

12a. Integrated Voice and Data ATP

12a. Overview

The STARS Integrated Voice and Data (IV&D) Acceptance Test Plan (ATP) is comprised of the following Acceptance Test Procedures (ATPs), which are representative of the acceptance tests which will be performed. The actual test documents will contain the customer specific names (i.e., talk groups, features, templates, configurations, etc.) and will be finalized in accordance with the Contract's Section 1 Statement of Work.

12a.1.1 General Guidelines

The following general guidelines apply to the IV&D ATP:

1. The Commonwealth reserves the right to substitute VHF portables for any mobile in any of the functional tests (coverage permitting) in this document.
2. Except as otherwise specified within this contract, Motorola will perform ATP tests both at Motorola's Customer Center for System Integration (CCSI) and in the field.
3. In accordance with the System Integration Statement of Work documentation requirements in Section 1, Motorola will provide the Commonwealth a detailed table indicating which of these tests is to be performed at CCSI and/or which is to be performed in the field.
4. All available IV&D transmitter sites associated with the respective Division involved in the testing will be operational during these tests.
5. For definitions of test abbreviations or acronyms, refer to the Glossary in Appendix 23.
6. As the functionality of certain items depends on their configuration or integration with other subsystems, several such items do not currently have ATPs included in this contract. For these items, Motorola will provide the Commonwealth test procedures in accordance with the System Integration Statement of Work documentation requirements in Section 1:
 - A representative sample of all the types of combinations of radios (including control stations) and control heads being provided to the Commonwealth.

- Control head functionality for XTL 5000 mobile radio models W3, W7, and W9, including external connections to lights, sirens, PA, DEK, etc.
 - Note: The Commonwealth will provide all external equipment (lights, sirens, PAs, etc.) to be interfaced with Motorola provided equipment.
- External accessory equipment to the XTL 5000 mobile radio model W9, including verification test of the following:
 - Door switch to activate DVRS
 - Radio speaker connection to PA
 - Emergency thumb switch, etc.
- Motorcycle radio and control head functionality
 - Lights
 - Siren functions
 - PA functions
 - External audio functions
 - Helmet microphone
- Aircraft radio functionality (This test will be performed in the field after completion of installation. Motorola will provide a test procedure for this.)
- LMR site testing (including deployable sites and tunnels) including base station parameters (trunked and conventional), antenna systems, data, gains and losses, VSWR, TDRs for all antenna systems, grounding, HVAC, MOSCAD site alarms, batteries, chargers, tower lights, etc. The ReadySet functionality will be tested with their associated deployable site(s).
- Logging recorder functionality - Motorola will provide a procedure checklist and demonstrate this functionality during console testing at the Divisions.
- Console operations and functionality including the administrative phone system, Instant Recall Recorder (IRR), etc. – Motorola will provide a procedure checklist and demonstrate these functions during console testing at the Divisions.
- Locality interoperability interfaces – Motorola will provide a test procedure and demonstrate functionality of these console interfaces during Division and NOC console testing.
- Agency interoperability interfaces – Motorola will provide a test procedure and demonstrate functionality of these console interfaces during Division and NOC console testing.

- Legacy system interfaces – Motorola will provide a test procedure and demonstrate functionality of these console interfaces during Division and NOC console testing.
- Failsoft control stations, operation from each communications center – Motorola will provide a test procedure and demonstrate functionality of these console interfaces during Division and NOC console testing.

Digital Vehicular Repeater System (DVRS) ATP

DIGITAL VEHICULAR REPEATER SYSTEM

FIRST VEHICLE ON SCENE

Description. Digital Vehicle Repeater Systems (DVRS) are used when a user has to leave his/her vehicle and use a portable radio. A DVRS will allow a portable radio, while outside of its main coverage area, to communicate with the rest of the radio network.

Setup. A vehicle with a cross-band DVRS installed, an 700/800 MHz portable radio, a portable radio charger, a VHF mobile radio and portable radio set to operate on talk group A.

Test Instructions.

Step	Description	Expected Result
1	Park the vehicle with the DVRS 1 installed outside of the STARS Project Management Team office.	
2	Pull the 700/800 MHz portable radio from the vehicular charger and activate it to operate on channel 1.	The DVRS will transmit three consecutive single tone bursts on the 700/800 MHz portable Rx frequency to see if there is any traffic on channel 1.
3	Walk 50 ft any direction away from the vehicle.	
4	Key the 700/800 MHz portable radio 1 and hold the PTT for a talk-in test.	DVRS 1 receives the transmission from the 700/800 MHz portable radio and retransmits the audio through the VHF mobile 1 radio on VHF talk group A. Verify that VHF portable 1 receives talk group A audio.
5	Initiate a Group Call on talk group A with VHF portable 1.	The VHF mobile 1 receives the transmission from the VHF portable radio and retransmits the audio through DVRS 1 on channel 1. Verify that the 700/800 MHz portable 1 receives the audio on channel 1.

Pass / Fail / Not Tested (Circle One)

DIGITAL VEHICULAR REPEATER SYSTEM

SECOND VEHICLE ON SCENE

Description. When a second DVRS arrives on scene, there are many factors that determine which unit will become the master unit. The factors consist of: received signal strength, last used unit, unit ID, and random time.

Setup. Two vehicles with cross band DVRS's installed, two 700/800 MHz portable radios, two portable radio chargers, and two VHF mobile and portable radios that can be set to operate on talk group A and B.

Test Instructions.

