

**A Demonstration of a Formal Specification & Requirements Language:
A Case Study**

by

Sean J.P. Sutherland

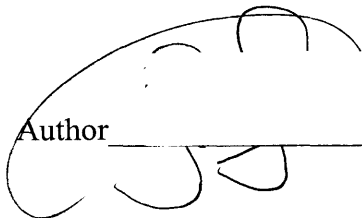
Submitted to the Department of Electrical Engineering and Computer Science
in fulfillment of the Requirements for the Degree of
Masters of Electrical Engineering and Computer Science
at the Massachusetts Institute of Technology

August 31, 2001

Copyright 2001 Sean J. P. Sutherland. All rights reserved.

The author hereby grants to M.I.T. permission to reproduce and
distribute publicly paper and electronic copies of this thesis
and to grant others the right to do so.

Author



Sean J. P. Sutherland
Department of Electrical Engineering and Computer Science
August 31, 2001

Certified
by



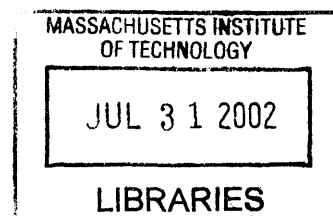
Professor Nancy G. Leveson
Thesis Supervisor

Accepted
by



Arthur C. Smith
Chairman, Department Committee on Graduate Theses

BARKER



**Demonstration of a Formal Specification & Requirements Language:
A Case Study**

by

Sean J.P. Sutherland

Submitted to the Department of Electrical Engineering and Computer Science
in fulfillment of the Requirements for the Degree of
Masters Of Electrical Engineering and Computer Science
at the Massachusetts Institute of Technology

August 6, 2001

Abstract

This document provides a demonstration of the application of Specification Tools and Requirements Methodology Requirements Language, SpecTRM-RL, to a component of an Air Traffic Control System called Sector Handoff. SpecTRM is a formal specification and requirements language that allows designers to incorporate safety concerns into their design process, paying particular attention to issues of human-machine interactions. SpecTRM uses the concept of means-end hierarchies to achieve traceability in both directions between its five levels of specification. Although this example only uses three of the five levels in SpecTRM-RL, it is complete with tracings of requirements to lower levels of the specification. The Sector Handoff function used is part of Raytheon's Standard Terminal Automation Replacement System (STARS).

Thesis Supervisor: Nancy G. Leveson
Title: MIT Professor of Aeronautics and Astronautics

ACKNOWLEDGEMENTS

I would like to express my sincerest appreciation to my thesis advisor, Professor Nancy Leveson of the Massachusetts Institute of Technology, and Jeffery Levine of Raytheon Corporation for all their assistance.

TABLE OF CONTENTS

Introduction	15
Related Work	19
Background	22
<i>Aerospace Accident Factors</i>	22
<i>The Goal of Intent Specifications</i>	25
<i>Intent Specification</i>	29
<i>Sector Handoff</i>	31
Analysis: Intent Specification for Sector Handoff	37
Level I	39
Level II	46
Level III	84
Conclusion	102
Appendix A: Future Work	103
Appendix B: List of Abbreviations and Definitions	105
References	109

LIST OF FIGURES

Figure 1: Diagram of Environment	46
Figure 2: Diagram of System Environment	84
Figure 3: Diagram of Modes showing Inputs and Outputs	85

LIST OF TABLES

Table 1: Handoff Events and Conditions	52
Table 2: Handoff Actions	81
Table 3: System Messages	86
Table 4: Initiate Handoff (Implied command)	87
Table 5: Recall Handoff (Implied command)	87
Table 6: Accept Handoff (Implied command)	88
Table 7: Take control of interfacility track (Implied command)	88
Table 8: Inhibit automatic handoff for a flight (Implied command)	88
Table 9: Accept handoff	88
Table 10: Initiate intrafacility handoff	89
Table 11: Initiate handoff to ARTCC	89
Table 12: Initiate NAS FP handoff to adjacent Tracon	90
Table 13: Initiate local FP handoff to adjacent Tracon	90
Table 14: Recall handoff	91
Table 15: Redirect incoming interfacility handoff	91
Table 16: Inhibit automatic handoff for a flight	92
Table 17: Current State = Not in Handoff	92
Table 18: Current State = Handoff Initiate Pending	94
Table 19: Current State = Non-Enroute FP Pending	94
Table 20: Current State = Non-Enroute CX Pending	94
Table 21: Current State = Outbound HO Accepted	95
Table 22: Current State = Handoff Ext To	95
Table 23: Current State = Handoff Recall Pending	95
Table 24: Current State = Handoff Ext From	96

Table 25: Current State = Handoff Accept Pending	96
Table 26: Current State = Inbound HO Accepted	96
Table 27: Current State = Handoff Int	96
Table 28: Current State = Local HO Accepted	97
Table 29: Current State = EFO Handoff Int	97
Table 30: Current State = EFO Local Accepted	97

INTRODUCTION

Recent advances in computer technology have driven engineers to increasingly incorporate computers into their systems. Many engineers now place complex control capabilities in the hands of software running on these computers under the impression that it is “easier” to modify code to add or modify functionalities than it is to change the hardware. However, this is not as simple as it appears. Research shows that the increased computerization of systems has made the systems far more complex and has resulted in more unexplainable system behavior. These failures are at the system level, as it is not the faulty software that causes the damage, but the instruments and hardware the software controls. [1] For systems where the software becomes critical to the safe operation of the system, software failures may lead to loss of human life and property.

The increase in automation, coupled with a decrease in physical interlocks, has made it even more crucial that software interacts safely with the rest of the system to avoid catastrophic outcomes. Formal Specification Languages are needed to help ensure that errors are eliminated from the software. However, Intent Specification Languages improve upon Formal Specification Languages as they additionally incorporate humans in the design process. This means that human psychological and physiological principles are used as guidelines in determining how one should design a system. [2] Intent specification languages, unlike formal specification languages, capture the rationale and assumptions made while humans set out to solve problems. This allows for traceability in the system as high-level requirements can be traced to the actual system implementation details, and vice versa. This also allows for safety critical design decisions to be enforced on the low-level implementation, such as software.

Intent specification uses a three-dimensional model to analyze a system. In the intent dimension, there are five hierarchical levels: system purpose, system principles, black box behavior, design representation, and physical representation (code). Each of these levels provides information about the system but at different degrees of complexity. Also in this dimension, one can do traceability from one level to another in both

directions. A second dimension, called the refinement dimension, allows one to create several design states or steps. The third dimension, the decomposition dimension, allows system designers to define boundaries such as the environment, operator, system and system components. [2]

Safeware Engineering Corporation [3] has developed an experimental toolset called Specification Tools and Requirements Methodology Requirements Language, SpecTRM_RL. This Intent Specification tool is part of ongoing research into formalizing and testing methodologies for completeness in complex software systems, spearheaded by Professor Nancy Leveson. SpecTRM addresses completeness issues including completeness with respect to mathematical theory and formal logic, and also with respect to cognitive engineering. SpecTRM attempts to establish solid design principles by working from the ground up and paying particular attention eliminating hazards from the design and incorporating Human-Machine Interface guidelines. SpecTRM also allows system designers to ensure the requirements are traced to all levels of their design. Traceability and human centered design guarantee SpecTRM's ability to contribute to creating safer designs.

The design of SpecTRM has three important objectives. The first is to determine important goals for specification languages based on experience with industrial applications. The second is to generate hypotheses about how these goals might be accomplished. The third is to make these hypotheses functional elements in the language. After the first versions of SpecTRM, the designers have come up with new concerns. Some of these include enhancing readability, eliminating error prone features, such as internal broadcast events, writing pure black box specifications, and allowing reuse and specification of program families. [4] This thesis uses the SpecTRM Version 2.3, to model one module of Raytheon's Standard Terminal Automation Replacement System (STARS).

STARS is an air traffic control system designed by Raytheon, and is responsible for managing terminal area airspace for both the FAA and the Department of Defense.

STARS can track up to 1350 airborne aircraft simultaneously within a terminal area. The system interfaces with multiple radars, 128 controller positions, 20 remote towers, and a 400 by 400 mile area of coverage. It comprises four functionally different systems: a STARS Central Support Complex (SCSC), nine Operational Support Facilities (OSFs), 9 Operations Control Centers (OCSs) and 311 Operational Sites.

The SCSC is located at the FAA Technical Center and provides for software development, testing, and field support. An OSF provides an environment that controls upgrades and modifications to the Operational Sites. It is responsible for distributing software and adaptation data to the STARS Operational Sites. Each OCC is associated with up to 80 STARS Operational Sites. It is responsible for Remote Monitoring and Control (RMC) of the associated Operational Site, and gathers and records performance data. An Operational Site has several computers connected by a dual Local Area Network (LAN) that accepts radar and flight plan data and displays aircraft movements on the Terminal Display Workstation and the Terminal Controller Workstation screens.

The goal of the air traffic control (ATC) system is to satisfy and balance the two critical goals: safety and efficiency. Human participants in the system must make continuous adjustments in flight scheduling and flight paths to maximize efficiency without compromising safety. The many redundant components in the system, and the smooth communications between its operators (both on the ground, and between ground and air) have generally allowed the ATC system to recover gracefully from failures, without accident. Because perfect system reliability can never be assumed, it is important that planners not change the ATC system in ways that will destroy these critical failure-recovery aspects.

Recently, many air traffic control functions have been automated, especially in the areas of sensing, warning, and information exchange. Generally, the attitude about these systems has been positive, but there is a concern that the human controllers lose alertness and awareness of automated functions and system functioning, which may become critical if sudden manual intervention is necessary. More importantly, humans

may distrust the automation because they fail to understand its complexities, and it is possible that reliance on automation may lead to a loss of human proficiency in the skills that the automation replaces. [5]

This thesis will provide a SpecTRM model of a subsection of STARS called Sector handoff. Sector Handoff refers to a change in aircraft controller that occurs whenever an aircraft is crossing the boundary between one controlling sector and another. [6] This thesis will also demonstrate that applying Intent Specification Languages, such as SpecTRM_RL can provide much more insight and lead to a safer design. This is a proof-of-concept demonstrating the power of SpecTRM Requirement Language. Seeing that STARS already exists, Sector handoff will only be modeled up to Level 3.

RELATED WORK

SpecTRM is a relatively new formal specification language and so there are few examples of it used to model existing systems. All of these models have been done by Professor Nancy Leveson herself, or by her students at the University of Washington and at the Massachusetts Institute of Technology.

TCAS II [7] Intent Specification, written by Professor Leveson and Jon Damon Reese, is the most expansive example of SpecTRM used to model a system. TCAS is an FAA developed airborne collision avoidance system that relies on analysis of aircraft's transponder responses to determine potential collision threats. The FAA also mandated that, as of December 30, 1991, TCAS II be standard equipment on every aircraft with more than 30 seats. The Intent Specifications for TCAS II described the system on all five levels of SpecTRM: System Purpose and Properties, System Design Principles, Black box Behavior, Physical and Logical Design Representation and Physical Implementation.

The Center TRACON Automation System (CTAS) was also modeled using SpecTRM. CTAS is a system that provides automation tools for planning and controlling arriving air traffic. CTAS generates air traffic advisories, which are aimed at increasing fuel efficiency, reducing delays, and providing automation assistance to air traffic controllers. Sean Sandys, with the assistance of Michael Shafer, Jon Reese and Professor Nancy Leveson, built the SpecTRM-RL model for CTAS. This work is described in a paper titled "A Demonstration Safety Analysis of Air Traffic Control Software." [8]

The Altitude Switch is another example of a SpecTRM model. [9] However, it is an incomplete model and does not quite completely express the altitude switch at all levels of SpecTRM. The altitude switch example was taken by Professor Nancy Leveson from an already existing specification by Steven Miller at Rockwell Collins, and which was part of a draft paper titled “Modeling Software Requirements for Embedded Systems.” [10] To Miller’s specification, Professor Leveson applied the SpecTRM modeling using a different methodology to that used by Miller.

The Software Engineering Research Laboratory has been working on two projects that apply SpecTRM software to Air Traffic Control Systems. The first of these is a Medium Term Conflict Detection (MTCD) for Eurocontrol Experimental Center (EEC). MTCD is a planning tool that will assist Controllers in identifying potential conflict situations. The goal is for early detection so that the controller has enough time to assess the severity of the situation and act accordingly to resolve the conflict. The conflicts that concern the MTCD system are aircraft conflicts, airspace conflicts, and descents below lowest usable flight level (ground proximities). Unlike many of the already applications of SpecTRM, this system is not yet functional and so this is one application of SpecTRM to the design process.

The second project of SERL is to apply SpecTRM tools to Raytheon’ Standard Terminal Automation Replacement System (STARS). SpecTRM is being applied to three modules of STARS. These modules are the Minimum Safe Altitude Warning (MSAW), Conflict Alert/Mode-C Intruder, and Sector Handoff Modules. This thesis will document the work done on the later module. In addition, William Melendez-Diaz has also created some guidelines to assist SpecTRM users and other intent specification users in distinguishing between the five levels of the specification. This, from experience, has always been extremely difficult, and the guidelines in Melendez-Diaz’s thesis, “The

Different levels of Intent Specifications: Analysis and Guidelines on Tracing,” [11] will be invaluable to anyone working with Intent Specifications.

Professor Leveson has also incorporated the use of SpecTRM in her class on System and Software Safety at the Massachusetts Institute of Technology. This past spring (2001), the class assignments included creating intent specifications for the Disney Matterhorn Roller Coaster Ride. There was also some SpecTRM modeling of the ride.

BACKGROUND

This section explains the role of Intent Specifications in designing systems by first examining the main factors that lead to aerospace accidents, describing the goals of Intent Specifications, and finally outlining the structure of an Intent Specification.

Aerospace Accident Factors

There are several factors that account for aerospace accidents. A recent study [12] by Professor Leveson and the Software Engineering Research Laboratory identified three systemic factors that have led to aircraft accidents. These are flaws in the Safety Culture, ineffective organizational structure and communication, and ineffective or inadequate technical activities.

Flaws in the Safety Culture

The Safety Culture of an industry refers to the philosophy of the people working in that industry towards ensuring that their work environment is safe and that the products they produce are able to operate safely when released. Like many other industries, the aircraft industry (though primarily focused on safety) is not without its share of flaws in its Safety Culture. There is overconfidence in automation that encourages the engineers to put the final authority in the automation rather than the pilot. For example, in Airbus aircraft, the pilot cannot disconnect the autopilot even if he applies force to the control wheel. Reports from the 1994 accident involving China Airlines A300 Flight 140 in Nagoya, Japan, recommend that Airbus considers design changes that would allow the autopilot to disconnect, and manual override functions so that crew can safely maneuver the aircraft if necessary. [12]

The commercial aviation industry is the first industry in which control of safety-critical functions by both humans and computers has been widely implemented. [12] This poses difficulty for the industry to quickly recognize and acknowledge problems associated with mode confusion and deficiencies. Because of this, it is more common to

blame the pilot for the accident than it is to investigate aspects of the system design that may have led to the human error(s). [12] Similarly, when changes are made to the automation, even if prompted by a previous accident linked to that design feature, it is not unusual for airlines to delay incorporating them into all their aircrafts. [12] This was a factor in two of the three aircraft accidents covered in Professor Leveson's paper, [12] where there was inadequate responses to prevent future loss when there are near misses and warnings. For example, in the Nagoya accident, modifications to the FMS were only recommended, as versus mandatory, and France did not issue an airworthiness directive (AD) to alert airlines to the flaw in the automation. [12]

Ineffective organizational structure and communication

Poor organizational structure and communication have led to information on many safety issues and concerns not being distributed to pilots. In the Nagoya accident, the flight crew had not been informed of similar incidents with China Airlines that had occurred prior to the accident. Also communication problems between crewmembers were cited as factors in the Nagoya accident, the 1993 accident involving Lufthansa Airbus A320 in Warsaw, Poland, and the 1995 accident involving American Airlines Flight 965, a Boeing 757-223, in California, USA.

Ineffective or Inadequate Technical Activities

The increase in the complexity of automated systems in the aviation industry has not been matched with adequate documentation of the intricacies of the design. Reports from the three accidents mentioned above noted this as a problem. [12] The Aircraft Operations Manual for the aircraft involved in the Warsaw accident contained inadequate, conflicting, or poorly designed documentation of the automatic flight systems. The Nagoya reports identify unclear descriptions of the Automatic Flight System in the Flight Crew Operating Manual. In the California accident, there were discrepancies between the display of identical data on the approach charts and on the FMS-generated displays. [12] This lack of commonality can be confusing to pilots, thus increasing their workload at critical phases of the flight. [12]

In the design process, automation designers have limited cognitive engineering resources, as research in that area, particularly that is directed at the influence of software design on human error, is still in its early stages. However, there is Human Factors research and guidelines on making the most use of the operator's time without overloading him or her at critical periods of flight or boring him or her at less critical periods. There is also research that addresses human-machine interaction with emphasis on designing displays and keyboards. The accident in California was an example of task saturation and overload, which led to distraction from the appropriate behavior. [12] Also, Human Factors research also addresses the in which the pilots are given feedback (warnings and advisories) and its effect on the way in which they process and react to the information in a crisis. The research shows that if the pilot is bombarded with warnings during an emergency, he or she will not be able to decipher which warning is more important. [12]

Professor Leveson's paper also addresses the problem that pilots are having understanding digital automation as evident from accidents, surveys and simulator studies. [12] In the California and Nagoya accidents mentioned above, the flight crew's limited understanding of the automation were factors in the accident. Both accidents show that proficient use of the FMS without adequate knowledge of the underlying logic can lead to misuse. [12] The problem arises especially when the crew encounters controls and operations that are seldom experienced in a daily flight. Professor Leveson proposes simplification of the automation so that is understandable or new training methods can combat this problem. [12]

There is also evidence of inadequate use of System and Safety Engineering in the commercial aircraft industry. [12] The inadequacy leads to poor integration of system components: software and hardware, even though both are usually thoroughly tested independently. The Nagoya accident report mentions the lack of automated protection against or nonalerting of the pilots to unsafe states. In the California accident, the pilots were not alerted to the extension of the speed brakes. [12]The use of intent specifications

at this level will assist in system integration and allow for traceability at all levels. Intent specifications would also help designers and implementers to better understand the function of each component and their interactions. This should help improve usability of systems and completeness of user manuals.

