Airport Resource Management Tool (ARMT) Technical Instruction Book

xx/xx/xxxx

Operational Support
ATO-T Terminal Programs Operations
Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City International Airport, New Jersey 08405
<table>
<thead>
<tr>
<th>CHANGE TO BASIC</th>
<th>SUPPLEMENT</th>
<th>OPTIONAL</th>
<th>CHANGE TO BASIC</th>
<th>SUPPLEMENT</th>
<th>OPTIONAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FAA Form 1320-5 (6-80) USE PREVIOUS EDITION
# Table of Contents

## Section 1.0 General Information

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Introduction</td>
</tr>
<tr>
<td>1.1.1</td>
<td>Background</td>
</tr>
<tr>
<td>1.1.2</td>
<td>Purpose</td>
</tr>
<tr>
<td>1.1.3</td>
<td>Scope</td>
</tr>
<tr>
<td>1.2</td>
<td>Related Publications</td>
</tr>
<tr>
<td>1.2.1</td>
<td>Government References</td>
</tr>
<tr>
<td>1.2.2</td>
<td>Other References</td>
</tr>
<tr>
<td>1.3</td>
<td>Support</td>
</tr>
<tr>
<td>1.3.1</td>
<td>Logistics Support</td>
</tr>
<tr>
<td>1.3.2</td>
<td>Maintenance Support</td>
</tr>
<tr>
<td>1.4</td>
<td>Equipment Description</td>
</tr>
<tr>
<td>1.4.1</td>
<td>ARMT Server Workstation</td>
</tr>
<tr>
<td>1.4.2</td>
<td>ARMT Clients</td>
</tr>
<tr>
<td>1.5</td>
<td>Concept of Operation</td>
</tr>
<tr>
<td>1.6</td>
<td>Requirements</td>
</tr>
<tr>
<td>1.7</td>
<td>Connectivity</td>
</tr>
<tr>
<td>1.8</td>
<td>Redundancy</td>
</tr>
<tr>
<td>1.9</td>
<td>Relationship of Components</td>
</tr>
<tr>
<td>1.10</td>
<td>Software Overview</td>
</tr>
<tr>
<td>1.11</td>
<td>Databases</td>
</tr>
<tr>
<td>1.12</td>
<td>ARMT System Administration</td>
</tr>
<tr>
<td>1.13</td>
<td>ARMT Information System Security</td>
</tr>
</tbody>
</table>

## Section 2.0 Technical Information

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Simplified Theory of Operation</td>
</tr>
<tr>
<td>2.2</td>
<td>Detailed Theory of Operation</td>
</tr>
<tr>
<td>2.2.1</td>
<td>Overview of ARMT Functional Capabilities</td>
</tr>
<tr>
<td>2.2.2</td>
<td>Application Security Access</td>
</tr>
<tr>
<td>2.2.3</td>
<td>Security and System Administration</td>
</tr>
</tbody>
</table>
# Table of Contents (continued)

## Section 3.0 Operation

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>3-1</td>
</tr>
<tr>
<td>3.1.1</td>
<td>3-1</td>
</tr>
<tr>
<td>3.1.1.1</td>
<td>3-2</td>
</tr>
<tr>
<td>3.1.2</td>
<td>3-3</td>
</tr>
<tr>
<td>3.1.3</td>
<td>3-3</td>
</tr>
<tr>
<td>3.1.4</td>
<td>3-3</td>
</tr>
<tr>
<td>3.1.4.1</td>
<td>3-4</td>
</tr>
<tr>
<td>3.1.4.2</td>
<td>3-5</td>
</tr>
<tr>
<td>3.1.4.3</td>
<td>3-10</td>
</tr>
<tr>
<td>3.1.4.4</td>
<td>3-10</td>
</tr>
<tr>
<td>3.1.4.5</td>
<td>3-12</td>
</tr>
<tr>
<td>3.1.4.6</td>
<td>3-13</td>
</tr>
<tr>
<td>3.1.4.7</td>
<td>3-14</td>
</tr>
<tr>
<td>3.1.4.8</td>
<td>3-15</td>
</tr>
<tr>
<td>3.1.5</td>
<td>3-15</td>
</tr>
<tr>
<td>3.1.6</td>
<td>3-18</td>
</tr>
<tr>
<td>3.2</td>
<td>3-19</td>
</tr>
<tr>
<td>3.2.1</td>
<td>3-19</td>
</tr>
<tr>
<td>3.2.2</td>
<td>3-20</td>
</tr>
<tr>
<td>3.2.2.1</td>
<td>3-21</td>
</tr>
<tr>
<td>3.2.2.2</td>
<td>3-22</td>
</tr>
<tr>
<td>3.2.2.3</td>
<td>3-23</td>
</tr>
<tr>
<td>3.3</td>
<td>3-29</td>
</tr>
<tr>
<td>3.4</td>
<td>3-30</td>
</tr>
<tr>
<td>3.5</td>
<td>3-30</td>
</tr>
<tr>
<td>3.6</td>
<td>3-31</td>
</tr>
</tbody>
</table>

## Section 4.0 Standards and Tolerances

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>4-1</td>
</tr>
</tbody>
</table>

## Section 5.0 Periodic Maintenance

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>5-1</td>
</tr>
</tbody>
</table>

## Section 6.0 Maintenance Procedures

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>6-1</td>
</tr>
<tr>
<td>6.2</td>
<td>6-1</td>
</tr>
<tr>
<td>6.2.1</td>
<td>6-1</td>
</tr>
<tr>
<td>6.2.2</td>
<td>6-2</td>
</tr>
<tr>
<td>6.2.3</td>
<td>6-2</td>
</tr>
</tbody>
</table>
Table of Contents (continued)

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.4</td>
<td>Uninterruptible Power Supply (UPS) ........................................</td>
</tr>
<tr>
<td>6.2.5</td>
<td>Anti-Virus .............................................................................</td>
</tr>
<tr>
<td>6.2.6</td>
<td>External Hard Drive ..................................................................</td>
</tr>
<tr>
<td>6.3</td>
<td>Other Maintenance Tasks ..........................................................</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Clean ARMT Client and Server Workstations ................................</td>
</tr>
<tr>
<td>6.3.2</td>
<td>User Account Review ..................................................................</td>
</tr>
<tr>
<td>6.4</td>
<td>Special Maintenance Procedures ..................................................</td>
</tr>
<tr>
<td>6.4.1</td>
<td>Ping Server from Client ..............................................................</td>
</tr>
<tr>
<td>6.4.2</td>
<td>Test Flight Strip Scan Function ..................................................</td>
</tr>
</tbody>
</table>

Section 7. Corrective Maintenance

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>General .................................................................................</td>
</tr>
<tr>
<td>7.2</td>
<td>Onsite Corrective Maintenance ..................................................</td>
</tr>
<tr>
<td>7.3</td>
<td>Reboot ARMT Server Workstation ................................................</td>
</tr>
<tr>
<td>7.4</td>
<td>Reserved ..................................................................................</td>
</tr>
<tr>
<td>7.5</td>
<td>Reboot ARMT Client Workstation ................................................</td>
</tr>
<tr>
<td>7.6</td>
<td>Reserved ..................................................................................</td>
</tr>
<tr>
<td>7.7</td>
<td>ARMT not receiving EFSTS Data ..................................................</td>
</tr>
<tr>
<td>7.8</td>
<td>ARMT not receiving ARTS/STARS Data ..........................................</td>
</tr>
<tr>
<td>7.9</td>
<td>ARMT Client Sever Connection .....................................................</td>
</tr>
<tr>
<td>7.10</td>
<td>ARMT Display ............................................................................</td>
</tr>
<tr>
<td>7.11</td>
<td>Network Module Switch (Ethernet Switch) ......................................</td>
</tr>
<tr>
<td>7.12</td>
<td>Uninterruptable Power Supply (UPS) ............................................</td>
</tr>
<tr>
<td>7.13</td>
<td>Serial Card (RS-232/422 Communication Card) ................................</td>
</tr>
<tr>
<td>7.14</td>
<td>ARMT Generated Strips not Printing .............................................</td>
</tr>
<tr>
<td>7.15</td>
<td>External Hard Drive ...................................................................</td>
</tr>
<tr>
<td>7.16</td>
<td>EFSTS Server A/B Switch ............................................................</td>
</tr>
<tr>
<td>7.17</td>
<td>Replication Issue .......................................................................</td>
</tr>
<tr>
<td>7.18</td>
<td>Surface Movement Advisory (SMA) ..............................................</td>
</tr>
</tbody>
</table>

Section 8. Parts List

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>General .................................................................................</td>
</tr>
<tr>
<td>8.2</td>
<td>ARMT Server Workstation ..........................................................</td>
</tr>
<tr>
<td>8.2.1</td>
<td>Ordering Information ...............................................................</td>
</tr>
<tr>
<td>8.2.2</td>
<td>Quantity ..................................................................................</td>
</tr>
<tr>
<td>8.3</td>
<td>ARMT Client Workstation ..........................................................</td>
</tr>
<tr>
<td>8.3.1</td>
<td>Ordering Information ...............................................................</td>
</tr>
<tr>
<td>8.3.2</td>
<td>Quantity ..................................................................................</td>
</tr>
<tr>
<td>8.4</td>
<td>Network Module Switch (Ethernet Switch) ......................................</td>
</tr>
<tr>
<td>8.5</td>
<td>Fiber Module (Fiber Card Switch Module) ......................................</td>
</tr>
<tr>
<td>8.6</td>
<td>Uninterruptable Power Supply (UPS) ............................................</td>
</tr>
<tr>
<td>8.7</td>
<td>Serial Card (RS-422 Communications Card) ...................................</td>
</tr>
</tbody>
</table>
Table of Contents (continued)

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8 Laser Printer</td>
<td>8-4</td>
</tr>
<tr>
<td>8.9 Ethernet Extenders (CAT 5e Extender)</td>
<td>8-4</td>
</tr>
<tr>
<td>8.10 External Hard Drive</td>
<td>8-4</td>
</tr>
</tbody>
</table>

Section 9. Installation Integration and Checkout

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 Site Information and Drawings</td>
<td>9-1</td>
</tr>
<tr>
<td>9.2 Installation Materials Required</td>
<td>9-1</td>
</tr>
<tr>
<td>9.3 Unpacking and Handling Instructions</td>
<td>9-2</td>
</tr>
<tr>
<td>9.4 ARMT Equipment Installation</td>
<td>9-3</td>
</tr>
<tr>
<td>9.4.1 Install / Replace Server Workstation</td>
<td>9-3</td>
</tr>
<tr>
<td>9.4.2 Install / Replace Client Workstation</td>
<td>9-4</td>
</tr>
<tr>
<td>9.4.3 Install / Replace Uninterruptable Power Supply (UPS)</td>
<td>9-5</td>
</tr>
<tr>
<td>9.4.4 Install / Replace Network Printer</td>
<td>9-6</td>
</tr>
<tr>
<td>9.4.5 Install / Replace Network Module Switch (Ethernet Switch)</td>
<td>9-7</td>
</tr>
<tr>
<td>9.4.6 Install / Replace Monitor</td>
<td>9-7</td>
</tr>
<tr>
<td>9.4.7 Install / Replace ARMT External Hard Drive</td>
<td>9-7</td>
</tr>
<tr>
<td>9.4.8 Replace ARMT/EFSTS Interface Cables</td>
<td>9-10</td>
</tr>
</tbody>
</table>

Section 10. Computer Software

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1 Programs</td>
<td>10-1</td>
</tr>
<tr>
<td>10.1.1 Server Programs</td>
<td>10-1</td>
</tr>
<tr>
<td>10.1.2 Client Programs</td>
<td>10-2</td>
</tr>
<tr>
<td>10.2 DataBase</td>
<td>10-2</td>
</tr>
<tr>
<td>10.2.1 Airport Management (APM) Database</td>
<td>10-2</td>
</tr>
<tr>
<td>10.3 Configuration Files</td>
<td>10-2</td>
</tr>
<tr>
<td>10.3.1 Server</td>
<td>10-2</td>
</tr>
<tr>
<td>10.3.2 Client</td>
<td>10-3</td>
</tr>
<tr>
<td>10.4 Open Database Connectivity (ODBC) Connections</td>
<td>10-3</td>
</tr>
<tr>
<td>10.5 ARMT Commercial-Off-the-Shelf (COTS) Software</td>
<td>10-5</td>
</tr>
</tbody>
</table>

APPENDIX A. MOA Sample

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1 MOA Sample</td>
<td>A-1</td>
</tr>
</tbody>
</table>

APPENDIX B. Glossary of Terms

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.1 Abbreviations and Acronyms</td>
<td>B-1</td>
</tr>
</tbody>
</table>
# Table of Contents (continued)

## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>ARMT Client/Server Configuration</td>
</tr>
<tr>
<td>2-1</td>
<td>Multiple Client ARMT System Configuration</td>
</tr>
<tr>
<td>3-1</td>
<td>A/B Switch for EFSTS Interface</td>
</tr>
<tr>
<td>3-2</td>
<td>EFSTS Interface</td>
</tr>
<tr>
<td>3-3</td>
<td>Terminal Interface</td>
</tr>
<tr>
<td>3-4</td>
<td>ARTS Message Types</td>
</tr>
<tr>
<td>3-5</td>
<td>STARS Message Types</td>
</tr>
<tr>
<td>3-6</td>
<td>Tools Dropdown</td>
</tr>
<tr>
<td>3-7</td>
<td>Interface Configuration</td>
</tr>
<tr>
<td>3-8</td>
<td>Position control Panel</td>
</tr>
<tr>
<td>3-9</td>
<td>Fix Pair Printing</td>
</tr>
<tr>
<td>3-10</td>
<td>Print Strip Exceptions</td>
</tr>
<tr>
<td>3-11</td>
<td>ARMT Server Application Window</td>
</tr>
<tr>
<td>3-12</td>
<td>ARMT System Monitor</td>
</tr>
<tr>
<td>3-13</td>
<td>ARMT Replication Server</td>
</tr>
<tr>
<td>3-14</td>
<td>SMA Interface</td>
</tr>
<tr>
<td>3-15</td>
<td>GuardDog</td>
</tr>
<tr>
<td>3-16</td>
<td>ARMT Command Bar – Red Status</td>
</tr>
<tr>
<td>3-17</td>
<td>ARMT Command Bar – Yellow Status</td>
</tr>
<tr>
<td>3-18</td>
<td>ARMT Command Bar – Orange Status</td>
</tr>
<tr>
<td>3-19</td>
<td>ARMT Command Bar – Green Status</td>
</tr>
<tr>
<td>3-20</td>
<td>ARMT Command Bar – Backup Status</td>
</tr>
<tr>
<td>3-21</td>
<td>ARMT Command Bar – No Server</td>
</tr>
<tr>
<td>3-22</td>
<td>Connection Status</td>
</tr>
<tr>
<td>3-23</td>
<td>Client Connectivity</td>
</tr>
<tr>
<td>3-24</td>
<td>FAA Security Warning Window</td>
</tr>
<tr>
<td>3-25</td>
<td>ARMT Login Window</td>
</tr>
<tr>
<td>3-26</td>
<td>ARMT Invalid Log In Warning</td>
</tr>
<tr>
<td>3-27</td>
<td>ARMT User Account Locked Message</td>
</tr>
<tr>
<td>3-28</td>
<td>Client Switch User Change Group Account Access</td>
</tr>
<tr>
<td>3-29</td>
<td>Administration Drop Down</td>
</tr>
<tr>
<td>3-30</td>
<td>User Maintenance Window</td>
</tr>
<tr>
<td>3-31</td>
<td>Set UP New Group Account</td>
</tr>
<tr>
<td>3-32</td>
<td>Password Alert: Used Previously</td>
</tr>
<tr>
<td>3-33</td>
<td>Password Alert: User ID in Password</td>
</tr>
<tr>
<td>3-34</td>
<td>Modify Group Account: Reset Password</td>
</tr>
<tr>
<td>3-35</td>
<td>Command Bar User History</td>
</tr>
<tr>
<td>3-36</td>
<td>On Demand User Group History</td>
</tr>
<tr>
<td>3-37</td>
<td>Alert Setup</td>
</tr>
<tr>
<td>3-38</td>
<td>CA Total Defense Antivirus Icon</td>
</tr>
</tbody>
</table>
# Table of Contents (continued)
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6-1.</td>
<td>ARMT Client Command Bar Normal Status</td>
<td>6-1</td>
</tr>
<tr>
<td>6-2.</td>
<td>ARMT System Monitor Icon</td>
<td>6-2</td>
</tr>
<tr>
<td>6-3.</td>
<td>UPS Status Monitor Panel Display</td>
<td>6-4</td>
</tr>
<tr>
<td>6-4.</td>
<td>CA Total Defense Antivirus Icon</td>
<td>6-5</td>
</tr>
<tr>
<td>6-5.</td>
<td>CA Total Defense Menu</td>
<td>6-5</td>
</tr>
<tr>
<td>6-6.</td>
<td>CA Total Defense Window</td>
<td>6-6</td>
</tr>
<tr>
<td>6-7.</td>
<td>CA Total Defense Security Overview</td>
<td>6-6</td>
</tr>
<tr>
<td>6-8.</td>
<td>CA Total Defense Window – LogView Button/Scheduled Scan Tab</td>
<td>6-7</td>
</tr>
<tr>
<td>6-9.</td>
<td>Sample ARMT User Account Access Request Form</td>
<td>6-11</td>
</tr>
<tr>
<td>6-10</td>
<td>Sample ARMT User Group Access Control List Form</td>
<td>6-12</td>
</tr>
<tr>
<td>7-1</td>
<td>No Server Alert</td>
<td>7-6</td>
</tr>
<tr>
<td>7-2</td>
<td>Sea Level Card 7404</td>
<td>7-7</td>
</tr>
<tr>
<td>7-3</td>
<td>ARMT Server</td>
<td>7-8</td>
</tr>
<tr>
<td>9-1</td>
<td>EFSTS to A/B Switch Pinout</td>
<td>9-10</td>
</tr>
</tbody>
</table>

## List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>Subject Matter Experts</td>
<td>1-7</td>
</tr>
<tr>
<td>3-1</td>
<td>Controls and Indicators</td>
<td>3-1</td>
</tr>
<tr>
<td>3-2</td>
<td>Turn On and Checkout</td>
<td>3-3</td>
</tr>
<tr>
<td>3-3</td>
<td>Equipment Shutdown</td>
<td>3-24</td>
</tr>
<tr>
<td>7-1</td>
<td>ARMT Symptom Chart</td>
<td>7-1</td>
</tr>
<tr>
<td>8-1</td>
<td>Equipment Options</td>
<td>8-1</td>
</tr>
<tr>
<td>9-1</td>
<td>Installation Materials Required and Supplied</td>
<td>9-1</td>
</tr>
<tr>
<td>9-2</td>
<td>Installation Materials Required But Not Supplied</td>
<td>9-2</td>
</tr>
<tr>
<td>10-1.</td>
<td>Server COTS Software</td>
<td>10-5</td>
</tr>
<tr>
<td>10-2.</td>
<td>Client COTS Software</td>
<td>10-5</td>
</tr>
</tbody>
</table>
1.0 General Information Air Traffic Control

1.1 INTRODUCTION

a. The Airport Resource Management Tool (ARMT) is an operational support tool using Federal Aviation Administration (FAA) developed software applications hosted using Commercial Off the Shelf (COTS) software platforms on a network of COTS personal computers interfaced with COTS switching and printer equipment that is located at traffic management positions on the control floor at secure FAA Air Traffic Control (ATC) facilities.

b. The ARMT is:
   (1) An operationally based server-client tool developed with COTS software and hardware to provide a low-cost, low-maintenance, scalable, and adaptable system capable of meeting specific site configuration requirements.
   (2) A real-time automated data recording, collection, processing, and analysis system.

c. The ARMT system:
   (1) Supports traffic management decision-making.
   (2) Provides airport performance benchmarking.
   (3) Assists traffic management specialists and managers with airport flows and logs delay information.

1.1.1 Background

a. Initially, the ARMT was a non-standard system developed and maintained by a single FAA employee. Currently, it is in use at over 35 major NAS terminal facilities by traffic management unit specialists and controllers, supporting over 27 million operations per year ARMT facilitates communications data between an Air Route Traffic Control Center (ARTCC), a Tower, and a Terminal Radar Approach Control (TRACON).

b. Development began in 1990 as a joint effort between the Air Traffic Control Tower (ATCT) in the Atlanta Airport and Delta Airlines. Prior to the commissioning of the new Atlanta consolidated TRACON (A80) in 2001, local resources focused on the enhancement of ARMT to function in conjunction with the Common Automated Radar Terminal Systems (CARTS) IIIE automation system.

c. The current ARMT fielded today is a result of recoding and reconfiguring the system for improvements and enhancements, and to provide a baseline that follows the National Airspace System (NAS) configuration management policies.

