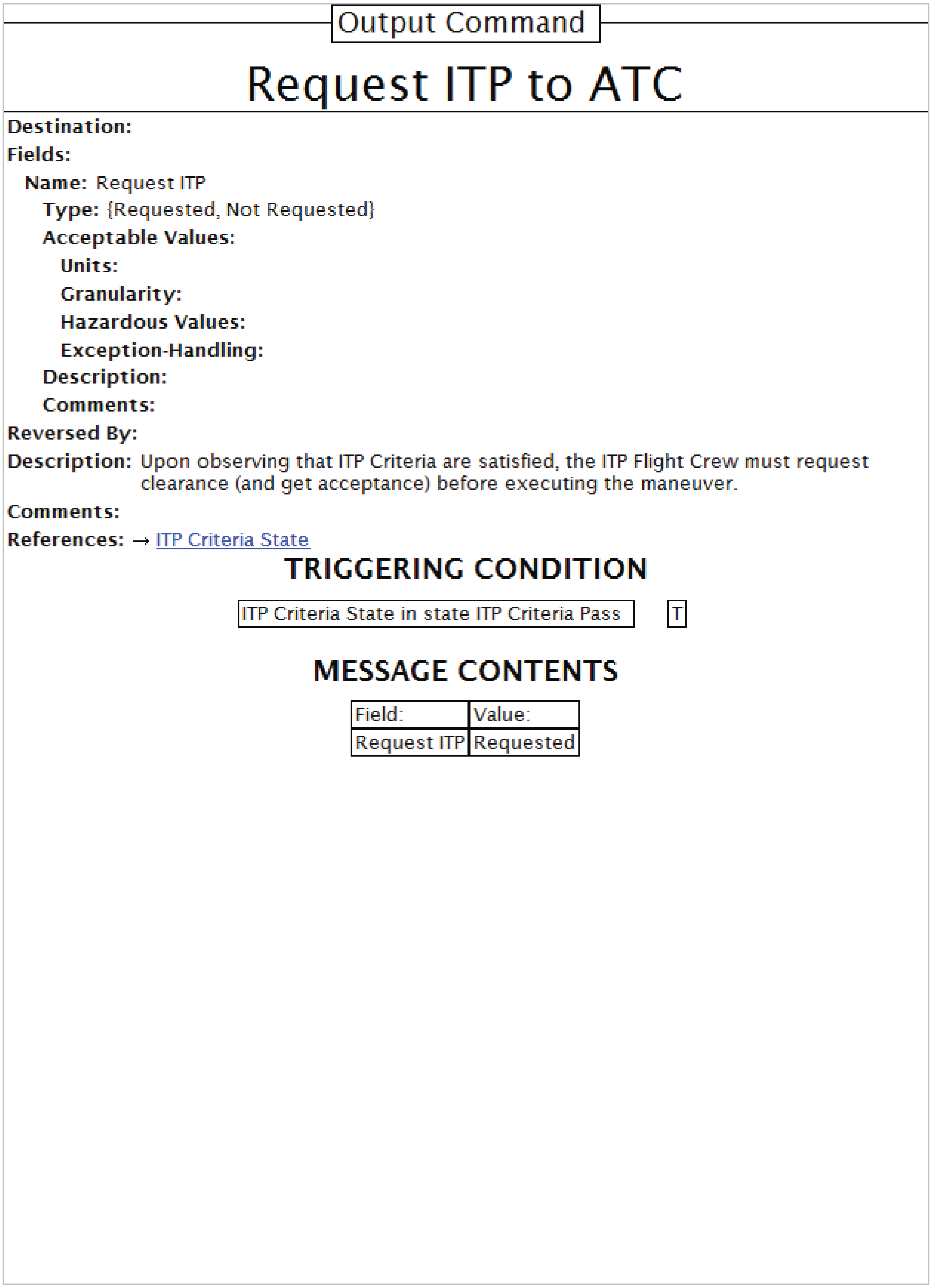
References: → ITP Criteria State, ATC Response State