The Goals of Intent Specification

Software that correctly implements an algorithm can become ineffective once introduced into a system. This phenomenon is exacerbated when humans are brought into the system. In designing problem-solving paradigms for software, we must be mindful of the cognitive problem-solving process that occurs in the human user. Intent specifications are designed to enhance the designing process by making the human cognitive psychology, system theory, and human-machine interaction fundamental in shaping the evolution of the system design. Intent Specifications serve to integrate formal and informal aspects of software development. The formal aspect of software is limited to the mathematical and logical components. There are other non-mathematical aspects that need to be integrated into the design and Intent Specifications allow for this to happen.

Intent Specifications also improve our ability to engineer for quality and to build evolvable systems. [2] Using intent specifications allows essential system safety properties to be built into the design from the outset of the design. This early planning allows for changes to be made at one level and to be traced to all levels of the design. The rationale behind design decisions is also captured and can be traced to design decisions and implementations at all levels of the system. Design choice, based on human factors guidelines, can also be captured. Also, intent specifications help designers to achieve uniformity in the system.

The biggest advantage of Intent Specifications is that it offers system designers several ways to view the system, depending on what the designer is looking. This ability to abstract the system differently allows specific designers to ensure that their work

cascades to all levels of the system, and also that there are no conflicts in the system. Also, allowing designers different system abstractions helps them to do better problem solving. Different abstractions reflect different human limitations and capabilities, thus allowing the designers to work using an abstraction that is most suited to their own problem solving capabilities. In other words, the representations available to the problem solver can either degrade or support performance. [13]

There are four aspects that intent specifications capture. The first is a process underlying the methodology. The other three, content, structure and form, are based on cognitive psychology. Content concerns what semantic information should be in the representation given the goals and tasks of the users. Structure encompasses how to design the representation so that the user can extract the needed information. Form is simply the notation or format of the interface. These four aspects are explained in more detail in the following subsections.

Process

Process describes how a logical structure for problem solving is attained. First the need or problem the system is trying to address must be specified in terms of clear system objectives and criteria for ranking design choices. The design choices are evaluated based on the objectives and design criteria, and a decision is made as to which design choice will be implemented. The design choices result from attempts to develop system architecture. The system is sub-divided, with constraints and functions created for each sub-system. Several aspects of the subsystem are analyzed in an effort to best meet the desired performance characteristics. At the end of this process, a preliminary design evolves. This design is detailed enough so that the implementation of each sub-system can proceed independently.

The difficulty with large systems, especially automated systems, is the interfacing of the sub-systems. Many accidents in aircraft occur because subsystems do not interact well with each other. In addition, when we put the human in the loop, there are other issues with human-machine interactions as well. Therefore, Intent Specifications must also capture design decisions and map them into system goals and constraints. If this

mapping is done correctly, there will be a seamless progression from the high-level requirements to the lower level component requirements. Also the interfaces between these levels of system detail would be accurately and unambiguously specified. [2]

Content

What the system specifications will be used for and the type of problems that the human is trying to solve determine content. It is important to have a complete representation of the problem to avoid degraded system performance. Incomplete representations lead to system designers being unaware of the missing information. In many cases, the missing information is crucial to their design, and, as a result, leads to design flaws.

The content depends on the system definition and where the system boundaries are set. It is important to determine what is in the system environment, which is “a set of components (and their properties) that are not part of the system but whose behavior can affect the system state.” [2] The system state at a specific point in time is defined as “the set of relevant properties describing the system at that time.” [2] Different designers look at the system in many different ways and so it is important to have different models or specifications of the system. However all system specifications must include the following:

- System boundary
- Inputs and outputs
- Components
- Structure
- Relevant interactions between components and the means by which the system retains its integrity
- Purpose or goals of the system that makes it reasonable to consider it to be a coherent entity. [14]

In determining the system content, it is also important to record and capture the design rationale (intent). Failure to do this will result in important decisions being undone during maintenance. [2]

Structure

The content should be structured so that the user can focus on the information that is relevant to the task that he or she is trying to solve. This makes it easier for him or her to retrieve information and to describe the information thoroughly and accurately. Therefore, a specification should have as a goal, making it easy for users to extract important information.

A major consideration in determining system structure is the complexity of the system. It should always be the goal to keep things as simple as possible. However, this does not hold with the increasing complexity of systems. Therefore, there must be ways to “augment human ability.” [2] One way to do that is to provide different levels of abstraction. This allows for viewing of the problem under lower resolutions so that the import points can be gleaned and the problem addressed. To make this possible information must be presented in a coherent and structured manner.

Research shows that humans are not able to sufficiently build systems using the bottom-up approach only. The top-down approach alone is also inadequate, because there is a need for information flow in both directions. The idea of hierarchies then emerged as systems can be thought of as having several levels of complexity, with each level having “emergent” properties. An emergent property refers to a property cannot be viewed at a higher resolution (lower level). Using this hierarchal approach allows us to better understand what generates the levels, why each level differs from another and what links one level to another. In software specifications, each level provides both *what* information, while the next lower level provides the *how* information. Intent Specification must contain *why* information, which contains the design rationale and is usually omitted from hierarchies. [2]

Means-ends Hierarchies allow for goal oriented problem solving. This is because each level in the means-end hierarchy represents a different model of the system. Information at one level acts as the goals (the ends), where as information at the next lower level acts as the means. This means that means-ends abstractions provide information on *what* at any level, on *how* at the level below and *why* at the level above. Because each level describes the system in terms of a different set of attributes or “language,” [2] changes in goals will propagate downward through the levels while changes in the physical resources will propagate upward.

Form

Form refers to manner in which content is presented to the user in a specified structure. There are four steps in determining the form: defining the process to be supported, determining content, determining how to structure the content so information is easy to find, and deciding on the form of the language. The format should take into account human perceptual and cognitive strategies to ensure usability. Notation and language should be chosen so that the information is correctly and unambiguously interpreted. [2]

Intent Specifications

Intent specifications can be thought of as possessing three dimensions. The first is parallel decomposition, which separates units into components of the same type. The second dimension is called refinement. This takes a function and breaks it down into more detailed steps. The third dimension, the Intent Dimension, contains five hierarchical levels. Each level provides “why” information about the level below. There are many-to-many mappings between each level, which allows for tractability high-level system requirements and constraints down to the physical representation (code) and vice-versa. These five levels are the system purpose, the system principles, black box behavior, design representation and the physical representation (code). [2] Each level is explained in detail below.

Level 1 is the highest level of the Intent Specifications describing the system purpose. It starts by giving a general introduction to the system, along with a brief history. It then outlines the environment including all assumptions and constraints on the environment and clearly outlines the system's boundaries. Particular attention is paid to safety at this level. A hazard analysis and a fault tree are key components of this level. These are then used to state the goals, limitations, high-level functional requirements and constraints of the system that would help alleviate some of the hazards. They are also used to stipulate the human interaction with the system by describing the operator's tasks and the interface requirements.

Level 2 outlines the system design principles. At this level, the system designers use the requirements and constraints developed in Level 1 to make design decisions. These design decisions are all captured at this level. Level 2 also describes the logic and functions that are central to the system. This is done at a high-level, and so only inputs and outputs are mentioned. The interface design is also handled at this level, and all interface design decisions, again based on the hazard analysis, are noted. The final component of this level is a statement of methods that will be used to test and validate the systems operation. All simulations and experiments are described at this level.

Level 3 describes the black box behavior of the system based on the logic and functions in Level 2. For each system component, inputs and outputs are described. The interfaces between the components are also described. All internal variables are hidden at this level. At this level, the description is enough to build hardware or software to test the requirements. This allows for refinement of earlier requirements and so avoids costly changes later on in the design path. New requirements may be added or existing requirements deleted at this point. The operator tasks requirements, and detailed human-machine interfaces and message formats can be stipulated at this level.

Level 4 encompasses the physical and logical functions. The design representation surfaces at this level. This is usually in a language that is chosen by the system designer. There are details about the software design and physical requirements for the system. Hardware design specifications and communication requirements also fall

on this level. Level 4 also includes the operator manuals, and human-machine interface design. In addition, verification requirements for the design are described.

Level 5 is simply the physical realization of the system. This includes all software, hardware assembly instructions, and training and maintenance requirements.

Sector Handoff

Sector handoff refers to a change in aircraft controller that occurs whenever an aircraft is crossing the boundary between one controlling sector and another. [6] Handoff involves communication between three parties: the current controller, the next (subsequent) controller, and the pilot. STARS is only responsible for the automated system behavior and not for the human interactions with the automated system.

The STARS Full System Configuration (FSC) [15] has several rules that ensure that there is consistency in the system and that the sector handoff modules are coherent with the other modules of STARS. There are rules about the display presentation for the tracks that are defined in the adaptation data (Rules). These rules must be consistent with the default system rules as specified in the FSC. [15] They also specify that amber is the color that would be used (Handoff Color) at both the initiating and receiving TDW/TCW. It stipulates that the amount of time that each track is displayed must meet the times defined in the adaptation data. It also describes details of the tracks that are to be selected.

The FSC further describes thirteen handoff commands that include several *initiate*, *recall*, and *accept* handoff commands between the parties, a *redirect* command, and a *control acquisition* command handoff. Each command's description includes some logic, and a list of responses and error messages associated with each possible action.

1. Initiate Handoff (Implied command)
2. Recall Handoff (Implied command)

3. Accept Handoff (Implied command)
4. Take Control of Interfacility Track (Implied command)
5. Inhibit Automatic Handoff for a Flight (Implied command)
6. Accept Handoff
7. Initiate Intrafacility Handoff
8. Initiate Handoff to ARTCC
9. Initiate NAS FP Handoff to Adjacent Tracon
10. Initiate Local FP Handoff to Adjacent Tracon
11. Recall Handoff
12. Redirect Incoming Interfacility Handoff
13. Inhibit Automatic Handoff for a Flight [15]

Handoff starts when a controller requests transfer of air traffic control responsibility for a flight to another controller position either at the current site or at another facility. If the receiving position is in this STARS facility, the initiating controller enters a position identifier (ID). However, if the receiving position is a non-STARS facility or a STARS position at another site, then it uses additional alphanumeric identifiers associated with the receiver. The receiving controller may then acknowledge taking air traffic control responsibility for the flight, and send a message to the initiating controller unless the initiating controller sends a *recall handoff* message. The receiving controller may also choose to redirect the request for handoff to another facility, unless there is a *recall handoff* message from the initiating controller.

Initiate Handoff (Implied command)

This allows an air traffic controller to request transfer of responsibility for a flight from another controller position either at this site or at another facility. There are two constraints on this command:

- Only a track owned by or coupled to the entering position can be initiated for a handoff using this command.
- Tracks that have a beacon code mismatch cannot be initiated for handoff.

The receiving position now has a blinking track with a full data block that includes the entered receiving position. If the initiated track is an external facility it will not blink until the external facility acknowledges receipt of the handoff.

Recall Handoff (Implied command)

The current owner of a track can issue a *recall handoff* command to revoke the requested transfer of air traffic control responsibility for a flight. If this command is successful, the entering TCP retains responsibility for controlling the flight.

Accept Handoff (Implied command)

The receiving position indicated in the data block can issue an *accept handoff* command and thereby acknowledging air traffic control responsibility for a flight where that receiving position is the pending owner. If the command is successful, the entering TCP is now responsible for the control of the flight and the track no longer blinks. If the interfacility handoff is unsuccessful, there is a blinking “IF” in the data block. After acceptance, the track retains its FDB at the initiator’s display and the FDB is only removed when the track is selected.

Take Control of Interfacility Track (Implied command)

This command allows for transferring of air traffic control responsibility of an interfacility track to the entering position. The constraint on this command is that the entering position must be the pending owner of the track, and the track must currently be controlled by an external facility. The command cannot be used in the following circumstances:

- Tracks in handoff status
- Tracks with *blinking* indicators in field 4 of their full data blocks
- Tracks with beacon mismatch
- Departure tracks

If this command is successful then the entering TCP is now responsible for controlling the flight. The receiver’s display has two changes: the position symbol changes from “C” to the entering controller’s symbol, and the label position changes according to the rules.

Inhibit Automatic Handoff for a Flight (Implied command)

A position can use this command to prevent automatic handoff actions for a selected associated track that the position owns or is coupled to. This command is only valid if AHOP is enabled for the track, the controlling position, and this STARS site. The following are constraints on using this command:

- Tracks not owned by or coupled to the entering position
- Tracks in handoff status
- Arrival tracks
- VFR tracks
- Tracks with blinking “DM” or “IF” in their full data blocks

The result of this command, if successful, is that the specified track is inhibited from automatic handoffs (AHOP). Once inhibited, AHOP cannot be re-enabled for the track. The track’s full data block shows the *AHOP Inhibit* indicator.

Accept Handoff

This command can be issued to acknowledge taking air traffic control responsibility for a flight that has been initiated for handoff. Only the indicated receiving TCP can accept the handoff unless the command override is invoked. If successful, the entering TCP is now responsible for controlling the flight. If the interfacility handoff accept is unsuccessful, there is a blinking “IF” in the data block. The track retrains the FDB at the initiator’s display until the track is selected.

Initiate Intrafacility Handoff

This command allows for an entering position to request transfer of air traffic control responsibility for a flight to another controller position at this site. Only an owned track can be initiated for handoff unless command override is invoked. Tracks that have a beacon code mismatch cannot be initiated for handoff. If successful, the track’s data block shows the intended receiving position’s ID.

Initiate Handoff to ARTCC

This command is similar to the previous one except that it is a request transfer of air traffic control responsibility for a flight to a host or non-host ARTCC facility.

Initiate NAS FP Handoff to Adjacent Tracon

This command is again similar to the previous initiate handoff commands except that it is a request transfer of air traffic control responsibility for a flight with a NAS FP to either an ARTSIIIIE or STARS facility.

Initiate Local FP Handoff to Adjacent Tracon

This command is again similar to the previous initiate handoff commands except that it is a request transfer of air traffic control responsibility for a flight with a locally created FP to an adjacent ARTS or STARS facility.

Recall Handoff

The current owner of a track can issue a recall handoff command to revoke the requested transfer of air traffic control responsibility for a flight. Command override can be used to recall a handoff to another facility even if data communications with that facility have failed. The resulting behavior depends on the facilities involved and if a command override was used.

Redirect Incoming Interfacility Handoff

This command allows an indicated receiving TCP to change the intended receiver of an inbound interfacility handoff to another controller at this STARS site. If successful, the indicated track is shown with a full data block and begins blinking at the entered receiving position.

Inhibit Automatic Handoff for a Flight

This command prevents automatic handoffs from occurring for a specified track. If this command is executed for a track, automatic handoffs cannot be re-enabled for that track, even after the track has been handed off within this STARS site. Only an owned track can

be inhibited from automatic handoffs unless command override is invoked. There are several constraints for this command. The command cannot be executed in any of the following conditions:

- Tracks owned by another facility
- Tracks in handoff status
- Arrival tracks
- VFR tracks
- Tracks with blinking “DM” or “IF” in their full data blocks

ANALYSIS

Sector Handoff Intent Specifications

LEVEL I	39
<hr/>	
Introduction	39
Historical Perspective	39
Environment	40
<i>Description</i>	40
<i>Environment Assumptions</i>	40
<i>Environment Constraints</i>	41
High-Level Functional Goals	41
High-Level Requirements	41
System Limitations	43
Operator Tasks and Procedures	44
Human Interface Requirements and Constraints	44
Hazard Analysis	45
LEVEL II	46
<hr/>	
General Description	46
Sector Handoff Components	47
Logic	48
<i>Determine Handoff Event</i>	49
<i>Perform Handoff Action</i>	60
<i>Update Crosstell Tracks</i>	74
<i>Determine Auto Handoff</i>	77
Performance Monitoring	82
Tasks and Procedures	82
Interface	82
Testing and Validation	83
LEVEL III	84
<hr/>	
Environment	84
Sector Handoff Interface	85
Behavior Requirements	86
<i>Message Formats</i>	86

<i>State Transitions</i>	92
Software Design Requirements	98
Capacity Requirements	99

NB. Traceability between levels is indicated by up and down arrows indicating the reference to a high or lower level respectively.