Step	Description	Expected Result
1	The second vehicle with DVRS 2 installed parks near the first vehicle with DVRS 1 installed. DVRS 1 will remain transmitting. Switch VHF mobile 2 radio to operate on talk group B.	
2	Pull the 700/800 MHz portable 2 radio from the vehicular charger of DVRS 2 and activate it to operate on channel 2.	DVRS 2 will transmit three consecutive single tone bursts on the 700/800 MHz portable Rx frequency to see if any traffic is on channel 2.
3	Go stand next to the tester of vehicle 1.	
4	Key the 700/800 MHz portable 2 and hold the PTT for a talk-in test.	DVRS 2 receives the transmission from the 700/800 MHz portable 2 radio and retransmits the audio through the VHF mobile 2 radio on VHF talk group B. Verify that VHF portable 2 receives talk group B audio. DVRS 2 will not interfere with DVRS 1 because they are operating on different frequencies.
5	Initiate a Group Call on talk group B with VHF portable 2.	The VHF mobile 2 receives the transmission from the VHF portable 2 radio through the VHF trunked radio system and retransmits the audio through DVRS 2 on channel 2. Verify that the 700/800 MHz portable 2 receives the audio on channel 2.
6	Stop all transmission on channel 1.	

7	Switch DVRS 2 and 700/800 MHz portable 2 to channel 1 and switch VHF mobile 2 and portable 2 to talk group A.	
8	Key the 700/800 MHz portable 2 and hold PTT for a talk-in test.	The master repeater is determined every time the DVRS transmitter has a PTT request. The master repeater is determined by signal strength. One of the DVRS's will receive the transmission from the 700/800 MHz portable 2 and retransmit the audio through either VHF mobile 1 or 2 on VHF talk group A. Verify that both VHF portable 1 and 2 receive talk group A audio.
9	Initiate a Group Call on talk group A with VHF portable 2.	Either VHF mobile 1 or 2 receives the transmission from the VHF portable 2 radio and retransmits the audio through either DVRS 1 or 2 on channel 1. Verify that the 700/800 MHz portables 1 and 2 receives the audio on channel 1.

Pass / Fail / Not Tested (Circle One)

DIGITAL VEHICULAR REPEATER SYSTEM

THIRD VEHICLE ON SCENE

Description. When a second or third DVRS arrives on scene, there are many factors that determine which unit will become the master unit. The factors consist of: received signal strength, last used unit, unit ID, and random time.

Setup. Three vehicles with cross-band DVRS's installed, three 700/800 MHz portable radios, three portable radio chargers, and three VHF mobile and portable radios that are set to operate on talk group A.

Test Instructions.

Step	Description	Expected Result
1	The third vehicle with DVRS 3 installed parks near the first and second vehicle with DVRS 1 and 2 installed.	
2	Stop all transmission on channel 1.	
3	Pull the 700/800 MHz portable 3 radio from the vehicular charger of DVRS 3 and activate it to operate on channel 1.	DVRS 3 will transmit three consecutive single tone bursts on the 700/800 MHz portable Rx frequency to see if there is any traffic channel 1.
4	Go stand next to the testers of vehicle 1 and 2.	
5	Key the 700/800 MHz portable 3 radio and hold PTT for a talk-in test.	The master repeater is determined every time the DVRS transmitter has a PTT request. The master repeater is determined by signal strength. One of the three DVRS's will receive the transmission from the 700/800 MHz portable 3 and retransmit the audio through either VHF mobile 1, 2, or 3 on VHF talk group A. Verify that both VHF portable 1, 2, and 3 receive talk group A audio.
6	Initiate a Group Call on talk group A with VHF portable 3	Either VHF mobile 1, 2, or 3 receives the transmission from the VHF portable 3 radio and retransmits the audio through either DVRS 1, 2, or 3 on channel 1. Verify that the 700/800 MHz portables 1, 2, and 3 receives the audio on channel 1

Pass / Fail / Not Tested (Circle One)

DIGITAL VEHICULAR REPEATER SYSTEM

THIRD VEHICLE LEAVES SCENE

Description. Regardless of which DVRS unit leaves the scene, one DVRS remaining on scene will retain or take over master repeater status.

Setup. Three vehicles with cross band DVRS's installed, three 700/800 MHz portable radios, three portable radio chargers, and three VHF mobile radios that are set to operate on talk group A.

Test Instructions.

Step	Description	Expected Result
1	Any one vehicle should leave the scene and turn its DVRS off.	
2	Either 700/800 MHz portable 1 or 2 will key-up and hold PTT for a talk-in test.	Whichever DVRS receiver has the better signal strength will take over and become the master repeater. Verify that VHF portables 1 and 2 receive the transmission from either DVRS 1 or 2 on talk group A.
3	Initiate a Group Call on talk group A with VHF portable 1 or 2.	Verify that both 700/800 MHz portables 1 and 2 receive the transmission from VHF mobile 1 or 2 on channel 1.

Pass / Fail / Not Tested (Circle One)

Other DVRS tests {These test procedures will be developed when the DVRS specific functionality characteristics are fully developed as a new Motorola product.}:

- Multiple DVRS units on scene on different talk groups using different 700/800 MHz portable radio channels.
- End to end encryption
- Talk permit tones
- 10-33 signaling
- Close proximity test

Generator / UPS Functionality Testing

Generator and UPS functionality will be tested and verified as meeting specifications in accordance with Motorola's R56 "Standards and Guidelines for Communication Sites." The following R56 Site Installation Audit checklist contains paragraph references to auditing and testing the Power Sources (see Section 5 in the following checklist) and the functionality of each item applicable to a specified site's installation configuration will be tested for proper operation prior to acceptance.