TRIGGERING CONDITION

ITP Criteria State in state ITP Criteria Pass	T
ATC Response State in state ATC Approve	T

MESSAGE CONTENTS

Field:	Value:
ITP Execution	Execute



Output Command

Request ITP to ATC

Destination:

Fields:

Name: Request ITP

Type: {Requested, Not Requested}

Acceptable Values:

Units:

Granularity:

Hazardous Values:

Exception-Handling:

Description:

Comments:

Reversed By:

Description: Upon observing that ITP Criteria are satisfied, the ITP Flight Crew must request clearance (and get acceptance) before executing the maneuver.

Comments:

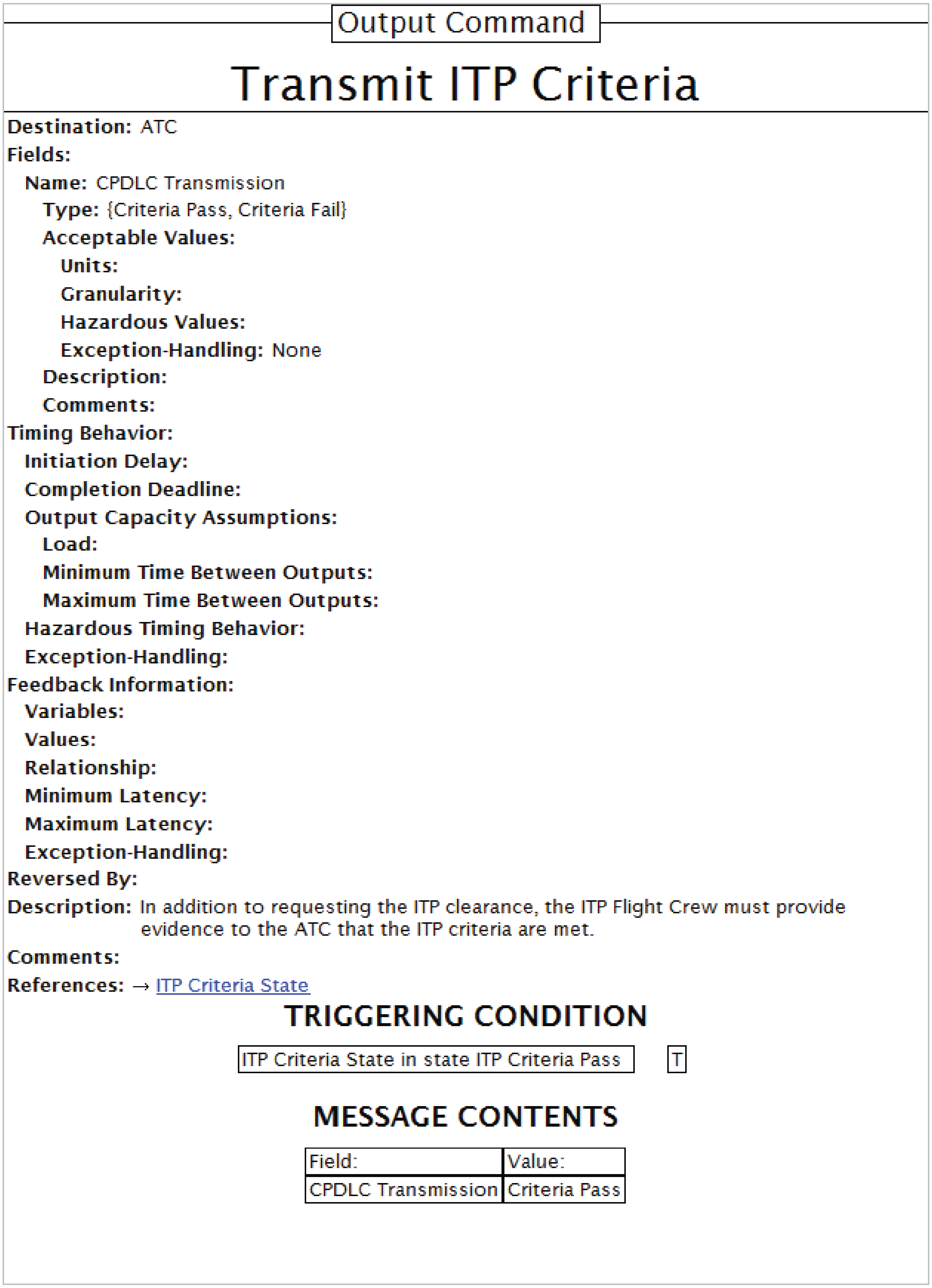
References: → ITP Criteria State

TRIGGERING CONDITION

ITP Criteria State in state ITP Criteria Pass	T

MESSAGE CONTENTS

Field:	Value:
Request ITP	Requested



Output Command

Transmit ITP Criteria

Destination: ATC

Fields:

- **Name:** CPDLC Transmission
  - **Type:** {Criteria Pass, Criteria Fail}
  - **Acceptable Values:**
    - **Units:**
    - **Granularity:**
    - **Hazardous Values:**
    - **Exception-Handling:** None
  - **Description:**
  - **Comments:**

Timing Behavior:

- **Initiation Delay:**
- **Completion Deadline:**
- **Output Capacity Assumptions:**
  - **Load:**
  - **Minimum Time Between Outputs:**
  - **Maximum Time Between Outputs:**
- **Hazardous Timing Behavior:**
- **Exception-Handling:**

Feedback Information:

- **Variables:**
- **Values:**
- **Relationship:**
- **Minimum Latency:**
- **Maximum Latency:**
- **Exception-Handling:**

Reversed By:

Description: In addition to requesting the ITP clearance, the ITP Flight Crew must provide evidence to the ATC that the ITP criteria are met.

Comments:

References: → ITP Criteria State

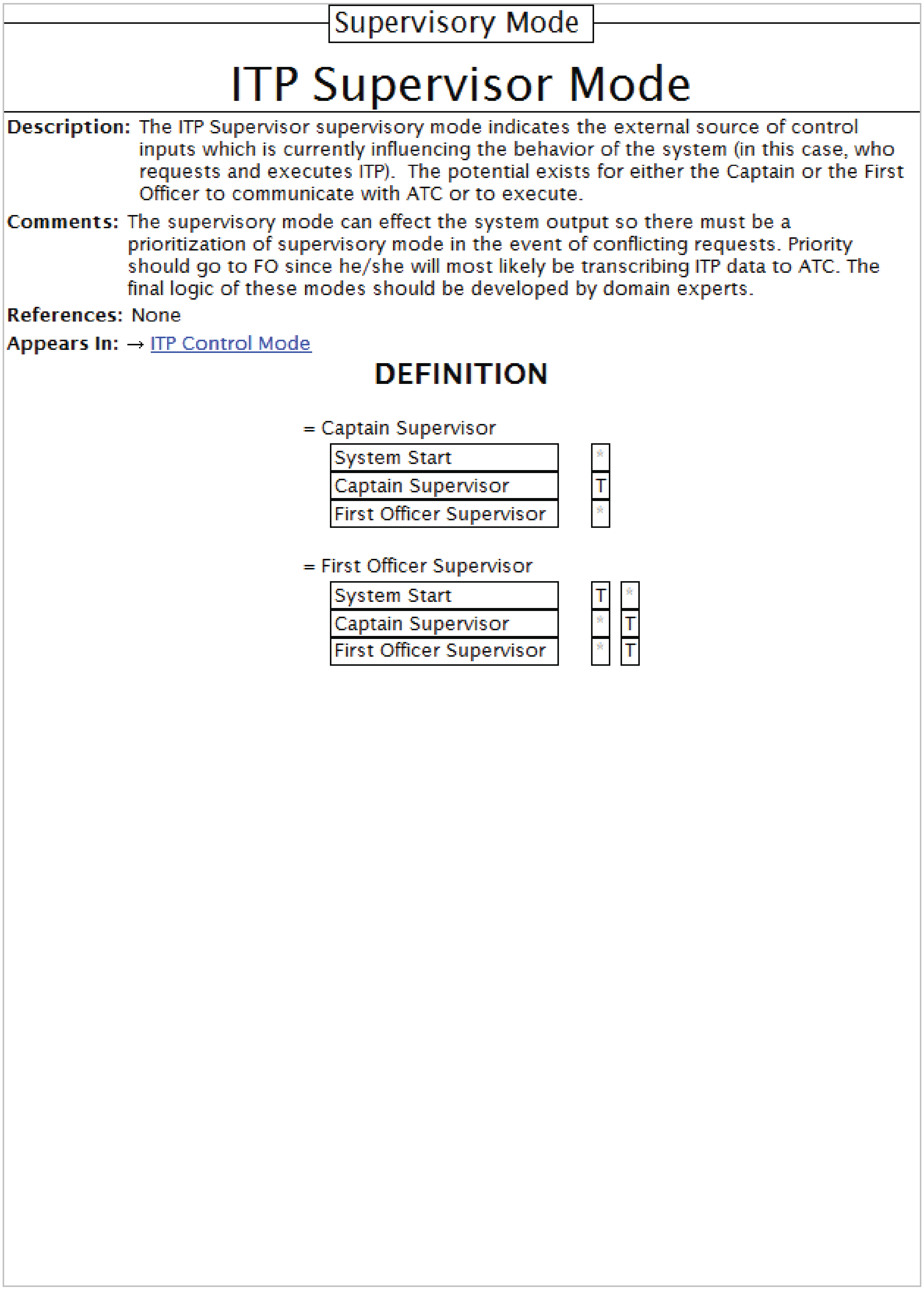
TRIGGERING CONDITION

ITP Criteria State in state ITP Criteria Pass	T

MESSAGE CONTENTS

Field:	Value:
CPDLC Transmission	Criteria Pass

MODES



Supervisory Mode

ITP Supervisor Mode

Description: The ITP Supervisor supervisory mode indicates the external source of control inputs which is currently influencing the behavior of the system (in this case, who requests and executes ITP). The potential exists for either the Captain or the First Officer to communicate with ATC or to execute.

Comments: The supervisory mode can effect the system output so there must be a prioritization of supervisory mode in the event of conflicting requests. Priority should go to FO since he/she will most likely be transcribing ITP data to ATC. The final logic of these modes should be developed by domain experts.