Level 1

Introduction

Sector handoff refers to a change in aircraft controller that occurs whenever an aircraft is crossing the boundary between one controlling sector and another. [6] Handoff involves communication between three parties: the current controller, the next controller, and the pilot. STARS is only responsible for the automated system behavior, and not for the human interactions with the automated system. Consequently, this Intent Specification only deals with the automation and its environment.

Controllers perform handoffs of controlled flights. A controlled flight refers to a flight plan that is currently associated with a track, or that has been associated with a track at some time in the past, or is currently active as an unsupported flight. The STARS automation supports hand off between the following positions:

- Two local controllers, i.e. both controllers are in the same Terminal are (intrafacility)
- Two controllers with each controller in a different facility (interfacility)

STARS provides support for communicating with other STARS or ARTS facilities (generally referred to as TRACON facilities), and with ARTCC facilities. The controllers are capable of five actions: Handoff Initiation, Handoff Acceptance, Handoff Recall, Handoff Redirect, and Handoff Transfer. These actions ensure that a controller always has control of a flight plan during the transfer.

Historical Perspective

The FAA has predicted that there would be a 50% increase in commercial air traffic between 2000 and 2020. [16] This means that there will be added pressure to make air traffic as efficient as possible by reducing delays and congestion. Currently, commercial air carriers incur costs of about \$3 billion dollars each year due to air traffic delays.

Sector Handoff is one of the most crucial factors in reducing air traffic delay, and so it is the focus of many research efforts.

Environment

Description

The STARS automation's environment with respect to Sector Handoff consists of the following:

1. Controller Displays of both Controllers involved in the handoff
2. Position Sensing Equipment for the aircraft (GPS, or Radar)
3. Radar of both Controllers
4. Operator Input Consoles

The Radar and other sensing equipment provide input to the automation with regard to the location of the aircraft. The displays and the operator consoles provide the output to, and receive input from the automation respectively.

Environment Assumptions

[EA.1] Communications that exist between the aircraft and the controllers is of high-integrity.

[EA.2] Aircraft that have no flight plans (not being tracked by the system) will abide by FAA's Visual Flight Rules (VFR).

[EA.3] The operator will be sufficiently trained to handle emergency situations.

[EA.4] The pilot will perform actions dictated by the controller, unless there is some clear threat to the safety of the aircraft.

[EA.5] The operator will use all available information to ensure the safety of the aircraft under his or her control.

[EA.6] There will be a small but perceptible time delay between the instant an acknowledgement is received and when it will have effect.

Environment Constraints

[EC.1] There **must not** be more than 1350 tracks in the system at any time.

Rational: The system was designed to only handle a maximum of 1350 tracks.

[EC.2] The operator **must not** have any distractions while doing his or her job.

Assumption: Noise and other interference can prevent the operator from performing duties.

[EC.3] Other system components **must not** interfere with the proper functioning of the sector handoff module.

Rational: Interference from other components can undermine the job of the sector handoff component leading to hazards.

High Level Functional Goals

These goals describe the basic functionalities that Sector Handoff provides.

[G.1] The Sector Handoff Module **shall** correctly and expediently transfer control of a flight plan from one controlling sector to another at the boundary between the controlling sectors, or from one controller to another within the same sector.

[G.2] The software in this CSCI **shall** make use of defensive coding techniques to ensure that unexpected data received from external sources does not cause anomalous behavior of the subsystem.

High-Level Requirements

[HL.R1] The sender **shall** be the controller from whom control is to be transferred.

[HL.R2] The receiver **shall** be the controller to whom control is to be transferred.

[HL.R3] The initiator, recaller and acceptor **shall** be controllers who perform the initiate, recall, or accept, operations respectively. The initiator and recaller **shall** typically be the sender, while the acceptor shall be identical to the receiver.

[HL.R4] Handoffs in which the initiating controller is not the sending controller, **shall** be permitted provided the initiating controller is not the receiver.

[HL.R5] An Initiate Handoff Command **shall** request the transfer of air traffic control responsibility for a flight to another controller position either at this site or at another facility.

[HL.R6] Only a track owned by, or coupled to, the entering position **shall** be initiated for handoff using the Initiate Handoff Command.

[HL.R7] A Recall Handoff command **shall** revoke the requested transfer of air traffic control responsibility for a flight.

[HL.R8] Only the current owner of a track **shall** recall its handoff initiate action.

[HL.R9] Only the receiving position of an Accept Handoff command **shall** be able to acknowledge taking air traffic control responsibility for a flight that has been initiated for handoff.

[HL.R10] A position **shall** be able to take control of Interfacility Track thereby transferring air traffic control responsibility of an Interfacility track to itself.

[HL.R11] A position **shall** be able to inhibit automatic handoff for a flight that the position owns or is coupled to.

[HL.R12] The software **shall** support the following message types: *Flight Plan, VFR Flight Plan, Amendment, Cancellation, Request Flight Plan, Departure, Beacon Terminate, Accept/Recall Transfer, Accept Transfer, Recall Transfer, Initiate Transfer, Initiate Transfer, Track Update, Track/Full Data Block Information, Transfer Secondary Radar Targets, Transfer Primary Radar Targets, Test Data, Acceptance, Rejection, Retransmit, Data Test.*

[HL.R13] The software **shall** validate the format of the received message in accordance with the Software Requirements Specification for the RDPS. [17]

[HL.R14] The software **shall** retransmit a message to an En Route/Adjacent Terminal facility when no response to it is received within an adaptable period of time as specified in the NAS Parameters Adaptation Table, and the adaptable number of retransmissions that may be attempted due to lack of response for that message as specified in the NAS Parameters Adaptation Table has not been exceeded.

[HL.R15] The software **shall** store and update all the necessary data in accordance to the Software Requirements Specification for the Radar Data Processing System (RDPS). [17]

System Limitations

System Design Constraints (General and Safety-Related)

[HL.C1] The sender **must** be the current owner of the flight.

[HL.C2] Tracks that have a beacon code mismatch **must not** be initiated for handoff

[HL.C3] There **must** be a message dialog between two facilities participating in an interfacility handoff.

[HL.C4] In an interfacility handoff, an acknowledgement **must** be received before a controller action can take effect.

[HL.C5] A position that takes control of Interfacility Track **must** be the pending owner of the track, and the track must currently be controlled by an external facility.

[HL.C6] A position **must not** take control of a Interfacility Track in the following circumstances:

- Tracks in handoff status
- Tracks with *blinking* indicators in field 4 of their full data blocks
- Tracks with beacon mismatch
- Departure tracks

[HL.C7] A position **must not** inhibit automatic handoff for a flight in the following circumstances:

- Tracks not owned by or coupled to the entering position
- Tracks in handoff status
- Arrival tracks
- VFR tracks
- Tracks with blinking “DM” or “IF” in their full data blocks

[HL.C8] AHOP **must** be enabled for the track, the controlling position, and this STARS site, before a position is able to inhibit automatic handoff of a flight it owns or is coupled to.

HL.C9] A position **must not** inhibit automatic handoffs of a flight if any of the following conditions are true:

- Tracks owned by another facility
- Tracks in handoff status
- Arrival tracks
- VFR tracks
- Tracks with blinking “DM” or “IF” in their full data blocks

[HL.C10] The software **must** respond only to valid inputs.

[HL.C11] Sub functions **must not** be able to execute when system is in standby.

[HL.C12] The software **must** respond to valid inputs in an adaptable time period, which is stipulated in the Software Requirements Specification for the Radar Data Processing System (RDPS). [17]

Operator Tasks and Procedures

The CSCI has no operator interface and, therefore has no operator tasks or procedures.

Human Interface Requirements and Constraints

These requirements were extracted from the RDPS. [17]

[HI.R1] The display presentation for tracks in an active Handoff **shall** be consistent with the definition in adaptation data (Rules), and also consistent with the description in this section for handoff is consistent with the default Rules. [17]

[HI.R2] *Preview response time* begins with input device activation (keyboard stroke or Touch Input Device touch) and ends with the display of the entered symbol.

This is a 95th percentile requirement.

[HI.R3] *Message acknowledge time* **shall** be defined as the time for the subsystem to acknowledge that it has accepted and is processing the entered message.

This time begins with the entering action and ends with the complete receipt of the subsystem acknowledgement. Completion of the entering action is when the operator selects “OK”, “ENTER”, “EXIT”, or “CONFIRM” buttons from a dialog box, selection of a menu option or the “ENTER/RETURN” key. Acknowledgement consists of: (1) a response message in the command response area of a dialog box, (2) the display of another window, menu or dialog box, or (3) the removal of a window, menu or dialog box. This is a 95th percentile requirement.

[HI.R4] *Message response time shall be defined as the time required for the complete processing of an accepted message.*

It begins with the completion of the entering action, includes the error or validity check portion of the message acknowledge processing and ends with the completion of all relevant responses. This requirement applies solely to transactions entered manually from a data entry device that is connected directly to the system.

[HI.R5] All displays shall follow rules given in the Software Requirements Specification for the Radar Data Processing System (RDPS). [17]

Hazard Analysis

This section lists the potential hazards associated with Sector Handoff.

[H.1] A flight becomes unsupported during a Sector Handoff.

[H.2] Tracks involved in a Handoff have a beacon code mismatch even though they are of the correct track type.

[H.3] Unauthorized track owners are able to perform Handoff commands with tracks that are not theirs.

[H.4] Tracks in Handoff Status are able to perform illegal commands, e.g. Take Control, or Inhibit Automatic Handoff Commands.

Level II

General Description

There are 5 possible Controller actions. They are:

1. *Handoff Initiation*. This causes an indication to be presented to the receiver that control is being offered for a flight.
2. *Handoff Acceptance*. This causes control to be acquired by the receiver.
3. *Handoff Recall*. This negates or cancels a handoff initiation.
4. *Handoff Redirect*. This operation is on an incoming external handoff, which changes the handoff receiver so that a different controller would receive the flight plan.
5. *Transfer*. This is initiated by Automatic Handoff or by a Take Control handoff request that requests that a flight is reassigned to a specified receiving controller. This only occurs in an atomic procedure in intrafacility handoff receivers.

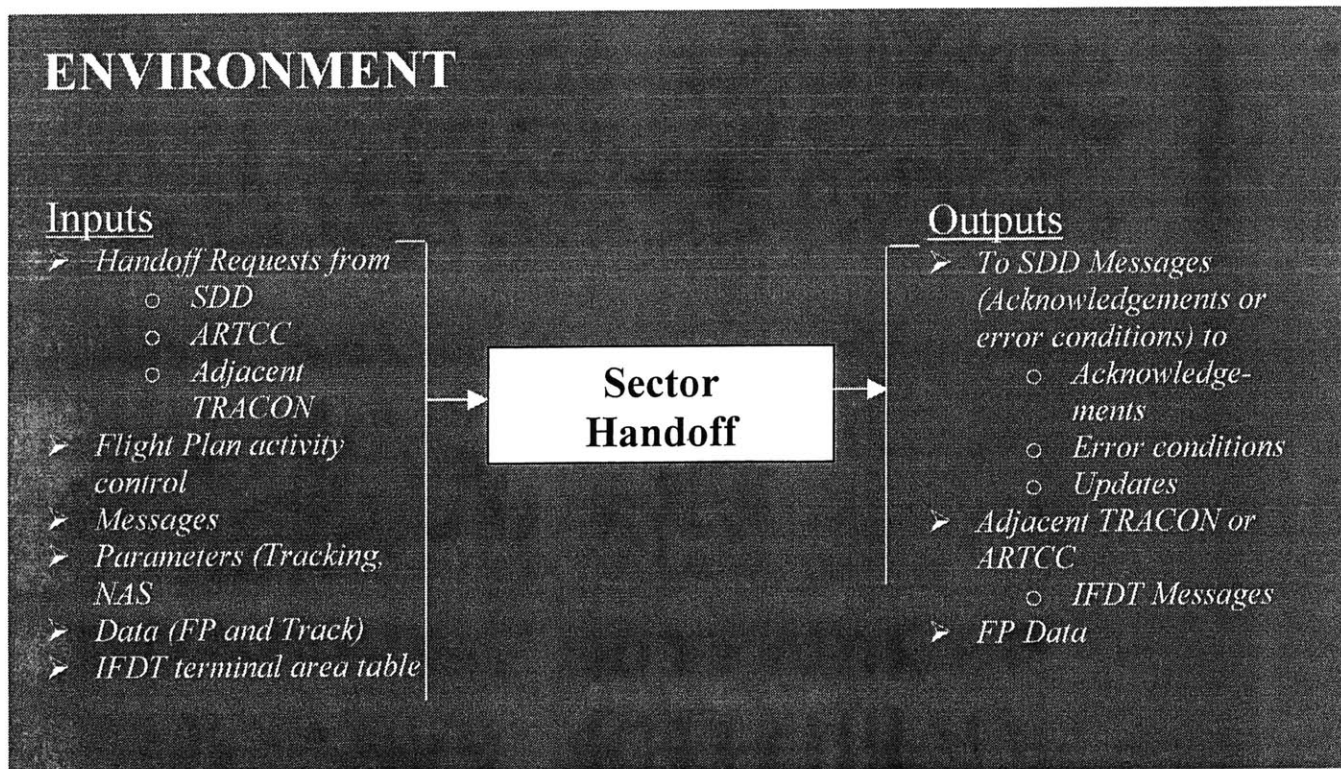


Figure 1: Diagram of Environment

Sector Handoff Components

There are two types of Sector Handoff: Interfacility Handoff, and External Facility Owned (EFO) Handoff. The Sector Handoff component has four main modes:

1. Determine Handoff Event
2. Perform Handoff Action
3. Update Crosstell Tracks
4. Determine Auto Handoff

Determine Handoff Event is responsible for interpreting:

- Handoff requests from the SDDs
- Handoff messages originating from automatic handoff processing
- Interfacility handoff messages originating from an ARTCC or TRACON (ARTS or STARS) facility (forwarded by the Manage IFDT messages function).

Perform Handoff Action processes requirements for each of a set of handoff actions. Actions are defined for Events (generated by the Determine Handoff Events Function) and Handoff States as shown in Figures 2 and 3. Actions also appear in the Control Specification. Handoff actions are broken into three groups:

- *Outbound Handoff Actions* – these are involved in handoff to other facilities, including recall of a handoff previously initiated by the local facility.
- *Inbound Handoff Actions* – There are involved in handoff from other facilities, including recall of a handoff previously initiated by the remote facility.
- *Local Handoff Actions* – There involve no interfacility dialog for any transition.

Update Crosstell Tracks describes the requirements for the interfacility track updating mechanism using the transmission of Track Update (TU) messages between TRACON and ARTCC Facilities for aircraft in Handoff.

Determine Auto Handoff discusses the requirements for monitoring the controlled tracks in the system to determine whether automatic handoff of flights can be performed, and

also to provide an indication of when automatic interfacility handoff will occur. Adaptation data and TCP input defines when and if initiation of automatic handoffs should be performed.

Logic

Sector Handoff Logic

General Principles

[2.1] The RDPS software will coordinate all handoff requests. (↑ G1) [2.1.1] All requests are from the SDDs, ARTCC or adjacent TRACON facilities, and automatic handoff initiation processing. (↑ Level 1: Introduction) [2.1.2] Output may be sent to the SDDs, ARTCC, or TRACON facilities (via the terminal area's host ARTCC). (↑ Level 1: Introduction)

SDDS

[2.1.3.1] The responses to the SDD actions will be sent to the SDDs to acknowledge the action and report any error conditions that may occur. (↑ HL.R9, HL.C4, HL.C9)

[2.1.3.2] Label Update Messages will be sent to the SDDs to update Pseudo-Track FDBs. (↑ HL.R9, HL.R12, HL.R15, HL.C3)

[2.1.3.3] Updates to Flight Data in the RDPS will result in the SDD copy of that data being updated. (↑ HL.R15, HL.C3)

[2.1.4] Message interchange with adjacent facility (↑ HL.C3)

[2.1.4.1] Handoffs between this STARS and an adjacent TRACON facility, all related messages are exchanged via the terminal area's host ARTCC. (↑ Level 1: Introduction, HL.C3)

[2.1.4.2] If the source or ultimate destination is an adjacent TRACON, messages will be relayed by the ARTCC. (↑ Level 1: Introduction, HL.C3)

[2.1.4.3] In the remainder of the Process Handoffs section, the ultimate source or destination will be referenced rather than the facility to which the message is intermediately transmitted. (↑ HL.R2, HL.C3)

[2.1.4.4] Communication with an ARTCC or another TRACON is done via the Manage IFDT Messages Function by sending IFDT Output requests and receiving NAS Handoff Messages. (↑ HL.C3)

Determine Handoff Event Logic

[2.2] The interpretation process for this module involves validating messages against current RDPS Flight and Track data and adaptation data, and if the message is valid, determining the event that has occurred or has been implied. (↓ 3.2) [2.2.1] Events can either be interpretive (in the case of most controller inputs) or explicit (as in the case of most interfacility messages). (↑ Level 1: Introduction) [2.2.2] Events are used along with the State Transition Diagram to derive required Actions. (↓ Figure 3) These Actions are specified in the Perform Handoff Action function:

- Handoff Receiver Determination
- Event Determination
- Handoff Request from the SDD
- NAS Handoff Messages
- Transmission of NAS messages
- Automatic Handoff Processing
- Handoff Completion Timer
- IFDT Mode Transition
- Validation
- Standby Processing Differences

Handoff Receiver Determination

[2.2.3] The handoff receiver will be derived from the field in the input message or from the Flight Plan as follows: (↓ 3.2, Figure 3)

[2.2.3.1] The CJI is specified in the Handoff request from the SDD or in the Initiate Transfer Message (TI) from the ARTCC or adjacent TRACON **shall** be used as the destination CJI for the handoff, unless the specified position is consolidated.