Customer Name:				Project Name:					
Project Manager:				Project #:					
Inspector's Name:				Audit Date:					
Site Name:									
		Motorola Responsibility		Customer Responsibility			Motorola Failure	Customer Failure	
DESCRIPTION	Passed	Failed	Passed	Failed	N/A	Date Corrected	Date Corrected	R56 Paragraph Reference	
1 GENERAL									
a.	A copy of the Project Manager's Compliance Sheet has been completed, certified and supplied for attachment to this audit.							-	
b.	Project Manager's Compliance Sheet shows that all appropriate requirements have been met.								
TOTALS FOR SECTION		0	0	0	0	0			
2 BUILDING DESIGN AND INSTALLATION									
a.	The ceiling height is sufficient to meet requirements for equipment installation.								Paragraph 5.6

b.	Cable runway system meets the proper installation requirements.								Paragraph 5.10
c.	The floor is sealed as required.								Paragraph 5.6
d.	Transmission line entry ports, holes or openings which penetrate the outer surface of the building have been properly sealed.								Paragraph 5.7
e.	Adequate lighting requirements have been met.								Paragraph 5.11
f.	Minimum required fire suppression equipment is properly installed.								Paragraph 5.12
g.	A first aid kit is available and meets requirements.								Paragraph 5.12.6.1
h.	Required personal protective safety items are available for servicing batteries which require such items.								Paragraph 5.12.6.2
i.	A telephone, microwave link, or cellular phone has been made available.								Paragraph 5.12.8

j.	Phone numbers of importance are posted at the site.								Paragraph 5.12.8
k.	The minimum required signage is posted at the site.								Paragraph 5.13
TOTALS FOR SECTION		0	0	0	0	0			
3 EXTERNAL GROUNDING									
a.	An External Ground Bus bar (EGB) of suitably sized material is properly installed at the transmission line entry point.								Paragraph 6.3.3
b.	The EGB grounding electrode conductor has been properly installed.								Paragraph 6.3.3
c.	When a tower ground bus bar (TGB) is used, it meets the proper installation and bonding requirements.								Paragraph 6.3.4

d.	Each transmission line outer shield is properly bonded to the tower or TGB at the transition of the vertical transmission line run with a weather sealed transmission line grounding kit.								Paragraph 6.4.6
e.	Each transmission line outer shield is properly bonded to the EGB with a weather sealed transmission line grounding kit.								Paragraph 6.4.6
f.	The tower is properly bonded with the required number grounding conductors.								Paragraph 6.4.5
g.	Ice bridges / cable supports have been properly bonded to the EGB.								Paragraph 6.4.3
h.	Each ice bridge / cable support post has been properly bonded to the grounding electrode system.								Paragraph 6.4.3

i.	Ice bridges / cable supports have been properly isolated from the tower.								Paragraph 6.4.3
j.	Guy wires are properly bonded and their grounding conductor maintains a continuous vertical drop to the grounding electrode.								Paragraph 6.4.5
k.	Fencing has been properly bonded to a ground system as required.								Paragraph 6.4.2
l.	Each fence gate is properly bonded to its supporting fence post as required.								Paragraph 6.4.2
m.	Gate supporting fence posts are properly bonded as required.								Paragraph 6.4.2
n.	Generator and support skids have been properly bonded as required.								Paragraphs 6.4.1 & 8.9.8.1
o.	Items listed below are properly bonded to the grounding electrode system as required.								Paragraph 6.4.1
o.1	Metallic entry ports								Paragraph 6.4.1

o.2	Cable conduits or raceways								Paragraph 6.4.1
o.3	Metallic piping (water, gas, electrical conduits, etc..)								Paragraph 6.4.1
o.4	Air conditioner units								Paragraph 6.4.1
o.5	Metal siding and/or roofing on buildings								Paragraph 6.4.1
o.6	Vent covers and grates								Paragraph 6.4.1
o.7	Metal fuel storage tanks (above or below ground)								Paragraph 6.4.1
o.8	Building skid or pier foundations								Paragraph 6.4.1
o.9	Anchors on prefabricated buildings								Paragraph 6.4.1
o.10	Metallic structures for antenna supports, light fixtures, etc.								Paragraph 6.4.1
o.11	Satellite dish supports								Paragraph 6.4.1
o.12	GPS antenna supports								Paragraph 6.4.1
o.13	Hand and safety rails								Paragraph 6.4.1
o.14	Ladders and safety cages								Paragraph 6.4.1
o.15	Security bars and window frames								Paragraph 6.4.1

o.16	Main electrical ground						Paragraph 6.4.1
o.17	Main telco ground						Paragraph 6.4.1
p.	Approved bonding techniques have been used for the connection of dissimilar metals.						Paragraph 6.5.2
q.	Approved methods have been used for conductor connection and termination.						Paragraph 6.5
r.	Bonding surfaces for lugs and clamps are free of paint and corrosion and a conductive anti-oxidant compound has been applied.						Paragraph 6.5
s.	All painted or galvanized bonding surfaces for exothermic welds were cleaned and painted to inhibit rusting.						Paragraph 6.5
t.	All grounding conductors have been routed towards the EGB, TGB or the grounding electrode system and the minimum bending radius has been observed.						Paragraph 6.4.4
u.	Grounding conductors are routed as straight as possible and						Paragraph 6.3.2

	protected from physical damage as required.								
v.	Grounding conductors maintain the minimum required separation from other cable groups.								Paragraph 6.3.2.3
w.	Grounding conductors are securely fastened as required.								Paragraph 6.3.2.3
x.	Grounding conductors meet or exceed the conductor size requirements.								Paragraph 6.4.9
y.	Braided grounding conductors are not used anywhere in the external ground system.								Paragraph 6.4.2
TOTALS FOR SECTION		0	0	0	0	0			
4 INTERNAL GROUNDING									
a.	A properly sized Master Ground Bus Bar (MGB) is installed as required.								Paragraph 7.2.