References: None

Appears In: → ITP Control Mode

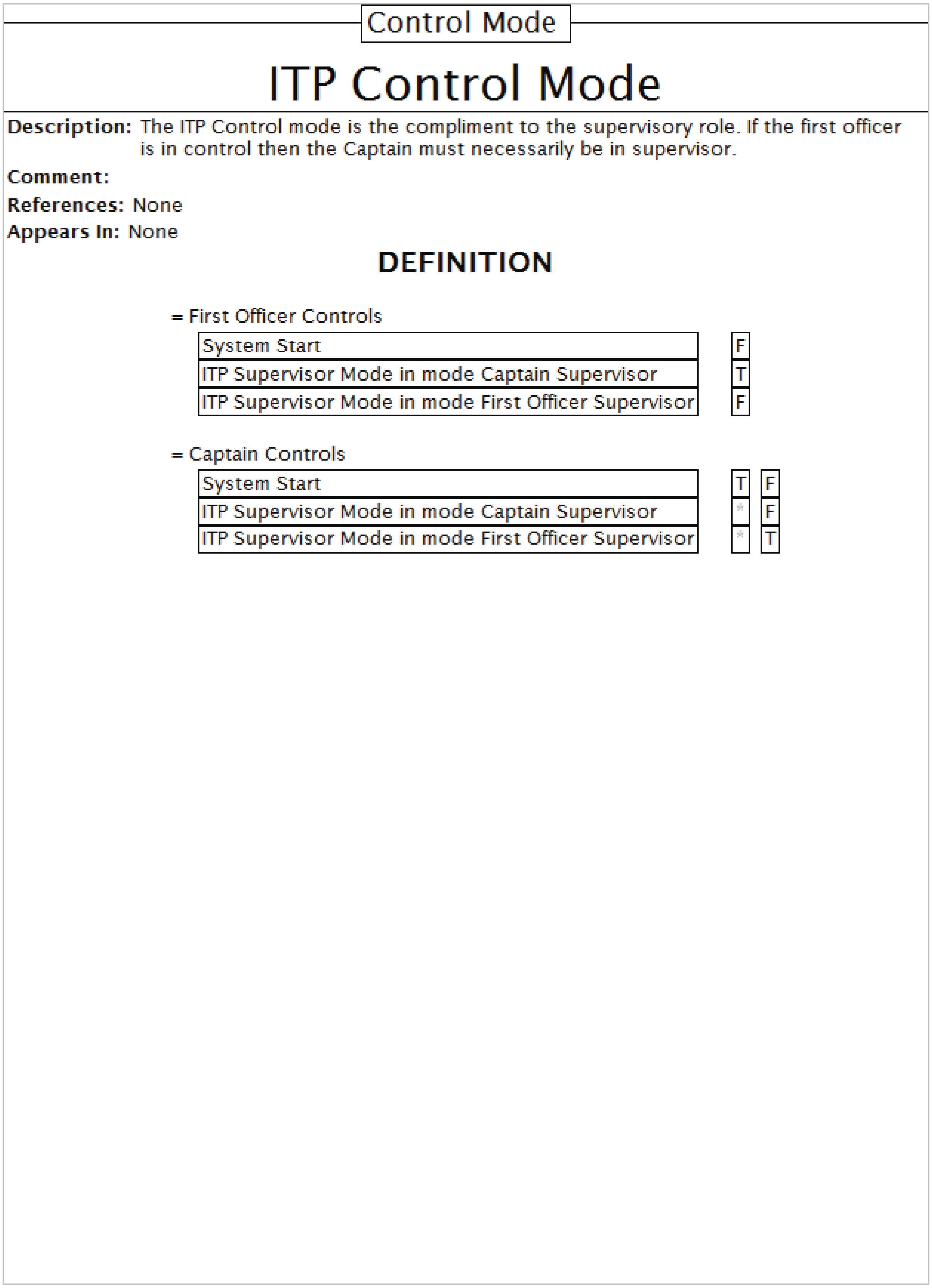
DEFINITION

= Captain Supervisor

System Start	*
Captain Supervisor	T
First Officer Supervisor	*

= First Officer Supervisor

System Start	T	*
Captain Supervisor	*	T
First Officer Supervisor	*	T



Control Mode

ITP Control Mode

Description: The ITP Control mode is the compliment to the supervisory role. If the first officer is in control then the Captain must necessarily be in supervisor.

Comment:

References: None

Appears In: None

DEFINITION

= First Officer Controls

System Start	F
ITP Supervisor Mode in mode Captain Supervisor	T
ITP Supervisor Mode in mode First Officer Supervisor	F

= Captain Controls

System Start	T	F
ITP Supervisor Mode in mode Captain Supervisor	*	F
ITP Supervisor Mode in mode First Officer Supervisor	*	T

STATES

State Value

ITP Criteria State

Obsolescence:

Exception-Handling:

Related Inputs:

Description: This is the process model state of the flight crew about whether the ITP Criteria are met or not

Comments: If ITP Criteria Input is neither Pass nor Fail the state defaults to unknown