(↑ HL.R3)

[2.2.3.2] In the case of consolidation of a position with the CJI specified in the Handoff request from the SDD or in the Initiate Transfer Message (TI) from the ARTCC or adjacent TRACON, the consolidated position **shall** be used as the destination CJI.

(↑ HL.R4)

[2.2.3.3] The CJI of the receiver **shall** be set to pending if the CJI of the receiver is not specified in the Initial Transfer message (TI) from the ARTCC of adjacent TRACON.

(↑ HL.R4)

[2.2.3.4] The CJI of the receiver **shall** be set to the adapted receiving CJI (or the CJI of the position it is consolidated to) determined by satisfying all the conditions listed below, if the CJI of the receiver is not specified in the Handoff request from an SDD. (↑ HL.R4)
The conditions are:

- a) The flight is in a handoff filter.
- b) The configuration plan currently in use for the flight plan's terminal area matches an adapted configuration plan for the handoff filter.
- c) The flight plan's owning controller matches an adapted owning controller for the handoff filter.
- d) The flight plan's type of flight matches an adapted type of flight for the handoff filter.
- e) The flight plan's entry fix matches an adapted entry fix for the handoff filter.
- f) The flight plan's exit fix matches an adapted exit fix for the handoff filter.
- g) The flight plan's requested level is within the adapted requested level band for the handoff filter.

- h) The flight plan's owning control does not match the adapted receiving controller for the handoff filter.
- i) If the flight is in more than one handoff filter, all filters will be considered until the first valid receiving CJI is determined (if any).
- j) The primary CJI of the next CJS (or the CHI of the position it is consolidated to) in the converted route **shall** be used (if none, the handoff will be invalid), if no receiving DJI is determined and the handoff request is automatic.

[2.2.3.5] The CJI of the receiver will be specified in the *Auto Handoff Initiate Request* from the Determine Auto Handoff process and will be used as the destination CJI for the handoff, unless the position is consolidated in which case the position with which it is consolidated will be used as the destination CJI. (↑ HL.R2, HL.R6; → 2.5)

[2.2.3.6] In the case of Pointout-Handoff, the CJI of the receiver will be specified in the request. (↑ HL.R2; ↓ 3.2.1)

[2.2.3.7] In the case of an EFO-Handoff, the CJI of the receiver will be specified in the Handoff request. This CJI will be used as the destination CJI for the EFO Handoff, unless the position is consolidated in which case the position with which it is consolidated will be used as the destination CJI. (↑ HL.R2, HL.R6; ↓ 3.2.1, 3..2.13)

Event Determination

[2.2.4] This is a function of the input request and the current Handoff State of the flight plan. (↓ 3.2) There are three groups:

[2.2.4.1] Outbound Handoffs – Interfacility handoff dialog associated with handoff to an ARTCC or adjacent TRACON. This includes recall of an earlier handoff to an adjacent facility. (↓ 3.2.1, 3.2.2)

[2.2.4.2] Inbound Handoffs – Interfacility handoff dialog associated with handoff from an ARTCC or adjacent TRACON. This includes recall of an earlier handoff to an earlier facility. (↓ 3.2.1)

[2.2.4.3] Local Handoffs – Handoff or EFO Handoffs between positions within the local STARS terminal area. (↑ Level 1: Introduction)

Handoff Request from the SDD

[2.2.5] A valid handoff request will result in a Handoff Event as follows:

Type of Handoff Event	Conditions
[2.2.5.1] Initiate Local Handoff Event	When handoff request is interpreted as <i>Initiate</i> , the current owner is local and Handoff Receiver CJI is within the facility. (↑ HL.C1; ↓ 3.2.1, 3.2.3)
[2.2.5.2] Recall Local Handoff Event	When Handoff State is <i>Handoff Int</i> and handoff request is interpreted as <i>Recall</i> (↑ HL.C7; ↓ 3.2.11)
[2.2.5.3] Accept Local Handoff Event	When Handoff State is <i>Handoff Int</i> and handoff request is interpreted as <i>Accept</i> . (↑ HL.R3; ↓ 3.2.11)
[2.2.5.4] Initiate External handoff	When handoff request is interpreted as <i>Initiate</i> , the current owner is local and Handoff Receiver CJI is within the adjacent facility, and the Flight Plan is a remote En Route Flight Plan. (↑ HL.R3)
[2.2.5.5] Initiate External Handoff	When handoff request is interpreted as <i>Initiate</i> , the current owner is local, Handoff Receiver CJI is an adjacent TRACON, and the Flight Plan is a Local Flight Plan. (↑ HL.R3; ↓ 3.2.1, 3.2.2)
[2.2.5.6] Recall External Handoff	When Handoff State is <i>Handoff Ext To</i> , handoff request is interpreted as <i>Recall</i> and the Force Option is not selected. (↑ HL.R7; ↓ 3.2.6)

<p>[2.2.5.7] Force Recall External Handoff</p>	<p>When Handoff State is <i>Handoff Ext To</i>, handoff request is interpreted as <i>Recall</i> and the Force Option is selected. (↑ HL.R7; ↓ 3.2.6)</p>
<p>[2.2.5.8] Accept External Handoff</p>	<p>When Handoff State is <i>Handoff Ext From</i>, handoff request is interpreted as <i>Recall</i> and the Force Option is not selected. (↑ HL.R3; ↓ 3.2.6)</p>
<p>[2.2.5.9] Force Accept External Handoff</p>	<p>When Handoff State is <i>Handoff Ext From</i>, handoff request is interpreted as <i>Recall</i> and the Force Option is selected. (↑ HL.R3; ↓ 3.2.8)</p>
<p>[2.2.5.10] Redirect External handoff</p>	<p>When Handoff State is <i>Handoff Ext From</i>, handoff request is interpreted as <i>Recall</i> and a Handoff Receiver CHI is included in the command. (↑ HL.R3; ↓ 3.2.8)</p>
<p>[2.2.5.11] Take Control</p>	<p>When a handoff request indicates <i>Take Control</i> and the requesting controller is, or is coupled to, the pending owner and the current owner is an external facility, the handoff request is a <i>Take Control</i> request. (↑ HL.R10; ↓ 3.2.1)</p>
<p>[2.2.5.12] Initiate EFO- Handoff</p>	<p>When the handoff request is interpreted as <i>Initiate</i> and the current owner is an external facility. (↑ HL.R3; ↓ 3.2.1, 3.2.3)</p>
<p>[2.2.5.13] Recall EFO- Handoff</p>	<p>When the handoff request is interpreted as <i>Recall</i> and the Handoff State is <i>EFO Handoff Int</i>. (↑ HL.R7; ↓ 3.2.4, 3.2.6)</p>
<p>[2.2.5.14] Accept EFO- Handoff</p>	<p>When the handoff request is interpreted as <i>Accept</i> and the Handoff State is <i>EFO Handoff Int</i>. (↑ HL.R3; ↓ 3.2.1-3.2.3, 3.2.5-3.2.7)</p>

Table 1: Handoff Events and Conditions

NAS Handoff Messages

[2.2.6] The resulting Handoff Event will most likely be unique to the message type received or the message type being responded to together with the nature of the response (Accept or Reject/Fail, in parentheses below). (↑ HL.R3; ↓ 3.2) [2.2.6.1] Valid inputs will result in one of the following Handoff Events:

1. TI/TM Initiate
2. TA/TL Recall
3. When a TA message is received, it will result in a TA/TL Recall event only if Handoff State is *Handoff Ext From*. A TL message will only be valid if Handoff State is *Handoff Ext From*.
4. TA/TN Accept
5. When a TA message is received, it will result in a TA/TN Accept event only if Handoff State is *Handoff Ext To* or *Handoff Initiate Pending*. A TN message will only be valid for those Handoff State values.
6. TI/TM Response (Accept)
7. TI/TM Response (Reject/Fail)
8. TA Response (Accept)
9. TL Response (Accept)
10. TA/TL Response (Reject/Fail)
11. TA/TN Response (Accept)
12. TA/TN Response (Reject/Fail)
13. FP Response (Accept)
14. FP Response (Reject/Fail)
15. CX Response

Transmission of NAS messages

[2.2.7] The software will acknowledge retransmissions of the following messages from ARTCC and adjacent TRACON facilities: (↑ HL.R14)

[2.2.7.1] TA/TN/TL messages – A received message of this type will be treated as a retransmission if the following conditions apply:

1. Handoff state is *Outbound HO Accepted* or *Not in Handoff* (↓ 3.2.2)
2. The flight plan is referenced in the message is owned by the facility sending the message. (↓ 3.2.4)
3. The message source id matches the previous message. (↑ HL.C10)

[2.2.7.2] TI/TM – A received message of this type will be treated as a retransmission if the following conditions apply: (↑ HL.R14)

1. Handoff state is *Handoff Ext From*. (↓ 3.2.1)
2. The message is received from the same facility that sent the original TI/TM. (↓ 3.2.2)
3. The message Source id matches the previous message. (↑ HL.C10; ↓ 3.2.2)

Automatic Handoff Processing

[2.2.8] The Determine Auto Handoff process sends out *Auto Handoff* requests for a specified aircraft. (→ 2.5) The initiation request will result in a Handoff event as follows:

1. **[2.2.8.1]** Initiate External Handoff (↑ HL.R3; ↓ 3.2.1)

When Handoff Receiver CJI is an adjacent facility, and the flight plan is a remote En Route flight plan.

2. **[2.2.8.2]** Initiate Local Handoff (↑ HL.R3; ↓ 3.2.1)

When handoff request is interpreted as Initiate and receiver is local.

3. **[2.2.8.3]** Accept Local handoff (↑HL.R3; ↓ 3.2.11)

When Handoff State is Handoff Int and the handoff request is interpreted as Accept.

4. [2.2.8.4] Transfer (↓ 3.2.1)

When the handoff request specifies transfer.

Handoff Completion Timer

[2.2.9] The Perform Handoff Action process sends out *Complete HO* requests for a specified flight to indicate that the deletion timer has expired and that the handoff can be completed (i.e. removed from the sender's and receiver's displays). (↑ G2) The request will result in a handoff event as follows:

1. [2.2.9.1] External HO Accepted Timeout (↓ 3.2.5)

When Handoff State is Outbound HO Accepted or Inbound HO Accepted.

2. [2.2.9.2] Local HO Accepted Timeout (↓ 3.2.12)

When Handoff State is Local HO Accepted

3. [2.2.9.3] External message response timer (↓ 3.2.4)

Timeout Response request for a specified flight will be received from the Perform handoff Action process, to indicate that the time allowed for a response from an external facility has expired and no response has been received. The handoff state for the flight is reverted to the state it had prior to its current pending state. The request will result in the Handoff event 'External Response Timeout'.

4. [2.2.9.4] EFO-HO Accepted Timeout (↓ 3.2.14)

When the handoff state is EFO_HO Accepted.

IFDT Mode Transition

[2.2.10] The software **shall** generate Handoff events as shown below when the Manage IFDT Messages process sends an IFDT mode transition indicating that an ARTCC has the FDP mode enabled. (↑ G2)

1. [2.2.10.1] Force Recall Outbound Handoff (↓ 3.2.6)

For each flight currently in handoff to the ARTCC, or to an adjacent TRACON via the ARTCC (Handoff state is Handoff Ext To).

2. [2.2.10.2] Force Accept Inbound Handoff (↓ 3.2.8)

For each flight which is in handoff from the ARTCC, or from an adjacent TRACON via the ARTCC (Handoff state is Handoff Ext From).

Validation

[2.2.11] Any NAS Handoff message received that is invalid **shall** cause a rejection response in an IFDT output request to be sent and the message will not be processed.

(↑ HL.C10)

[2.2.11.1] Any SDD handoff request received which is invalid **shall** cause a rejection response in an Operator Controller entry error to be sent to the requesting SDD and the request will not be processed. (↑ HL.C10)

[2.2.11.2] Handoff Requests/message will be validated as described below.

[2.2.11.2.1] General Validation (↑ HL.C10)

The software **shall** reject handoff requests/NAS handoff messages if any of the following apply:

1. The message/request does not reference a Flight Plan that exists in the RDPS.
2. The referenced flight is not in a Handoff State for which a transition is defined for the Handoff Event in the State Transition Diagram.

[2.2.11.2.2] Initiate Requests (↑ HL.C10)

The software **shall** reject handoff initiation requests if any of the following apply:

[2.2.11.2.2.1] *Local*

- a) The referenced flight plan is unassociated and is not active as an unsupported flight. (↑ EA.2)
- b) The referenced flight plan is associated with a track and the reported beacon code differs from the assigned beacon code. (↑ HL.C2)
- c) For an initiate Local EFO Handoff, the handoff receiver CJI is not within the same terminal area as the TCP issuing the handoff command. (↑ Level 1: Introduction)
- d) The referenced flight is in the suspend state. (↑ HL.C10)

[2.2.11.2.2.2] *Inbound* (↑ HL.C3, HL.C10)

- a) The flight is an overflight and the system-wide overflight rejection option parameter is set in NAS parameters adaptation data.
- b) The flight in the *Initiate Transfer* (TI/TM) message is a departure flight.
- c) The flight in the *Initiate Transfer* (TI/TM) message from an adjacent TRACON is already owned by this facility.
- d) The *Initiate Transfer* (TI/TM) message is received from an ARTCC (or routed via an ARTCC), which is in flight data processing mode, as determined from the IFDT terminal area table.
- e) The routing information in the *Initiate Transfer* (TI/TM) message from an ARTCC or adjacent TRACON does not match adapted STARS values.
- f) The velocity contained within an *Initiate Transfer* (TI/TM) message from an ARTCC or adjacent TRACON is not within system-wide adaptable limits defined in NAS parameters adaptation data. [17]
- g) The track coordinates contained in an *Initiate Transfer* (TI/TM) message from an ARTCC or adjacent TRACON are not within adaptable limits, which

define the STARS radar mosaic, as defined in System parameters adaptation data. [17]

- h) The flight in the *Initiate Transfer* (TI/TM) message is already in handoff from another facility.
- i) There is a departure flight with the same ACID and beacon code as the arrival flight being handed off and the departure flight is under STARS control.
- j) There is another active flight with the same ACID as the flight being handed off except if the flight pair is part of a Round Robin. [17]
- k) The *Initiate Transfer* message is received from an adjacent TRACON not adapted for the transfer of Non-En Route flight plans.

[2.2.11.2.2.3] Outbound (↑ HL.C10)

- a) The flight is an overflight and the system-wide overflight rejection option parameter is set in NAS parameters adaptation data.
- b) The referenced flight plan is not associated with a track.
- c) The receiving facility is an ARTCC or adjacent TRACON, and the ARTCC is in flight data processing mode, and defined in IFDT terminal area data.
- d) The receiving facility is an ARTCC, and the flight plan did not originate in that ARTCC.
- e) The flight's reported beacon code differs from its assigned beacon code.
(↑ HL.C2)
- f) Interfacility communication is currently disabled.
- g) The referenced flight is in the suspended state.

Accept Requests

[2.2.12] The software **shall** reject handoff accept requests if any of the following apply: (↑ HL.C10)

- a) [2.2.12.1] For an Accept External handoff action, the referenced flight plan's radar or pseudo track's position is outside the adapted coverage distance (from the Radar Parameters adaptation) of the prime sensor associated with the terminal area (from the IFDT Terminal Area adaptation).
- b) [2.2.12.2] The routing information in the Accept Transfer (TA/TN) message from an ARTCC or adjacent TRACON does not match adapted values.

Transfer Requests

[2.2.13] The software **shall** reject transfer requests if the following applies:

- a) The referenced flight is in handoff. (↑ HL.R14, HL.C10)

Standby Processing Differences

[2.2.14] In the standby RDPS, the Determine Handoff Event sub function will be dormant. (↑ HL.C11)

Perform Handoff Action Logic

[2.3] The three types of Handoff Actions are Outbound Handoff, Inbound Handoff and Local Handoff Actions.