b.	The MGB grounding electrode conductor has been properly bonded and routed towards the grounding electrode system.								Paragraph 7.2.
c.	All conductor connections to the MGB follow approved connection methods.								Paragraphs 7.4
d.	Where required a Sub System Ground Bus Bar (SSGB) has been properly installed.								Paragraph 7.2.2
e.	The SSGB has been bonded back to the MGB as required.								Paragraph 7.2.2
f.	All conductor connections to the SSGB follow the approved connection methods.								Paragraphs 7.4
g.	Where required an Internal Perimeter Ground Bus (IPGB) is properly installed.								Paragraph 7.3.2
h.	Only ancillary equipment is bonded to the IPGB.								Paragraph 7.3.5.3

i.	Each ancillary support apparatus is properly bonded to the IPGB, MGB, or SSGB.								Paragraph 7.3
j.	Items listed below are properly bonded to the MGB, SSGB, or IPGB by the approved connection methods.								Paragraph 7.3.2
j.1	Piping systems								Paragraph 7.3.2
j.2	Steel roof trusses								Paragraph 7.3.2
j.3	Exposed support beams or columns								Paragraph 7.3.2
j.4	Ceiling grids								Paragraph 7.3.2
j.5	Raised equipment floor support structure at the proper intervals.								Paragraph 7.3.2
j.6	Any exposed metallic building materials (metal siding)								Paragraph 7.3.2
k.	Surge Suppression Device (SPD) metal housings are bonded to the MGB, SSGB or IPGB as required.								Paragraph 7.3.5.5

i.	Separately derived AC electrical systems are bonded to the MGB or SSGB as required.								Paragraph 8.3.2
m.	Primary telephone, control, and data network circuit SPDs are properly installed bonded to the MGB or SSGB as required.								Paragraph 7.3.5.6
n.	RF transmission line SPDs are bonded to the MGB or a separate equipment area SSGB as required.								Paragraph 7.3.5.5
o.	Cable runways are bonded to the MGB or SSGB as required.								Paragraph 7.3.3.4
p.	Each cable runway section is bonded to the adjoining section as required.								Paragraph 7.3.4
q.	Ground bus conductors and their extensions are sized as required.								Paragraph 7.3.1

r.	All ground bus conductors, ground bus extensions and equipment grounding conductors are routed towards the MGB or SSGB as required.								Paragraph 7.3.1.3
s.	Bonding connections to a ground bus or its extensions have been properly insulated as required.								Paragraph 7.3.1.3
t.	Cabinets have been properly bonded back to the MGB, SSGB or ground bus by approved methods.								Paragraph 7.2.2.4
u.	Racks have been properly bonded back to the MGB, SSGB or ground bus by approved methods.								Paragraph 7.2.2.4
v.	Any RGB located within a cabinet or rack is properly bonded back to the MGB, SSGB or ground bus as required.								Paragraph 7.2.3
w.	Individual system component chassis equipment is properly bonded as required.								Paragraph 7.2.3

x.	Secondary telephone, control, and data network circuit SPDs are properly installed and bonded back to MGB or SSGB as required.							Paragraph 7.3.5.6
y.	All required control center and dispatch equipment is properly bonded back to the MGB, SSGB, or ground bus conductor as required.							Paragraph 7.6
TOTALS FOR SECTION		0	0	0	0	0		
5 POWER SOURCES								
a.	Circuit breakers are labeled to identify the receptacle outlet they are protecting.							Paragraph 8.3.3
b.	Proper clearance requirements are being observed for power panels.							Paragraph 8.3.3
c.	Outlet boxes are permanently marked to identify their assigned circuit breakers and panels.							Paragraph 8.3.10

d.	Power receptacle outlets are mounted securely to the supporting structure.								Paragraph 8.3.9
e.	Adequate service receptacle outlets are provided for the technician.								Paragraph 8.3
f.	Each critical piece of equipment has a dedicated branch circuit and dedicated simplex receptacle.								Paragraph 8.3.10
g.	Power receptacles are installed by the equipment load as required.								Paragraph 8.3.10
h.	Extension cords including temporary outlet strips are not used in the final installation.								Paragraph 8.3.9
i.	Exterior receptacle outlets and circuits are GFCI protected as required.								Paragraph 8.3.5
j.	AC power receptacle outlets and strips are of the proper type and securely mounted off the floor.								Paragraph 8.4

k.	Appropriate clearance is being observed for safe servicing of UPS and battery banks.								Paragraph 8.6.2
l.	The neutral - ground bonding conductor has been properly installed in the main service disconnect as required.								Paragraph 8.3.7
m.	Equipment grounding conductors have been installed as required.								Paragraph 8.3.8
n.	Solar panels have been located away from objects that could damage or block sunlight to the panel.								Paragraph 8.7.2
o.	Proper mounting practices are being observed for solar panels or wind generators.								Paragraph 8.7.2
p.	Battery racks are bolted to the floor or wall.								Paragraph 8.8.8
q.	Battery conductors are enclosed in PVC, metallic conduit or raceways.								Paragraph 8.8.8

r.	A battery disconnect and suitable circuit protection device has been installed as required.								Paragraph 8.8.8
s.	When a standby power generator has been installed, it meets the proper installation requirements.								Paragraph 8.9.2
t.	Standby generators are located in areas only accessible by authorized personnel.								Paragraph 8.9.2
u.	Standby generators have an adequate area provided for servicing.								Paragraph 8.9.2
v.	Fuel storage tanks for standby generators are located within a secured area.								Paragraph 8.9.3
w.	A dedicated electrical circuit has been provided at the generator.								Paragraph 8.9.5

x.	A transfer switch of the proper ampacity rating has been installed to perform the switching between commercial power and standby generator power.								Paragraph 8.9.4
y.	A main service disconnect has been installed as required.								Paragraph 8.9.4
z.	Electrical panelboard ampacity ratings are properly coordinated.								Paragraph 8.9.4
TOTALS FOR SECTION		0	0	0	0	0			
6 TRANSIENT VOLTAGE SURGE SUPPRESSION									
a.	A Type 1 SAD/MOV surge protection device (SPD) is installed as required.								Paragraph 9.4.1
b.	A Type 2 MOV surge protection device (SPD) is installed as required.								Paragraph 9.4.1
c.	Primary SPDs for telephone circuits are installed as required.								Paragraph 9.5