1.1.2 Purpose

The purpose of this book is to provide information on operation, maintenance, installation, setup, and system administration of the ARMT.

1.1.3 Scope

This document was developed using the functional specifications of the ARMT. There is no impact to the existing terminal automation system requirements or functionality through this effort. No validation of flight data will occur within the ARMT.
1.2 RELATED PUBLICATIONS

1.2.1 Government References

a. FAA JO 6131.5, Maintenance of the Airport Resource Management Tool (ARMT)

b. FAA Order 6000.15, General Maintenance Handbook for National Airspace System (NAS) Facilities

c. FAA Order 6980.29, Maintenance of Static Uninterruptible Power Supply Systems

d. FAA Order 1370.96, Air Traffic Organization (ATO) System Access Control

e. FAA Order 1370.82, Information Systems Security Program

f. FAA Order 1370.91, Information Systems Security Patch Management

h. FAA Order 1370.100, Media Sanitization and Destruction Policy

i. FAA Order 1370.109, Software Assurance Policy

j. FAA Order 1370.111, Removable Media Security Policy

k. FAA Order 1600.1, Personnel Security Program

l. FAA Order 1600.2, Safeguarding Classified National Security Information

m. FAA Order 1600.6, Facility Security Policy

n. FAA Order 1600.69, FAA Facility Security Management Program

o. FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI)

p. FAA Order 1370.114, Implementation of Federal Aviation Administration (FAA) Telecommunications Infrastructure (FTI) Services and Information Security Requirements in the National Airspace System (NAS)

q. FAA Order 1920.5, Technical Field Operations Services Field Incident Response (FIR)

r. ARMT System Characterization Document (SCD)

s. ARMT Information System Security Plan (SSP)

t. ARMT Information System Contingency Plan

u. ARMT Security Rules of Behavior (RoB)

v. ARMT Security & System Administration Procedures Handbook

w. ARMT Security User Access & Group Lists Forms

1.2.2 Other References

COTS manuals provided to each site by the ARMT Program Office. The R:\ drive on each ARMT system contains a folder called ARMT User Guides that serves as a repository for all ARMT COTS hardware and software manuals.
1.3 SUPPORT

1.3.1 Logistic Support

Replacement parts for the ARMT are available through the Logistics Center at the William J. Hughes Technical Center (WJHTC), Atlantic City International Airport, NJ. ARMT does not require or support on site spares.

1.3.2 Maintenance Support

Air Traffic Organization-Terminal (ATO-T) at the WJHTC provides second Level Engineering Support (202) 409-2959.

1.4 EQUIPMENT DESCRIPTION

The ARMT system consists of the following operational hardware:

a. ARMT Server Workstation System:
   (1) Monitor, Keyboard and Mouse
   (2) Network Switch Module (Ethernet Switch)
      (a) Fiber Module (Fiber Card Switch Module) optional
      (b) Ethernet Extender (CAT5e Extender) optional
   (3) Serial Card (RS-422 Communications Card)
   (4) Ethernet 10/100 LAN Card
   (5) A/B Switch for EFSTS connectivity
   (6) Uninterruptable Power Supply
   (7) External Hard Drive

b. ARMT Client Workstation system:
   (1) Monitor, Keyboard and Mouse
   (2) Uninterruptable Power Supply
   (3) Network Switch Module (Ethernet Switch)
      (a) Fiber Switch Module optional
      (b) CAT5e Ethernet Extender optional
   (4) Speakers (ATCTs only)
   (5) Network Laser Printer

1.4.1 ARMT SERVER WORKSTATION

a. The ARMT server workstation manages the users, stores data, is transparent to the user, and supports the ARMT client workstations located throughout the facility at key traffic management positions. It serves as the interface to the NAS to retrieve flight plan and NAS delay information from the primary interfaces, which are the Automated Radar Terminal Systems (ARTS), Electronic Flight Strip Transfer System (EFSTS), and Standard Terminal Automated Replacement System (STARS).
b. The ARMT server workstation runs the ARMT server application. The server workstation consists of, at a minimum:

1. Pentium processor
2. Windows operating system
3. 500 GB hard drive
4. 16X DVD+/-RW drive
5. 8 GB RAM memory
6. Two Ethernet 10/100 Local Area Network (LAN) Cards, (one communicates information to the network and the other communicates to the automation system - C ARTS / STARS)
7. A Serial RS-422 Communication Card to interface with the EFSTS system. The RS-422 communications card is a four port Peripheral Component Interconnect (PCI) serial card. This card must be configured to use RS-422 communications after installation.
8. Monitor, Keyboard and Mouse
9. Microsoft Office Professional software suite
10. Other COTS applications, such as antivirus/malicious code software.

c. Connected to the Server Workstations is:

1. External hard drive. The external hard drive is connected to the server named “Primary” and used to store backup data.
2. UPS. The UPS is required to be connected to each of the server and client workstations because the ARMT system is not certified to be on critical power. The UPS connects to the computer USB port and provides information, such as battery time remaining to allow the software to automatically shut down before complete loss of power.
3. Network Switch Module (Ethernet Switch). The network switch module provides connectivity from the ARMT server to the ARMT client network. The minimum requirement is a 16 port 10/100 Mbps switch with an optional fiber card switch module. The number of ports is dependent on the number of positions at the facility.
   (a) Fiber Switch Module – optional. This optional fiber card switch module is only used in conjunction with the network switch module, and only if there is more than one switch and they are located more than 100 meters from each other. This module allows for a standard connector (SC) fiber connection between two switches to enable extended transmission control protocol/internet protocol (TCP/IP) communication.
   (b) CAT5e Ethernet Extender - optional. This optional CAT5e Extender is used only in facilities when the distance between switches exceeds the maximum length of CAT5e (100 meters).
4. A/B Switch. The A/B switch is connected to both Server Workstations and the EFSTS. Selecting one of the servers allows two-way communication between the EFSTS and server.
1.4.2 **ARMT Clients.**

a. The ARMT clients display airport data received from the server. ARMT client workstations provide the user access to the system. All servers will have an interface to EFSTS used by ground controllers at the tower cab and for ARMT to support the taxi list. Use of the EFSTS scanners is the building block for the taxi list that is the cornerstone of the ARMT functions for managing departures.

b. The total number of client workstations is dependent on the configuration required for each site.

c. The client workstation consists of, at a minimum:
   1. Pentium processor
   2. Windows operating system
   3. 8X DVD+/-RW drive
   4. 8 GB RAM memory
   5. 250 GB Hard drive
   6. One Ethernet 10/100 LAN Card
   7. Monitor, Keyboard and Mouse
   8. Microsoft Office Professional software suite
   9. Other COTS applications, such as antivirus/malicious code software.

d. Connected to the Client Workstation is:
   1. UPS. The UPS is required to be connected to each of the server and client workstations because the ARMT system is not certified to be on critical power. The UPS connects to the computer USB port and provides information, such as battery time remaining to allow the software to automatically shut down before complete loss of power.
   2. Network Switch Module (Ethernet Switch). The network switch module provides connectivity from the ARMT server to the ARMT client network. The minimum requirement is a 16 port 10/100 Mbps switch with an optional fiber card switch module. The number of ports is dependent on the number of positions at the facility.
      a. Fiber Switch Module – Optional. This optional fiber card switch module is only used in conjunction with the network switch module, and only if there is more than one switch and they are located more than 100 meters from each other. This module allows for a standard connector (SC) fiber connection between two switches to enable extended transmission control protocol/internet protocol (TCP/IP) communication.
      b. Ethernet Extender (CAT5e Extender) optional. This optional CAT5e Extender is used only in facilities when the distance between switches exceeds the maximum length of CAT5e (100 meters).
   3. Network Laser Printer. The network laser printer is used to print out reports generated by ARMT.
   4. Speakers (optional). Speakers are installed at ATCT sites only.
1.5 CONCEPT OF OPERATION
   a. ARMT pre-configured COTS workstations equipped with the ARMT application software interfaces to the NAS through a one-way data-receive secure connection between the ARMT server and the facility Air Traffic Control (ATC) automation system which could be ARTS or STARS.
   b. ARMT activity does not affect the presentation of any interfacing ATC system.
   c. ARMT uses COTS hardware to interface with the following systems to receive data:
      (1) Electronic Flight Strip Transfer System (EFSTS)
      (2) Surface Movement Advisory (SMA)

1.6 REQUIREMENTS
The ARMT system is a server/client architecture based system. The minimum hardware for the ARMT system consists of two Personal Computer (PC) servers, a client workstation with display, a switch, an external hard drive, and a UPS.

1.7 CONNECTIVITY
   a. ARMT sites are connected through the existing FAA Telecommunications Infrastructure (FTI) using 512 kbs for data traffic.
   b. Locally attached ARMT server workstations, client workstations, and printers are connected with CAT5e Plenum cable.
   c. The ARMT server provides two network interface cards: one for the FTI connection and one for the ARTS or STARS interface.
   d. The ARMT server is connected to the EFSTS system via an A/B switch to the RS-422 serial communication card installed in each servers. The A/B switch is installed at the ARMT rack to connect the EFSTS to the active ARMT server.

1.8 REDUNDANCY
   a. ARMT utilizes a backup server that maintains a replica of the primary server database.
   b. The second server connects to the main server, is updated on a continuing basis from the main server, and acts as a standby backup server for recovery.
1.9 RELATIONSHIP OF COMPONENTS

![Diagram of ARMT Client/Server Configuration]

1.10 SOFTWARE OVERVIEW

a. The ARMT application runs on a Windows-based operating system.

b. ARMT software development and modification is controlled by the FAA at the WJHTC in Atlantic City, NJ. Software issues should be directed to the Subject Matter Expert (SME) at the WJHTC between the hours of 8am and 4pm Monday through Friday. During off hours and weekends, contact the National Operation Control Center (NOCC) helpdesk. Refer to table 1.1 for SME contact information.
Table 1.1 Subject Matter Experts

<table>
<thead>
<tr>
<th>Name/Title</th>
<th>Area of Expertise</th>
<th>Location</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brian Schell, Program Manager</td>
<td>ARMT Program Management Office</td>
<td>WJHTC, Terminal Second Level Engineering Support (AJM-2440)</td>
<td>609-485-8264</td>
</tr>
<tr>
<td>Mike Everland</td>
<td>ARMT Program Management Office, Software &amp; Field Support</td>
<td>WJHTC, Terminal Second Level Engineering Support (AJM-2440)</td>
<td>609-485-8080</td>
</tr>
</tbody>
</table>

1.11 DATABASES
a. The ARMT uses the MySQL database.
b. MySQL resides on the ARMT server workstations.
c. For detailed information, refer to Section 10, Computer Software.

1.12 ARMT SYSTEM ADMINISTRATION
ARMT System Administration tasks are defined in accordance with the ARMT Requirements Document and provide sufficient guidance for maintenance personnel to execute routine system administration functions at local facilities to support ARMT operations.

1.13 ARMT INFORMATION SYSTEM SECURITY
a. On site technical maintenance personnel provide support for the ARMT information system security compliance by performing specific system administration tasks for security monitoring and reporting.
b. ARMT information system security maintenance support objectives are to ensure that ARMT system operations comply with existing FAA information system security policies and procedures to ensure security performance and protection in keeping with the approved ARMT System Security Authorization Certification Package (SCAP) obtained for the system.

c. ARMT information system security activities are required during normal operations and as part of routine, scheduled, and emergency operational conditions. ARMT system-specific security policies, procedures and supporting documentation (forms, processes, etc.) are provided in the ARMT Security & System Administration Procedures Handbook.

d. Security-specific conditions, environmental drivers, and events are provided in the ARMT System Characterization Document (SCD), Information System Security Plan (ISSP) and the ARMT Information System Contingency Plan (ISCP). These documents are located on each workstation, on the R: drive under the Resources folder.
2.0 TECHNICAL DESCRIPTION

2.1 SIMPLIFIED THEORY OF OPERATION

a. The Airport Resource Management Tool (ARMT) system consists of a network of server and corresponding client(s) that provide workstations, displays, and printers.

b. The ARMT server is typically located at Terminal Radar Approach Control facility (TRACONs) and the ARMT client systems are at TRACONs, Air Traffic Control Tower (ATCTs), Air Route Traffic Control Center (ARTCCs), and the Air Traffic Control System Command Center (ATCSCC).

c. ARMT communicates with the following ATC automation systems:

   (1) Automated Radar Terminal System (ARTS)
       (a) ARMT systems interfaced to ARTS facilities receive flight and radar data through the ARTS Gateway (AGW).

   Or

   (2) Standard Terminal Automation Replacement System (STARS)
       (a) ARMT systems interfaced to STARS facilities receive flight and radar data through the STARS Applications Interface Gateway (AIG).

   (3) Electronic Flight Strip Transfer System (EFSTS)

   (4) National Aeronautics and Space Administration (NASA) Surface Movement Advisory (SMA) – Atlanta (A80) only

   (5) FAA Future Telecommunications Infrastructure (FTI) Operational Data Network (FTI OPS)

   Note: The validity of the data presented by the ARMT to the user is only as accurate as the data received from the ATC or other interfacing system.

d. The system consists of two server workstations that receive data off the Transmission Control Protocol/Internet Protocol (TCP/IP) Ethernet port on the ARTS Local Area Network (LAN) or from STARS. The data is distributed to clients through the ARMT network.

e. The ARMT server workstations are located at the TRACON and receive traffic data from the ATC systems through either the ARTS AGW or the STARS AIG. The ARMT receives flight plan data from the EFSTS, ARTS or STARS, and SMA. This data is processed at the server workstation and sent to the client workstations for display at traffic management positions. The client workstation positions are physically located at TRACONs, ATCTs, ARTCCs, and the ATCSCC. The server communicates with the clients over CAT 5e Ethernet cable connected through an Ethernet Switch.

   Note: In Atlanta, Georgia only, the SMA server located at the A80 TRACON provides ramp and pushback data to the ARMT server.

f. Figure 2-1 provides an illustration of the typical ARMT configuration and connectivity in a multiple-client environment.
FIGURE 2-1. MULTIPLE CLIENT ARMT SYSTEM CONFIGURATION
2.2 DETAILED THEORY OF OPERATION

2.2.1 Overview of ARMT Functional Capabilities

ARMT is used to perform the following functions:

a. Receive real-time track data from the automation system. Communicate with the automation system (ARTS / STARS) at the facility. For example, ARMT will communicate through the ARTS AGW at an ARTS IIIE facility, and receive data from STARS facilities through the AIG. Data is transmitted to the ARTS through the following message: \textit{PC Heartbeat Msg}.

Data from the AGW/AIG are made up of the following:

1. Active Track Maintenance Message
2. Delete Flight Data Message
3. Delete Track Message
4. Flight Plan Maintenance Message
5. HeartBeat Message
6. Continuous Data Recording (CDR) Autofunction Message for ARMT

b. Communicate and/or exchange data with other tracking systems (EFSTS and SMA).

c. Receive flight plans from the ARTCC through the connection with the EFSTS.

d. Process departure data for the facility. Tracks flight plan inventory, aircraft taxi information, departure delays, and departure rates.

e. Process arrival data for the facility. Tracks the inventory of aircraft, arrival delays, handoffs from Host sectors, track vector time, airspace utilization, and arrival landing rate.

f. Track NAS delays and, if adapted, has the ability to send a flight strip request message to EFSTS. Tracks both arrival and departure delays based upon arrival and departure strip times at adapted positions. User receives:

1. Aural notification stating call sign and visual notification for flight strip timeout within ten minutes of NAS removal time.

2. Notification and display of volume delays, and Estimated Departure Clearance/Control Time (EDCT) delays.

3. Notification of NAS holding delays. When an aircraft enters the Tower taxi list and it is destined for an apreq, ground delay (EDCT) or ground stop airport, the user will receive a visual and aural alarm, if adapted.

g. Display current facility conditions, general weather conditions, and traffic impact conditions such as runway, approach and landing direction.

h. Generate reports on gathered data for arrival performance, departure performance, runway efficiency, capacity utilization, and analysis of arrival and departure push data. Calculations on collected data for departures and arrivals.
2.2.2 Application Security Access

Refer to the ARMT Information System Security Plan, (SSP) for detailed information on ARMT Security features and functions. This document is accessible from all ARMT workstations via the network resources drive (R: drive) and is located in the Resources folder.

a. ARMT retains a log of users and system administrators each time they successfully complete log in, fail to log in, or exit the program. Local site System Administrators should maintain a secure log of authorized users and individuals and their assigned membership in user or administrator group accounts including user names, passwords and credentials for the ARMT. These records are archived as backup files to the WJHTC every 45 days.

b. When a user selects the application and enters a user ID and password, this feature provides user authentication and starts an internal clock to provide reporting data as to the time on position calculation for each user. Log in activates a clock start time to run until the user logs out/off of the ARMT. At a new user log in, the clock restarts using the new user ID and password.

c. This data is stored internally to ARMT and is available for retrieval as a data file/export file when requested. These files should be retained for a minimum of 45 days.

d. Passwords are managed locally by site system administrators designated to provide security access and control functions.

2.2.3 Security and System Administration

Local site maintenance personnel are responsible for basic security and system administration functions for the ARMT, including the following activities.

a. Management and administration of operating system and application user accounts, preparation, completion and retention of ARMT User Access Account Request forms, generation of on-demand user group account lists for verification/validation and inspection.

b. Review and reporting of security events logs and security incident reporting.

c. Ensuring that security-related confirmation management processes are adhered to, including verification that security patches, security software and other applications are installed and operating correctly.

d. Ensuring that annual security training is completed for all ARMT users, completing training logs and coordinating with the program office.

e. Utilizing procedures, forms and policies detailed in the ARMT Security & System Administration Procedures Handbook for a description of special maintenance tasks assigned to designated site automation system maintenance managers/personnel.

f. The ARMT Security & System Administration Procedures Handbook document is available from ARMT client and server workstations in the ARMT Resources folder, the ARMT Knowledge Sharing Network (KSN) site, and/or from the ARMT Program Office.
3.0 Operation

3.1 GENERAL
This section describes how to operate ARMT. It is assumed that users are familiar with the operation of all government-furnished equipment used in conjunction with ARMT and all equipment has been installed as directed in chapter 9 of this instruction book. Refer to paragraph 1.2 for a list of relevant documentation.

b. Operation is described for:
   (3) Controls and indicators
   (4) Turn-on and checkout
   (5) Remote monitoring and control
   (6) Client workstation operation
   (7) Equipment shutdown

3.1.1 Controls and Indicators

<table>
<thead>
<tr>
<th>TABLE 3–1. CONTROLS AND INDICATORS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control or Indicator</strong></td>
</tr>
<tr>
<td>1) ARMT SERVER WORKSTATION</td>
</tr>
<tr>
<td>Power Switch On/Off</td>
</tr>
<tr>
<td>Power Indicator Light</td>
</tr>
<tr>
<td>2) ARMT CLIENT WORKSTATION</td>
</tr>
<tr>
<td>Power Switch On/Off</td>
</tr>
<tr>
<td>Power Indicator Light</td>
</tr>
<tr>
<td>3) UPS</td>
</tr>
<tr>
<td>Power Switch On/Off</td>
</tr>
<tr>
<td>Power Indicator Light</td>
</tr>
<tr>
<td>4) ETHERNET SWITCH</td>
</tr>
<tr>
<td>Power Switch On/Off</td>
</tr>
<tr>
<td>Power Indicator Light</td>
</tr>
<tr>
<td>Link Indicator Light</td>
</tr>
<tr>
<td>5) ARMT DISPLAY</td>
</tr>
<tr>
<td>Power Switch On/Off</td>
</tr>
<tr>
<td>Power Indicator Light</td>
</tr>
<tr>
<td>6) A/B SWITCH</td>
</tr>
<tr>
<td>“A” position enables the server labeled “primary” to send messages to efsts.</td>
</tr>
<tr>
<td>“B” position enables the server labeled “primary” to send</td>
</tr>
</tbody>
</table>
3.1.1.1 A/B Switch Controls

The ARMT A/B switch device provides for manual selection between primary server connection and stand by backup server connection to the EFSTS. The A/B switch is located in the TRACON equipment room, installed with the servers in the ARMT equipment rack. Connectivity to the back of the device includes a port for the EFSTS input (RS422) and an “A” port to connect to the ARMT primary server, the “B” port connection is for the standby back up server. Should the primary server fail, or during scheduled performance checks to perform a manual switchover between servers, maintenance technicians will also be required to manually establish the connectivity to EFSTS using the control on the A/B switch device. Figure 3-1 provides the control and configuration for the ARMT A/B switch used to manage EFSTS connections.