Perform Outbound HO Step

[2.3.1] There are different processing requirements for each of the following handoff Actions associated with the handoff of flights to other facilities:

- Launch Outbound Handoff
- Establish Outbound Handoff
- Cancel Outbound Handoff

- Launch Non-En Route RP
- Complete Outbound Handoff
- Clear Outbound Handoff Indicators
- Launch Recall Outbound Handoff
- Complete Recall Outbound Handoff
- Cancel Recall Outbound Handoff
- Launch Non-En Route CX
- Force Recall Outbound Handoff

[2.3.1.1] Launch Outbound Handoff

1. An IFDT output request **shall** be sent to the *Manage IFDT Messages* function containing an Initiate Transfer (TI/TM) message for transmission to the receiving facility. (↑ HL.C3)

If the Flight Plan is a remote En Route flight plan, the TI form of the message will be sent, otherwise the TM form will be used. (↓ 3.2)

2. Handoff state for the flight will be set to *Handoff Initiate Pending*. (↓ 3.2)
3. A timer is started for an adaptable time period and is incremented while in this handoff state. When the timer expires, a *Timeout Response* request is sent to the *Determine Handoff Event Process*. (↑ HL.C12)
4. If an active pointout exists from the handoff sender, the pointout will be removed. (↓ 3.2)

[2.3.1.2] Establish Outbound Handoff

1. The following actions **shall** be performed to indicate that the Handoff Initiate request has been accepted by the external facility:
 - a. Handoff state for the flight will be set to *Handoff Ext To*. (↓ 3.2.1)

2. The controller identifier from Field 71 in the *Data Accept* (DA) message (if included) **shall** be stored in the Flight Plan record. (↑ HL.R15)

[2.3.1.3] Cancel Outbound Handoff

1. Handoff state for the flight will be set to *Not in Handoff*. (↑ 3.2.5)
2. The Interface *Handoff Error Status* indicator will be set in the flight plan:
 - a) If initial Handoff state for the flight is *Handoff Initiate Pending*, *Handoff Error Status* indicator will be set to indicate that the Initiate request (TI/TM) was rejected. (↓ 3.2.2)
 - b) If initial Handoff state for the flight is *Non-En Route FP Pending*, *Handoff Error Status* indicator will be set to indicate that the FP message was rejected. (↓ 3.2.2)
3. If Handoff state was *Handoff Initiate Pending* and the flight plan is Non-En Route (a TM failed or was rejected), an IFDT output request **shall** be sent to the Manage IFDT Message function containing a Cancellation (CX) message for transmission to the receiving TRACON facility. (Note: Any failure of this message will be ignored). (↑ HL.C3; ↓ 3.3.2)

[2.3.1.4] Launch Non-En Route RP

1. An IFDT output request **shall** be sent to the *Manage IFDT Messages* function containing a Flight Plan (FP) message for transmission to the receiving TRACON facility. (↑ HL.C3; ↓ Figure 3)
2. Handoff state for the flight will be set to *Non-En Route Handoff Pending*. (↓ 3.2.1)
3. A timer is stated for an adaptable period and is incremented while in this handoff state. When the timer expired, a *Timeout Response* request is sent to the *Determine Handoff Event* Process. (↓ 3.3.3)

[2.3.1.5] Complete Outbound Handoff

1. The following actions **shall** be performed to complete the handoff: (↓ 3.2.6)

- a) An IFDT output request will be sent to the *Manage IFDT Messages* function containing an *Acceptance* (DA) response for transmission to the receiving facility. (↓ Figure 3)
 - b) Handoff state for the flight will be set to *Outbound Handoff Accepted*.
(↓ 3.2.6)
 - c) A timer is started for an adaptable time period, and is incremented while in this handoff state. When the timer expires, a *Complete HO* request is sent to the *Determine Handoff Event* process. (↑ HL.C12)
 - d) A Handoff route update request will be sent to the *Assign Sectors* function for the purpose of updating the flight plan's progress along the route and determining the new flight plan controller. (↑ HL.C15)
2. If Handoff state was *Handoff initiate Pending*, a *TA/TN* message **shall** be interpreted as the acknowledgement to a *TI/TM Initiate* message, in place of a DA under the following circumstances: (↑ HL.C3)
- The TA/TN was received before a NAS response message to the TI/TM indicating acceptance, rejection or transmission failure. (↑ HL.C10)
- 3. The contents of Field 48 in the *Transfer Accept* message (if included) **shall** be stored in the Flight Plan record. (↑ HL.R15)
 - 4. If the TA message contains a beacon code, the beacon code will be stored in the flight plan. (↑ HL.R15)

[2.3.1.6] Clear Outbound Handoff Indicators

- 1. Handoff state for the flight will be set to *Not in Handoff*. (↓ 3.2.5)

[2.3.1.7] Launch Recall Outbound Handoff (↓ 3.2.6)

- 1. The recall **shall** only occur if the ARTCC or adjacent TRACON has not sent an *Accept Transfer (TA)* message. (The state transition diagram implies this). (↑ HL.C3)
- 2. An IFDT output request **shall** be sent to the *Manage IFDT Messages* function containing a *Recall Transfer (TA/TL)* message for transmission to the receiving

facility. If the Flight Plan is a remote En Route flight plan, the TA form of the message will be sent, otherwise the TL form will be used.

(↑ HL.C3; ↓ Figure 3)

3. Handoff state for a flight will be set to *Handoff Recall Pending*. (↓ 3.2.6)
4. A timer is started for an adaptable time period, and is incremented while in this handoff state. When the timer expires, a *Timeout Response* request is sent to the *Determine Handoff Event* process. (↑ HL.C12)

[2.3.1.8] Complete Recall Outbound Handoff

1. The following actions **shall** occur to remove the flight from handoff:
 - a) Handoff state for the flight will be set to *Not in Handoff*. (↓ 3.2.4)

[2.3.1.9] Cancel Recall Outbound Handoff

1. Handoff state for the flight will be set to *Handoff Ext To*. (↓ 3.2.7)
2. The Interface *Handoff Error Status* indicator will be set in the flight plan.
(↑ HL.R15)

[2.3.1.10] Launch Non-En Route CX

1. [2.3.1.10.1] The following actions **shall** be performed:
 - a) Handoff state for the flight will be set to *Non-En Route CX Pending*.
(↓ 3.2.7)
 - b) An IFDT output request is sent to the *Manage IFDT Messages* function containing a *Cancellation (CX)* message for transmission to the receiving TRACON facility. (↓ Figure 3)
2. [2.3.1.10.2] A timer is started for an adaptable time period and is incremented while in this handoff state. When the timer expires, a *Timeout Response* request is sent to the *Determine Handoff Event* process. (↑ HL.C12)

[2.3.1.11] Force Recall Outbound Handoff

1. The recall **shall** only occur if the ARTCC or adjacent TRACON has not sent an *Accept Transfer (TA)* message. (The state transition diagram implies this).
(↑ HL.R7; ↓ 3.2, Figure 3)
2. If the Flight Plan is a remote En Route Flight Plan, an IFDT output request **shall** be sent to the *Manage IFDT Messages* function containing a *Recall Transfer (TA)* message for transmission to the receiving facility, indicating that any acknowledgement received to this message should be discarded. (↓ Figure 3)
3. If the Flight Plan is a local Non-En Route Flight Plan and if RDP mode is enabled for the ARTCC< as IFDT output request **shall** be sent to the *Manage IFDT Messages* function containing a *Recall Transfer (TL)* message for transmission to the receiving facility, indicating that any acknowledgement received to this message should be discarded. (↑ HL.C3; ↓ Figure 3)
4. If the Flight Plan is a local Non-En Route flight plan and if RDP mode is enabled for the ARTCC, an IFDT output request **shall** be sent to the *Manage IFDT Message* function containing a *Cancellation (CX)* message for transmission to the receiving TRACON facility, indicating that any acknowledgement received to this message should be discarded. (↑ HL.C3)
5. The Interface *Handoff Error Status* indicator will be cleared in the flight plan.
(↑ HL.R15)
6. All the processing described above for the *Complete Recall Outbound Handoff* action will be performed. (↑ G1)

Perform Inbound HO Step

[2.3.2] Below are the processing requirements for each of the following handoff Actions associated with the handoff of flights from other facilities:

- Setup Inbound Handoff

- Undo Inbound Handoff
- Launch Accept inbound Handoff
- Cancel Accept Inbound Handoff
- Complete Accept Inbound Handoff
- Clear inbound Handoff Indicators
- Force Accept Inbound Handoff
- Redirect Inbound Handoff

Setup Inbound Handoff

[2.3.2.1.1] On receipt of an *Initiate Transfer (TI/TM)* message, the following actions **shall** be performed:

- a. Handoff state for the flight plan referenced in the TI message will be set to *Handoff Ext Form.* (↓ 3.2.1)
- b. The X/Y Coordinates and X/Y velocities from NAS Filed 23 are stored in the flight plan. (↑ HL.R15)
- c. An *Inbound Handoff Setup Route Update Request* will be sent to the *Update Route* function to establish or update Current CJI. If the *TI/TM* message contained a Field 13, the Current CJI sent will be that of the originating facility contained in Field 13, otherwise the CJI of the facility that originated the *TI/TM* message, contained in Field 00, will be sent. (↑ HL.C3)
- d. The controller identifier from Field 13 (if included) will be stored in the Flight Plan record. (↑ HL.R15)

[2.3.2.1.2] An IFDT output request **shall** be sent to the *Manage IFDT Messages* function containing an *Acceptance Response (DA)* message for transmission to the initiating ARTCC or TRACON facility. If and only if the initiate request contained a Field 13, the DA will contain the receiver's CJI in NAS Field 71, will the DA contain the receiver's CJI in HAS Field 71. (↑ HL.C3)

[2.3.2.1.3] If the triggering *Initiate Transfer (TI)* message contains a NAS Field 41 (Handoff Code) and the Handoff Code is different to the flight plan's assigned code, then the software **shall** perform the following:

- a) Then hand off Code will be assigned in the flight plan referenced by the *TI* message, as described in the SSR Code Table Maintenance section of the *Manage Flight Plans* function. [17] (↑ G1)
- b) If the Flight is associated and the track's code is not the handoff code, a Disassociation request will be sent to the Associate Flight Plans function to request that the flight plan be disassociated from the track. (↑ G1, HL.R15)
- c) A system acquisition control request to disable auto-acquisition on the assigned code will be sent to the Associate Flight plans function for any flight plans whose assigned beacon code equals the Handoff code in the *TI* message. (↑ G1, HL.R15)

[2.3.2.1.4] If the flight plan is associated, the X/Y coordinates will be compared with those of the associated track. If they differ by more than the adaptable ambiguous pseudo track distance, the *Crosstell Ambiguity* indicator **shall** be set in the flight plan.

(↑ HL.C10)

[2.3.2.1.5] A label update message will be sent to the SDD. (↑ HL.C2)

[2.3.2.1.6] If the flight plan is not associated, the software **shall** send an Association Request to the Associate Flight Plans function for the flight plan. (↑ HL.C3)

[2.3.2.1.7] The following requirements apply to Round Robin handoff initiation. If the flight plan is an arrival and there is an active departure flight plan with the same ACID and beacon code as the arrival, the software **shall** send a *Delete Flight Plan* request to the *Manage Flight Plans* function to delete the departure flight plan. (↑ HL.C3) If the departure flight plan is associated to a track, the software **shall** send an Association request to the *Associate Flight Plans* function for the arrival flight plan and the departure's track. (This functionality is part of the processing of Round Robin flights.

[17] (↑ HL.C3)

Undo Inbound Handoff

[2.3.2.2.1] When a *Recall (TA/TL)* message is received, the software **shall** set the handoff state in the flight plan to *Not in Handoff*. (↓ 3.2.8)

[2.3.2.2.2] The following actions **shall** be performed when a *Recall (TA/TL)* message is received:

1. If a pseudo-track entry is being maintained for an SDD a label update message indicating a track drop should be sent to the SDD. (↑ HL.R15)
2. The *Crosstell Ambiguity* indicator will be cleared in the flight plan.
(↑ HL.R15)
3. An *Inbound Handoff Undo Route Update Request* will be sent to the *Update Route* function to restore Current CJI to the value it had at the handoff initiation. This will take into account the restored value of the association state. (↑ HL.R15)

[2.3.2.2.3] An IFDT output request **shall** be sent to the *Manage IFDT Messages* function containing an *Acceptance Response (DA)* message for transmission to the initiating ARTCC or TRACON facility. (↑ HL.C3)

[2.3.2.2.4] If the flight is currently associated on the handoff code, the software **shall** send a Disassociation request to the *Associate Flight Plans* function to request that the flight plan is disassociated and that it is returned to unassociated state. (↑ HL.C3)

[2.3.2.2.5] If the flight is not currently associated but had previously associated on the handoff code, the software **shall** set the flight plan in unassociated state. (↑ HL.R15)

[2.3.2.2.6] If the flight is currently or previously associating on the beacon code in the *TI Initiate* message (Handoff code) when the *Recall (TA)* message was received, and the Handoff code was different to the assigned code, then the following actions **shall** be performed: (↑ HL.C2)

- a) A System acquisition control request to enable auto-acquisition on the assigned code will be sent to the *Associate Flight Plans* function for any other flight plan with an assigned beacon code equal to the Handoff Code, which had auto-acquisition disabled when the handoff was initiated. (↑ HL.C3)

b) The handoff Code will be deleted. (↑ HL.R15)

[2.3.2.2.7] If the flight is currently associated on the flight plan's assigned code when *Recall (TA/TL)* message was received and the flight was not associated when the handoff initiate was received, the software **shall** send a *Disassociation* request to the *Associate Flight Plans* function to request that the flight plan is disassociated. (↑ HL.C3)

[2.3.2.2.8] If the flight is not currently associated on the flight plan's assigned code when *Recall (TA/TL)* message was received and the flight was not associated when the handoff initiate was received, the software **shall** retain the current association state. (↑ HL.C3)

[2.3.2.2.9] If the flight is currently or was previously associated on the flight plan's assigned code when *Recall (TA/TL)* message was received and the flight was associated when the handoff initiate was received, the software **shall** retain the current association state. (↑ HL.C3)

[2.3.2.2.10] The software **shall** retain the auto-acquisition eligibility state that the flight had at the handoff initiation. (↑ G1)

Launch Accept Inbound Handoff

[2.3.2.3.1] An IFDT output request **shall** be sent to the *Manage IFDT Messages* function containing an *Accept Transfer (TA/TN)* message for transmission to the receiving facility. (↑ HL.C3)

If the Flight Plan is a remote En Route flight plan, the TA form of the message will be sent otherwise the TN form will be used. The TA/TN message will indicate if the acceptor of the flight is not the original receiver of the flight specified in the initiate transfer (TE/TM) message. (↓ Figure 3)

[2.3.2.3.2] Handoff state for the flight will be set to *Handoff Accept Pending*. (↓ 3.2.8)

[2.3.2.3.3] A timer is started for an adaptable time period and is incremented while in this handoff state. When the timer expires, a *Timeout Response* request is sent to the Determine Handoff Event process. (↓ 3.2.8)

Cancel Accept Inbound Handoff

[2.3.2.4.1] Handoff state for the flight will be set to *Handoff Ext From*. (↓ 3.2.9)

[2.3.2.4.2] The *Interface Handoff Error Status* indicator will be set in the flight plan.

(↑ HL.R15)

Complete Accept Inbound Handoff

[2.3.2.5.1] The following actions **shall** be performed to complete acceptance of an inbound handoff.

- a. If a pseudo-track entry is being maintained for an SCC a label update message indicating a track drop should be sent to the SDD. (↑ HL.R15)
- b. Handoff state for the flight will be set to *Inbound HO Accepted*. (↓ 3.2.9)
- c. The *Crosstell Ambiguity* indicator will be cleared in the flight plan.
(↑ HL.C15)
- d. A handoff route update request will be sent to the *Assign Sectors* function for the purpose of updating the flight plan's progress along the route and determining the new flight plan controller. (↑ HL.C15)

[2.3.2.5.2] If the track was already auto-acquired, then tracking **shall** continue.