d.	Secondary SPDs for telephone circuits are installed as required.								Paragraph 9.5
e.	Primary SPDs for control circuits are installed as required.								Paragraph 9.5
f.	Secondary SPDs for control circuits installed as required.								Paragraph 9.5
g.	Primary SPDs for data network circuits are installed as required.								Paragraph 9.5
h.	Secondary SPDs for data network circuits are installed as required.								Paragraph 9.5
i.	All RF transmission lines, including unused spares, have coaxial RF type SPDs properly installed as required.								Paragraph 9.6
j.	Where a tower top amplifier has been installed, the sample port and its control cables have SPDs installed as required.								Paragraph 9.6

k.	Tower lighting system AC power and data/alarm circuits have SPDs properly installed as required.								Paragraph 9.8
TOTALS FOR SECTION		0	0	0	0	0			
7 EQUIPMENT INSTALLATION									
a.	Equipment spacing and aisle widths conform to guidelines.								Paragraph 11.3
b.	Equipment is level and plumb.								Paragraph 11.4
c.	Equipment is square with surrounding equipment and walls.								Paragraph 11.4
d.	Where applicable, seismic installation practices have been observed.								Paragraphs 11.6
e.	Cabinets and racks are secured as required.								Paragraphs 11.6
f.	Cables and cable groups of different function maintain a minimum 5 cm (2 in.) separation as required.								Paragraph 11.8.1
g.	RF cables meet or exceed minimum								Paragraph 11.8.9

	bending radius requirements.								
h.	Plenum-rated cables are installed as required.								Paragraph 11.8.2
i.	Proper cable lengths are used.								Paragraph 11.8.1
j.	Cables are properly secured at the required intervals.								Paragraph 11.8.1
k.	AC power conductors installed on cable runway systems meet installation requirements.								Paragraph 11.8.3
l.	Cables are properly identified with a standard, double-ended system.								Paragraph 11.8.13
m.	Distribution frame wiring conforms to the proper punch-down or wire-wrap techniques.								Paragraph 11.8.12
n.	CAT-5 cables maintain the proper separation from AC power cables.								Paragraph 11.8.7.4
o.	CAT-5 cables do not have any sharp bends.								Paragraph 11.8.7.4

p.	CAT-5 cables meet all other installation requirements.								Paragraph 11.8.7															
q.	Cables installed below raised flooring systems are properly installed.								Paragraph 11.8.7															
r.	Cables installed above suspended ceilings are properly installed.								Paragraph 11.8.2															
s.	Electrostatic discharge practices are observed as required.								Paragraph 11.9															
TOTALS FOR SECTION		0	0	0	0	0																		
<table border="1"> <thead> <tr> <th>MOTOROLA</th> <th></th> <th>CUSTOMER</th> <th></th> <th></th> </tr> <tr> <th>Number of Passed</th> <th>Number of Failed</th> <th>Number of Passed</th> <th>Number of Failed</th> <th>Total N/A</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> </tr> </tbody> </table>										MOTOROLA		CUSTOMER			Number of Passed	Number of Failed	Number of Passed	Number of Failed	Total N/A	0	0	0	0	0
MOTOROLA		CUSTOMER																						
Number of Passed	Number of Failed	Number of Passed	Number of Failed	Total N/A																				
0	0	0	0	0																				
AUDIT TOTALS		0	0	0	0	0																		

Wide-Area Trunking Features

Wide-Area Trunking Features

Talkgroup Call

1. DESCRIPTION

The Talkgroup is the primary level of organization for communications on a trunked radio system. Radios with Talkgroup Call capability will be able to communicate with other members of the same Talkgroup. This provides the effect of a private channel down to the Talkgroup level. This test will demonstrate that a Talkgroup transmission initiated by a radio user will only be heard by system users who have the same Talkgroup selected. As with other types of calls, Talkgroup Calls can take place from anywhere in the system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 2

VERSION #1.06

2. TEST

- Step 1. Initiate a wide area call with RADIO-1 in TALKGROUP 1.
- Step 2. Observe that only RADIO-2 will be able to monitor and respond to the call.
- Step 3. Initiate a wide area call with RADIO-3 in TALKGROUP 2.
- Step 4. Observe that only RADIO-4 will be able to monitor and respond to the call.

Pass _____ Fail _____

Wide-Area Trunking Features

Secure Operation

1. DESCRIPTION

Digital encryption is used to scramble a transmission so only properly equipped radios can monitor the conversation. A "Key" is used to encrypt the transmit audio. Only radios with the same "Key" can decrypt the audio and listen to it.

SETUP

RADIO-1 - TALKGROUP 1 (Secure TX Mode)
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1 (Secure TX Mode)
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1 (Secure TX Mode & No Key)
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 1 (Clear TX Mode)
RADIO-4 - SITE - SITE 2

VERSION #1.06

2. TEST

- Step 1. Initiate a secure wide area call with RADIO-1 on TALKGROUP 1. Keep this call in progress until instructed to end the call.
- Step 2. Observe that RADIO-2 will be able to monitor and respond to the call.
- Step 3. Observe that RADIO-3 does not receive the call.
- Step 4. Observe that RADIO-4 will also receive the call even with the secure switch set to the non-secure mode of operation.
- Step 5. End the call from RADIO-1.
- Step 6. For radios equipped with dual algorithm encryption modules, select a talkgroup using the second algorithm and repeat Steps 1-5.