**FIGURE 3-1. A/B SWITCH for EFSTS INTERFACE**
3.1.2 Turn-On and Checkout

TABLE 3–2. TURN ON AND CHECKOUT

<table>
<thead>
<tr>
<th>Location</th>
<th>Item</th>
<th>Action</th>
<th>Indication-Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) ARMT Rack</td>
<td>UPS - Power Switch</td>
<td>On</td>
<td>Power indicator illuminated</td>
</tr>
<tr>
<td>2) ARMT Rack</td>
<td>Network Switch Module - Power Switch</td>
<td>On</td>
<td>Power indicator illuminated</td>
</tr>
<tr>
<td>3) ARMT Rack</td>
<td>ARMT A/B Switch</td>
<td>On</td>
<td>Power to device. “A” selected for Primary server as normal ops</td>
</tr>
<tr>
<td>4) ARMT Rack</td>
<td>ARMT Monitor</td>
<td>On</td>
<td>Power indicator illuminated</td>
</tr>
<tr>
<td>5) ARMT Rack</td>
<td>Primary Server</td>
<td>On</td>
<td>Power indicator illuminated</td>
</tr>
<tr>
<td>6) ARMT Rack</td>
<td>Primary Server Display</td>
<td>Read</td>
<td>Verify primary server starts up</td>
</tr>
<tr>
<td>7) ARMT Rack</td>
<td>Backup Server</td>
<td>On</td>
<td>Power indicator illuminated</td>
</tr>
<tr>
<td>8) ARMT Rack</td>
<td>Backup Server Display</td>
<td>Read</td>
<td>Verify backup server starts up</td>
</tr>
<tr>
<td>9) ARMT Client</td>
<td>Client Monitors</td>
<td>On</td>
<td>Power indicator illuminated</td>
</tr>
<tr>
<td>10) ARMT Client</td>
<td>Client Workstations</td>
<td>On</td>
<td>Power indicator illuminated</td>
</tr>
<tr>
<td>11) ARMT Client</td>
<td>Client Displays</td>
<td>Read</td>
<td>Verify backup server starts up</td>
</tr>
</tbody>
</table>

3.1.3 Remote Monitoring and Control

ARMT servers and workstations include the Remote Administrator (RADMIN) remote control software package. With RADMIN, ARMT second level support can access site servers, clients and interfaces to manage ARMT network configuration for all server and client connections, to provide COTS software updates, network resources drives, system software adaptation, retention of system logs, system backups and archives for site data.

3.1.4 ARMT Server Interfaces and Programs

The ARMT is a distributed client-server system with primary and backup servers residing at TRACON facilities. The system uses Visual Basic programming language and a MySQL
database system. The server is configured to provide software and hardware tool to support to external NAS interfaces and internal ARMT program interfaces/components, including:

- **a.** EFSTS interface (server software utility and A/B switch for connectivity)
- **b.** Terminal (CARTS/ STARS) interface (server software utility to support automation gateway interfaces)
- **c.** ARMT Server (application core used to process data from internal and external sources, updates a MySQL database)
- **d.** ARMT System Monitor (software utility that monitors ARMT status for workstations and interfaces)
- **e.** ARMT Replication Monitor (server software utility that syncs the ARMT primary and backup servers databases)
- **f.** GuardDog (server software utility that monitors interfaces)
- **g.** SMA (A80 only, server utility to monitor interface status)
- **h.** FTI Operational Data Network (operating system configuration for IP addressing, server utility to determine status of FTI TCP/IP connectivity on ARMT network)

### 3.1.4.1 EFSTS Interface

The EFSTS sends a scan message when an aircraft taxies on the runway and again when it departs. These scan messages also determine when an aircraft is in delay or gate hold. The EFSTS program monitors the communication connection for flight plan data, scans the data, and then inserts the data into the database. Data communication is serial and is received through the Sea Level card.

- **a.** The ARMT receives data from the EFSTS for:
  1. analysis
  2. flight plan data for departure aircraft and amendments
  3. scan data when a flight strip is scanned

- **b.** This data updates the ARMT Taxi List form, the Departure Demand form, and determines delay or removal of strip data.

---

**FIGURE 3-1. EFSTS INTERFACE**
c. The EFSTS Interface launches automatically when the server is started. The EFSTS Interface can also be initiated by selecting the EFSTSMON icon on the ARMT server desktop. View real-time EFSTS input from this window. Refer to figure 3-1A.

(3) Input from EFSTS window displays the EFSTS data being received.

(4) Output to EFSTS shows the ARMT print strip requests being sent to the EFSTS.

(5) Click the Reset button to reset the EFSTS message counter.

(6) Select the Multi Strip Prevention Override (MOVR On/MOVR Off) to send/not send request strip print messages to EFSTS.

(7) Port displays the port number that connects the ARMT server to the EFSTS server.

(8) HandShake indicator value will be 0 for handshaking off or 1 for on.

3.1.4.2 Terminal (ARTS / STARS) Interface

The Terminal Interface software receives data from ARTS or STARS, depending on the site configuration, and uses that data to provide information to ARMT. Every minute, at the 00:00 second mark, the ARMT system time is reset to the ARTS/STARS time. The server time is synchronized when a 1394 message is received from the ARTS system or an AIG100 message is received from the STARS system. The client systems synchronize their clocks every minute to propagate the time throughout the system.

a. At startup, the Terminal Interface software reads the ARMT database to get configuration data from these tables:

   (1) sensors
   (2) message_history
   (3) handoff
   (4) printers
b. The Terminal Interface program launches automatically when the server is started. If necessary, the Terminal Interface program can be initiated by double-clicking the Terminal Interface icon on the ARMT server desktop. Refer to figure 3-2 Terminal Interface.

Note: Refer to the ARMT ISSP for IP addresses for Terminal Interfaces to the Automation Gateways.

(3) **Connection Status** shows the current status of ARMT/Automation Gateway.

(a) When **Auto Connect** is checked, the Terminal Interface will automatically attempt to connect to the Automation Gateway. The **Auto Connect** option should remain checked at all times.

(b) If **Auto Connect** is not checked, the user needs to manually attempt to connect by selecting the corresponding **Connection Status** window.

- Green Window with text: Connected
- Green Window with text: Connected-Standby
- Yellow Window with text: Connecting
- Blue Window with text: Closed

(c) The **Heart Beat Monitors** colors will match the **Connection Status** indicator colors. Once connected, the **Heartbeat Monitors** will pulse between light green and dark green to indicate heartbeat activity from each gateway.

(4) The **HB Threshold** indicates how many seconds ARMT will wait for an automation gateway system heartbeat before alerting the user. If the threshold has been exceeded, a red message will appear above the **HB Threshold** indicating a loss of heartbeat.
**Note:** The GuardDog application will restart the interface if it does not receive a heartbeat message within the site adapted time limit.

(5) Select the **Stats** button to display a pop-up window for a quantitative breakdown of ARTS or STARS Automation Gateway message types. Refer to figures 3-3A and 3-3B.

![FIGURE 3-3A. ARTS MESSAGES TYPES](image)

![FIGURE 3-3B. STARS MESSAGES TYPES](image)

(6) Check **Capture Raw** to output raw Automation Gateway data to file.

(7) Check **Show Message** to display Automation data in the output window.

(8) Click the **Tools** menu to access the configuration options, position control panel, fix pair printing and print strip exceptions. Refer to figure 3-4A.
FIGURE 3-4A. TOOLS DROPDOWN

(a) Clicking on the View/Edit Configuration opens the Interface Configuration window. Refer to Figure 3-4B. This window is used for setting up configuration parameters for the Terminal Interface and should only be accessed by direction of Second Level Support.

FIGURE 3-4B. INTERFACE CONFIGURATION
(b) The Position Control Panel
For site adapted positions this panel can be used to set up the area, printer
printer number, and print parameters. **This is only used for sites that print
strips at handoff.** Refer to Figure 3-4C.

![Position Control Panel](image).

**FIGURE 3-4C. POSITION CONTROL PANEL**

(c) The Position Control Panel

The **Fix Pair Printing** option brings up the pair printing configuration window
and **should only be accessed by direction of Second Level Support.**

This screen is used as a security feature when there are restricted airspaces.
It can be configured to alert controllers when a VFR flight plan has a
configured fix pair in the route of the flight plan. Refer to Figure 3-4D.
FIGURE 3-4D.  FIX PAIR PRINTING

(d)  Print Strip Exceptions.

This window allows editing of print exceptions and should only be accessed by direction of Second Level Support.  Refer to Figure 3-4E

This window is used to configure strip printing exceptions for handoffs between specific controller positions.

Delete exceptions with the red “X”, or enter positions and click “add” to enter a new exception.

FIGURE 3-4E.  PRINT STRIP EXCEPTIONS

3.1.4.3  ARMT Server Application
The MySQL database is the backbone of the ARMT system. ARMT uses one MySQL database for storage and data manipulation on each server computer. All data is passed to the database and referenced from the client systems from this database.

a. The server hosts the interface programs, and all external interfaces are connected through the server. The servers communicate with one another and with the clients through an Ethernet switch. All ARMT functions are sent to the server for database storage and distribution to the clients. All queries and views are through MySQL.

![ARMT Server Application Window](image)

**FIGURE 3-5. ARMT SERVER APPLICATION WINDOW**

b. The ARMT Server application launches automatically when the server is turned on. If needed it can also be launched by clicking the **ARMT Server** icon on the ARMT server desktop to open. The ARMT Server application processes the messages stored in the ARMT database by the interface applications to be retrieved by ARMT client applications. Refer to figure 3-5.

1. Select Process Messages to enable the ARMT Server application to process incoming messages.
2. Current indicates the number of ARMT messages being processed.
3. Total is the number of messages queued up for processing.
4. Last Message Date is the time stamp of the last message processed.
5. Last Message is the scroll of ARMT messages.

### 3.1.4.4 ARMT System Monitor

The ARMT System Monitor program monitors the ARMT clients and servers of the local network. The System Monitor runs on the servers and displays connectivity status.

a. The System Monitor program launches automatically when the server is started. If necessary, the System Monitor program can be initiated by double-clicking the System Monitor icon on the ARMT server desktop. Refer to figure 3-6.

1. Facilities drop-down menu allows for some display filtering by site. This is for facilities with multiple sites configured.
(2) Select **Show Servers Only** to display only workstations defined as server in the type field.

(3) Select **Show Errors Only** to display only workstations that currently are in error.

### FIGURE 3-6. ARMT SYSTEM MONITOR

b. Facility, ID, and IPAddress are defined in the armt.ini file located on ARMT servers in C:\ARMT\Adapt.

1. Field is shaded green when ARMT status is determined to be operational.

2. Field is shaded red (Type=client) when ARMT is not running or destination cannot be pinged. Data is not accessible at the client workstation.

3. Field is shaded red (Type=server) when ARMT application is down or replication is more than 12 seconds behind.
(4) Field is shaded orange (Type=server) when replication is 9-12 seconds behind.

(5) The ID column will identify the following:
   - For Type = server the ID will be either server_primary or server_backup.
   - For Type = server_interface the ID will be either arts, stars, or efsts.
   - For Type = Client the ID will be the terminal ID of the client as shown on the client taskbar. This terminal ID is defined in the com.ini file associated with the client system connecting to the server.

(6) The IP address column, displays the IP addresses for the servers and clients.

   a. The Active column indicates which server is currently active. Active will have a checkmark indicating the current active server. This only applies to Type identified as either server_primary or server_backup.

   b. The Type column defines the system type (server_primary, server_backup, server_interface, or client).

   c. The Ping column indicates whether the server can ping the computer the application is running on. Ping value is either 0 or 1 depending on the ping status of the destination IPAddress.
      - 0 indicates ping failed and will change system color to red.
      - 1 indicates ping is successful, meaning connection is good.

   d. The Replication column should display the number 0 or 1, indicating that replication status is good for the servers. Only the servers run replication. Replication shows status (seconds behind) of replication between the two servers.
      - Field is shaded orange if replication is 9-12 seconds behind.
      - Field is shaded red if replication is more that 12 seconds behind.

3.1.4.5 ARMT Replication Monitor

The ARMT Server Replication Monitor runs on each server (primary and backup) to maintain, and restart replication between primary and backup server databases. The Replication Monitor also keeps track of which server is the primary. The Replication Monitor replication rate is every 10 seconds.

a. If a replication error occurs it will be indicated by an orange or red in the Replication column for Type=server. The monitor will try to restart the replication process. Figure 3-7, ARMT Replication Monitor, shows a deadlock error. The error will clear out at the next run, and then a normal continuation of the replication.
FIGURE 3-7. ARMT REPLICATION MONITOR

b. The Replication Monitor program launches automatically when the server is started. If necessary, the Replication Monitor program can be initiated by double-clicking the Replication Monitor icon on the ARMT server desktop.

1. Replicate, when checked, will allow the server to replicate with the other ARMT server.
2. Make Active, when clicked, the ARMT server will attempt to take over as the Primary ARMT server.
3. Replication Pulse Running field is grayed out with a pulsating check mark indicating that replication is functioning properly.
4. Last Replication Event Time is the time stamp of the last replication event received from the other ARMT server.
5. Last Replication Completion Time is the time stamp of the last replication event sent from the current server.
6. Status window displays OK or a MySQL data error. If “Status” is not “OK”, contact Second Level Support.

CAUTION: Do not close the ARMT Replication Window, as this will terminate replication processes required for database integrity.

3.1.4.6 Surface Movement Advisory (SMA) Interface

The ARMT Surface Movement Advisory (SMA) interface on ARMT Server Workstations receives gate and pushback data to provide status of aircraft in push back sequence prior to entering the ATC ramp for ground control.

Note: This functionality is currently only available at Atlanta TRACON and runs on the Backup Server Workstation.
3.1.4.7 GuardDog

The ARMT GuardDog application monitors the connection status of other ARMT applications. If an application exceeds its designated limit between updates, GuardDog will stop the process, if running, and restart it. This ensures that all interfaces are operating with the most current data available. GuardDog is adapted per site and can be configured to monitor any of the ARMT applications. The ARMT GuardDog application launches automatically when the server is turned on. If needed, it can also be initiated by clicking the GuardDog icon on the ARMT server desktop to open.
3.1.4.8 FTI Operational Data Network

- ARMT connectivity between local clients and the servers at TRACON facilities is supported by a local area network hosted on the facility operational data network provided by FTI.
- To support connectivity between the server and remote clients (at ATCTs and ARTCCs, for example), connectivity is established by dedicated TCP/IP services provided for ARMT as a service level agreement with the FTI program office. Each facility has a unique FTI circuit that has been established to support secure data network connectivity between sites. Bandwidth ranges from 526kbs to 1024kbs, depending upon the facility and network utilization requirements.
- All ARMT servers and clients are installed and configured with the appropriate/authorizes FTI service IP and computer IP addressing. WJHTC second level support maintains a list of all FTI service identification data, IP addresses and other information to assist sites with any service interruptions or troubleshooting activities.
- If it is apparent that FTI services are not within normal operations (via the System Monitor or client status indication) contact WJHTC second level support for instructions and contact the FTI NOCC 877-384-6622 to report an FTI service outage.

3.1.5 Client Applications - Command Bar Window

The ARMT application opens a command bar window that provides a banner of menu items for operators to select from to view traffic management information. The command bar is a static window that remains open while the application is running. Menu items are selectable using mouse click entries that activate drop down lists of ARMT display features.

- Selecting/Deselecting the speaker icon on the Command Bar will mute/unmute all ARMT audible instances. (Note: ATCT client workstations include speakers with manual volume controls. Ensure that speaker volume is on. Command bar provides quick action control for mute/unmute of speakers.)
- When the Command Bar Status Indicator is other than green, it mostly likely means that there is a problem with the Server Workstation or connection to it. If the client is located in a satellite facility (i.e. Tower), contact the TRACON to check the status of the ARMT servers. If the client is located in a TRACON facility, check the status of the ARMT servers using steps in Par. 6.2.2.
- Observe the Status Indicator on the Command Bar:

  **NOTE:** If the Command Bar Status Indicator is a color other than **GREEN**, refer to Table 7-1 for ARMT Symptoms and possible faults.

  1. Red (refer to figure 3-10). The ARMT Server application is not running.

![ARMT Command Bar - Red Status](image-url)
(2) Yellow (refer to figure 3-11). EFSTS interface is not functioning or has not sent any recent information.

FIGURE 3-11. ARMT COMMAND BAR – YELLOW STATUS

(3) Orange (refer to figure 3-12). ARTS/STARS interface is not functioning.

FIGURE 3-12. ARMT COMMAND BAR – ORANGE STATUS

(4) Green (refer to figure 3-13). System status is OK. The client workstation is operational. All interfaces are functioning and the ARMT client is connected to the ARMT server workstation.

FIGURE 3-13. ARMT COMMAND BAR – GREEN STATUS

d. If text is displayed to the right of the status indicator:
   (1) Backup (orange background). All interfaces are running on the backup server workstation. Refer to figure 3-14. If the ARMT client is located in a satellite facility (i.e. Tower), contact the TRACON to check the status of the ARMT primary server. If the client is located in a TRACON facility, check the status of the ARMT primary server.
FIGURE 3-14. ARMT COMMAND BAR – BACKUP STATUS

(2) NO SERVER (orange background). There is either a communications failure to the server, or both servers are down. Refer to figure 3-15. In this condition, there is no real time data exchange over the network between the server and the client and any display information will be obsolete and not suitable for operations. Coordination between client site and TRACON server site maintenance personnel is required to resolve this status condition.

FIGURE 3-15. ARMT COMMAND BAR – NO SERVER

Note: For more information regarding the ARMT Command Bar Air Traffic Functions, refer to the ARMT Job Aid.pdf located in the ARMT Resources folder on any ARMT workstation desktop.

e. The command bar banner row at the top of the window provides:

   (1) Name of the facility
   (2) Terminal ID
   (3) Arrival configuration
   (4) Departure configuration
   (5) Current date and time in Zulu

f. ARMT menu items will include drop down lists for the following features:

   (1) Tools
   (2) Arrivals
   (3) Departures
   (4) NAS Departure Delays
   (5) Administration (when logged in as a system administrator)
   (6) Exit ARMT
   (7) Switch User
   (8) Help
3.1.6 Suspending the EFSTS Alert during slow periods of traffic

During slow periods of traffic, use the following procedure to suspend or ignore the EFSTS alert on ARMT clients.

a. Locate the ARMT command bar on the ARMT client workstation. Refer to figure 3-12.

b. Double click the round status button on the ARMT command bar.

c. The connection status window will display. Refer to figure 3-29.

d. Locate the EFSTS connection and double-click the time (00:00:00) in the Ignore Until column for EFSTS.

e. The Client Connectivity window will be displayed. Refer to figure 3-30.
f. Select a **value** from the Ignore for how many minutes dropdown, and then click the **Submit** button. The EFSTS alert can be ignored for 0, 30, 60, 120, 180, or 240 minutes.

**Note:** During the ignore period the EFSTS alert will not be displayed on all ARMT clients that are connected to the local TRACON.

### 3.2 START UP AND CONFIGURATION SETTINGS

Features and functions related to the initial start up and basic ARMT configuration settings are defined in the armt.ini adaptation file located in C:\ARMT\Adapt, of the server workstations. Client configurations are defined in the com.ini file located in C:\Clients\ARMT\Directory.

#### 3.2.1 User Log In to ARMT Server Workstation and/or Client Workstation

a. Both the Server and Client workstations are setup to automatically log into Windows with a user level account. An administrator account and password are required for facility level access to Windows files. (**Note:** Contact WJHTC Second Level Engineering Support for troubleshooting or access to Windows operating system configurations.)

b. Server workstations at ATC facilities store user identification and password information, and maintain logs of user access to ARMT resources.

c. User logs are stored locally for 45 days, archived to a remote site at the WJHTC for at least 1 year (5 years if data is related to a NAS incident or accident), and accessed remotely using secure access media and controls by the National ARMT System Administration Technical Lead at the WJHTC.

d. ARMT retains system settings, privileges, and other user information on local drives and in network storage and archives retained at the WJHTC.

e. ARMT client workstations provide two types of user access to system resources:
   1. Log in for traffic management via USER or REGULAR group account.
2. Log in for local site system administrators via ADMIN group account.

3.2.2 Launching ARMT Application Server/Client

a. The Server application will launch automatically.

b. The Client application is launched when the APT_ARMT.exe desktop icon is double-clicked.

**Note:** APT is the three letter id of the facility. For example, IAD_ARMT

(1) When the FAA Warning Window (refer to figure 3-18) appears select the OK button at the bottom of the window. Users must accept terms and conditions included in the FAA warning banner to access ARMT application.