(↑ HL.C10)

Clear Inbound Handoff Indicators

[2.3.2.6] Handoff state for the flight will be set to *Not in handoff*. (↓3.2.12)

Force Accept Inbound Handoff

[2.3.2.7.1] If RDP mode is enabled for the ARTCC, an IFDT output request **shall** be sent to the *Manage IFDT Messages* function containing an *Accept Transfer (TA/TN)* message

for transmission to the receiving facility indicating that any acknowledgement received to this message should be discarded. (↓3.2.8)

If the Flight Plan is a remote En Route flight plan, the TA form of the message will be sent, otherwise the TN for will be used. (↑ HL.C3)

[2.3.2.7.2] The *Interface Handoff Error Status* indicator will be cleared in the flight plan. (↑ HL.R15)

[2.3.2.7.3] All the processing described above for the *Complete Accept Inbound Handoff* action will be performed. (↑ G1)

Redirect Inbound Handoff

[2.3.2.8] The following actions **shall** be performed:

- a) The new receiver's CHI is stored in the flight plan. (↑ HL.R15)

Standby Processing Differences

[2.3.2.9] In the standby RDPS, the *Perform Inbound HO Step* sub function will be dormant. (↑ HL.C11)

Perform Local HO Step

[2.3.3] Below there are processing requirements for each of the following handoff Actions associated with the handoff of flights between positions at the local facility including transfer of an externally owned flight to a position at the local facility:

- Initiate Local Handoff
- Accept Local Handoff
- Recall local handoff
- Clear Local Handoff Indicators
- Transfer

- Initiate EFO Handoff
- Accept EFO Handoff
- Recall EFO Handoff
- Clear EFO Handoff

Initiate Local Handoff

[2.3.3.1.1] A successfully initiated handoff **shall** result in the following updates to the Flight Plan File for the flight plan:

- a) Handoff state for the flight will be set to *Handoff Int.* (↓ 3.2.1)
- b) If an active Pointout exists from the Handoff sender, the Pointout will be removed. (↓ 3.2.1)

[2.3.3.1.2] A Handoff indication will be sent to the *Generate MSAW Alerts* and *Generate Conflict Alerts* sub functions. (↑ C1, HL.C3)

Accept Local Handoff

[2.3.3.2.1] A valid *Handoff Accept* **shall** result in the following updates to the Flight Plan File for the flight plan:

- a. Handoff state for the flight will be set to *Local Handoff Accepted.* (↓ 3.2.11)
- b. A timer is started for an adaptable time period, and is incremented while in this handoff state. When the timer expires a *Complete HO* request is sent to the *Determine Handoff Event* process. (↑ HL.C12)

[2.3.3.2.2] A Handoff route update request will be sent to the *Assign Sectors* function for the purpose of updating the flight plan's progress along the route and determining the new flight plan controller. (↑ HL.R15)

Recall Local handoff

[2.3.3.3] A successfully recalled handoff **shall** result in the following updates to the Flight plan File for the flight plan:

- a) Handoff state for the flight will be set to *Not in Handoff*. (↓ 3.2.11)

Clear Local Handoff Indicators

[2.3.3.4] Handoff state for the flight will be set to *Not in Handoff*. (↓ 3.2.12)

Initiate EFO Handoff

[2.3.3.5] A successfully initiated EFO Handoff **shall** result in the following update to the Flight Plan File for the flight plan:

- a. [2.3.3.5.1] Handoff state for the flight will be set to *EFO-Handoff Int.* (↓ 3.2.1)
- b. [2.3.3.5.2] If an active pointout exists from the handoff sender, the Pointout will be removed. (↑ G1)

Accept EFO Handoff

[2.3.3.6.1] A valid EFO handoff Accept **shall** result in the following update to the Flight Plan File for the flight plan:

- a. Handoff State for the flight will be set to *EFO-Handoff Accepted*. (↓ 3.2.13)
- b. A timer is started for an adaptable time duration and is incremented while in this Handoff State. When the duration expires, a *Complete HO* request is sent to the *Determine Handoff Event* process. (↑ HL.C12)

[2.3.3.6.2] An EFO Handoff route update request will be sent to the *Assign Sector* function for the purpose of determining the new Previous CHI and updating the flight plan. (↑ HL.C15)

Recall EFO Handoff

[2.3.3.7] A successfully recalled EFO Handoff **shall** result in the following update to the Flight Plan File for the flight plan:

- a) Handoff State for the flight will be set to *Not in Handoff*. (↓ 3.2.13)

Clear EFO Handoff

[2.3.3.8] Handoff State for the flight **shall** be set to *Not in Handoff*. (↓ 3.2.14)

Transfer

[2.3.3.9] A Handoff route update request will be sent to the *Assign Sectors* function for the purpose of updating the flight plans progress along the route and setting the new flight plan controller. (↑ HL.C15)

Standby Processing Differences

[2.3.3.10] In the standby RDPS, the *Perform local HO Step* sub function will be dormant.

1. Clear EFO Handoff. (↑ HL.C11)

Update Crosstell Tracks Logic

[2.4] The Update Crosstell Tracks function processes Track Update messages from ARTCC and adjacent TRACON facilities, cyclically generates Track Update messages containing position and velocity for tracks in handoff to ARTCC and adjacent TRACON facilities, and sends messages to the facility receiving the handoff.

This function supports the NAS/RDPS interface by providing:

- Incoming Track Update
- Track Update Generation

Incoming Track Update.

[2.4.1] Incoming messages contain pairs of repeating fields containing *Track Position* and *Velocity* updates for from one to six tracks in handoff to the local STARS facility. Each set of repeating fields in the message will be processed as follows:

Validation

[2.4.1.1] The software **shall** discard the set of fields if any of the following conditions are not met: (↑ HL.R15, HL.C10)

1. The TCID (which is a System Flight Number) **must** reference a flight plan that exists.
2. The light plan handoff state **must** be Handoff Ext
3. The track update is received via an ARTCC that is in TDP mode as determined from the IFDT terminal area table.

Processing After Acceptance

[2.4.1.2.1] The X/Y coordinates and X/Y-velocities will be stored in the flight plan.

(↑ HL.R15)

[2.4.1.2.2] If the flight plan is associated, the X/Y coordinates will be compared with those of the associated track. If they differ by more than an adaptable ambiguous pseudo track distance, the *Crosstell Ambiguity* indicator **shall** be set in the flight plan.

(↑ HL.R15)

[2.4.1.2.3] The software **shall** send a *Label Update* message to the SDD. (↑ HL.R15)

[2.4.1.2.4] If the flight plan is not associated, the software **shall** send an *Association Request* to the Associate Flight Plans function for the flight plan. (↑ HL.R15)

Lack of TU messages

[2.4.1.3.1] If a Track Update message is not received for an inbound interfacility handoff track for an adaptive time period, then an indication **shall** be set in the flight plan. (↑ HL.C12) The software **shall** transmit a *Label Update* message to the SDD and generate a flight plan update every adaptive time period so long as the *TU* messages are not received. Doing so supports the consolidation or start-up of TCPs while *TU* messages are not received for existing pseudo tracks. (↑ HL.C3)

Track Update Generation

[2.4.2] The software **shall** perform the following every adaptive number of seconds, for each flight plan in the RDPS Flight Plan file that has a Handoff State of *Handoff Ext To* and is currently associated with a track that is not coasting: (↑ HL.R15)

[2.4.2.1] AN IFDT output request is sent to the *Manage IFDT Messages* function containing a *Track Update (TU)* message for transmission to the receiving ARTCC or adjacent TRACON facility.

[2.4.2.2] Each *TU* message can be populated with up to design parameter (normally 6) sets of repeating X/Y Coordinates and Velocity components for flights in handoff to the same facility. The CID in the *TU* message will be the transfer CID retained in the RDPS flight plan on receipt of the NAS Response indicating Acceptance for the outgoing *Initiate Transfer (TI/TM)* message.

[2.4.2.3] If flight Data Processing mode is enabled for the routing ARTCC, as determined by the IFDT terminal area table, then *TU* messages **shall** not be sent.

Determine Auto Handoff Logic

[2.5] The following conditions determine if a particular flight can be subject to an automatic handoff initiation/acceptance:

1. *Automatic Handoff System-wide*: this enables/disables the automatic handoff initiate and accept functions for the entire STARS.
2. *Handoff Initiate TCP*: this enables/disables the automatic handoff of flights under the control of a particular TCP
3. *Handoff Initiate flight*: This enables/disables the automatic handoff initiate of the flight.
4. *Handoff Accept TCP*: this enables/disables the automatic handoff acceptance of flights to come under then control of a particular TCP.
5. *Handoff Accept Flight*: this enables/disables the automatic handoff acceptance of the flight.

[2.5.1] If the automatic handoff initiation/acceptance of a flight is to be enabled, the flags relating to the flight, the controlling TCP for the flight and for the entire system, **must** be set to *enabled*. (↑ HL.R15)

[2.5.2] If this process determines that a late-handoff warning should be set for an interfacility flight, it sets a flag to indicate this in the flight plan. (↑ HL.R15)

It processes the following:

- SDD Requests:
- Interfacility Automatic Handoff Initiation
- Late-Handoff Warnings
- Intrafacility Automatic Handoff Initiation/Acceptance

SDD Requests

[2.5.3.1] This process will receive the following requests from the SDD:

1. TCP control containing handoff initiate/accept enable/disable requests for a specified TCP. (↑ HL.C3)
2. Flight plan activity control containing handoff initiate/accept enable/disable requests for a specified flight. (↑ HL.C3)
3. Flight plan activity controls containing a request to disable auto handoff processing for both initiate and accept actions for a specified flight. (↑ HL.C3)

[2.5.3.2] The software **shall** send an operator controller entry error to the SDD as a response to the SDD request. If any of the following conditions apply the response will indicate an error, otherwise it will indicate success: (↓ 3.1)

1. The initiating controller has no modification access to the flight plan
2. A handoff enable is requested, but the flight/TCP already has handoff enabled
3. A handoff disable is requested but the flight/TCP already has handoff disabled
4. A handoff disable is requested for a track, but auto handoff processing is disabled for the owning TCP or system-wide.
5. Flight is externally owned.

[2.5.3.3] On receipt of a valid request from the SCC, the software **shall** update the flight plan data or sector data as appropriate for the use by the automatic handoff initiation processing. (↑ HL.C10)

Interfacility Automatic Handoff Initiation (↑ HL.C9)

[2.5.4.1] The software **shall** qualify a flight for automatic handoff initiation if all the following conditions are true:

1. Automatic initiation of handoff is allowed for the entire STARS, as determined by System Parameters adaptation data.
2. The flight has automatic handoff initiation enabled, as indicated by FP data.
3. The flight plan's handoff state is *Not in Handoff* or *Handoff Accepted*, and a STARS controller controls the flight plan.
4. The TCP controlling the flight has automatic handoff initiation enabled, as indicated by Sector data adaptation.
5. The flight is a remote en-route departure or overflight with a discrete assigned beacon code.

6. The associated IFDT link (determined from the flight plans owning terminal area) is enabled (function and link), as indicated by the IFDT terminal area table.
7. The flight plan is not in late handoff state.
8. The system has not already unsuccessfully attempted to initiate an automatic handoff.
9. A handoff recall has not previously been performed on the flight.
10. The flight plan is not in the suspend state.
11. The flight's report beacon code matches its assigned beacon code.
12. The track with which the flight plan is associated is not coasting.

[2.5.4.2] If a qualifying flight's horizontal-predicted position using the flight's lookahead time plus a system time parameter is outside of the controlling STARS terminal area, then the software **shall** set an auto-handoff initiation in the flight plan data. (↑ HL.C9)

[2.5.4.3] If a flight ceases to qualify for automatic handoff initiation then the software **shall** clear the auto-handoff initiation indication in the flight plan data. (↑ HL.C9)

[2.5.4.4] If a qualifying flight's horizontally-predicted position using the flight's lookahead time is outside of the controlling STARS terminal area then the software **shall** send an *Auto_handoff_initiate_request* to the *Process_handoff* function. In addition, the software **shall** send an *Event Recording* request of type '*automatic interfacility handoff initiate*' to the *Record System Event* function. (↑ HL.C9)

Late-Handoff Warnings

[2.5.5] For any flight outside its controlling STARS terminal area, the software **shall** set a late-handoff warning flag in the flight plan if all the following conditions are true:

(↑ HL.C3)

1. The flight is a remote en-route (NAS) flight plan that is a departure or overflight
2. The flight has an exit external facility defined in the fix-pair adaptation
3. The flight is controlled by a controller of the flight's terminal area.
4. The flight was previously detected in its controlling terminal area.
5. The flight's late-handoff warning inhibit status is clear.

Intrafacility Automatic Handoff Initiation/Acceptance

[2.5.6.1] The software **shall** qualify a flight for automatic intrafacility handoff action if all of the following conditions are true: (↑ HL.C9)

1. Automatic initiation of handoff is allowed for the entire STARS system as determined from the System Parameters data.
2. A STARS controller controls the flight.
3. The flight plan has either automatic handoff initiation or acceptance enabled.
4. The flight plan's state is *Not in Handoff*, *Handoff Int* or *Handoff Accepted*.
5. The flight plan is not in late handoff state.
6. The flight plan is not in suspended state.
7. *The flight's reported beacon code matches its assigned beacon code.*
8. *The track with which the flight plan is associated is not coasting.*

[2.5.6.2] The software **shall** identify a qualifying flight as a candidate for handoff action if all the following conditions are true: (↑ G1)

1. The flight is in a handoff filter.
2. The configuration plan currently in use for the flight plan's terminal area matches an adapted configuration plan for the handoff filter.
3. The flight plan's owning controller matches an adapted owning controller for the handoff filter.
4. The flight plan's type of flight matches an adapted type of flight for the handoff filter.
5. The flight plan's entry fix matches an adapted entry fix for the handoff filter.
6. The flight plan's exit fix matches an adapted exit fix for the handoff filter.
7. The flight plan's requested level is within the adapted requested level band for the handoff filter.
8. The flight plan's owning controller does not match the adapted receiving controller for the handoff filter.

[2.5.6.3] If the flight is in more than one handoff filter, all filters will be considered until the first valid handoff action for the flight is initiated (if any). (↑ G1)

[2.5.6.4] If the flight is determined to be a candidate for handoff action, the adaptation will define the required handoff action and the associated receiving controller. [2.5.6.5] The software **shall** process the required handoff action as defined in Table 2: (↓ 3.2)

ADAPTED ACTION	PROCESS
Initiate	Providing the handoff state is <i>Not in Handoff</i> or <i>Handoff Accepted</i> , the flight has automatic initiate enabled, the current controller has automatic initiate enabled and the flight plan has not had an automatic handoff initiation re-called, send an <i>Auto Handoff</i> request for a handoff initiate to the adapted receiving controller to <i>Determine Handoff Event</i> .
Accept	Providing the handoff state is <i>Handoff Int</i> to the adapted receiving controller, the flight has automatic accept enabled and the receiving controller has automatic accept enabled, send an <i>Auto handoff</i> request for a handoff accept to <i>Determine Handoff Event</i> .
Transfer	Providing the handoff state is <i>Not in Handoff</i> , the flight has automatic initiate and automatic accept enabled, the current controller has automatic initiate enabled and the receiving controller has automatic accept enabled, send an <i>Auto Handoff</i> request for a transfer to the adapted receiving controller to <i>Determine Handoff Event</i> .

Table 2: Handoff Actions

[2.5.6.6] If the above handoff action is *Initiate* and an *Auto_handoff_initiate_request* is sent, the software **shall** send an *Event Recording* request of type *automatic intrafacility handoff initiate* to the *Record System Event* function. (↑ HL.R15)

Performance Monitoring

There are no performance monitoring specifications in the Raytheon documentation.

Tasks and Procedures

[2.6] In a training exercise, the receiving CJI may be internal but not be assigned to an SDD (Or Tower positions). [2.6.1] In this case, if the handoff request is valid, then the handoff accept will be simulated automatically. (↑ HL.C10)

Interface

(↑ HL.R1, HL.R5) [15]

[2.7.1] The display presentation for tracks in an active Handoff is defined in adaptation data (Rules). The description in this section for handoff is consistent with the default Rules.

[2.7.2] Tracks, which have been initiated for Handoff, are displayed in the Handoff color (amber) with full data blocks at both the initiating and receiving position. Tracks that are initiated for handoff to an external facility will not be displayed as in Handoff mode until the external facility has acknowledged receipt of the handoff.

[2.7.3] Tracks ready for handoff acceptance will blink in the Handoff Color (amber) at the receiving TDW / TCW.

[2.7.4] Tracks in active handoff at the initiating position are displayed in the Handoff Color (amber). The intended receivers TCP appears in the data block. After the handoff has been accepted, the track at the initiating position will display a blinking Full Data Block for an amount of time defined in adaptation data.

[2.7.5] After acceptance, the track at the receiver s display stops blinking and remains in the handoff color for an amount of time defined in adaptation data.

[2.7.6] Tracks in handoff include the *handoff* indicator (H) in the data block, followed by either a space or a slash (/), which is followed by the sending or receiving TCP as appropriate. The slash appears for tracks that:

[2.7.6.1] have been handed off to an external facility which has not yet accepted the handoff.

[2.7.6.2] are involved in a local handoff and the handoff has been accepted.

[2.7.6.3] are involved in a handoff from an external facility and the handoff has been accepted.

[2.7.7] To identify a specific track for handoff, either select the track with the trackball, or enter the track s ACID, unique discrete beacon code, or tab line number in the Preview area.

[2.7.8] When initiating a track for handoff, the receiving TCP **must** always be specified.

[2.7.9] To perform a Handoff function on a flight owned by another TCP and to which the entering TCP is not coupled, the command logic override (<O> <K>) **must** be entered into the Preview area prior to flight selection.

[2.7.10] Enabling an automatic handoff feature disables any previously enabled automatic handoff feature.