References: → ITP Criteria Input

Appears In: ← Execute ITP Command, Request ITP to ATC

DEFINITION

= Unknown

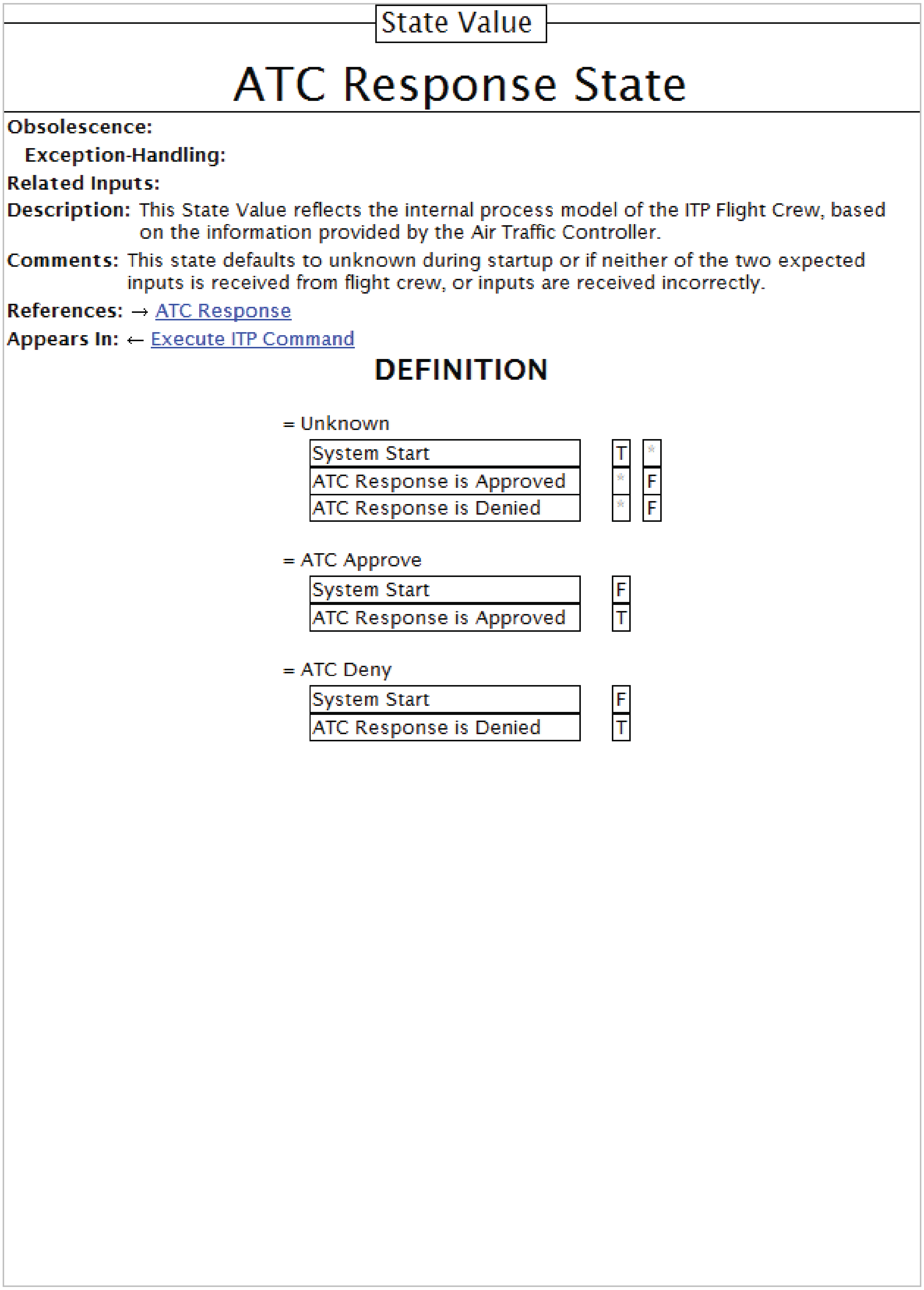
System Start	T	*
ITP Criteria Input is Criteria Pass	*	F
ITP Criteria Input is Criteria Fail	*	F

= ITP Criteria Pass

System Start	F
ITP Criteria Input is Criteria Pass	T

= ITP Criteria Fail

System Start	F
ITP Criteria Input is Criteria Fail	T



State Value

ATC Response State

Obsolescence:

Exception-Handling:

Related Inputs:

Description: This State Value reflects the internal process model of the ITP Flight Crew, based on the information provided by the Air Traffic Controller.