![FAA Security Warning Window](image1)

**FIGURE 3-18. FAA SECURITY WARNING WINDOW**

(2) The ARMT login window appears (refer to figure 3-19).

![ARMT Login Window](image2)

**FIGURE 3-19. ARMT LOGIN WINDOW**

**Note:** The ARMT login window will also appear when Switch User is selected from the Command Bar.
(3) Enter group username and 13-character password, and then click on the Login button.

**Note:** Passwords must be 13-characters, combinations of letters, numbers and special characters. (See para 3.2.2.3 for password management requirements.)

(4) Wait for the system to load and the ARMT Command Bar to display.

(5) The color of the round Status display in the top right corner of the ARMT Command Bar should be green indicating the Client Workstation is operational; all interfaces are functioning and the ARMT client is connected to the ARMT server workstation. If the Status indicator is a color other than green, refer to paragraph 3.1.5, Command Bar Window, for a description of status indications on client applications.

### 3.2.2.1 Invalid or Failed Log In

a. Three (3) incorrect attempts to log-in will prohibit access to ARMT. Each failed log in will generate a warning display window, locking the system from log-in after the third failed attempt. (See Figure 3-20.)

b. On the third failed log-in attempt, the system will lock and prohibit group user log on. (See Figure 3-21) Users will need to contact the site tech ops or air traffic system administrator (or if not on duty, contact WJHTC technical support) to unlock the group login account and/or change the group account password.

**FIGURE 3-20. ARMT INVALID LOG IN WARNING**

**FIGURE 3-21. ARMT USER ACCOUNT LOCKED MESSAGE**
User access (either Regular Users or System Administrators group accounts) as well as user preferences and access privileges are established, controlled and managed in the Administration features of ARMT available from the Command Bar Menu, including unlocking group accounts. (See para 3.2.2.3 for details about account management and password resets.)

Switch User Functions

a. ARMT Switch User menu item on the command bar allows for continued ARMT operations while complying with security requirements to log each user group type onto the system. Switch User applies when client settings need to be accessed by System Administrators while ARMT is in use by a regular user. Administration functions are not accessible to regular users, as such, when ARMT settings need to be changed (unlock a group account, change alerts and warning configurations, access user log settings, etc.)

b. The Switch User function is activated to change user group log in and provide access to privileged resources.

c. Switch User is also used to revert back to Regular User operations once System Administrator activity and access is completed.

d. Typically, normal operations require that ARMT traffic management specialists log in as REGULAR users via the established user group account. If site maintenance is required for client workstations, then tech ops personnel must log in to the client using the ADMIN group account. To change from a regular user group account to access to administration resources available to site admins, the ARMT client application menu item “Switch User” must be implemented. Refer to Figure 3-22.
FIGURE 3-22. CLIENT SWITCH USER-CHANGE GROUP ACCOUNT ACCESS
e. To log in as local site System Administrator (assumes client workstation is in use by a regular user group account).

1. Select the Switch User control from the command bar.

2. Enter the System Administrator’s user identification and password.

3. Once required access to Administration menu controls has been completed, use the Switch User menu to return access to the regular user group account.

Note: Do not leave the client workstation until you have the specialist log in as a regular user. Access to ADMIN group accounts are privileged access for site administrators only and should only be active when in use by site administrators for maintenance or configuration activities only.

3.2.2.3 Administrator Functions – Client Workstations Only

a. Select **Administrator** from the ARMT toolbar drop down menu. These features and functions are available when logged on as a user with administrator privileges.

(1) User Setup - Select User Set up from the Administration drop down menu to manage user accounts. This provides the system administrator the ability to add/save new users, and to lock/unlock current user groups. (Refer to Figure 3-23). Upon selection of User Set Up from the drop down menu list, the user account maintenance window opens. When you highlight a user from the left panel, it will automatically populate the fields on the right.
Set up New Group Account. When setting up a new user group account, access the user maintenance window from the Administration menu. (See Figure 3-24.)

a) Type the UserID information into the entry row, top right of the User Maintenance window. (FACID_type)

b) Next, using the keyboard, enter 13-character password into the “Password” entry row.

c) Retype the password in the text input window titled “Password confirm”.

d) Select the user group type from the drop down menu. Select from 2 choices: ADMIN or REGULAR user group types.

e) Select “Add/Save”
FIGURE 3-24. SET UP NEW GROUP ACCOUNT

Note: The SUPER user is reserved for Second Level Support.
Restrictions on reuse of passwords include:

Passwords must be complex, meaning at least one upper case letter, one number and one character (such as l@^%^)

Passwords must be unique and not include the same character sequence as UserID. (It is recommended that the facility ID not be included in the password.)

Passwords can not be reused in 10 password change cycles. The ARMT application will provide an automatic alert in this case. (See Figure 3-25.)

FIGURE 3-25. PASSWORD ALERT: USED PREVIOUSLY

UserID cannot be included in the password. The ARMT application will provide an automatic alert in this case. (See Figure 3-26.)

FIGURE 3-26. PASSWORD ALERT: USED PREVIOUSLY

Modify Existing Group Account. Maintenance personnel are required to change group account passwords within 3 days of an individual member of the group changing status (retirement, transfer, termination, change of duties, etc. IAW JO 1370.96) to ensure that only active ARMT users have access to system resources. (See Figure 3-25.) Passwords should be changed immediately if a password has been compromised.

1. Open the User Maintenance Window
2. Select the User Group from the User List window
3. Overwrite the current password with a new 13-character complex password
4. Confirm the new password
5. Select Save
6. Exit the User Maintenance Window

![User Maintenance Window]

**FIGURE 3-27. MODIFY GROUP ACCOUNT: RESET PASSWORD**

**Unlock Group Account.** Users are locked out of system after 3 invalid log in attempts. Unlocking user group accounts is performed by site maintenance (Tech Ops) or Air Traffic System Administrators only.

1. Open the User Maintenance Window
2. Select group account name from the user list that needs to be unlocked.
3. Click the Locked checkbox to remove the X
4. Reset group password if needed (not always required)
5. Select Add/Save
6. Select Exit

**Lock Group Account.** In the event of a suspected security incident or access control issue with ARMT, there are rare cases that site administrators may need to lock a group account to prohibit access until ARMT program office can take action.

1. Select the username to be locked from the **User List**.
2. Check the **Locked** check box.
3. Click **Add/Save** button to lock the user.
4. Click **Exit** button to close the User Maintenance application.
**Note:** Do not intentionally lock an ADMIN account without first contacting WJHTC second level support to explain why the account must be locked (security incident, stolen/lost password, etc.) Only second level support can unlock/reset an ADMIN group account password.

**Note:** If you believe a group password has been compromised, or have to lock a group account for any reason, immediate action is required:

1. Inform your facility System Administrator, and,
2. Contact ARMT WJHTC Second Level Support.

(2) User History – This provides the system administrator the ability to verify, log and archive ARMT Users and user activity. To comply with ATO ISSM security policy, site system administrators need to be able to provide user logs to support access and control policies and procedures and produce an on-demand user list for security personnel. (Section 6.3.2 provides additional information about management of group account lists and scheduled group account list reviews.)

To view, monitor, save and print logs of user access, select **User History** from the Administration drop down menu. (See Figure 3-28.) This opens the user log for the system, shown as Figure 3-29.

![FIGURE 3-28. COMMAND BAR USER HISTORY](image-url)
FIGURE 3-29. ON DEMAND USER GROUP HISTORY

- **Refresh** – Select for latest User Status.
- **Close** – Select to close User History application.
- **Export to Excel** – export User History to excel spreadsheet.
- **UserID** – Id used by user to login to ARMT Client.
- **Logon** – Date/Time User logged onto the system.
- **LastUpdate** – Date/Time of last system refresh.
- **ID** – Internal MySQL identifier.
- **TerminalID** – ID of workstation, defined in workstations com.ini.

(3) Alert Setup - This provides the system administrator the ability to specify which ARMT alerts are enabled, visually/aurally, per ARMT client workstation. Refer to Figure 3-30. Provided for System Administrator control of workstation aural alerts and display warnings for specific ARMT features and functions.

System Administrators configure local ARMT client workstations to provide for aural alarms (typically used in towers using digitized voice wave files over the ARMT speakers) and/or for individual settings to display alerts and warnings for systems users.

ADMINs configure either or both visual and aural alarms for individual workstation positions at the facility.
**CAUTION:** Changes to the Alert Setup will affect AT operations. Refer to R:\ for more information. Coordinate any changes to the alert set up with Air Traffic prior to implementing.

![Alert Setup](image)

**FIGURE 3-30. ALERT SETUP**

(4) Speech Test - The Speech Test feature, when selected, provides a test sound file to adjust speaker and/or computer sound volume. Simply selecting the Speech Test control from the ADMINISTRATION drop down menu activates the sample digitized voice file to check sound quality and allow for volume control adjustments to speakers or workstation sound settings. If the Speech Test fails, check that the speaker icon in the Command Bar is not muted. Check the PC volume setting. If the speaker test continues to fail, contact Second Level Support.

### 3.3 NETWORK SWITCH MODULE (ETHERNET SWITCH)

The ARMT system communicates through a network switch. The network switch connects all clients with the two servers. The ARMT network switch requires no configuration, but it must be replaced after a failure.

a. To ensure that the switch is working correctly, the network clients are connected, and the data packets are being sent and received by the clients:

(1) Confirm that the status indicators on the network switch show status ready.

(2) Check connectivity at any client workstation by checking the status button in the ARMT Command Bar window. Refer to paragraph 3.1.5.
b. Refer to the manufacturer’s manual to verify that the network switch is functioning properly.

3.4 ANTIVIRUS/SPYWARE SCAN

The antivirus and spyware software protects the system from malicious code by scanning the hard drive regularly. The results of these scans are then placed into a local log file. The virus and spyware checker on ARMT is scheduled to run at a time when the system is not busy. Due to the security constraints of the FAA Telecommunications Infrastructure (FTI) operations network, the virus checker cannot receive daily internet updates. All updates will be pushed on a quarterly calendar year cycle from Second Level Support.

a. The antivirus software needs to be running continuously on each Server and Client workstation.

(1) An icon should be present in the Windows System Tray to indicate that the software is running.

![CA TOTAL DEFENSE ANTIVIRUS ICON]

(2) Clicking on this icon will open a menu and further actions can be initiated.

3.5 EQUIPMENT SHUTDOWN

<table>
<thead>
<tr>
<th>TABLE 3–3. EQUIPMENT SHUTDOWN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location</strong></td>
</tr>
<tr>
<td>1) ARMT Client</td>
</tr>
<tr>
<td>2) ARMT Rack</td>
</tr>
<tr>
<td>3) ARMT Rack</td>
</tr>
<tr>
<td>4) ARMT Rack</td>
</tr>
<tr>
<td>5) ARMT Rack</td>
</tr>
</tbody>
</table>
3.6 **SHUTDOWN ARMT CLIENT WORKSTATION**

a. At the Command Bar, select Exit ARMT. When prompted, select Yes to continue.
b. Shutdown the PC. Select **START – Shut Down**.
4.0 Standards and Tolerances

4.1
Refer to Order JO 6131.5, Maintenance of the Airport Resource Management Tool (ARMT) Equipment, for the ARMT system Standards and Tolerances.
This Page Intentionally Left Blank
5.0 Periodic Maintenance

5.1 Refer to Order JO 6131.5, Maintenance of the Airport Resource Management Tool (ARMT) Equipment, for Periodic Maintenance of the ARMT.
This Page Intentionally Left Blank
6.0 Maintenance Procedures

6.1 GENERAL.

This section provides procedures required for accomplishing the various maintenance activities, both periodic and random.

Performance check procedures: includes procedures or methods for the performance checks that are listed in JO 6131.5 Maintenance of the Airport Resource Management (ARMT) Equipment.

Other Maintenance tasks procedures: includes procedures or methods for doing the other maintenance tasks that are listed in JO 6131.5.

Special maintenance tasks: procedures or methods for special, nonrecurring tasks that are listed in JO 6131.5.

6.2 PERFORMANCE CHECK PROCEDURES

6.2.1 ARMT Client Workstation

This procedure is used to ensure that the ARMT Client Workstation operates correctly. The ARMT client workstation runs the ARMT client software to display arrival, departure, and flight plan information.

a. At the Client Workstation, observe the Status Indicator on the right of the ARMT Command Bar. The Status Indicator should be green indicating that the ARMT Client Workstation is operational and all interfaces are functional, as shown in Figure 6-1.

   FIGURE 6-1. ARMT Client Command Bar Normal Status

b. If the Status Indicator is not green, refer to Section 3.1.5 Command Bar Window – Client Only.
6.2.2 ARMT Server Workstation

This procedure is used to ensure that the primary and backup server workstations are operating correctly.

a. At the Server Workstation desktop, observe the ARMT System Monitor (refer to figure 3-12). If the ARMT System Monitor is not on the desktop, <Double-click>ArmtSystem Monitor icon on the desktop (Refer to figure 6-2).

![ArmtSystem Monitor Icon]

**FIGURE 6-2. ARMT System Monitor Icon**

This will open the ARMT System Monitor window illustrated as Figure 3-12.

b. The server workstations receive data from external interfaces EFSTS, SMA (A80 only), and either ARTS (through the AGW gateway) or STARS (through the AIG gateway) depending on which type of automation system your ARMT is using.

   (1) Ensure that the Facility, ID and IPAddress fields for Type = server_primary, server_backup, arts or stars and efsts are green.

c. The primary and backup servers communicate by replication where the data written to the active Server’s database and is copied to the Non-active Server’s database over a network connection. The process replicates to the non-active server and verifies that the data can be accessed by both ARMT servers. If either the server_primary or server_backup server fails, it must be replaced using procedures in Par. 9.4.1. Install / Replace Server Workstation.

   (1) Ensure that the Replication field for the server_primary or server_backup has a value less than 9. This indicates that the last replication has occurred less than 9 seconds ago. If the replication value is over 9, then the Facility, ID, IPAddress and Replication fields for server_primary/server_backup would be orange as well.

d. If the Facility, ID IPAddress and Replication fields for server_primary, server_backup, arts or stars and efsts are not green for each refer to Table 7-1 Symptom Chart to isolate the problem.

6.2.3 ARMT Server Workstation Switchover

This procedure is used to switch over the non-active Server Workstation and ensures it can successfully operate as the active ARMT server. This procedure is also used as an ARMT Performance Check.

The ARMT servers run in replication mode which allows them to share the data from the active server to the non-active server for automatic client switchover.

The switchover is transparent to the client systems and there is no loss of data due to a server going down. The interface programs are redundant on both systems and they monitor the database to determine which server is active.
To perform an ARMT server switchover:

a. On either server, locate the ARMT System Monitor. Refer to Figure 3-12 and paragraph 3.1.4.4. ARMT System Monitor
   (1) The current active server (server_primary/server_backup) is designated by a checkmark in the Active column.
   (2) Before proceeding, verify the Replication value for both servers is less than 9 and the status color is not orange or red.

b. On the non-active server, locate the Replication Server (refer to Figure 3-13).
   (1) Stop the GuardDog application if it is running.
   (2) Click the Make Active button.
   (3) When the active server demotes itself to the non-active server, ARMT will check to see if a backup has been created during the last 24 hours. If a backup has not been created, the active server will create a backup before demoting itself to the non-active server. If the backup takes place, a Freebyte.zip program will run and display a status window while the backup is created.

   **Note:** Do not cancel the Freebyte.zip operation. Wait until the backup has completed and the Freebyte.zip window closes before continuing.
   (4) Observe the ARMT System Monitor. The previous non-active server will now have a checkmark indicating that it is now active.
   (5) Locate the Server A/B Switch. Select the now active server (A for Primary Server Workstation and B for Backup Server Workstation).
   (6) Verify operational status of server and client workstations. Refer to paragraphs 6.2.1 ARMT Client Workstation and 6.2.2 ARMT Server Workstation.
   (7) Verify that applications running on the now-active server will show "Primary" in the title bar. These applications include ARMT Server application, Replication Server, ARTS/STARS Interface and EFSTS Interface.
   (8) If necessary, switch back to the primary server by repeating above steps a and b.

c. If switchover is unsuccessful, contact Second Level Support.

### 6.2.4 Uninterruptible Power Supply (UPS)

This procedure is used to ensure that the UPS is online and the battery does not need to be replaced. This is a performance check.

The UPS supplies uninterruptable power to the ARMT equipment. The ARMT UPS must be replaced after a failure. The front panel of the UPS will display icons indicating the current state of the UPS and battery.

a. Check the UPS front panel status icons to check the state of the UPS.
b. Confirm that the ON LINE icon is displayed in the top left corner of the UPS front panel (see Figure 6-3).

   1) If the ON LINE icon is displayed, the UPS is supplying conditioned utility power and no further action is required.

   2) If the ON LINE icon is not displayed, the UPS is not supplying conditioned utility power. Either the UPS is not connected to an energized utility power source, or the UPS has failed. Confirm that the UPS is connected to utility power. Replace the UPS.

c. Confirm that the REPLACE BATTERY icon is not displayed on the UPS front panel (see Figure 6-3).

   1) If the REPLACE BATTERY icon is not displayed, the UPS battery does not need to be replaced. No further action is required.

   2) If the REPLACE BATTERY icon is displayed on the UPS front panel, the UPS battery is not connected to the UPS or the UPS battery needs to be replaced.

      (a) Confirm that the UPS battery is connected to the UPS.

      (b) Replace the UPS.

FIGURE 6-3. UPS Status Monitor Panel Display
6.2.5 Anti-Virus

This procedure is used to ensure that the antivirus and spyware software is performing daily scans. The antivirus and spyware software protects the system from malicious code. The antivirus and spyware software checks the hard drive regularly and logs the results to a local log file. The virus and spyware checker on ARMT is scheduled to run at a time when the system is not busy. Due to the security constraints of the Federal Aviation Administration (FAA) Telecommunications Infrastructure (FTI) Operations (OPS) network, the virus checker cannot receive daily internet updates. All updates will be pushed on a quarterly calendar year cycle from Second Level Support.

The antivirus software is a centrally managed software package. Updates are distributed to the ARMT workstations by the ARMT Domain Controller. All antivirus settings are controlled by the ARMT Domain Controller and these settings are locked on the ARMT workstations and cannot be modified locally. Additionally, all ARMT workstations “phone home” to the ARMT Domain Controller and receive policy updates and transmit local logs to the Domain Controller.

a. **Launch the CA Total Defense software**
   (1) Log on to the ARMT workstation.
   (2) Find the Windows toolbar.
   (3) On the Windows toolbar, left-click the CA Total Defense antivirus icon shown in Figure 6-4, and then select the Launch Total Defense menu item shown in Figure 6-5.

![FIGURE 6-4. CA Total Defense Antivirus Icon](image1)

![FIGURE 6-5. CA Total Defense Menu](image2)

(4) Ensure that the CA Total Defense window show in Figure 6-6 appears.
(5) Click on the arrow button to the right of the Real-time protection status indicator to expand and view the security overview. Refer to Figure 6-6 and 6-7.
b. **Confirm that Real-time Protection is enabled**
   
   (1) If Real-time protection is enabled, no further action is required.
   
   (2) If Real-time protection is not enabled, this may indicate a problem with the communication between the antivirus server software on the ARMT Domain Controller and the affected ARMT workstation. Contact second level support as they must troubleshoot the issue starting with the ARMT Domain Controller. Second level support will direct any further action after checking the antivirus server software.

c. **Confirm that the antivirus software is scanning daily.**
   
   (1) In the CA Total Defense window, click on the LogView button on the lower left side of the window (see Figure 6-8).
   
   (2) In the CA Total Defense window, click on the Scheduled Scan tab on the top right (see Figure 6-8).
   
   (3) In the upper portion of the window, review the Completion Time column to confirm that scheduled scans have run daily. There should be one entry for each day a scan was run and completed (see Figure 6-8).
   
   (a) If the Completion Time column indicates that scheduled scans have run daily, no further action is required.
   
   (b) If the Completion Time column indicates that scheduled scans have not run daily, this may indicate a problem with the communication between the antivirus server software on the ARMT Domain Controller and the affected ARMT workstation. Contact second level support as they must troubleshoot the issue starting with the ARMT Domain Controller. Second level support will direct any further action after checking the antivirus server software.

---

**FIGURE 6-8. CA Total Defense Window – LogView Button/Scheduled Scan Tab**
d. **Confirm that any malicious code found during the scheduled scans was cleaned, quarantined, or deleted.**
   
   (1) From the CA Total Defense window scheduled scan tab, click on the last scheduled scan listed in the upper portion of the window. Refer to Figure 6-8.
   
   (2) Review the number in the Malware Found column for the last scan.
      
      (a) If the Malware Found column value is zero (0), no further action is required.
      