Pass____ **Fail**____

Wide-Area Trunking Features

Multigroup Call in Wait Mode

1. DESCRIPTION

This trunking feature allows an equipped radio user to transmit an announcement to several different talkgroups simultaneously. The multigroup (MG) call can be flagged for Wait Mode in the User Configuration Manager (UCM) database forcing all attached talkgroups to finish calls in progress before the trunked system will process the multigroup call. The system does not permit inactive, attached talkgroups to initiate Talkgroup Calls during the "wait" timeframe. As with other types of calls, multigroup calls can take place from anywhere in the system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 - RANDOM
RADIO-3 - SITE - SITE 2
RADIO-4 - ATG 1
RADIO-4 - SITE - SITE 2

* TALKGROUP 1, TALKGROUP 2 are members of ATG 1.

* RANDOM is any talkgroup not a member of ATG 1.

* Multigroups are set up through both the UCM and the Subscriber Programming software.

VERSION #1.03

2. TEST

- Step 1. Verify ATG 1 is set for the Wait mode in the UCM database.
- Step 2. Using RADIO-1, initiate a call on TALKGROUP 1.
- Step 3. While RADIO-1 is keyed, attempt to initiate a multigroup call using RADIO-4 on ATG 1. Verify RADIO-4 receives a busy tone because one of the talkgroups attached to ATG 1 is involved in a Talkgroup Call.
- Step 4. Dekey RADIO-1 and verify RADIO-4 receives a callback.
- Step 5. Key RADIO-4 and verify both RADIO-1 and RADIO-2 hear the multigroup call while RADIO-3 does not unmute.

Pass ____ Fail ____

Wide-Area Trunking Features

Multigroup Call in Interrupt Mode

1. DESCRIPTION

This trunking feature allows an equipped radio user to transmit an announcement to several different talkgroups simultaneously. The multigroup (MG) call can be flagged for Interrupt Mode in the User Configuration Manager (UCM) database, this means that the trunked system does not wait for attached talkgroups to finish calls in progress. Upon dekeying, the interrupted radios will join the multigroup call in progress. As with other types of calls, multigroup calls can take place from anywhere in the system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 - RANDOM
RADIO-3 - SITE - SITE 2
RADIO-4 - ATG 1
RADIO-4 - SITE - SITE 2

* TALKGROUP 1, TALKGROUP 2 are members of ATG 1.

* RANDOM is any talkgroup not a member of ATG 1.

* Multigroups are set up through both the UCM and the Subscriber Programming software.

VERSION #1.05

2. TEST

- Step 1. Verify ATG 1 is set for the Interrupt mode in the UCM database.
- Step 2. Using RADIO-1, initiate a call on TALKGROUP 1.
- Step 3. While RADIO-1 is keyed, initiate a multigroup call using RADIO-4 on ATG 1. Verify RADIO-2 receives the call but RADIO-3 does not unmute.
- Step 4. Dekey RADIO-1 and verify RADIO-1 unmutes and joins the multigroup call in progress.

Pass _____ Fail _____

Wide-Area Trunking Features

Private Call

1. DESCRIPTION

Private Call is a selective calling feature that allows a dispatcher or radio user to carry on one-to-one conversation that is only heard by the 2 parties involved. Subscriber units receiving a private call will sound an alert tone. As with other types of calls, Private Calls can take place from anywhere in the system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 3

VERSION #1.07

2. TEST

- Step 1. Using RADIO-1, press the Private Call button.
- Step 2. Enter the unit ID of RADIO-2 with the keypad, or scroll to the location where this ID is stored.
- Step 3. Press the PTT to initiate the call.
- Step 4. Verify that RADIO-2 hears tones and the display indicates that a call has been received, but RADIO-3 receives no indications.
- Step 5. Answer the call at RADIO-2 by pressing the Private Call button. Verify its display shows the ID number of RADIO-1.
- Step 6. Press the PTT switch on RADIO-2 and respond to the call. Note that if you do not press the Private Call button before pressing PTT, your audio will be heard by all members of the talkgroup, and not by the radio initiating the Private Call.
- Step 7. Verify that RADIO-2 can communicate with RADIO-1.
- Step 8. Verify that RADIO-3 does not monitor the Private Call.
- Step 9. End the Private Call and return to normal talkgroup operation.

Pass _____ Fail _____

Wide-Area Trunking Features

Call Alert

1. DESCRIPTION

Call Alert is a tone page that allows a user to selectively alert another radio unit. The initiating radio will receive notification from the trunked system as to whether or not the page was received by the target radio. Units receiving a Call Alert will sound an alert tone. As with other types of calls, Call Alerts can take place from anywhere in the system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 3

VERSION #1.04

2. TEST

- Step 1. Using RADIO-1, press the page button.
- Step 2. Enter the unit ID of RADIO-2 with the keypad, or scroll to the location where this ID is stored
- Step 3. Press the PTT to initiate the call alert. Verify that the RADIO-1 user receives audible indication that the Call Alert was sent.
- Step 4. Verify that RADIO-2 user receives an audible indication of an incoming Call Alert was sent but RADIO-3 does not.
- Step 5. Verify RADIO-1 gets an audible indication that the Call Alert was successfully received at the target radio.
- Step 6. Turn off RADIO-2. Send a Call Alert from RADIO-1 to RADIO-2.
- Step 7. Verify that the RADIO-1 user receives audible indication that the Call Alert was sent.
- Step 8. Verify RADIO-1 receives an indication that the Call Alert was not successfully received at the target radio.

Pass ____ Fail ____

Wide-Area Trunking Features

Emergency Alarm and Call with Top of Queue

1. DESCRIPTION

Users in life threatening situations can use the Emergency button on the radio to immediately send a signal to the dispatcher and be assigned the next available voice channel. An Emergency Call can be set to either Top of Queue or Ruthless Preemption operation. To accomplish this, an Emergency Alarm and Call will be initiated from a portable which will be received by a portable affiliated at any site of any zone in the system.

NOTE : If the subscriber does not have the PTT Display option, the Emergency ID will not be displayed.