Comments: This state defaults to unknown during startup or if neither of the two expected inputs is received from flight crew, or inputs are received incorrectly.

References: → ATC Response

Appears In: ← Execute ITP Command

DEFINITION

= Unknown

System Start	T	*
ATC Response is Approved	*	F
ATC Response is Denied	*	F

= ATC Approve

System Start	F
ATC Response is Approved	T

= ATC Deny

System Start	F
ATC Response is Denied	T

INPUTS

Input Value

ITP Criteria Input

Source: ITP Equipment Model

Type: {Criteria Pass, Criteria Fail}

Possible Values (Expected Range):

Units:

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description: The ITP Criteria are not necessarily decided real-time by the flight crew, but are instead taken as inputs (external source of information) from the ITP Equipment.

Comments: The Type field should match that of the ITP Criteria Display Output in the ITP Equipment black box model

References: ↑ ITP Criteria Display Output (ITP Equipment)

Appears In: ← ITP Criteria State

DEFINITION

= New Data for ITP Criteria Input

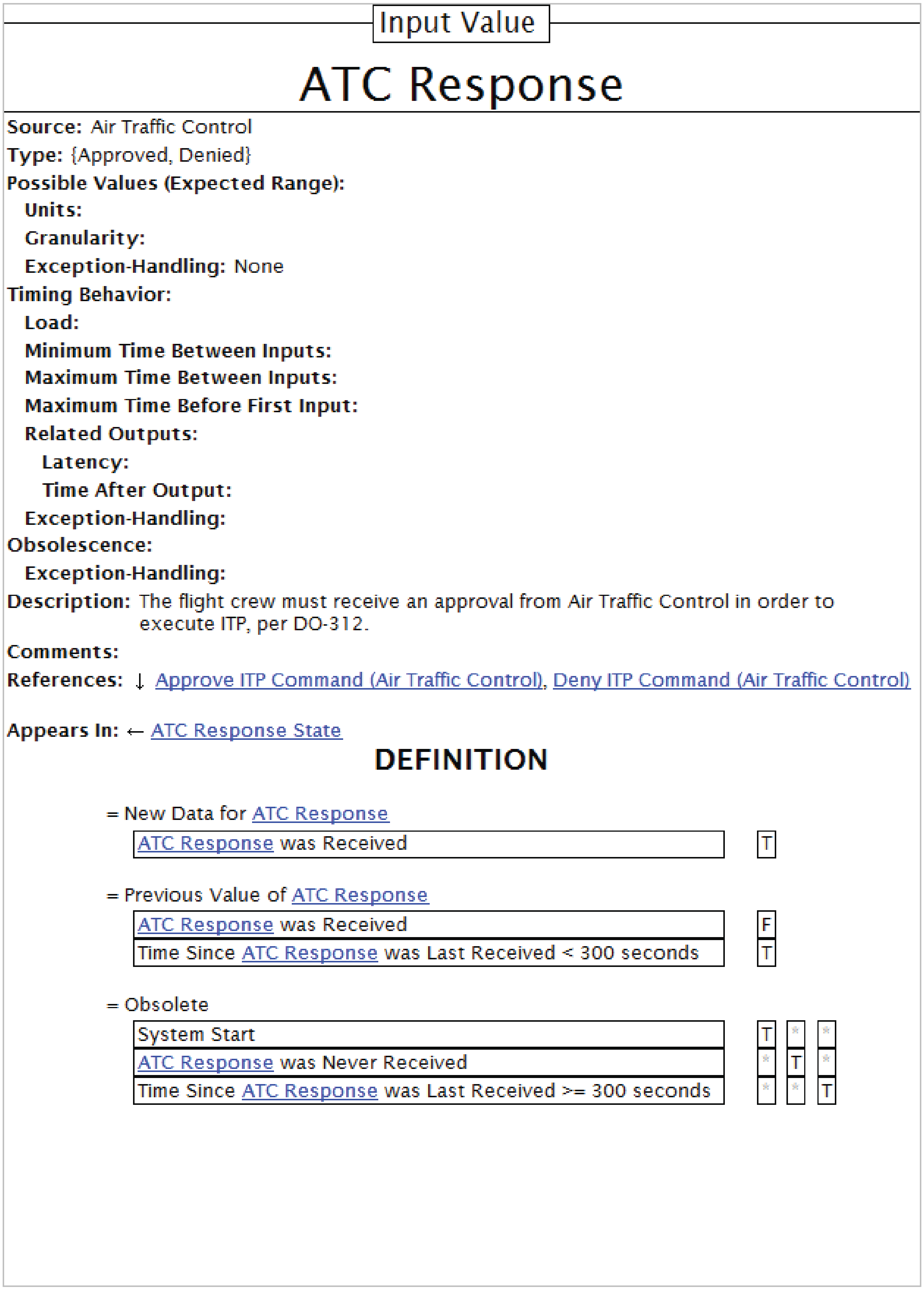
ITP Criteria Input was Received	T

= Previous Value of ITP Criteria Input

ITP Criteria Input was Received	F
Time Since ITP Criteria Input was Last Received < 300 seconds	T

= Obsolete

System Start	T	*	*
ITP Criteria Input was Never Received	*	T	*
Time Since ITP Criteria Input was Last Received >= 300 seconds	*	*	T



Input Value

ATC Response

Source: Air Traffic Control

Type: {Approved, Denied}

Possible Values (Expected Range):

Units:

Granularity:

Exception-Handling: None

Timing Behavior:

Load:

Minimum Time Between Inputs:

Maximum Time Between Inputs:

Maximum Time Before First Input:

Related Outputs:

Latency:

Time After Output:

Exception-Handling:

Obsolescence:

Exception-Handling:

Description: The flight crew must receive an approval from Air Traffic Control in order to execute ITP, per DO-312.

Comments:

References: ↓ Approve ITP Command (Air Traffic Control), Deny ITP Command (Air Traffic Control)

Appears In: ← ATC Response State

DEFINITION

= New Data for ATC Response

ATC Response was Received	T

= Previous Value of ATC Response