      (b) If the Malware Found column has a number greater than zero (0), review the lower portion of the window to determine if the threat was removed. The lower portion of the window will list each threat and show the status of the threat. If the status indicates the threat was cleaned, quarantined, or deleted, no further action is required.
      
      (c) If the status does not indicate the threat was cleaned, quarantined, or deleted, the threat may still be active on the system. Contact second level support as the response and method of removal will vary based on the type of threat.
   
   e. **Confirm the license is active and scheduled software updates are installed and operational.**
      
      (1) If the License has a green circle with a white check mark, no further action is required.
      
      (2) If the License does not have a green circle with a white check mark, this may indicate a problem with the communication between the antivirus server software on the ARMT Domain Controller and the affected ARMT workstation. Contact second level support as they must troubleshoot the issue starting with the ARMT Domain Controller. Second level support will direct any further action after checking the antivirus server software. Note that if the software is in an unlicensed state, it will not receive policy updates, antivirus signature updates, and will not perform scans of the local system.

6.2.6 **External Hard Drive**

This procedure is used to ensure that the external hard drive is functioning properly. If the external drive is not functioning properly, logs will be written to the C: drive where space is more limited.

The external hard drive is a USB hard drive connected to the ARMT primary server workstation. The drive is set up as drive letter Z: on the ARMT server. The ARMT workstation hard drives are preloaded with software for your workstation prior to shipment from ARMT Second Level Support. After the ARMT workstation hard drives are installed, contact ARMT Second Level Support to complete the ARMT software installation and configuration.

   a. Ensure that the external hard drive is accessible. This test can only be run on the primary server. The backup server is not connected to an external hard drive.
      
      (1) Navigate to Simpledrive(Z:) and its subdirectories.
      
      (2) Click on any Simpledrive(Z:) subdirectory and ensure that individual files can be selected.
6.3 OTHER MAINTENANCE TASKS

6.3.1 Clean ARMT Client and Server Workstations

If dust builds up and restricts the airflow to the Server/Client workstations, it may overheat.

a. Look for dust buildup in the front and back of all workstations and around and inside all workstation vents.

b. If there is dust buildup, use a vacuum to clean dust buildup.

c. Ensure that the monitors do not show excessive wear, is free from dust buildup.

d. If necessary, remove dust or smudges from the screen and exterior with clean dry dust free cloth.

e. Dust buildup should not prevent the operation of the keyboard. If it impedes the users ability to enter information into the system, then use a vacuum to clean the keyboard.

6.3.2 User Account Review

The objective of this task is to ensure that only authorized users access ARMT system assets, that user documentation is reviewed on a scheduled basis, and that generation of on-demand user account lists can be completed at the sites to support FAA security policies in accordance with JO1370.96 and NIST800-53, Revision 3 requirements. This task involves coordination with site air traffic personnel. This procedure is to be performed locally at each ARMT site. Appendix A provides a sample Memorandum of Agreement (MOA) that site personnel may elect to use to share or delegate responsibility for quarterly group account reviews with designated air traffic ARMT system administrators. The ARMT Security & System Administration Procedures Handbook provides additional information, user access forms, group account forms, and supporting material to assist site maintenance personnel in completing the procedures below.

a. Locate facility individual user access request forms from ARMT workstations, ARMT Resources folder. Air traffic users and system administrators as well as site maintenance personnel responsible for ARMT support must complete an individual user access form prior to accessing ARMT system. The user access form is provided in the ARMT Security & System Administration Procedures Handbook, is also available on the shared network resources drive and client workstation hard drive in the “ARMT Resources” folder. (See Figure 6-9, Sample ARMT User Account Request Form.)

b. Using individual user access forms, generate or update the site group access control list form. Locate the site group access control list form from ARMT workstation ARMT resources folder(s). Once individual user access forms are completed at the site they are approved by the WJHTC Second Level Engineering team and authorized individuals added to either the group list for regular users, or the group list for system administrators. Site administrators are responsible for generating and updating the group list using the forms provided in the ARMT Security & System Administration Procedures Handbook, and available from the ARMT resources folder. (See Figure 6-10, Sample ARMT User Access Control List (ACL) Form.)

c. Respond to ARMT program office email request to provide quarterly group list updates. (Request transmits to designated site administrators the current version of
the facility ARMT User Group Access Control List form based upon group list last submitted/provided to the program office.) The ARMT program office security lead, WJHTC Second Level Engineering Support, provides designated site system administrators the facility group list form for update quarterly via encrypted email to support this performance check. Designated site maintenance personnel review the group list, verify the list against current users, verify that individual forms for each member of the group are on file, update the list with any changes and return the form by email to the program office.

d. Update ARMT User Group Access Control List form. If any individual included in a group list changes status (transfer from the facility, retirement, termination or change of duties/responsibilities impacting ARMT access) then the designated site system administrator must update the group list to remove the individual within 3 business days to comply with JO 1370.96. (Note: a copy of this order is also provided on the ARMT shared network resources drive (R drive).

(1) Personnel changes require an update to the ARMT site group list form.

(2) A change to the group membership list requires a change to the group 13-character password.

(3) The individual’s user access form must be changed/updated to deactivate access. If the personnel change involves a change of duties impacting ARMT access (for example a regular user requires administrator access), then the individual user access form is updated accordingly and submitted to the ARMT program office security lead for approval.

e. If there is no change in status, and reviewers and users are not aware of any unauthorized person gaining knowledge of an ARMT account password, then the review is complete. Respond to the program office email to confirm that the current group list(s) is accurate.

f. Update group list password. Submit updated individual user access forms and group access control list to ARMT program office security lead via encrypted email. If any change to the group list is required (per 6.3.2 d. (2)) and any ARMT user no longer requires access, or if any unauthorized person may have gained knowledge of an ARMT account password, then the following must be performed:

(1) Change all ARMT site account passwords using the User SetUp functions of the client application to change the group password (refer to paragraph 3.2.2.3);

(2) Update the list of authorized ARMT site users and email the updated group list form to the ARMT program office security team via encrypted email; and,

(3) Provide the ARMT program office security lead with the updated individual user access form indicating the change (deactivate account, modify account access, etc.)
ARMT Security User Access Form

To obtain access to ARMT, the users will complete a request form via the facility System Administrator or the ARMT Program Management Office (PMO) Help Desk and forward to their FAA Management. FAA Management approves, signs, and forwards to the appropriate ARMT Administrator and ARMT Program Office Security Lead/Security Administrator.

The ARMT Administrator will activate the user account and e-mail, under separate cover, the user’s group access login password and password. The ARMT Administrator will then forward the completed action to the ARMT PMO Security Lead for auditing purposes and copy the requesting FAA Management.

If the user does not have a local System Administrator (SA) or if they have not been through ARMT SA training, then the FAA Management request will be forwarded to the ARMT Help Desk.

The ARMT Help Desk will contact the ARMT PMO and/or ARMT Designated Security Lead, for approval of user accounts.

Upon creating an account, notification e-mail will be sent to the new user, the FAA Manager, and ARMT Security Lead for auditing purposes.

The ARMT User Access Form will be archived and provide an audit trail for ARMT security reporting.

1. Check One: ☐ New ☐ Reactivate ☐ Retire ☐ Re-certify ☐ Modify ☐ Delete

(See Instructions on Page 2) ☐ FAA Applicant ☐ Contractor Applicant

2. Name:

3. FAA Routing Symbol (e.g., AJW27):

4. Org Name:

5. Title:

6. Telephone No.:

7. E-mail:

8. Mailing Address and Room No.:

9. Signature: __________________________ Date:

Contract Information (Required if applicant is not an FAA employee)

10. Contract Number:

11. Contract Name:

12. Company:

13. Contract Expiration Date:

FAA Organization Manager’s signature—Please sign on line number 16.

Access Request and Authorization


☐ ARMT System Administrator Group ☐ ARMT User Group ☐ ARMT Maintenance Group ☐ ARMT Training Academy Group

15. ARMT System Administrator:

Date:

I certify and approve this applicant’s request. In accordance with OMB Circular A-130, the Applicant has been instructed not to misuse government ADP resources, to protect the confidentiality of log-in/sign-on passwords, and to report compromises of such passwords. I agree to ensure effective implementation and application of the provisions outlined in OMB Circular A-130 and to immediately notify the FAA PM Systems Coordinator if the applicant’s employment status changes or if the employee has no further need for the items requested above.

ARMT Access Authorization:

16. Name: Brian J. Schell

Or Amy Lynn Prutzman Date


18. To Be Completed by ARMT Program Management Office

Date

ARMT-PMO-User Access Form, V3, June 2011

FIGURE 6-9. Sample ARMT User Account Access Request Form
(Appendix C, ARMT Security & System Administration Procedures Handbook)
ARMT Site User Group List Form

Prepared by Site System Administrator: 

Date: _______________ Facility: 

Phone: _______________

<table>
<thead>
<tr>
<th>First Name</th>
<th>Last Name</th>
<th>ARMT User Type</th>
<th>Group Account List</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ARMT Program Office Inputs

ARMT PMO Received: ________________________________

Logged to Security Lead Database (Initials and date) ________________________________

FIGURE 6-10, Sample ARMT User Group Access Control List Form
(Appendix B, ARMT Security & System Administration Procedures Handbook)
6.4 SPECIAL MAINTENANCE PROCEDURES

6.4.1 PING SERVER FROM CLIENT

It may become necessary to use a ping command to troubleshoot a network connection between the client and server.

a. From the Client desktop, lower left hand corner, click the Windows icon. In the text box, type cmd and press Enter.

b. At the DOS prompt, type ping xxx.xxx.xxx.xxx where xxx.xxx.xxx.xxx is the IP address of the Server.
   (1) If you do not know the IP address of the Server, at the Client desktop, lower left hand corner, click the Windows icon>Control Panel>Administrative Tools>Data Sources(OBDC)>System DSN.
   (2) For the Primary Server, select APM and click ConFigure. The IP address will appear in the Server text box.
   (3) For the Backup Sever, select APM_Bakcup and click ConFigure. The IP address will appear in the Server text box.
   (4) Hit “Cancel”. Do not apply any changes.

c. For a successful ping, the results will NOT display an error.

6.4.2 TEST FLIGHT STRIP SCAN FUNCTION

a. This procedure is used to verify that ARMT is receiving data from EFSTS.

b. Close and restart the EFSTS Interface to clear the windows.

c. Use test flight strips to verify ARMT is receiving EFSTS scan data:
   (1) Request that one of the satellite towers create a test flight plan strip and scan that strip under the EFSTS ground and local scanner in that order.
   (2) Look at the Input from EFSTS window for the test flight strip information to appear. Refer to Par. 3.1.4.1 and Figure 3-2 EFSTS Interface.
   (3) At the ARMT Server workstation, check ARMT System Monitor. The efsts row should be green. If the efsts row remains red, contact ARMT Second Level Support.
7.0 Corrective Maintenance

7.1 GENERAL
This section describes corrective maintenance and reconfiguration information in the event of a software or hardware failure.

7.2 ONSITE CORRECTIVE MAINTENANCE
Troubleshooting ARMT problems can be isolated to one of the possible symptoms found in Table 7-1. This table can be used as a starting point to identifying and correcting ARMT problems.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible Fault(s)</th>
<th>Restoration Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Monitor displays red background behind the Facility, ID, and IPAddress columns where the Type = server_xxxx Where xxxx = primary or Backup. AND Client Command Bar Status Indicator = Red</td>
<td>PC Failure</td>
<td>ARMT Server is not running properly. Restart the ARMT (Message-Handler) Par. 3.1.4.3.b Restore ARMT service to AT - Make the Non-Active server, Active Par. 6.2.3.b Troubleshoot - Restart the Non-Active (failed) Server Workstation (Refer to 7.3) Replace Server Workstation 9.4.1</td>
</tr>
<tr>
<td>Client Command Bar Status Indicator = Yellow</td>
<td>EFSTS problem EFSTS Interface is not running properly Server A/B Switch &amp; Cables Serial Communications Card</td>
<td>Check operational Status of EFSTS. ARMT not receiving EFSTS data Par. 7.7. Server A/B Switch Par. 7.16 EFSTS Interface Cable par. 9.4.8 Serial Communications Card Par. 7.13</td>
</tr>
</tbody>
</table>
### Client Command Bar Status indicator = Orange

<table>
<thead>
<tr>
<th>Condition</th>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARTS/STARS problem. Terminal Interface not operating properly</td>
<td>Check operational Status of ARTS/STARS.</td>
<td>ARMT not receiving ARTS/STARS data Par. 7.8</td>
</tr>
<tr>
<td>Server Network Card (NIC)</td>
<td></td>
<td>ARMT not receiving ARTS/STARS data Par. 7.8</td>
</tr>
</tbody>
</table>

### Client Command Bar displays Orange **NO SERVER**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Problem</td>
<td>ARMT Client Server Connection Par. 7.9</td>
<td></td>
</tr>
</tbody>
</table>

### ARMT generated Flight Strips are not printing.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMA communication failure</td>
<td>Restart SMA Interface (Refer to 7.18)</td>
<td></td>
</tr>
</tbody>
</table>

### Pushback and Gate Information not updating

<table>
<thead>
<tr>
<th>Condition</th>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server communication failure</td>
<td>Check Server Status (Refer 3.1.4.4) If active server status is down restart active server application (Refer to 7.3)</td>
<td></td>
</tr>
</tbody>
</table>

### System Monitor (3.1.4.4) indicates a client workstation failure

<table>
<thead>
<tr>
<th>Condition</th>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC failure</td>
<td>Restart Client Workstation (Refer to 7.5)</td>
<td></td>
</tr>
</tbody>
</table>

### System Monitor (3.1.4.4) indicates that server replication has fallen behind

<table>
<thead>
<tr>
<th>Condition</th>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication Monitor settings.</td>
<td>Replication Issue Par. 7.17</td>
<td></td>
</tr>
</tbody>
</table>

### External Drive is not accessible

<table>
<thead>
<tr>
<th>Condition</th>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Refer to 7.15</td>
<td></td>
</tr>
</tbody>
</table>

### ARMT Printer fails to print

<table>
<thead>
<tr>
<th>Condition</th>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Printer</td>
<td>Replace Printer. Par. 9.4.4</td>
<td></td>
</tr>
</tbody>
</table>

---

### 7.3 REBOOT A SERVER WORKSTATION

**CAUTION**

**DO not** restart the Active Server before doing a switchover.

a. If the Server you need to restart is the Active Server, perform the switchover operation described in 6.2.3 ARMT Server Workstation Switchover.

b. On the now Non-Active server locate the ARMT Server window.

   1. **Uncheck** Process Messages
(2) Close the ARMT applications
   (a) ARMT Server application (refer to figure 3-5)
   (b) EFSTS Interface (refer to figure 3-1)
   (c) Terminal Interface (refer to figure 3-2)
   (d) Replication Server (figure 3-7)
   (e) System Monitor

c. Reboot the Server workstation. When the ARMT server workstation restarts, the
   ARMT server applications will be launched automatically. Some of the applications
   may take a few minutes to launch and connect.
   (1) If the Server workstation does not boot successfully, replace the Server. Refer to paragraph 9.4.1, Install / Replace Server Workstation.

d. Observe the System Monitor to:
   (1) Verify the operational status of the ARMT server/client software. Refer to 6.2.2.
   (2) In the Replication field, verify that seconds behind is 0 or 1.

e. Locate the Replication Monitor (refer to figure 3-7).
   (1) Click the Make Active button.

7.4 RESERVED

7.5 REBOOT ARMT CLIENT WORKSTATION

If ARMT is not running correctly, indicated by the Command bar status indicator being a color other than green, the client workstation may need to be rebooted.

a. At each instance of the Command Bar (refer to paragraph 3.6, Equipment Shutdown) select Exit ARMT. When prompted, select Yes to continue.

b. Reboot the Client Workstation.
   (1) If the client workstation does not boot successfully, replace the client. Refer to paragraph 9.4.2, Install / Replace Client Workstation.

c. Launch the Client application using the procedure in Par. 3.2.2

d. The color of the round Status display in the top right corner of the ARMT Command Bar(s) should be green indicating the Client Workstation is operational; all interfaces are functioning and the ARMT client is connected to the ARMT server workstation. If the Status indicator is a color other than green, refer to Table 7-1 ARMT Symptom Chart.

7.6 RESERVED

7.7 ARMT NOT RECEIVING EFSTS DATA

a. INDICATIONS: When the ARMT is not connected to EFSTS, there are several indications:
(1) The Client’s Command Bar displays a yellow status indicator (refer to figure 3-13).

(2) and/or the Server’s System Monitor (refer to figure 3-6) displays a red background behind the Facility, ID, and IPAddress columns where the ID = efsts.

Note: During low traffic periods, when no data has been received for more than 15 minutes, the clients may display this error even though there is no problem with the EFSTS connection. During slow periods the EFSTS alert can be suspended for a period of time. To suspend the EFSTS alert, refer to paragraph 3.7.

(3) The ARMT Client software no longer displays new EFSTS data.

(4) Or ARMT generated strips do not print (if configured).

b. POSSIBLE FAULTS:

(1) EFSTS not working properly.

(2) The EFSTS Interface application is not running properly.

(a) Perform the Test Flight Strip Scan Function using Par. 6.4.2. If the scan function is not working, then proceed to next step.

(3) EFSTS A/B Switch. Check the operation of the EFSTS A/B Switch per Par. 7.16

(4) ARMT/EFSTS Interface cables. Check cable pinout and connectivity with information in Par. 9.4.8.

(5) Server RS-422 Serial Communication Card fault.

(a) Refer to Par. 7.13 to further isolate a fault with the Serial Communications Card.

7.8 ARMT NOT RECEIVING ARTS/STARS DATA

c. INDICATIONS:

(1) The ARMT command bar displays an orange status indicator (refer to figure 3-14)

(2) and/or the Server’s System Monitor displays a red background behind the Facility, ID, and IPAddress columns where the ID = arts/stars (refer to figure 3-6).

d. POSSIBLE FAULTS:

(1) ARTS/STARS gateway problem.

(2) At the Server, the Terminal Interface may not be running properly.

(a) Locate the Terminal Automation Interface (refer to figure 3-2). The window might be minimized to the taskbar. If the Terminal Automation Interface is not present on ARMT server, double click the Terminal Automation Interface icon on the desktop to launch it.
1. Observe the Terminal Automation Interface and confirm that data is present in the output data window (refer to figure 7-1 below).

![FIGURE 7-1. CURRENT CONNECTION STATUS](image)

(b) If the AGW/AIG interface indicator is still not green, proceed to next step to check the Network Card.

(3) **Network Card** properties are incorrect or not physically connected.

(a) To check the network card properties,

1. At the Server Desktop, lower left hand corner, click the Windows icon. In the text box, type `cmd` and press **Enter**.
2. At the DOS prompt, type `ipconfig`.
3. Ensure that the IPs addresses are correct according to the information in the ARMT Site Binder. If the IP address is correct, then proceed to the next step.

(b) To check the connectivity between the ARMT Server and the ARTS/STARS gateway,

1. Right-click the network icon in the system tray.
2. Select **Open Network and Sharing Center**. A new window appears.
3. On the right side of the window, Click **ARTS_AGW** or **STARS_AIG** depending on the type of Terminal Automation System the ARMT is connected to.
4. Verify that bytes are being sent and received.
(c) At the Network Interface card used to connect the ARTS/STARS gateway, ensure the link light is on. If the link light is not lit, replace the cable.
   a If the link light remains off after replacing the cable, proceed to next step.

(4) If all steps above fail, follow steps in Par. 9.4.1 Install/Replace Server Workstation.

7.9 ARMT CLIENT SERVER CONNECTION
   a. INDICATIONS: When a client is not connected to the Server the following indications may be displayed.
      (1) The ARMT Command Bar will have an orange “NO SERVER”. (Refer to figure 3-15)
      (2) A dialog box at Client startup that reads “Server and Backup not responding, Shutting Down”
      ![ARMT Dialog Box]
      FIGURE 7-3.

      (3) The ARMT client software no longer displays new data

   b. POSSIBLE FAULTS
      (1) Client workstation. Reboot the ARMT client workstation (refer to Par. 7.5). If this does not resolve the error, proceed to the next step.
      (2) ARMT Server Workstations. Verify that both ARMT Server workstations are operational. If servers are operational, then check the network in the following step.
      (3) Network connection between the ARMT client workstation and the ARMT server workstation. At the Client workstation’s Command Prompt, ping the ARMT server workstation using Par. 6.4.1. If the ping is not successful then check the following and replace faulty components as necessary:
         (a) Network Module Switch
         (b) Network cable between the Client workstation and the Network Module switch.
         (c) Client Workstation NIC (If NIC is bad, replace the Client Workstation. Refer to Par. 9.4.2.)
         (d) FTI
To verify operational status, of the client refer to paragraph 6.2.1.