Testing and Validation

[2.8] The receiving CJI may be internal but **shall** not be assigned to an SDD (Or Tower position). [2.8.1] If handoff case is valid, then the handoff accept **shall** be simulated automatically. (↑ HL.C10)

Level III Environment

Below is a diagram of the system environment showing the various modes within each component. (→ 3.2)

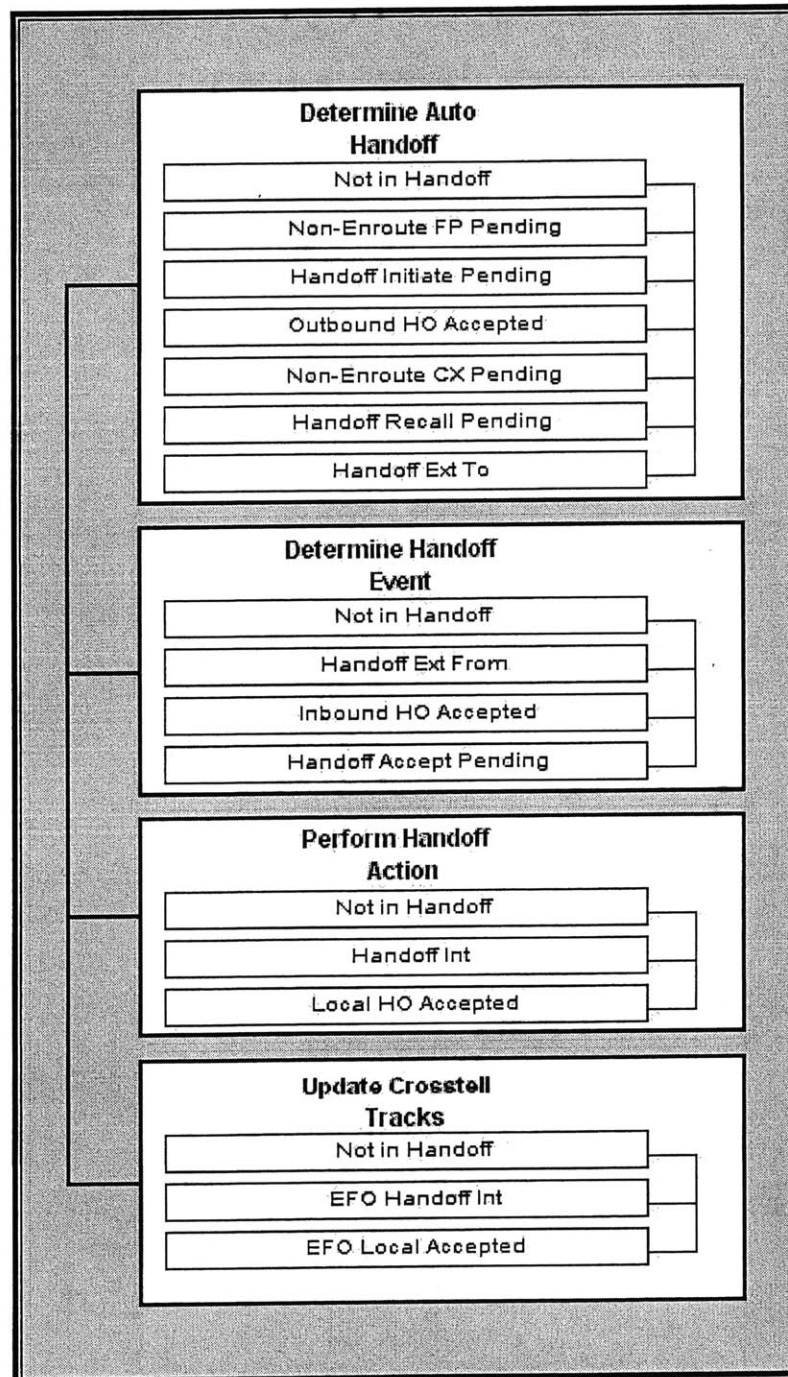


Figure 2: Diagram of System Environment

Sector Handoff Interface

The figure below shows the inputs and out puts to each of the system components.

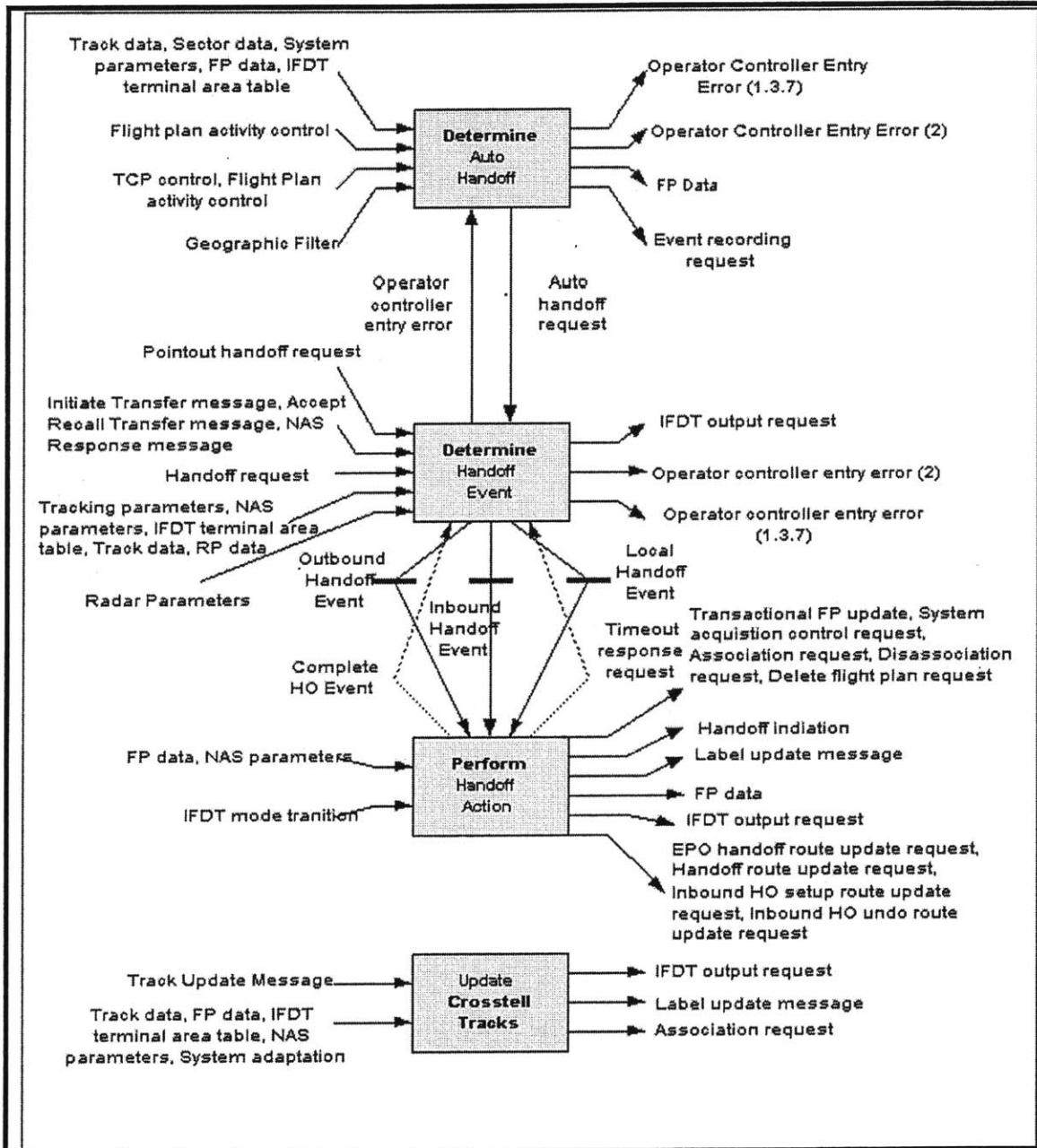


Figure 3: Diagram of Modes showing Inputs and Outputs

Behavior Requirements

Message Formats

Table 3 lists the message formats, which supported by the system. (↑ HL.R12) Tables 3-16 are the error messages associated with each Handoff Command.

Message Type	Message Description
	<i>Flight Data</i>
FP	Flight Plan
FP	VFR Flight plan
AM	Amendment
CX	Cancellation
RF	Request Flight Plan
DM	Departure
TB	Beacon Terminate
	<i>Track Data</i>
TA	Accept/Recall Transfer
TN	Accept Transfer
TL	Recall Transfer
TI	Initiate Transfer
TM	Initiate Transfer
TU	Track Update
TZ	Track/Full Data Block Information
TS	Transfer Secondary Radar Targets
TP	Transfer Primary Radar Targets
	<i>Test</i>
TR	Test Data

	<i>Response</i>
DA	Acceptance
DR	Data Rejection
DX	Retransmit
DT	Data Test

Table 3: [3.1] System Messages

Message Text	Description / Recommended Action
ILL TRK	Entering position is not the track's controlling position or is not coupled with the controlling position. / Informational.
ILL TRK	Identified track is already in handoff status. / Informational.
ILL POS	For interfacility, receiving controlling position is not an external ARTCC or adjacent Tracon. / TBS
ILL TRK_LCL FP	For interfacility NAS FP, the ARTCC facility did not originate flight plan data. / TBS
ILL TRK-NAS FP	For interfacility non-host FP, the STARS facility did not originate flight plan data. / TBS
BCN MISMATCH	Track has an RBC/ABC in data block. / Either change track's assigned code to match transponded code, or change transponded to match assigned.
IF INHIB	For interfacility, the interfacility interface does not exist or is not enabled. / Informational.
IF WAIT	An IF output message is pending for this track. / WHAT SHOULD THEY DO??
ILL SECTOR	For ARTCC handoff, specified sector is not adapted as adjacent. / TBS
ILL SECTOR	For Adjacent Tracon handoff, specified destination position not adapted as allowed. / TBS
ILL FNCT	Adjacent Tracon not adapted for FP interface. / TBS

Table 4: [3.1.1] Initiate Handoff (Implied command)

Message Text	Description / Recommended Action
ILL TRK	Designated track has No Acquired Track (NAT) status. / Informational.

Table 5: [3.1.2] Recall Handoff (Implied command)

Message Text	Description / Recommended Action
ILL TRK	Designated track has No Acquired Track (NAT) status. / Informational.

Table 6: [3.1.3] Accept Handoff (Implied command)

Message Text	Description / Recommended Action
ILL TRK	Designated track has No Acquired Track (NAT) status. / Informational.

Table 7: [3.1.4] Take control of interfacility track (Implied command)

Message Text	Description / Recommended Action
ILL FNCT	AHOP is already inhibited for either the specified track, the controlling position, or this STARS site. / Informational.
ILL TRK	The track is not controlled by (nor coupled to) the entering position. / Use the non-implied version of this command as described on page 172.
ILL TRK	The track is either an arrival track or is a VFR track. / Informational—it is not possible to inhibit AHOP for VFR or Arrival flights.
ILL TRK	The track's position symbol is "C" or a unique adjacent ARTS/STARS facility identifier. / Informational—it is not possible to inhibit AHOP for flights owned by another facility.
ILL TRK	The track is currently involved in an interfacility or intrafacility handoff. / Informational—it is not possible to inhibit AHOP for tracks in handoff.
ILL TRK	The track's FDB contains a blinking "DM" or "IF". / Informational.

Table 8: [3.1.5] Inhibit automatic handoff for a flight (Implied command)

Message Text	Description / Recommended Action
FORMAT	Invalid aircraft identity entered. / Correctly identify the aircraft.
ILL TRK	Entering TCP is not (nor is coupled to) the designated handoff receiver and command override was not invoked. / Use command override.
NO FLIGHT	No track file exists for the specified track. / WHAT SHOULD THEY DO??
DUP BCN	Discrete beacon code not unique. / Specify track using ACID or slew.
DUP ACID	Entered ACID not unique. / Specify track using beacon code or slew.

Table 9: [3.1.6] Accept handoff

Message Text	Description / Recommended Action
FORMAT	Invalid aircraft identity entered. / Correctly identify the aircraft.
DUP BCN	Discrete beacon not unique in system. / Specify track using ACID or slew.
DUP ACID	Entered ACID not unique. / Specify track using beacon code or slew.
NO FLIGHT	No track file exists for the identified flight. / WHAT SHOULD THEY DO??
ILL TRK	Entering position is not the track's owner, is not coupled to the owner's position, or command override was not invoked. / Use command override.
ILL TRK	Track is already in handoff status. / Informational.
ILL POS	Receiving position does not exist / Correctly identify the receiving position.
BCN MISMATCH	Track has an RBC/ABC displayed. / WHAT SHOULD THEY DO?? and how is this different from DUP BCN??

Table 10: [3.1.7] Initiate Intrafacility Handoff

Message Text	Description / Recommended Action
FORMAT	Invalid aircraft identity entered. / Correctly identify the aircraft.
DUP BCN	Discrete beacon not unique in system. / Specify track using ACID or slew.
BCN ACID	Entered ACID not unique. / Specify track using beacon code or slew.
NO FLIGHT	No track file exists for the identified flight. / WHAT SHOULD THEY DO??
ILL TRK	Entering position is not the track's owner, is not coupled to the owner's position, or command override was not invoked. / Use command override.
ILL TRK	Track is already in handoff status. / Informational.
ILL TRK_LCL FP	The ARTCC facility did not originate flight plan data. / WHAT SHOULD THEY DO??
BCN MISMATCH	Track has an RBC/ABC displayed. / WHAT SHOULD THEY DO?? And how is this different from DUP BCN??
IF INHIB	The interfacility interface does not exist or is not enabled. / Use command override.
IF WAIT	An IF output message is pending for this track. / WHAT SHOULD THEY DO??
ILL SECTOR	Specified sector not adapted as adjacent. / Initiate handoff to an adjacent sector.

Table 11: [3.1.8] Initiate handoff to ARTCC

Message Text	Description / Recommended Action
FORMAT	Invalid aircraft identity entered. / Correctly identify the aircraft.
DUP BCN	Discrete beacon not unique in system. / Specify track using ACID or slew.
DUP ACID	Entered ACID not unique. / Specify track using beacon code or slew.
NO FLIGHT	No track file exists for the identified flight. / WHAT SHOULD THEY DO??
ILL TRK	Entering position is not the track's owner, is not coupled to the owner's position, or command override was not invoked. / Use command override.
ILL TRK	Track is already in handoff status. / Informational.
ILL TRK-LCL FP	The ARTCC facility did not originate flight plan data, / WHAT SHOULD THEY DO??
BCN MISMATCH	Track has an RBC/ABC in data block. / Either change track's assigned code to match transponded code, or change transponded to match assigned.
IF INHIB	The interfacility interface does not exist or is not enabled. / Use command override.
IF WAIT	An IF output message is pending for this track. / WHAT SHOULD THEY DO??

Table 12: [3.1.9] Initiate NAS FP handoff to adjacent Tracon

Message Text	Description / Recommended Action
FORMAT	Invalid aircraft identity entered. / Correctly identify the aircraft.
DUP DCN	Discrete beacon not unique in system. / Specify track using ACID or slew.
DUP ACID	Entered ACID not unique. / Specify track using beacon code or slew.
NO FLIGHT	No track file exists for the identified flight. / WHAT SHOULD THEY DO??
ILL TRK	Entering position is not the track's owner, is not coupled to the owner's position, or command override was not invoked. / Use command override.
ILL TRK	Track is already in handoff status. / Informational.
ILL TRK-NAS FP	The STARS facility did not originate flight plan data. / WHAT SHOULD THEY DO??
ILL FNCT	ILL FNCT Identified track has an RBC/ABC displayed in the data block. / WHAT SHOULD THEY DO??

ILL FNCT	Adjacent Tracon not adapted for FP interface. / WHAT SHOULD THEY DO??
IF INHIB	The interfacility interface does not exist or is not enabled. / Use command override.
IF WAIT	An IF output message is pending for this track. / WHAT SHOULD THEY DO??

Table 13: [3.1.10] Initiate local FP handoff to adjacent Tracon

Message Text	Description / Recommended Action
FORMAT	Invalid aircraft identity entered. / Correctly identify the aircraft.
DUP DCN	Discrete beacon not unique in system. / Specify track using ACID or slew.
DUP ACID	Entered ACID not unique. / Specify track using beacon code or slew.
NO FLIGHT	No track file exists for the identified flight. / WHAT SHOULD THEY DO??
ILL TRK	Entering position is not the track's owner, is not coupled to the owner's position, or command override was not invoked. / Use command override.

Table 14: [3.1.11] Recall handoff

Message Text	Description / Recommended Action
FORMAT	Invalid aircraft identity entered. / Correctly identify the aircraft.
DUP DCN	Discrete beacon not unique in system. / Specify track using ACID or slew.
DUP ACID	Entered ACID not unique. / Specify track using beacon code or slew.
NO FLIGHT	No track file exists for the identified flight. / WHAT SHOULD THEY DO??

Table 15: [3.1.12] Redirect incoming interfacility handoff

Message Text	Description / Recommended Action
ILL FNCT	Automatic handoffs are already inhibited for either the specified track, the controlling position, or for this STARS site. / Informational.
ILL TRK	Entering TCP is not (nor is coupled to) the current owner of the track and command override was not invoked. / Use command override.
ILL TRK	The specified track is an arrival track or is a VFR track. / Informational.
ILL TRK	The specified track is owned by another facility. / Informational.
ILL TRK	The specified track is currently involved in a handoff. / Informational.
ILL TRK	The specified track's data block contains a blinking "DM" or "IF". / Informational.
DUP BCN	Discrete beacon code is not unique. / Specify track using ACID or slew.
DUP ACID	Entered ACID is not unique. / Specify track using beacon code or slew.