NOTE: All radios and talkgroups should start with default priorities. Default is 10.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 3
RADIO-4 - SITE - SITE 1

VERSION #1.13

2. TEST

- Step 1. The emergency type for TALKGROUP 1's template must be set up through the User Configuration Manager (UCM) as Top of Queue.
- Step 2. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 3. Press the PTT to initiate a call with RADIO-3 and hold the PTT switch until instructed to release.
- Step 4. Key RADIO-4 and verify the radio receives a busy tone. Release the PTT switch on RADIO-4.
- Step 5. Using RADIO-1 send an Emergency Call by depressing the emergency switch. .
- Step 6. Press the PTT switch. Observe that RADIO-1 cannot transmit due to the voice channel being busy. An Emergency Alarm is displayed at a console position monitoring TALKGROUP 1.
- Step 7. Release the PTT switch on RADIO-3.
- Step 8. Observe that RADIO-1 receives the call back before RADIO-4 and is able to proceed with the call.
- Step 9. ****For radios with displays only**** Observe that the display on RADIO-2 denotes an emergency and the unit ID of RADIO-1.
- Step 10. Dekey RADIO-1 and end the Emergency Call by holding down the Emergency button on RADIO-1 until an alert tone sounds. Verify RADIO-1 returns to normal operation and that RADIO-4 receives a callback.

Pass _____ Fail _____

Wide-Area Trunking Features

Emergency Alarm and Call with Ruthless Preemption

1. DESCRIPTION

Users in life threatening situations can use the Emergency button on the radio to immediately send a signal to the dispatcher and be assigned the next available voice channel. An Emergency Call can be set to either Top of Queue or Ruthless Preemption operation. To accomplish this, an Emergency Alarm and Call will be initiated from a portable which will be received by a portable affiliated at any site of any zone in the system.

NOTE : If the subscriber does not have the PTT Display option, the Emergency ID will not be displayed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 2

VERSION #1.09

2. TEST

- Step 1. The emergency type for TALKGROUP 1's template must be set up through the User Configuration Manager (UCM) as Ruthless Preemption.
- Step 2. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 3. Press the PTT to initiate a call with RADIO-4 and hold the PTT switch until instructed to release. Verify RADIO-3 receives the call.
- Step 4. Key RADIO-1 and verify the radio receives a busy tone. Release the PTT switch on RADIO-1.
- Step 5. Using RADIO-1 send an Emergency Call by depressing the emergency switch.
- Step 6. Press the PTT switch. Observe that RADIO-1 is granted the channel immediately and the Talkgroup Call is dropped for RADIO-3. An Emergency Alarm is displayed at a console position monitoring TALKGROUP 1. Dekey RADIO-4.
- Step 7. Key RADIO-3 and verify the radio receives a busy tone. Release the PTT switch on RADIO-3.
- Step 8. End the Emergency Call by holding down the Emergency button on RADIO-1 until an alert tone sounds. Verify RADIO-1 returns to normal operation and that RADIO-3 receives a callback after the emergency hang time expires.
- Step 9. Return the emergency type for TALKGROUP 1's back to Top of Queue.

Pass _____ Fail _____

Wide-Area Trunking Features

Emergency Alarm and Call with Talkgroup Revert

1. DESCRIPTION

Users in life threatening situations can use the Emergency button on the radio to immediately send a signal to the dispatcher and be assigned the next available voice channel. An Emergency Call can be set to either Top of Queue or Ruthless Preemption operation. This test verifies the Emergency ID will appear on the display of the subscribers. To accomplish this, an Emergency Alarm and Call will be initiated from a portable which will be received by a portable affiliated at any site of any zone in the system.

A portable has the ability to revert to a specific talkgroup when an emergency is initiated. This is useful when the users have a designated talkgroup for handling emergencies.

The revert talkgroup must be set in the portable via software.

NOTE : If the subscriber does not have the PTT Display option, the Emergency ID will not be displayed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - EMERGENCY TG
RADIO-3 - SITE - SITE 3 (SITE 2 if only 2 Sites)

* EMERGENCY TG is the talkgroup programmed for emergency reverts.

VERSION #1.05

2. TEST

- Step 1. Make a Talkgroup Call from RADIO-1 and verify only RADIO-2 can hear the audio.
- Step 2. Dekey RADIO-1.
- Step 3. Using RADIO-1 send an Emergency Call by depressing the emergency switch and then the PTT switch.
- Step 4. ****For radios with displays only**** Observe the display on RADIO-3 denotes an emergency and the unit ID of the unit sending the emergency and that RADIO-3 can hear RADIO-1's audio. An Emergency Alarm is displayed at a console position monitoring Emergency TG.
- Step 5. In addition observe that RADIO-2 can not hear RADIO-1's audio.
- Step 6. Release the PTT switch on RADIO-1 and cancel the emergency.

Pass _____ Fail _____

Wide-Area Trunking Features

Emergency Alarm and Call with Hot Mic

1. DESCRIPTION

Users in life threatening situations can use the Emergency button on the radio to immediately send a signal to the dispatcher and be assigned the next available voice channel. An Emergency Call can be set to either Top of Queue or Ruthless Preemption operation. This test verifies the Emergency ID will appear on the display of the subscribers. To accomplish this, an Emergency Alarm and Call will be initiated from a portable which will be received by a portable affiliated at any site of any zone in the system.

If the Hot Mic option is chosen, the subscriber will send an emergency and after a voice channel is assigned, the subscriber will automatically transmit for a programmable period of time.

Emergency Alarm with Voice to Follow (Hot Mic) is an option in the portable and must be enabled via software.

This test case works for all portable radios. For mobile radios, specific mobile microphone models are required.