7.10 ARMT DISPLAY
a. If the ARMT display fails, Contact the Logistics Center for a replacement.

7.11 NETWORK MODULE SWITCH (ETHERNET SWITCH)
a. A faulty network switch can cause network communication problems with ARMT clients and servers. If the Server/Client NICs, cables and FTI are functional then:
b. Power cycle the Network Module Switch. If the link lights do not come on, contact the Logistics Center for replacement.

7.12 UNINTERRUPTABLE POWER SUPPLY (UPS)
a. If the REPLACE BATTERY icon is displayed on the UPS front panel, the UPS battery needs to be replaced.
   (1) Contact the Logistics Center for replacement.

7.13 SERIAL CARD (RS-232/422 COMMUNICATIONS CARD)
a. INDICATIONS: The following are system indications if the RS-422 Communications card in the server fails or is not working properly.
   (1) EFSTS Data is not received at the Servers.
      (a) The Server's System Monitor displays a red background behind the Facility, ID, and IPAddress columns where the ID = efsts
      (b) The Client Command Bar displays a yellow status indicator (refer to figure 3-13)
   (2) ARMT generated flight strips do not print.

b. A variety of problems can cause the RS-232/432 Communications Card to stop functioning correctly. Use the following procedure to troubleshoot the RS-232/432 Communications Card or refer to the manufacturer's user manual.
   (1) Server RS-422 Communication Card connection.
      (a) Check the Sea Level Card 7404 (refer to figure 7-4) on the back of the server and ensure that EFSTS RS-422 wire is plugged into port P1 of the card octopus cable assembly. Each port on the Sea Level Card is labeled (P1 through P4) on the body of the connector.
      (b) If port P1 is not plugged in, find the EFSTS cable and plug it into the Sea Level 7404 Card port P1.
      (c) Perform the Test Flight Strip Scan Function using Par. 6.4.2. If the scan function is not working, then proceed to next step.
Server RS-422 Communication Card not seated.

(a) Perform a Server Workstation Switchover using Par. 6.2.3.
(b) Shut down the ARMT server.
(c) Ensure cables are marked on the back of the system. If cables have no marking, tag them with labels to make it easier when plugging the cables back in again.
(d) Remove all cables from the rear of the server including unplugging the power plug.
(e) Before opening the case, hold the power button in for 15 seconds to drain residual power.
(f) The server is screw-less and only needs to be popped open with the quick release lever.
(g) Unlatch the holding bar to release all the PC Cards in place (refer to figure 7-5).
(h) Ensure the Sea Level 7404 card is securely mounted to the mother board (refer to figure 7-5).
(i) Re-seat card into Peripheral Component Interconnect (PCI) slot and secure holding bar.
(j) Plug cables back into the rear of the server and restart.
(k) Perform the Test Flight Strip Scan Function using Par. 6.4.2. If the scan function is not working, then proceed to next step.
(3) Follow steps Par. 9.4.1 Install/Replace Server Workstation.

7.14 ARMT GENERATED STRIPS NOT PRINTING

a. INDICATIONS:
   (1) The Client Command bar status indicator is green, but ARMT generated strips are not printing.

b. POSSIBLE FAULTS:
   (1) Server A/B Switch in the wrong position. If the Active Server is the Primary server then the switch needs to be in the “A” position. If the Active Server is the Backup server then the switch needs to be in the “B” position.
   (2) Server configuration for EFSTS. At the Server, check EFSTS Interface status to see if the MOVR On is selected.
   (3) Faulty A/B Switch. Following procedures in Par. 7.16

7.15 EXTERNAL HARD DRIVE

a. Use the following procedure to troubleshoot the external hard drive.
   (1) Confirm that the external hard drive is powered on and connected to the ARMT primary server with a USB cable. If it is not, then power on the external hard drive and connect the USB cable to the primary server.
   (2) From the ARMT primary server Workstation confirm the external hard drive is accessible:
      (a) Navigate to the Z: drive.
      (b) Confirm that the Z: drive window opens and displays the files located on the external hard drive (drive Z:).
      (c) If the drive is not accessible, troubleshoot the external hard drive.
1. Check to see if a Z: drive exists.
2. If the Z: drive exists but is not accessible, unplug the USB cable from the primary server and plug it back into a different USB port on the primary server.
4. If the external hard drive is still not accessible, check the drive configuration in Computer Management – Disk Management.
   a. Click on Windows Logo>Control Panel> Administrative Tools> Computer Management.
   b. In the left pane of the Computer Management window click on Storage>Disk Management.
   c. Confirm that the external hard drive is listed under Disk Management.
      (i) If the external hard drive is not listed under Disk Management, call the Logistics Center for a replacement external hard drive.
      (ii) If the external hard drive is listed under disk management, check to see if the drive is assigned a drive letter.
         (a) The assigned drive letter should be Z and it will be listed at the end of the title on the drive volume.
         (b) If the volume displays that the drive is drive Z but the drive is still not accessible, replace the external hard drive.
         (c) If the volume is not assigned a drive letter or is assigned a drive letter other than Z, change the drive letter to Z:
            (i) Right-click on the external hard drive volume and choose Change Drive Letter and Paths.
            (ii) Click the Change button.
            (iii) From the dropdown on the right side of the dialog window choose drive letter Z and click OK twice.
            (iv) Close the Computer Management window and navigate to the Z: to verify if the drive is accessible.
            (v) If the drive is still not accessible, replace the external hard drive.

7.16 EFSTS SERVER A/B SWITCH
   a. INDICATIONS:
(1) The EFSTS A/B switch allows the Servers to receive EFSTS simultaneously and designates which ARMT server communicates back to EFSTS.

b. POSSIBLE FAULTS:

(1) To isolate a cable problem between the ARMT Servers and the Server A/B Switch, use Par. 6.2.4 to determine that each of the Servers are receiving data from EFSTS. If one of the servers is not receiving data, then most likely it is the cable between the switch and the Server. To verify, swap the cables from to server to the opposite ports A-B/B-A on the switch. Replace the cable using straight-thru pinout in Par. 9.4.8

(2) If both servers are not receiving EFSTS data, check the cable between the EFSTS and Server A/B Switch.
   (a) At the A/B switch, remove the cable from the port labeled **EFSTS IN**. At the Active server, remove cable on the P1 plug of the Serial Communications card. Connect the P1 plug of the Serial Communication card with the cable removed from the **EFSTS IN** port.
   (b) Verify that the ARMT is receiving data using par. 6.2.4. If data is received, then replace the Server A/B switch using Par. If data is not received, then replace cable between the EFSTS and A/B switch using pinout in Par. 9.4.8.

7.17 REPLICATION ISSUE

a. INDICATIONS:

   (1) Server’s System Monitor displays a red background behind the Replication column where the Type = server_xxxxx. Where xxxx = primary or backup.

   (2) Replication value of either server is greater than 12 and increasing in value.

b. POSSIBLE FAULT:

   (1) The Replication Server application is not running properly.

      (a) Ensure that the **Replication** box is checked on both servers. If both are checked, then the replication value should be decreasing.

      (b) If the replication value continues to get larger, this indicates a MySQL error. Uncheck Replication on both servers and contact ARMT Second Level Support.

7.18 SURFACE MOVEMENT ADVISORY (SMA)

a. INDICATIONS:

   (1) SMA data is not being received.

   (2) Server’s System Monitor displays a red background behind the **Facility**, **ID**, and **IP Address** columns where the ID = **sma** (refer to figure 3-6).

   (3)

b. POSSIBLE FAULTS:

   (1) The SMA interface application is not running properly.
(a) Exit the SMA interface.
(b) From the server desktop, launch the SMA interface by double-clicking the SMA INTERFACE icon.

(2) **SMA problem.**

(3) **Network Card** properties are incorrect or not physically connected.
(a) To check the network card properties,
   1. At the Server Desktop, lower left hand corner, click the Windows icon. In the text box, type *cmd* and press Enter.
   2. At the DOS prompt, type *ipconfig*.
   3. Ensure that the IPs addresses are correct according to the information in the ARMT Site Binder. If the IP address is correct, then proceed to the next step.

(b) To check the **connectivity between the ARMT Server and SMA**
   1. Right-click the network icon in the system tray.
   2. Select **Open Network and Sharing Center**. A new window appears.
   3. On the right side of the window, Click **SMA**.
   4. Verify that bytes are being sent and received.

(c) At the Network Interface card used to connect the SMA gateway, ensure the link light is on. If the link light is not lit, replace the cable.
   1. If the link light remains off after replacing the cable, proceed to next step.

(4) Follow steps in Par. 9.4.1 Install/Replace Server Workstation.
8.0 Parts List

8.1 GENERAL

This section provides a description of the equipment required for the ARMT. Order the equipment listed below from Second Level Support at the WJHTC. Table 8-1 lists equipment options.

- Server Workstation
- Client Workstation
- Ethernet Switch
- Fiber Module (site specific)
- UPS
- Serial Card (servers only)
- Laser Printer
- Ethernet Extenders (site specific)
- External Hard Drive
- ARMT Server A/B Switch (EFSTS interface)

<table>
<thead>
<tr>
<th>PART</th>
<th>MODEL</th>
<th>MANUFACTURER</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 inch MONITOR</td>
<td>1708FP</td>
<td>DELL</td>
</tr>
<tr>
<td>19 inch MONITOR</td>
<td>SDM-S95FR</td>
<td>SONY</td>
</tr>
<tr>
<td>19 inch MONITOR</td>
<td>P190S</td>
<td>DELL</td>
</tr>
<tr>
<td>24 inch MONITOR</td>
<td>U2410</td>
<td>DELL</td>
</tr>
<tr>
<td>EXTERNAL HARD DRIVE</td>
<td>34919</td>
<td>IOGMEMA</td>
</tr>
<tr>
<td>ETHERNET PLUS</td>
<td>NVF-200 EKIT</td>
<td>NET SYS</td>
</tr>
<tr>
<td>ETHERNET PLUS</td>
<td>HUBS-110VDSL EXT</td>
<td>STARTECH</td>
</tr>
<tr>
<td>FIBER MODULE</td>
<td>EF31SC</td>
<td>LINKSYS</td>
</tr>
<tr>
<td>LASER PRINTER</td>
<td>E250DN</td>
<td>LEXMARK</td>
</tr>
<tr>
<td>LASER PRINTER</td>
<td>E260DN</td>
<td>LEXMARK</td>
</tr>
<tr>
<td>SERIAL CARD</td>
<td>7404</td>
<td>SEA LEVEL</td>
</tr>
<tr>
<td>SWITCH*</td>
<td>EF3116</td>
<td>LINKSYS</td>
</tr>
<tr>
<td>SWITCH*</td>
<td>EF3124</td>
<td>LINKSYS</td>
</tr>
<tr>
<td>SWITCH</td>
<td>JFS524</td>
<td>NETGEAR</td>
</tr>
<tr>
<td>UPS</td>
<td>BR1000G</td>
<td>APC</td>
</tr>
<tr>
<td>A/B SWITCH (Server EFSTS interface)</td>
<td>724-746-5500</td>
<td>BLACK BOX</td>
</tr>
<tr>
<td>SPEAKERS (ATCT clients only)</td>
<td>SPK_ALL_AX210_502_PD</td>
<td>DELL</td>
</tr>
<tr>
<td>WORKSTATION</td>
<td>OPTIPLEX 790</td>
<td>DELL</td>
</tr>
<tr>
<td>WORKSTATION</td>
<td>OPTIPLEX 990 Mini Tower</td>
<td>DELL</td>
</tr>
</tbody>
</table>

*Note: Existing Linksys network switches will be phased out as required and replaced with NetGear Model JFS524 as part of technology refresh.
8.2 ARMT SERVER WORKSTATION

The ARMT server system must consist of, at a minimum, those commercial-off-the-shelf components listed below.

- A minimum of a 3.4 GHZ Pentium 8 main processor,
- Windows 7 Professional operating system platform (upgraded from Windows XP), or better,
- 16X DVD-RW drive,
- 8 GB RAM memory,
- 500 GB SCSI Hard drive,
- Two Ethernet 10/100 Network Interface Cards,
- RS-422 COM board (interfaces with the EFSTS system),
- Microsoft Office Professional software suite, antivirus/malicious code software, among other COTS software applications,
- USB Keyboard and Mouse,
- Internal sound card, external speakers,
- Display, minimum 17-inch flat panel display, non-glare surface, 1280 X 1024 pixels (typical configuration 24 inch display sized determined based upon rack compatibility and available space at position),
- Uninterruptable Power Supply (UPS),
- USB External Memory Device, and,
- Fiber Module/Cat5e Extender (site specific, optional).

**Note:** Server interface components include an A/B Switch to support primary and backup server connectivity to EFSTS during server switchover. Previous “Y” cable connections will be replaced with the A/B switch.

**Note:** ARMT components (servers, clients, etc.) are not certified on critical power and cannot be connected to critical power service. ARMT is supported by essential service only.

8.2.1 Ordering Information

- One complete system includes the following:
  1. Server Workstation as described above
  2. All associated COTS and ARMT application software
b. If replacing Server CPU Workstation components only.
   (1) Server PC, Keyboard, Mouse only
   (2) Flat Panel Display
   (3) RS-422 COM Card

8.2.2 Quantity
Two ARMT Server Workstations are required at each TRACON:
   a. One Primary Server Workstation.
   b. One Backup Server Workstation.

8.3 ARMT CLIENT WORKSTATION
ARMT client system must consist of, at a minimum, those commercial-off-the-shelf components listed below.

   a. A minimum of a 3.1 GHZ Pentium 6 main processor,
   b. Windows 7 Professional operating system platform (upgraded from Windows XP), or better,
   c. USB Keyboard and Mouse,
   d. 8X DVD/RW drive,
   e. 8 GB RAM memory,
   f. 250 GB Hard drive,
   g. One Ethernet 10/100 Network Interface Card,
   h. Microsoft Office Professional software suite, antivirus/malicious code software, among other COTS software applications,
   i. Internal sound card, external speakers (ATCT clients only),
   j. Display, minimum 17-inch flat panel display, non-glare surface, 1280 X 1024 pixels,
   k. Uninterruptable Power Supply (UPS), and,
   l. Fiber Module/Cat5e Extender (site specific, optional).

Note: ARMT components (servers, clients, etc.) are not certified on critical power and cannot be connected to critical power service. ARMT is supported by essential service only.

8.3.1 Ordering Information
a. One complete workstation system includes the following:

(1) Client Workstation as described above.
(2) All associated COTS and ARMT application software.

8.3.2 Quantity
Depending on the facility configuration more than one ARMT Client Workstation may be needed.

8.4 ETHERNET SWITCH (NETWORK SWITCH MODULE)
Depending on the facility configuration more than one Ethernet Switch may be needed. COTS manuals for network switch modules are located on ARMT shared resources network drive (R drive).

8.5 FIBER MODULE (FIBER CARD SWITCH MODULE)
Depending on the facility configuration more than one Fiber Module may be needed. COTS manuals are located on ARMT shared resources network drive (R drive).

8.6 UNINTERRUPTABLE POWER SUPPLY (UPS)
Depending on the facility configuration more than one UPS may be needed. UPS equipment is required for all server and client workstations and the ARMT network switch. COTS manuals are located on ARMT shared resources network drive (R drive).

Note: The ARMT server and client workstations are required to be connected to a UPS. The ARMT network switch installed in TRACON equipment rooms on designated racks is also connected to the UPS equipment.

8.7 SERIAL CARD (RS-422 COMMUNICATIONS CARD)
The ARMT server workstation and backup workstation both require one serial card each.

8.8 LASER PRINTER
One ARMT Laser Printer is required per facility. COTS printer drivers are pre-installed on server and client workstations. COTS manuals are located on ARMT shared resources network drive (R drive).

8.9 ETHERNET EXTENDERS (CAT5E EXTENDER)
Depending on the facility configuration more than one Ethernet Extender maybe required. COTS manuals are located on ARMT shared resources network drive (R drive).

8.10 EXTERNAL HARD DRIVE
Each ARMT TRACON requires one External Hard Drive at the ARMT Rack with USB connection to the primary ARMT server. COTS manuals are located on ARMT shared resources network drive (R drive).
8.11 ARMT Server A/B Switch. New A/B gang switches will be implemented to replace existing Y cable connectivity between ARMT servers and the EFSTS servers at TRACON sites. The A/B switch will connect to both primary and backup servers to support continuous EFSTS services during server switchover and in the event of a primary server failure. COTS manuals are located on the ARMT shared network drive (R drive).
This Page Intentionally Left Blank
9.0 Installation, Integration, and Checkout

9.1 SITE INFORMATION AND DRAWINGS - No site information is provided in this instruction book.

9.2 INSTALLATION MATERIALS REQUIRED - Table 9–1 lists the ARMT equipment supplied for installation. Equipment required but not supplied with ARMT equipment is listed in table 9-2. This list does not include wire, conduit, hardware, or other materials required to install the equipment.

### TABLE 9-1. INSTALLATION MATERIALS REQUIRED AND SUPPLIED

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Component</th>
<th>Logistics Center Label Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Primary server for each TRACON</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>Backup server for each TRACON</td>
<td>TBD</td>
</tr>
<tr>
<td>Determined by local site requirements</td>
<td>Client workstation</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>UPS for each server and each client workstation</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>Printer for the ARMT system</td>
<td>TBD</td>
</tr>
<tr>
<td>2</td>
<td>Serial cards for each TRACON (1 each for primary and backup server. Pre-installed/configured in the primary and backup servers.)</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>ARMT network switch per facility</td>
<td>TBD</td>
</tr>
<tr>
<td>Minimum:</td>
<td>Display (shipped with 4 ft VGA cord and 4 ft power plug)</td>
<td>TBD</td>
</tr>
<tr>
<td>1 display for every Client</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 display for the Primary Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 display for the Backup Server</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TABLE 9-1. INSTALLATION MATERIALS REQUIRED AND SUPPLIED (CONTINUED)

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Component</th>
<th>Logistics Center Label Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only if distance exceeds 100 meters between ARMT switch and peripheral equipment.</td>
<td>Ethernet extender</td>
<td>TBD</td>
</tr>
<tr>
<td>Determined by local site requirements</td>
<td>CAT5E plenum cable for all facilities</td>
<td>TBD</td>
</tr>
<tr>
<td>Determined by local site requirements</td>
<td>CAT5E connector plugs for all facilities</td>
<td>TBD</td>
</tr>
<tr>
<td>1 per TRACON where EFSTS is present</td>
<td>RS422 shielded serial cable with one male and one female end.</td>
<td>TBD</td>
</tr>
<tr>
<td>1 A/B Switch per TRACON where EFSTS is present</td>
<td>A/B Switch with (2) straight through RS422 Cables</td>
<td>TBD</td>
</tr>
<tr>
<td>1 per ARMTATCT client</td>
<td>Pair of desktop speakers for ATCT clients only (speakers are not provided for servers or clients at TRACONs or ARTCCs.</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>External hard drive (for primary server)</td>
<td>TBD</td>
</tr>
</tbody>
</table>

TABLE 9-2. INSTALLATION MATERIALS REQUIRED BUT NOT SUPPLIED

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 per TRACON</td>
<td>ARMT equipment rack (dimensions to be determined)</td>
</tr>
</tbody>
</table>

9.3 UNPACKING AND HANDLING INSTRUCTIONS

a. ARMT equipment is packaged in standard cardboard cartons and shipped to the site.
Note: Handle equipment carefully to prevent damage.

b. Remove all protective packaging materials, and inspect each item for damage that may have occurred during shipment.

c. File a claim with the carrier for any damage found when unpacking the equipment.

d. Retain all packaging for shipping the old ARMT equipment to the ARMT Depot.

9.4 ARMT EQUIPMENT INSTALLATION

Additional configuration is required for some ARMT equipment, and will be performed by ARMT Second Level Support after the new ARMT equipment is installed. Follow the procedures in this section to install ARMT equipment.

9.4.1 Install / Replace Server Workstation

After the ARMT server workstation is installed, ARMT Second Level Support must be contacted to complete the ARMT software configuration.