Table 16: [3.1.13] Inhibit automatic handoff for a flight

State Transitions

[3.2] Modes

<i>Next State</i>	<i>Handoff Initiate Pending</i>	<i>Non-Enroute FP Pending</i>	<i>Handoff Ext From</i>	<i>EFO Local Accepted</i>	<i>EFO Handoff Int</i>	<i>Not in Handoff</i>	<i>Handoff Int</i>
Launch Non-En Route RP	*	T	*	*	*	*	*
Initiate Non-Enroute Handoff	*	T	*	*	*	*	*

<i>Next State</i>	<i>Handoff Initiate Pending</i>	<i>Non-Enroute FP Pending</i>	<i>Handoff Ext From</i>	<i>EFO Local Accepted</i>	<i>EFO Handoff Int</i>	<i>Not in Handoff</i>	<i>Handoff Int</i>
Initiate External Handoff	T	*	*	*	*	*	*
Launch Outbound Handoff	T	*	*	*	*	*	*
TI/TM Initiate	*	*	T	*	*	*	*
Setup Inbound Handoff	*	*	T	*	*	*	*
Take Control Event	*	*	*	*	*	T	*
Transfer	*	*	*	*	*	T	*
Pointout-Handoff (EFO) Event	*	*	*	T	*	*	*
Accept EFO-HO Event	*	*	*	T	*	*	*
Initiate EFO-HO Event	*	*	*	*	T	*	*
Initiate EFO-Handoff	*	*	*	*	T	*	*
Initiate Local Handoff	*	*	*	*	*	*	T
Pointout Handoff (local) event	*	*	*	*	*	*	T

Table 17: [3.2.1] Current State = Not in Handoff (↑ 2.2, 2.3, 2.4, 2.5)

<i>Next State</i>	<i>Not in Handoff</i>	<i>Not in Handoff</i>	<i>Outbound HO Accepted</i>	<i>Handoff Ext To</i>
External Response timeout	*	T	*	*
Cancel Outbound Handoff	T	T	*	*
TI/TM Response Accept	*	*	*	T
TI/TM Response (Receipt/Fail)	T	*	*	*
TA/TN Accept	*	*	T	*
Complete Outbound Handoff	*	*	T	*
Establish Outbound Handoff	*	*	*	T

Table 18: [3.2.2] Current State = Handoff Initiate Pending (↑ 2.2)

<i>Next State</i>	<i>Not in Handoff</i>	<i>Not in Handoff</i>	<i>Handoff Initiate Pending</i>
External Response timeout	T	*	*
Initiate Non-Enroute Handoff	*	*	*
Cancel Outbound Handoff	T	T	*
FP Response (Receipt/Fail)	*	T	*
FP Response (Accept)	*	*	T
Initiate External Handoff	*	*	*
Launch Outbound Handoff	*	*	T

Table 19: [3.2.3] Current State = Non-Enroute FP Pending (↑ 2.2)

<i>Next State</i>	<i>Not in Handoff</i>	<i>Not in Handoff</i>
External Response timeout	*	T
CX Response	T	*
TA Response (accept)	*	*
Complete Recall Outbound Handoff	T	T

Table 20: [3.2.4] Current State = Non-Enroute CX Pending (↑ 2.2)

<i>Next State</i>	<i>Not in Handoff</i>
External HO Accepted Timeout	T
Clear Outbound Handoff indicators	T

Table 21: [3.2.5] Current State = Outbound HO Accepted (↑ 2.2)

<i>Next State</i>	<i>Outbound HO Accepted</i>	<i>Handoff Recall Pending</i>
Launch Recall Outbound Handoff	*	T
Force External Handoff	*	T
TA/TN Accept	T	*
Complete Outbound Handoff	T	*

Table 22: [3.2.6] Current State = Handoff Ext To (↑ 2.2)

<i>Next State</i>	<i>Not in Handoff</i>	<i>Non-Enroute CX Pending</i>	<i>Handoff Ext To</i>	<i>Handoff Ext To</i>
External Response timeout	*	*	T	*
TL Response (accept)	*	T	*	*
TA Response (accept)	T	*	*	*
Complete Recall Outbound Handoff	T	*	*	*
Launch Non-Enroute CX	*	T	*	*
Cancel Recall Outbound Handoff	*	*	T	T
TA/TL Response (Receipt/Fail)	*	*	*	T

Table 23: [3.2.7] Current State = Handoff Recall Pending (↑ 2.2)

<i>Next State</i>	<i>Not in Handoff</i>	<i>Not in Handoff</i>	<i>Handoff Accept Pending</i>
TA/TI Recall	T	*	*
Undo Inbound Handoff	T	*	*
Force Accept External Handoff	*	T	*
Force Accept Inbound Handoff	*	T	*
Launch Accept Inbound Handoff	*	*	T
Accept External Handoff	*	*	T

Table 24: [3.2.8] Current State = Handoff Ext From (↑ 2.3)

<i>Next State</i>	<i>Handoff Ext From</i>	<i>Handoff Ext From</i>
External Response timeout	T	*
Cancel Accept Inbound Handoff	T	*
Complete Accept Inbound Handoff	*	T
TA/TN Response (Reject/Fail)	*	T

Table 25: [3.2.9] Current State = Handoff Accept Pending (↑ 2.3)

<i>Next State</i>	<i>Not in Handoff</i>
Clear Local Handoff Indicators	T
External HO Accepted Timeout	T

Table 26: [3.2.10] Current State = Inbound HO Accepted (↑ 2.3)

<i>Next State</i>	<i>Not in Handoff</i>	<i>Local HO Accepted</i>
Recall Local Handoff Event	*	T
Recall Local Handoff	*	T
Accept Local Handoff Event	T	*
Accept Local Handoff	T	*

Table 27: [3.2.11] Current State = Handoff Int (↑ 2.4)

<i>Next State</i>	<i>Not in Handoff</i>
Clear Inbound Handoff Indicators	T
Local HO Accepted Timeout	T

Table 28: [3.2.12] Current State = Local HO Accepted (↑ 2.4)

<i>Next State</i>	<i>EFO Local Accepted</i>	<i>Not in Handoff</i>
Accept EFO-HO Event	T	*
Accept EFO-Handoff	T	*
Recall EFO-HO Event	*	T
Recall EFO-Handoff	*	T

Table 29: [3.2.13] Current State = EFO Handoff Int (↑ 2.5)

<i>Next State</i>	<i>Not in Handoff</i>
Clear EFO Handoff	T
EFO-HO Accepted Timeout	T

Table 30: [3.2.14] Current State = EFO Local Accepted (↑ 2.5)

Software Design Requirements

[3.3] Design constraints for the software are specified in the Software Development Plan for the ATCC. (↑ G1, 2.1)

[3.3.1] Where new software is required to implement software requirements, program design language **shall** be used to translate the software requirements into a program design, in accordance with Raytheon Practices Manual.

[3.3.2] Where existing software is used to implement software requirements, program design language was used to describe the design, and the process described below was generally followed.

[3.3.2.1] The program design language **shall** be subjected to formal inspections, in accordance with Raytheon Practices Manual and the STARS Software Development Plan, and the ATCC Design and Coding Standards.

Modular design techniques have been used for existing modules and will be used for all newly developed software.

[3.3.2.2] The size of new modules **shall** be limited, as described in the Design and Coding Standards.

[3.3.2.3] Only structured coding techniques **shall** be used to determine the flow of control within modules.

[3.3.2.4] The selection of control constructs **shall** be in accordance with the ATCC Design and Coding Standards.

[3.3.2.5] The adaptation data items referred to in section 3.2 **shall** be used to parameterize certain data structure sizes and logical quantities.

[3.3.2.6] The design parameters referred to in section 3.2 **shall** be treated as symbolic parameters.

Use of the above-referenced design parameters will be deemed sufficient to meet the expandability requirement expressed by requirements of the System Segment Specification.

[3.3.2.7] All the software in this CSCI **shall** be written in the C language.

[3.3.2.8] All the application software in this CSCI **shall** be designed to run under the NWS operating system whose functions are described in the SRS.

[3.3.2.9] The software **shall** be coded in accordance with the program design language described above.

CAPACITY REQUIREMENTS

[3.4] The capacity requirements for CSCI-1 are as follows: (↑ EC.2)

[3.4.1] The system **shall** have a flight plan file capacity of 999 flight plans.

NOTE: This capacity accommodates the ISC system workload requirement of 733 flight plans plus a 20% overhead of at least 147 flight plans for simulation capacity.

When the system is in normal mode, the software will discard any new flight plans from the simulator that would cause the allotted 20% of the total flight plan file capacity to be exceeded.

[3.4.2] The system **shall** accept an average of 600 radar tracks/plots per second from three radar sources (2 short range and 1 long range). NOTE: This requirement accommodates the ISC system workload requirements plus simulation capacity corresponding to additional 100 aircraft targets.

[3.4.3] The system **shall** accept and process weather data from 16 surveillance sensors in each data context.

[3.4.4] The system **shall** accept a peak of 935 radar tracks/plots per second from three radar sources. NOTE: This requirement accommodates the ISC system workload requirements plus simulation capacity corresponding to an additional 100 aircraft targets.

[3.4.5] The system **shall** be capable of processing a minimum of 450 post-mosaic radar tracks/plots per second. The term post-mosaic refers to those radar tracks/plots that remain after undergoing the processing described in the process specifications for Process Radar Input Data, Convert Radar Data Format, Suppress SSR Reflections, Convert Coordinates, and Perform Selective Rejection. (This processing eliminates some data from further consideration). NOTE: This requirement accommodates the ISC system workload requirements plus simulation capacity corresponding to additional 100 aircraft targets.

[3.4.6] The system **shall** have a system track file capacity of 750 tracks. NOTE: This requirement accommodates the ISC system workload requirement of 435 tracked aircraft, plus simulation capacity corresponding to an additional 100 aircraft targets, plus capacity to accommodate additional tracks from non-aircraft targets.

When the system is in normal mode, the software will exclude any new tracks from the simulator that would cause the allotted 20% of the total track file capacity to be exceeded.

[3.4.7] The system **shall** accommodate a mosaic grid size of at least 512 by 512 nautical miles using 16 n.mi. x 16 n.mi. tiles.

[3.4.8] The system **shall** accommodate 255 CJSs

[3.4.9] The system **shall** accommodate up to 32 CJSs in any one Terminal Area.

[3.4.10] The system **shall** accommodate up to eight (8) Terminal Areas.

[3.4.11] The software **shall** support one En Route/terminal interfacility interface per terminal area.

[3.4.12] Up to *twelve (12)* Fix-Pair Configuration Plans **shall** be adaptable for each Terminal Area within the system.

[3.4.13] The system **shall** accommodate 16 Arrival filters and 16 Departure Filters.

[3.4.14] The system **shall** process six output levels of weather.

[3.4.15] The system **shall** accommodate up to *24 meteorological* stations.

[3.4.16] The system **shall** accommodate 200 geographic sectors.

[3.4.17] The system **shall** accommodate four Total Filters.

[3.4.18] The system **shall** accommodate *24* concurrent training exercises *and 1 certification exercise, which* will be generated by the SIM.

[3.4.19] The system **shall** use a maximum of twenty defined reflection surfaces per radar for SSR reflection suppression.

[3.4.20] The system **shall** support message inputs from and responses to up to three uniquely addressable input device sets (with associated response areas) at each TCW subsystem.

[3.4.21] The system **shall** support message inputs from and responses to up to two uniquely addressable input device sets (with associated response areas) at each TDW subsystem.

[3.4.22] The system **shall** accommodate any tangency point longitude, and any tangency point latitude between 85_N and 85_S.

[3.4.23] The system **shall** accommodate up to 16 surveillance sensors in each data context.

[3.4.24] The system **shall** accommodate up to 8 MSAW primary airports and up to 32 MSAW satellite airports.

[3.4.25] The system **shall** accommodate up to 20 MSAW runways per primary airport and up to 10 MSAW runways per satellite airport.

[3.4.26] The software **shall** be able to construct a composite weather picture set that includes data from up to 4400 weather messages from En Route radars (total number for all En Route radars)

[3.4.27] The software **shall** be able to construct a composite weather picture set consisting of at least 9000 horizontal lines.

[3.4.28] The system **shall** accommodate up to 150 users that can save preference sets.

[3.4.29] The system **shall** store and process up to 32 preference sets per user.

CONCLUSION

This project has provided a proof of concept for the use Formal Specification and Requirements Languages in the design of automated systems. This work has provided a more comprehensive approach to view the Sector Handoff Module of Raytheon's Standard Terminal Automation Replacement System (STARS). The manner in which SpecTRM-RL partitions the system design into varying levels of resolution helps to illuminate many elements of Sector Handoff. Even though STARS is not intended as a system that involves humans, its design has many human-machine interaction factors that surfaced in the process of building the SpecTRM model. SpecTRM-RL also made it easy to trace design requirements to design decisions and vice versa. This work can be used to provide insights as to type of information that is missing or hard to locate in the current system specifications. This human-centered approach, even for a purely automated system, would lead to safer designs, which would therefore contribute to the reduction in the risk of aerospace accidents and consequent loss of life and property.

APPENDIX A: FUTURE WORK

SpecTRM is a relatively new Formal Specification and Requirements Language, and there is further work need to add other tracing functionalities to the software package. Work that expands upon this thesis may include differentiating between the types of tracing based on their function. This would allow engineers to extract different properties of the system, thus enhancing reviewability. Further work can also be done in modeling other components of Raytheon's STARS using SpecTRM software.

APPENDIX B: LIST OF ABBREVIATIONS AND DEFINITIONS

ACC Area Control Center
ACID Aircraft Identification
AHOP Automatic Handoff
AM Amendment
ARTCC Air Route Traffic Control Center
ATC Air Traffic Control, Air Traffic Center
ATCC Air Traffic Control Center

CHI Computer Human Interface
CJI Controller Jurisdiction Indicator
CJS Controller Jurisdiction Symbol
CSCI Computer Software Configuration Item
CX Cancellation

DA Acceptance
DM Departure
DR Date Rejection
DT Data Test
DUP Duplicated Track
DX Retransmit

EFO External Facility Owned
FAA Federal Aviation Association
FDB Full Data Block
FP Flight Plan

GPS Global Positioning System

HO Handoff

ID Identification
IFDT Interfacility Data Transfer
LAN Local Area Network

MSAW Minimum Safe Altitude Warning
MTCD Medium Term Conflict Detection
NAS National Airspace System

OOC Operations Control Center
OSF Operation Support Facility

RDPS Radar Data Processing System

RF Requested Flight Plan
RMC Remote Monitoring Control
RSML Requirements State Machine language

SCSC STARS Central Support Complex
SDD Situation Data Display
SRS Software Requirement Specification
SpecTRM Specification Tools and Requirements Methodology
STARS Standard Terminal Automation Replacement System
STARS FSC Standard Terminal Automation Replacement System Full System Configuration

TA Accept/Recall Transfer
TB Beacon Terminate
TBS To be Supplied
TCID System Flight Number
TCP Terminal Control Position
TCW Terminal Control Workstation
TDW Terminal Display Workstation
TCAS Traffic Collision and Avoidance System
TCW Terminal Controller Workstation
TDW Tower Display Workstation
TI Initiate Transfer
TL Recall Transfer
TM Initiate Transfer
TN Accept Transfer
TR Test Data
TRACON Terminal Radar Approach Control
TU Track Update
VFR: Visual Flight Rules

Data Block - Attached to a position symbol, the data block includes textual information about the aircraft including cleared and actual flight levels, cleared headings, speed, destination, aircraft type, wake turbulence category, beacon code, and ACID.

Track - Identifies a detected aircraft's current location using a position symbol and information about the aircraft in an attached data block. Optionally, the track can include a history trail and predicted track line.

REFERENCES

- [1] Nancy Leveson and Janice Stolzy. "Safety Analysis using Petri Nets." IEEE Transactions on Software Engineering, Volume SF 13, no 3, March 1970
- [2] Nancy Leveson. "Intent Specifications: An Approach to Building Human-Centered Specifications." IEEE Trans. on Software Engineering, January 2000.
- [3] <http://www.safeware-eng.com>
- [4] Nancy Leveson. "Completeness in Formal Specification Language Design for Process-Control Systems." Proceedings of Formal Methods in Software Practice Conference, August 2000.
- [5] <http://www.nap.edu/html/flight/>
- [6] Molly Brown and Nancy Leveson, Modeling Controller Tasks for Safety Analysis, University of Washington, Seattle, WA, April 1998.
- [7] Nancy Leveson and Jon Damon Reese, Sample TCAS Intent Specification, Safeware Engineering Corporation, May 1993.
- [8] Lilian Alfaro, Christine Alvarado, Molly Brown, Earl Hunt, Matt Jaffe, Susan Joslyn, Nancy Leveson, Denise Pinnel, Jon Reese, Jeffrey Samarziya, Sean Sandys, Michael Shafer, Alan Shaw, Zelda Zabinsky, A Demonstration Safety Analysis of Air Traffic Control Software, University of Washington, September 1997.
- [9] Nancy Leveson, Sample Intent Specification: Altitude Switch, Safeware Engineering Corporation, December 1999.
- [10] Steven Miller, Modeling Software Requirements for Embedded Systems, NEC Research Institute, 1999.
- [11] William Melendez-Diaz, The Different Levels of Intent Specifications: Analysis and Guidelines on Tracing, MIT, May 2001
- [12] Nancy Leveson, Evaluating Accident Models using Recent Aerospace Accidents, SERL, MIT, June 28, 2001
- [13] David Woods. Toward a theoretical base for representation design in the computer medium: Ecological perception and aiding human cognition. In J.M. Flach, P.A. Hancock, K. Caird and K.J. Vicente, editors An Ecological Approach to Human Machine Systems I: A Global Perspective, Erlbaum, Hillsdale, New Jersey, 1995.
- [14] Peter Checkland. Systems Thinking, Systems Practice. John Wiley & Sons, 1981.

[15] STARS FSC " FS TDW / TCW SUM Software Version 8.0 Rev. DRAFT Cage Code 49956, Document Number MUGxxxxxxx, February 2001

[16] <http://www.avweb.com/other/mead9744.html>

[17] Software Requirements Specification for the Radar Data Processing System, Federal Aviation Administration, Revised February 2001.