ATC Response was Received	F
Time Since ATC Response was Last Received < 300 seconds	T

= Obsolete

System Start	T	*	*
ATC Response was Never Received	*	T	*
Time Since ATC Response was Last Received >= 300 seconds	*	*	T

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 01- 03 - 2012	**2. REPORT TYPE** Contractor Report	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE

Safety Assurance in NextGen

5a. CONTRACT NUMBER
NNL10AA13C

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Fleming, Cody Harrison; Spencer, Melissa; Leveson, Nancy; Wilkinson, Chris

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
534723.02.02.07.10

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, Virginia 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/CR-2012-217553

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified - Unlimited
Subject Category 62
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES

Langley Technical Monitor: C. Michael Holloway

14. ABSTRACT

The generation of minimum operational, safety, performance, and interoperability requirements is an important aspect of safely integrating new NextGen components into the Communication Navigation Surveillance and Air Traffic Management (CNS/ATM) system. These requirements are used as part of the implementation and approval processes. In addition, they provide guidance to determine the levels of design assurance and performance that are needed for each element of the new NextGen procedures, including aircraft, operator, and Air Navigation and Service Provider. Using the enhanced Airborne Traffic Situational Awareness for InTrail Procedure (ATSA-ITP) as an example, this report describes some limitations of the current process used for generating safety requirements and levels of required design assurance. An alternative process is described, as well as the argument for why the alternative can generate more comprehensive requirements and greater safety assurance than the current approach.

15. SUBJECT TERMS

Assurance; NextGen; Safety; Software

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER ***(Include area code)***
U	U	U	UU	187	(443) 757-5802