Note: The ARMT server must be replaced after a failure.

a. To remove the existing ARMT server workstation:
   (1) Shut down the ARMT server workstation.
   (2) Disconnect the existing ARMT server workstation by performing the following procedure:
       (a) Disconnect the following items from the existing ARMT primary server workstation:
           • power cable
           • display cable
           • network cables
           • RS232/422 harness
           • keyboard and mouse
           • external hard drive cable
       (b) Remove the existing ARMT server workstation from the ARMT rack and repackage it using the packing materials from the new ARMT server workstation.
       (c) Place the return shipping label on the repackaged ARMT server workstation and give it to the local shipping department.

b. To install the new ARMT server workstation:
   (1) Place the new ARMT server workstation in the ARMT rack.
   (2) Connect the new ARMT server workstation by performing the following procedure:
       (a) Connect the following items to the new ARMT server workstation:
           • monitor, keyboard and mouse cables
- RS232/422 harness
- network cables
- power cable
- If server being replaced is the Primary server, reconnect external hard-drive Refer to 9.4.7

(3) Configure the network card.
   (a) Select START> Control Panel> Network Connections.
   (b) Right click the ARMT_Network connection and select Properties.
   (c) Highlight the Internet Protocol (TCP/IP) in the protocol list and click the Properties button.
   (d) Select the Use The Following IP Address radio button
   (e) Enter the IP Address, Subnet Mask, and Default Gateway. This information is located in the ARMT Site Binder.
   (f) The DNS and WINS address is pre-configured for the ARMT_Network connection. Do not change these addresses.
   (g) Click OK.
   (h) Click OK.

(4) Contact ARMT Second Level Support to complete the installation.

(5) To verify operational status, perform steps in Par. 6.2.2 ARMT Server Workstation.

9.4.2 Install / Replace Client Workstation

After the ARMT client workstation is installed, ARMT Second Level Support must be contacted to complete the ARMT software installation and configuration.

a. To remove the existing ARMT client workstation:
   (1) Shut down the existing ARMT client workstation. Refer to paragraph 3.6.
   (2) Disconnect the existing ARMT client workstation by performing the following procedure.
      (a) Disconnect the following items from the existing ARMT client workstation:
          • power cable
          • network cable
          • monitor, keyboard and mouse cables
      (b) Remove the existing ARMT client workstation and repackage it using the packing materials from the new ARMT client workstation.
      (c) Place the return shipping label on the repackaged ARMT client workstation and give it to the local shipping department.

b. To install the new ARMT client workstation:
(1) Place the new ARMT client workstation in the location of the old ARMT client workstation.

(2) Connect the new ARMT client workstation by performing the following procedure:
   (a) Connect the following items to the new ARMT client workstation:
       - monitor, keyboard and mouse cables
       - network cable
       - power cable

(3) Configure the network card.
   (a) Select **START** > **Control Panel** > **Network Connections**.
   (b) Right click the **ARMT_Network** connection and select Properties.
   (c) Highlight the **Internet Protocol (TCP/IP)** in the protocol list and click the **Properties** button.
   (d) Select the **Use The Following IP Address** radio button
   (e) Enter the IP Address, Subnet Mask, and Default Gateway. This information is located in the ARMT Site Binder.
   (f) The DNS and WINS address is pre-configured for the ARMT_Network connection. Do not change these addresses.
   (g) Click **OK**.
   (h) Click **OK**.

(4) Contact ARMT Second Level Support to complete the installation, restart ARMT, and test the installation.

(5) To verify operational status, refer to the ARMT TI, paragraph 6.2.1.

### 9.4.3 Install / Replace Uninterruptable Power Supply (UPS)

Follow this procedure for initial installation or, to replace a faulty ARMT UPS:

a. To remove the existing ARMT UPS that will be replaced, perform the following:
   (1) Power-down all equipment that is plugged into the UPS and any equipment that will be affected during the outage.
      (a) To replace an ARMT client workstation UPS, power-down the attached ARMT client workstation.
      (b) To replace an ARMT primary server workstation UPS, power-down the ARMT backup and primary server workstations.
      (c) To replace an ARMT backup server workstation UPS, power-down the ARMT backup server workstation.
   (2) Turn the UPS switch to the Off position.
   (3) Unplug the existing equipment power cables from the UPS.
   (4) Unplug the existing UPS USB data cable.
(5) Unplug and then remove the existing UPS.
(6) Discard UPS using local environmental battery disposal plan/procedure.

b. To install the new UPS:
   (1) Connect the UPS battery to the UPS.
   (2) Place the new UPS in the appropriate location for your ARMT equipment component.
   (3) Plug in the power cable for the UPS.
   (4) Plug in the equipment power cables to the UPS.
   (5) Plug in the UPS USB data cable.
   (6) Turn the UPS switch to the On position.
   (7) Power-on all equipment plugged into the UPS and any equipment that was turned off in step 9.4.3 a. (1).
      (a) When installing an ARMT client workstation UPS, power-on the attached ARMT client workstation.
      (b) When installing an ARMT primary server workstation UPS:
         1. Power-on the backup server workstation.
         2. Power-on the primary server workstation.
         3. Reboot the ARMT client workstations.
      (c) When installing an ARMT backup server workstation UPS, power-on the ARMT backup server workstation.
   (8) To verify operational status of the UPS, refer to Par. 6.2.4.
   (9) Refer to paragraph 6.2.1. to verify the operational status of the ARMT Client or 6.2.2 to verify the operational status of the ARMT server.

9.4.4 Install / Replace Network Printer

The ARMT network printer must be replaced after a failure.

Note: Refer to the manufacturer's user manual for detailed installation and removal procedures

a. To remove the existing ARMT network printer:
   (1) Shut down and disconnect the existing ARMT network printer.
   (2) Disconnect the power cable and the network cable from the existing ARMT network printer.
      (a) Remove the existing ARMT network printer.
      (b) Repackage the existing ARMT network printer using the packing materials from the new ARMT network printer.
      (c) Place the return shipping label on the repackaged ARMT network printer and give it to the local shipping department.
b. To install the new ARMT network printer:
   (1) Place the new ARMT network printer in the location of the old ARMT network printer.
   (2) To connect the new ARMT network printer:
      (a) Connect the network cable and the power cable to the new ARMT network printer.
      (b) Power-on the ARMT network printer.
      (c) Refer to the manufacturer’s user manual to set up the printer network IP address, subnet mask, and default gateway. Refer to the ARMT site binder for the printer network IP address information.
      (d) Refer to the manufacturer’s user manual to install the printer on all ARMT client workstations that require a printer.

c. To verify operational status, refer to the manufacturer’s user manual.

9.4.5 Install / Replace Network Switch (Ethernet Switch)
The ARMT network switch does not require configuration, but must be replaced after a failure. Refer to the manufacturer's user manual for detailed removal and installation procedures.

   a. To remove the existing ARMT network switch:
      (1) Disconnect the network cables and the power cable from the existing ARMT network switch.
      (2) Remove the existing ARMT network switch from the ARMT rack.
      (3) Repackage the existing ARMT network switch using the packing materials from the new ARMT network switch.
      (4) Place the return shipping label on the repackaged ARMT network switch, and give it to the local shipping department.

   b. To install the new ARMT network switch:
      (1) Install the new ARMT network switch in the ARMT rack.
      (2) Connect the power cable and the network cables to the new ARMT network switch.

   c. To verify operational status, refer to the manufacturer’s user manual.

9.4.6 Install / Replace Monitor
The ARMT monitors are attached to ARMT server workstations and ARMT client workstations. They must be replaced after a failure.

   a. Refer to paragraph 6.2.1 to verify the operational status of the ARMT Client or 6.2.2 to verify the operational status of the ARMT server.

9.4.7 Install/ Replace ARMT External Hard Drive
The ARMT external hard drive is attached to the ARMT primary server workstation. It must be replaced after a failure. Refer to the manufacturer's user manual for detailed installation and removal procedures. The ARMT primary server uses the external hard drive to write log files.
Before disconnection the external hard drive, the backup server must be promoted to primary and the interfaces on the primary server must be shut down. Follow the following procedure to replace the external hard drive:

a. On either server, locate the ARMT System Monitor (refer to figure 3-6).
   (1) The current active server (server_primary/server_backup) is designated by a checkmark in the Active column.
   (2) Before proceeding, verify the Replication value for both servers = 0 or 1.

b. If the backup server is not designated as primary (9.4.7.a.1), make it the primary server:
   (1) On the backup server, locate the ARMT Replication Monitor (refer to figure 3-7).
   (2) Select the Make Primary button.
   (3) Observe the ARMT System Monitor. The non-active server will now have a checkmark indicating that it is now active.
   (4) Verify operational status of servers/clients. Refer to paragraph 3.1.4.4.

c. On the primary server, locate the EFSTS Monitor Window (refer to figure 3-1).
   (1) Select Exit to terminate the EFSTS Monitor.
   (2) When prompted, select Yes to continue.

d. On the primary server, locate the Terminal Interface (refer to figure 3-2).
   (1) Select Exit to terminate the Terminal Interface.
   (2) When prompted, select Yes to continue.

e. Remove the existing ARMT external hard drive.
   (1) Power-off the ARMT external hard drive.
   (2) Disconnect the existing ARMT external hard drive USB cable and power cable from the ARMT primary server workstation.
   (3) Remove the existing ARMT external hard drive.
   (4) Repackage the existing ARMT external hard drive using the packing materials from the new ARMT external hard drive.
   (5) Place the return shipping label on the repackaged ARMT external hard drive and give it to your local shipping department.

f. Install the new ARMT external hard drive.
   (1) Install the new ARMT external hard drive in the same location as the old ARMT external hard drive.
   (2) Connect the new ARMT external hard drive USB cable and power cable to the ARMT primary server workstation.
   (3) Power-on the new ARMT external hard drive.
   (4) On the ARMT primary server workstation, set the external hard drive letter to Z:
      (a) Log on to the ARMT primary server.
(b) Click on **Start / Control Panel / Administrative Tools / Computer Management**.
(c) On the left menu choose **Disk Management**.
(d) Locate the external hard drive in the drive list, and right click on it.
(e) Choose **Change Drive Letter and Paths** from the menu.
(f) Click the **Change** button.
(g) Confirm that the **Assign New Drive Letter** radio button is selected.
(h) Select letter **Z**: from the drive letter choice dropdown.
(i) Click **OK**.
(j) Click **OK** again.

(5) Remove existing files from the new hard drive.
(a) Click on **START – My Computer**.
(b) Double click the **Z Drive**.
(c) Select all files and folders on the Z Drive, and press the **Delete** key.
(d) Click the **OK** button in the warning dialog.

(6) Create the ARMT Interface Log file folder on the external hard drive.
(a) Click on **START – My Computer**.
(b) Double click the **Z Drive**.
(c) Click on the **File Menu – New – New Folder**.
(d) Name the new folder **ARMT_INTERFACE_LOGS**, and then press the **Enter** key.

**g.** On either server, locate the ARMT System Monitor (refer to figure 3-6).
(1) The current active server (server primarieserver_backups) is designated by a checkmark in the Active column.
(2) Before proceeding, verify the Replication value for both servers = 0 or 1.

**h.** On the primary server desktop, double click the **EFSTS Monitor** icon to start the EFSTS Monitor.

**i.** On the primary server, double click the **Terminal Automation Interface** icon to start the Terminal Automation Interface.

**j.** Make the primary server the primary server:
(1) On the primary server, locate the Replication Monitor (refer to figure 3-7).
(2) Select the **Make Primary** button.
(3) Observe the ARMT System Monitor. The primary server will now have a checkmark indicating that it is now active.
(4) Verify operational status of servers/clients. Refer to paragraph 3.1.4.4.

**9.4.8 Replace ARMT / EFSTS Interface Cables**
A custom pinout RS-422 cable is needed to interface with EFSTS to the Server A/B switch to receive and send information.

a. Fabricate a RS-422 cable from the Server A/B switch to the EFSTS. Length is determined on site specific distance between the two racks in the equipment room.

b. The DB9 end at the Server A/B switch EFSTS IN port should be a Female end.

c. The DB9 end at the EFSTS rack should be a Male end.

d. Figure 9-1 shows the pinouts diagram.

e. The pinout for the cables from the Server A/B switch to the P1 plugs of the Server's Serial Communication Card are straight – thru. Pins 1-1, 2-2, 3-3, 4-4,5-5.

---

**Figure 9-1 EFSTS to A/B Switch pinout**

---

9-10
9.0 Installation, Integration, and Checkout

9.1 SITE INFORMATION AND DRAWINGS - No site information is provided in this instruction book.

9.2 INSTALLATION MATERIALS REQUIRED - Table 9–1 lists the ARMT equipment supplied for installation. Equipment required but not supplied with ARMT equipment is listed in table 9-2. This list does not include wire, conduit, hardware, or other materials required to install the equipment.

### TABLE 9-1. INSTALLATION MATERIALS REQUIRED AND SUPPLIED

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Component</th>
<th>Logistics Center Label Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Primary server for each TRACON</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>Backup server for each TRACON</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>Client workstation</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>UPS for each server and each client workstation</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>Printer for the ARMT system</td>
<td>TBD</td>
</tr>
<tr>
<td>2</td>
<td>Serial cards for each TRACON (1 each for primary and backup server. Pre-installed/configured in the primary and backup servers.)</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>ARMT network switch per facility</td>
<td>TBD</td>
</tr>
<tr>
<td>Minimum:</td>
<td>Display (shipped with 4 ft VGA cord and 4 ft power plug)</td>
<td>TBD</td>
</tr>
</tbody>
</table>
### TABLE 9-1. INSTALLATION MATERIALS REQUIRED AND SUPPLIED (CONTINUED)

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Component</th>
<th>Logistics Center Label Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only if distance exceeds 100 meters between ARMT switch and peripheral equipment.</td>
<td>Ethernet extender</td>
<td>TBD</td>
</tr>
<tr>
<td>Determined by local site requirements</td>
<td>CAT5E plenum cable for all facilities</td>
<td>TBD</td>
</tr>
<tr>
<td>Determined by local site requirements</td>
<td>CAT5E connector plugs for all facilities</td>
<td>TBD</td>
</tr>
<tr>
<td>1 per TRACON where EFSTS is present</td>
<td>RS422 shielded serial cable with one male and one female end.</td>
<td>TBD</td>
</tr>
<tr>
<td>1 A/B Switch per TRACON where EFSTS is present</td>
<td>A/B Switch with (2) straight through RS422 Cables</td>
<td>TBD</td>
</tr>
<tr>
<td>1 per ARMTATCT client</td>
<td>Pair of desktop speakers for ATCT clients only (speakers are not provided for servers or clients at TRACONs or ARTCCs.)</td>
<td>TBD</td>
</tr>
<tr>
<td>1</td>
<td>External hard drive (for primary server)</td>
<td>TBD</td>
</tr>
</tbody>
</table>

### TABLE 9-2. INSTALLATION MATERIALS REQUIRED BUT NOT SUPPLIED

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 per TRACON</td>
<td>ARMT equipment rack (dimensions to be determined)</td>
</tr>
</tbody>
</table>

### 9.3 UNPACKING AND HANDLING INSTRUCTIONS

a. ARMT equipment is packaged in standard cardboard cartons and shipped to the site.
Note: Handle equipment carefully to prevent damage.

b. Remove all protective packaging materials, and inspect each item for damage that may have occurred during shipment.

c. File a claim with the carrier for any damage found when unpacking the equipment.

d. Retain all packaging for shipping the old ARMT equipment to the ARMT Depot.

9.4 ARMT EQUIPMENT INSTALLATION

Additional configuration is required for some ARMT equipment, and will be performed by ARMT Second Level Support after the new ARMT equipment is installed. Follow the procedures in this section to install ARMT equipment.

9.4.1 Install / Replace Server Workstation

After the ARMT server workstation is installed, ARMT Second Level Support must be contacted to complete the ARMT software configuration.

Note: The ARMT server must be replaced after a failure.

a. To remove the existing ARMT server workstation:
   
   (1) Shut down the ARMT server workstation.
   
   (2) Disconnect the existing ARMT server workstation by performing the following procedure:
      
      (a) Disconnect the following items from the existing ARMT primary server workstation:
          - power cable
          - display cable
          - network cables
          - RS232/422 harness
          - keyboard and mouse
          - external hard drive cable
      
      (b) Remove the existing ARMT server workstation from the ARMT rack and repackage it using the packing materials from the new ARMT server workstation.
      
      (c) Place the return shipping label on the repackaged ARMT server workstation and give it to the local shipping department.

b. To install the new ARMT server workstation:
   
   (1) Place the new ARMT server workstation in the ARMT rack.
   
   (2) Connect the new ARMT server workstation by performing the following procedure:
      
      (a) Connect the following items to the new ARMT server workstation:
          - monitor, keyboard and mouse cables
• RS232/422 harness
• network cables
• power cable
• If server being replaced is the Primary server, reconnect external hard-drive Refer to 9.4.7

(3) Configure the network card.
   (a) Select START> Control Panel>Network Connections.
   (b) Right click the ARMT_Network connection and select Properties.
   (c) Highlight the Internet Protocol (TCP/IP) in the protocol list and click the Properties button.
   (d) Select the Use The Following IP Address radio button
   (e) Enter the IP Address, Subnet Mask, and Default Gateway. This information is located in the ARMT Site Binder.
   (f) The DNS and WINS address is pre-configured for the ARMT_Network connection. Do not change these addresses.
   (g) Click OK.
   (h) Click OK.

(4) Contact ARMT Second Level Support to complete the installation.

(5) To verify operational status, perform steps in Par. 6.2.2 ARMT Server Workstation.

9.4.2 Install / Replace Client Workstation

After the ARMT client workstation is installed, ARMT Second Level Support must be contacted to complete the ARMT software installation and configuration.

a. To remove the existing ARMT client workstation:
   (1) Shut down the existing ARMT client workstation. Refer to paragraph 3.6.
   (2) Disconnect the existing ARMT client workstation by performing the following procedure.
      (a) Disconnect the following items from the existing ARMT client workstation:
          • power cable
          • network cable
          • monitor, keyboard and mouse cables
      (b) Remove the existing ARMT client workstation and repackage it using the packing materials from the new ARMT client workstation.
      (c) Place the return shipping label on the repackaged ARMT client workstation and give it to the local shipping department.

b. To install the new ARMT client workstation:
(1) Place the new ARMT client workstation in the location of the old ARMT client workstation.

(2) Connect the new ARMT client workstation by performing the following procedure:

(a) Connect the following items to the new ARMT client workstation:
   - monitor, keyboard and mouse cables
   - network cable
   - power cable

(3) Configure the network card.

(a) Select START> Control Panel> Network Connections.
(b) Right click the ARMT_Network connection and select Properties.
(c) Highlight the Internet Protocol (TCP/IP) in the protocol list and click the Properties button.
(d) Select the Use The Following IP Address radio button
(e) Enter the IP Address, Subnet Mask, and Default Gateway. This information is located in the ARMT Site Binder.
(f) The DNS and WINS address is pre-configured for the ARMT_Network connection. Do not change these addresses.
(g) Click OK.
(h) Click OK.

(4) Contact ARMT Second Level Support to complete the installation, restart ARMT, and test the installation.

(5) To verify operational status, refer to the ARMT TI, paragraph 6.2.1.

9.4.3 Install / Replace Uninterruptable Power Supply (UPS)

Follow this procedure for initial installation or, to replace a faulty ARMT UPS:

a. To remove the existing ARMT UPS that will be replaced, perform the following:

(1) Power-down all equipment that is plugged into the UPS and any equipment that will be affected during the outage.
   (a) To replace an ARMT client workstation UPS, power-down the attached ARMT client workstation.
   (b) To replace an ARMT primary server workstation UPS, power-down the ARMT backup and primary server workstations.
   (c) To replace an ARMT backup server workstation UPS, power-down the ARMT backup server workstation.

(2) Turn the UPS switch to the Off position.

(3) Unplug the existing equipment power cables from the UPS.

(4) Unplug the existing UPS USB data cable.
(5) Unplug and then remove the existing UPS.
(6) Discard UPS using local environmental battery disposal plan/procedure.

b. To install the new UPS:
   (1) Connect the UPS battery to the UPS.
   (2) Place the new UPS in the appropriate location for your ARMT equipment component.
   (3) Plug in the power cable for the UPS.
   (4) Plug in the equipment power cables to the UPS.
   (5) Plug in the UPS USB data cable.
   (6) Turn the UPS switch to the On position.
   (7) Power-on all equipment plugged into the UPS and any equipment that was turned off in step 9.4.3 a. (1).
      (a) When installing an ARMT client workstation UPS, power-on the attached ARMT client workstation.
      (b) When installing an ARMT primary server workstation UPS:
          1. Power-on the backup server workstation.
          2. Power-on the primary server workstation.
          3. Reboot the ARMT client workstations.
      (c) When installing an ARMT backup server workstation UPS, power-on the ARMT backup server workstation.
   (8) To verify operational status of the UPS, refer to Par. 6.2.4.
   (9) Refer to paragraph 6.2.1. to verify the operational status of the ARMT Client or 6.2.2 to verify the operational status of the ARMT server.

9.4.4 Install / Replace Network Printer

The ARMT network printer must be replaced after a failure.

Note: Refer to the manufacturer's user manual for detailed installation and removal procedures

a. To remove the existing ARMT network printer:
   (1) Shut down and disconnect the existing ARMT network printer.
   (2) Disconnect the power cable and the network cable from the existing ARMT network printer.
      (a) Remove the existing ARMT network printer.
      (b) Repackage the existing ARMT network printer using the packing materials from the new ARMT network printer.
      (c) Place the return shipping label on the repackaged ARMT network printer and give it to the local shipping department.
b. To install the new ARMT network printer:
   (1) Place the new ARMT network printer in the location of the old ARMT network printer.
   (2) To connect the new ARMT network printer:
      (a) Connect the network cable and the power cable to the new ARMT network printer.
      (b) Power-on the ARMT network printer.
      (c) Refer to the manufacturer’s user manual to set up the printer network IP address, subnet mask, and default gateway. Refer to the ARMT site binder for the printer network IP address information.
      (d) Refer to the manufacturer’s user manual to install the printer on all ARMT client workstations that require a printer.
   c. To verify operational status, refer to the manufacturer’s user manual.

9.4.5 Install / Replace Network Switch (Ethernet Switch)
The ARMT network switch does not require configuration, but must be replaced after a failure. Refer to the manufacturer’s user manual for detailed removal and installation procedures.
   a. To remove the existing ARMT network switch:
      (1) Disconnect the network cables and the power cable from the existing ARMT network switch.
      (2) Remove the existing ARMT network switch from the ARMT rack.
      (3) Repackage the existing ARMT network switch using the packing materials from the new ARMT network switch.
      (4) Place the return shipping label on the repackaged ARMT network switch, and give it to the local shipping department.
   b. To install the new ARMT network switch:
      (1) Install the new ARMT network switch in the ARMT rack.
      (2) Connect the power cable and the network cables to the new ARMT network switch.
   c. To verify operational status, refer to the manufacturer’s user manual.

9.4.6 Install / Replace Monitor
The ARMT monitors are attached to ARMT server workstations and ARMT client workstations. They must be replaced after a failure.
   a. Refer to paragraph 6.2.1 to verify the operational status of the ARMT Client or 6.2.2 to verify the operational status of the ARMT server.

9.4.7 Install/ Replace ARMT External Hard Drive
The ARMT external hard drive is attached to the ARMT primary server workstation. It must be replaced after a failure. Refer to the manufacturer's user manual for detailed installation and removal procedures. The ARMT primary server uses the external hard drive to write log files.
Before disconnection the external hard drive, the backup server must be promoted to primary and the interfaces on the primary server must be shut down. Follow the following procedure to replace the external hard drive:

a. On either server, locate the ARMT System Monitor (refer to figure 3-6).
   (1) The current active server (server_primary/server_backup) is designated by a checkmark in the Active column.
   (2) Before proceeding, verify the Replication value for both servers = 0 or 1.

b. If the backup server is not designated as primary (9.4.7.a.1), make it the primary server:
   (1) On the backup server, locate the ARMT Replication Monitor (refer to figure 3-7).
   (2) Select the **Make Primary** button.
   (3) Observe the ARMT System Monitor. The non-active server will now have a checkmark indicating that it is now active.
   (4) Verify operational status of servers/clients. Refer to paragraph 3.1.4.4.

c. On the primary server, locate the EFSTS Monitor Window (refer to figure 3-1).
   (1) Select **Exit** to terminate the EFSTS Monitor.
   (2) When prompted, select **Yes** to continue.

d. On the primary server, locate the Terminal Interface (refer to figure 3-2).
   (1) Select **Exit** to terminate the Terminal Interface.
   (2) When prompted, select **Yes** to continue.

e. Remove the existing ARMT external hard drive.
   (1) Power-off the ARMT external hard drive.
   (2) Disconnect the existing ARMT external hard drive USB cable and power cable from the ARMT primary server workstation.
   (3) Remove the existing ARMT external hard drive.
   (4) Repackage the existing ARMT external hard drive using the packing materials from the new ARMT external hard drive.
   (5) Place the return shipping label on the repackaged ARMT external hard drive and give it to your local shipping department.

f. Install the new ARMT external hard drive.
   (1) Install the new ARMT external hard drive in the same location as the old ARMT external hard drive.
   (2) Connect the new ARMT external hard drive USB cable and power cable to the ARMT primary server workstation.
   (3) Power-on the new ARMT external hard drive.
   (4) On the ARMT primary server workstation, set the external hard drive letter to **Z**:
      (a) Log on to the ARMT primary server.
(b) Click on Start / Control Panel / Administrative Tools / Computer Management.
(c) On the left menu choose Disk Management.
(d) Locate the external hard drive in the drive list, and right click on it.
(e) Choose Change Drive Letter and Paths from the menu.
(f) Click the Change button.
(g) Confirm that the Assign New Drive Letter radio button is selected.
(h) Select letter Z: from the drive letter choice dropdown.
(i) Click OK.
(j) Click OK again.
(5) Remove existing files from the new hard drive.
(a) Click on START – My Computer.
(b) Double click the Z Drive.
(c) Select all files and folders on the Z Drive, and press the Delete key.
(d) Click the OK button in the warning dialog.
(6) Create the ARMT Interface Log file folder on the external hard drive.
(a) Click on START – My Computer.
(b) Double click the Z Drive.
(c) Click on the File Menu – New – New Folder.
(d) Name the new folder ARMT_INTERFACE_LOGS, and then press the Enter key.

On either server, locate the ARMT System Monitor (refer to figure 3-6).

(1) The current active server (server_primary/server_backup) is designated by a checkmark in the Active column.
(2) Before proceeding, verify the Replication value for both servers = 0 or 1.

h. On the primary server desktop, double click the EFSTS Monitor icon to start the EFSTS Monitor.

i. On the primary server, double click the Terminal Automation Interface icon to start the Terminal Automation Interface.

j. Make the primary server the primary server:
(1) On the primary server, locate the Replication Monitor (refer to figure 3-7).
(2) Select the Make Primary button.
(3) Observe the ARMT System Monitor. The primary server will now have a checkmark indicating that it is now active.
(4) Verify operational status of servers/clients. Refer to paragraph 3.1.4.4.

9.4.8 Replace ARMT / EFSTS Interface Cables
A custom pinout RS-422 cable is needed to interface with EFST to the Server A/B switch to receive and send information.

a. Fabricate a RS-422 cable from the Server A/B switch to the EFST. Length is determined on site specific distance between the two racks in the equipment room.

b. The DB9 end at the Server A/B switch **EFST IN** port should be a Female end.

c. The DB9 end at the EFST rack should be a Male end.

d. Figure 9-1 shows the pinouts diagram.

![EFST to A/B Switch Pinout](image)

**Figure 9-1** EFST to A/B Switch pinout

e. The pinout for the cables from the Server A/B switch to the P1 plugs of the Server’s Serial Communication Card are straight – thru. Pins 1-1, 2-2, 3-3, 4-4,5-5.
10.0 Computer Software

10.1 PROGRAMS

10.1.1 Server Programs

a. Replication Monitor
   (1) The Replication Monitor replicates the primary server’s database to the backup server’s database.
   (2) Program location C:\armt\replication\ArmtReplicationMonitor.exe
   (3) If this program is not running or not responding, shut it down and then double click on the executable to restart.

b. Server (Message_Handler)
   (1) The Server (Message_Handler) processes the messages sent by the EFSTS and Interface programs and uses the data to populate the Airport Management (APM) database.
   (2) Program Location C:\armt\server\armtsserver.exe
   (3) If this program is not running or not responding, shut it down and then double click on the executable to restart.

c. System Monitor
   (1) The System Monitor shows the status of the ARMT servers and terminals/clients.
   (2) Program location C:\armt\systemmonitor
   (3) If this program is not running or not responding, shut it down and then double click on the executable to restart.

d. EFSTS Monitor
   (1) The EFSTS Monitor receives output from EFSTS, and writes necessary information to the database for ARMT processing.
   (2) Program location C:\armt\efsts\efstsmom.exe
   (3) If this program is not running or not responding, shut it down and then double click on the executable to restart.

e. Terminal Interface
   (1) The Terminal Interface receives and processes data from ARTS or STARS and writes information to the database for ARMT processing.
   (2) Program location C:\armt\interface\terminal_interface.exe
   (3) If this program is not running or not responding, shut it down and then double click on the executable to restart.

f. GuardDog
   (1) The GuardDog program monitors connection status of other ARMT server applications. If a monitored program does not update within the adapted time frame, GuardDog will stop and restart the application.
(2) Program location C:\armt\GuardDog\guarddog.exe
(3) If this program is not running or not responding on the primary server, shut it down and then double click on the executable to restart.

10.1.2 Client Programs
a. ARMT Client
   (1) The ARMT Client is the user interface for the ARMT system, showing Arrival and Departure information in various ways.
   (2) Program Location: C:\armt\clients\??\armt.exe (There can be multiple clients on a machine, one for each airport ARMT is monitoring).
   (3) If this program is not running or not responding, shut it down and then double click on the executable to restart.

10.2 DATABASE.

10.2.1 Airport Management (APM) Database
a. ARMT uses the MySQL database engine for data storage on the primary and backup servers. The database engine starts automatically as a Windows service. To double check that it is running take the following steps on XP:
   (1) Click on Start
   (2) Select Control Panel
   (3) Double click on Administrative Tools
   (4) Double click on Services
   (5) Find the service called MySQL. If the status is “Started”, then it is running. If the status is “blank”, then click on Start the service to start it.

10.3 CONFIGURATION FILES.

10.3.1 Server
a. Location - C:\armt\adapt\armt.ini
b. Sections. - If any of these are missing, the affected programs will not function. The missing section will need to be configured by ARMT Second Level Support. Each section is noted by the word, section, at the start of a new line followed by:
   (1) message_handler (Message_Handler/Server program)
   (2) replication_monitor (Replication Monitor program)
   (3) system_monitor (System Monitor program)
   (4) terminal interface (Terminal Interface program)
   (5) efsts (EFSTS Interface program)
   (6) guarddog (GuardDog program)

10.3.2 Client
1. Location C:\armt\clients\xxx\com.ini  Where xxx is the three character airport code.
   (1) Each client program has a separate ini file with the following options.
      (a) FacID: Facility ID, this will be the same for every client except in cases
          where the machine gets data from more then one server (Miami and West
          Palm Beach is an example).
      (b) Airpt: The three character AirportID this client will display. If the airport
          is BWI, for example, it will be: Airpt: BWI
      (c) The four character airportID, continuing the BWI example, Airp4: KBWI
      (d) TrmTp: client (this line should appear exactly like this) TrmTp: client
      (e) TrmID: Terminal ID, this is assigned to differentiate each terminal that
          attaches to the ARMT system using the following pattern:
          1. TrmID: bwitwr01 (BWI Tower PC #1)
          2. TrmID: bwitwr02 (BWI Tower PC #2)
      (f) DBLogVerbose: Make this a Y (DBLogVerbose: Y)
      (g) Svr01: APM (primary MySQL connection name)
      (h) Svr02: APM_BACKUP (backup MySQL connection name)
      (i) The connection names are APM and APM_BACKUP by default. If the
          terminal connects to more then one pair of servers, then the names will be
          different for the second server. Refer to Open Database Connectivity
          (ODBC) Connections paragraph 10.4.

10.4 OPEN DATABASE CONNECTIVITY (ODBC) CONNECTIONS

a. The ARMT programs use ODBC connections to talk with the APM database. Those
   files are setup in:
   (1) Start
   (2) Control Panel
   (3) Administrative Tools
   (4) Data Sources (ODBC)
   (5) Click on the system dsn tab.

b. For each master/backup server the system will connect with, there should be an
   ODBC connection. Check to make sure they exist.
   (1) APM – this is the primary ODBC connection. If the client connects to more then
       one master, the second will be named APM2, for example.
   (2) APM_BACKUP – this is the backup ODBC connection.

c. If any connection is missing do the following to create it.
   (1) Click the add button.
   (2) Select the MySQL ODBC 3.51 selection.
(3) Data source name: (APM or APM_BACKUP)
(4) Description: (same as data source name)
(5) Server: IP address of the server being setup.
(6) User: apm
(7) Password: apm
(8) Database: apm
(9) Click on the Advanced tab, and select the top two items
   (a) Do not optimize column width
   (b) Return matching rows
(10) Click the test button, and it should return with success. If not, then double check the entries. If there is still an error, call Second Level Support.

10.5 ARMT Commercial-Off-The-Shelf (COTS) Software

a. ARMT servers (both primary and standby backup) have pre-configured and installed licensed COTS software applications, including, as a minimum, the following:

<table>
<thead>
<tr>
<th>Windows 7 Professional</th>
<th>MySQL Database 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acrobat Reader 8</td>
<td>MySQL Connector 5.2.2</td>
</tr>
<tr>
<td>Computer Associates Total Defense R12 Client</td>
<td>RAdmin Server and Viewer 3.4</td>
</tr>
<tr>
<td>Wireshark 1.6.4</td>
<td>Sea Level 7404</td>
</tr>
<tr>
<td>Lexmark 250dn Drivers, or, Lexmark E240dn Drivers, or, Lexmark E260dn Drivers</td>
<td>ToadForMySQLFreeware_4.5.0.903</td>
</tr>
<tr>
<td>MS Office Pro 2003 (or 2010 upgrade)</td>
<td>VB6 Runtime Files</td>
</tr>
<tr>
<td></td>
<td>PowerChute Personal Edition v 2.0.0</td>
</tr>
</tbody>
</table>

*Note: ARMT Second Level Engineering Support will install COTS software applications updates via remote maintenance support, quarterly or as needed, for all server workstations.

b. ARMT client workstations have pre-configured and installed licensed COTS software applications, including, as a minimum, the following:

<table>
<thead>
<tr>
<th>Windows 7 Professional</th>
<th>MySQL Database 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acrobat Reader 8</td>
<td>MySQL Connector 5.2.2</td>
</tr>
<tr>
<td>Computer Associates Total Defense R12 Client</td>
<td>RAdmin Viewer 3.4</td>
</tr>
<tr>
<td>Wireshark 1.6.4</td>
<td>Sea Level 7404</td>
</tr>
<tr>
<td>Lexmark 250dn Drivers, or, Lexmark E240dn Drivers, or, Lexmark E260dn Drivers</td>
<td>ToadForMySQLFreeware_4.5.0.903</td>
</tr>
<tr>
<td>MS Office Pro 2003 (or 2010 upgrade)</td>
<td>VB6 Runtime Files</td>
</tr>
<tr>
<td></td>
<td>PowerChute Personal Edition v 2.0.0</td>
</tr>
</tbody>
</table>
*Note: ARMT Second Level Engineering Support will install COTS software applications updates via remote maintenance support, quarterly or as needed, for all client workstations.
This Page Intentionally Left Blank
Appendix A. MOA Sample

Federal Aviation Administration

Memorandum

Date: [Insert date]

To: [Insert facility manager, facility name]

From: [Insert supervisor/manager Facility Name System Support Center]

Prepared by: [Type name and title of individual who prepared memo here]

Subject: Maintenance Agreement on FACID Airport Resource Management Tool (ARMT) System

On [insert month, day, year] we accepted site maintenance responsibilities for the Airport Resource Management Tool (ARMT) for the [insert facility name and FACID]. In order to maintain this equipment, it is required that maintenance be performed as directed by JO 6131.5, Maintenance of the Airport Resource Management Tool Equipment (referred to as the ARMT maintenance handbook or MTHB), and specific procedures for ARMT user account management provided in the technical instruction book (TI 6131.15).

This memorandum acts as an agreement with AT to perform:

(1) daily checks of client workstation status “green/normal” operations and to notify site maintenance personnel of conditions other than normal, and,

(2) quarterly reviews and updates of ARMT user/admin group account lists for AT personnel to the designated facility TechOps site ARMT system administrator(s) to support required quarterly group account access reviews IAW FAA Order 1370.96 and the ARMT MTHB 6131.5.

This agreement will remain in affect until there is a change in the JO6131.5 or both parties mutually agree to modify.

Signature Facility Manager, Facility Name

Date

Signature Supervisor/Manager, Facility ID SSC

Date

CC: ARMT Program Office, AJM-2440, Dan Costello or Brian J. Schell
Appendix B. Glossary of Terms

A.1 ABBREVIATIONS AND ACRONYMS.

The following is the list of abbreviations and acronyms used in this technical instruction book.

AFAAR  Technical Operations Aircraft Accident Representative
AGW  ARTS Gateway
AIG  Applications Interface Gateway
APM Database  Airport Management Database
ARMT  Airport Resource Management Tool
ARTCC  Air Route Traffic Control Center
ARTS  Automated Radar Terminal Systems
AT  Air Traffic
ATC  Air Traffic Control
ATCT  Air Traffic Control Tower
ATCSCC  Air Traffic Control System Command Center
ATL  Atlanta
ATO  Air Traffic Organization
ATO-T  Air Traffic Organization-Terminal
ATSS  Airway Traffic System Specialist
BWI  Baltimore/Washington International Thurgood Marshall Airport
CARTS  Common Automated Radar Terminal System
CAT5  Category 5 Unshielded Twisted Pair(UTP) Cable
CCD  Configuration Control Decision
CDR  Continuous Data Recording
C/DRP  Contingency/Disaster Recovery Plan
CID  Computer Identification
CM  Configuration Management
COM  Communication
COTS  Commercial Off The Shelf
EDCT  Estimated Departure Clearance/Control Time
FAA  Federal Aviation Administration
EFSTS  Electronic Flight Strip Transfer System
FDIO  Flight Data Input Output
FIR  Field Incident Response
FSEP  Facility, Service, and Equipment Profile
FTI  FAA Telecommunications Infrastructure
FTI OPS  FAA Telecommunications Infrastructure Operational Data Network
GUI  Graphical User Interface
HCS  Host Computer System
IS  Information Security
ISCP  Information System Contingency Plan
ISSP  Information System Security Plan
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>KSN</td>
<td>Knowledge Sharing Network</td>
</tr>
<tr>
<td>LCD</td>
<td>Liquid Crystal Display</td>
</tr>
<tr>
<td>LIS</td>
<td>Logistics Inventory System</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LRU</td>
<td>Lowest Replaceable Unit</td>
</tr>
<tr>
<td>MMS</td>
<td>Maintenance Management System</td>
</tr>
<tr>
<td>MOVR</td>
<td>Multi Strip Prevention Override</td>
</tr>
<tr>
<td>NAPRS</td>
<td>National Airspace Performance Reporting System</td>
</tr>
<tr>
<td>NAS</td>
<td>National Airspace System</td>
</tr>
<tr>
<td>NASA</td>
<td>National Aeronautics and Space Administration</td>
</tr>
<tr>
<td>NCP</td>
<td>NAS Change Proposal</td>
</tr>
<tr>
<td>NIC</td>
<td>Network Interface Card</td>
</tr>
<tr>
<td>NOCC</td>
<td>National Operation Control Center</td>
</tr>
<tr>
<td>NOM</td>
<td>NAS Operations Manager</td>
</tr>
<tr>
<td>ODBC</td>
<td>Open Database Connectivity</td>
</tr>
<tr>
<td>OEP</td>
<td>Operational Evolution Plan</td>
</tr>
<tr>
<td>OpsConfig</td>
<td>Operations Configuration</td>
</tr>
<tr>
<td>OpsNet</td>
<td>Operations Network</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PCI</td>
<td>Peripheral Component Interconnect</td>
</tr>
<tr>
<td>POC</td>
<td>Point of Contact</td>
</tr>
<tr>
<td>RoB</td>
<td>Security Rules of Behavior</td>
</tr>
<tr>
<td>RADMIN</td>
<td>Remote Administrator</td>
</tr>
<tr>
<td>RCU</td>
<td>Remote Control Unit</td>
</tr>
<tr>
<td>SC</td>
<td>Standard Connector</td>
</tr>
<tr>
<td>SCAP</td>
<td>System Security Authorization Certification Package</td>
</tr>
<tr>
<td>SCD</td>
<td>System Characterization Document</td>
</tr>
<tr>
<td>SCU</td>
<td>System Control Unit</td>
</tr>
<tr>
<td>SMA</td>
<td>Surface Movement Advisory</td>
</tr>
<tr>
<td>SME</td>
<td>Subject Matter Expert</td>
</tr>
<tr>
<td>STARS</td>
<td>Standard Terminal Automated Replacement System</td>
</tr>
<tr>
<td>SUI</td>
<td>Sensitive Unclassified Information</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
<tr>
<td>TBD</td>
<td>To Be Determined</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TRACON</td>
<td>Terminal Radar Approach Control Facility</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>WJHTC</td>
<td>William J. Hughes Technical Center</td>
</tr>
</tbody>
</table>