NOTE : If the subscriber does not have the PTT Display option, the Emergency ID will not be displayed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 3

VERSION #1.06

2. TEST

- Step 1. Using RADIO-1 send an Emergency Alarm by depressing the emergency switch.
- Step 2. ****For radios with displays only**** Observe the display on RADIO-2 and RADIO-3 denotes an emergency and the unit ID of RADIO-1. An Emergency Alarm is displayed at a console position monitoring TALKGROUP 1.
- Step 3. Observe that RADIO-2 and RADIO-3 can hear any audio from RADIO-1 even though RADIO-1 does not have its PTT switch depressed.
- Step 4. Observe that RADIO-1 PTT times out and the radio dekeys.
- Step 5. Cancel the emergency.

Pass _____ Fail _____

Wide-Area Trunking Features

Busy Queuing and Callback with Ten Talkgroup Priority Levels

1. DESCRIPTION

If no voice channel resources are available, radios requesting channels for new conversations are placed in a queue. Users of the same priority will move through the queue in a FIFO (first in, first out) sequence; however, users of higher priority will be inserted ahead of lower priority users in queue. When a voice channel becomes available, the radio at the top of the busy queue gets a channel assignment and generates a callback tone. The callback tone alerts the user that a channel assignment was made and transmitting is now possible on the selected talkgroup.

Note that an Emergency Call has the highest priority at level 1. The highest assignable priority is 2 and 10 is the lowest.

NOTE: All radios and talkgroups should start with default priorities. Default is 10.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 3
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 2

VERSION #1.07

2. TEST

- Step 1. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 2. The priority level for TALKGROUP 2's template must be set up through the User Configuration Manager (UCM) as 9.
- Step 3. Initiate a Talkgroup Call with RADIO-1. Keep this call in progress until instructed to end the call.
- Step 4. Key RADIO-3 and observe that the radio receives a busy.
- Step 5. Key RADIO-2 and observe that the radio receives a busy.
- Step 6. End the Talkgroup Call established in Step 3.
- Step 7. Observe RADIO-2 receives the first callback and can now make a call to RADIO-4 upon receipt of the callback indication.
- Step 8. End the call between RADIO-2 and RADIO-4.
- Step 9. Observe RADIO-3 now receives a callback and can make a call upon receipt of the callback indication.
- Step 10. Repeat steps 1 through 9 with a different voice channel.

Pass _____ Fail _____

Wide-Area Trunking Features

Recent User Priority

1. DESCRIPTION

This test verifies that a recent user of the channel has priority over other users of equal priority of being assigned a channel when a busy queue exists. The maximum number of consecutive times that a user may be elevated to recent user priority is two.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 3
RADIO-3 - SITE - SITE 1

VERSION #1.2

2. TEST

- Step 1. Ensure that the priority level for all talkgroups is the same. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 2. De-press and hold the PTT switch of RADIO-1.
- Step 3. De-press and hold the PTT switch on RADIO-2 and then depress and hold the PTT switch on RADIO-3. Verify that both radios receive a busy tone.
- Step 4. Release the PTT switches on RADIO-2 and RADIO-3.
- Step 5. Release the PTT switch on RADIO-1.
- Step 6. De-press and hold the PTT switch on RADIO-2 after it receives a callback tone.
- Step 7. Within 2 seconds of callback, re-key RADIO-1. Verify that RADIO-1 receives a busy tone. Release the PTT switch on RADIO-1.
- Step 8. Release the PTT switch on RADIO-2. Verify that RADIO-1 receives a callback tone before RADIO-3.
- Step 9. Repeat Steps 2-8. Verify that the priority of RADIO-1 is once more elevated in the busy queue.
- Step 10. Repeat Steps 2-8 once more. Verify that in Step 9 that RADIO-3 receives the callback tone since RADIO-1 cannot be elevated in the busy queue more than two consecutive times.

Pass _____ Fail _____

Wide-Area Trunking Features

Continuous Assignment Updating

1. DESCRIPTION

When a talkgroup is assigned a voice channel, the site controller continues to transmit the channel assignment on the control channel for the duration of the Talkgroup Call. Radios coming into use on the system are automatically sent to voice channels with conversations in progress involving their selected talkgroups.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 2

VERSION #1.04

2. TEST

- Step 1. Turn OFF RADIO-1.
- Step 2. Initiate a Talkgroup Call using RADIO-2.
- Step 3. While the Talkgroup Call is in progress, turn ON RADIO-1.
- Step 4. Observe that RADIO-1, which was just brought back into service, joins the Talkgroup Call already in progress.
- Step 5. Release the PTT of RADIO-2.
- Step 6. Switch RADIO-1 to TALKGROUP 2.
- Step 7. Initiate a Talkgroup Call using RADIO-2.
- Step 8. While the Talkgroup Call is in progress, turn RADIO-1 back to TALKGROUP 1.
- Step 9. Observe that RADIO-1, which was just set back to TALKGROUP 1, joins the Talkgroup Call already in progress.

Pass____ Fail____

Wide-Area Trunking Features

Site Access Control/"Individual Only" Site Access Denial

1. DESCRIPTION

The User Configuration Manager (UCM) can be used to limit radio or talkgroup access to selected valid sites. Control can be exercised to restrict radio users or talkgroups to certain sites, or to steer radio activity away from smaller sites in an effort to avoid busies. UCM flags establish which sites are valid for each individual radio user, talkgroup and multigroup. An overall Site Access Denial flag for the system governs how these radio and talkgroup settings affect the affiliation or rejection of radios to individual sites. Four possible values for the Site Access Denial flag exist: Individual Only, Talkgroup Only, Either, or Both.

"Individual Only" Site Access Denial dictates that a radio will not be allowed to affiliate to a particular site if the radio user does not have access to that site. If the Site Access Denial flag is set to "Individual Only", the talkgroup record for valid sites is not used in the determination of actual site affiliation permissions.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

VERSION #1.04

2. TEST

- Step 1. Set the Site Access Denial Flag to Individual Only via the User Configuration Manager (UCM).
- Step 2. Initiate a call from RADIO-2 on TALKGROUP 1. Verify that RADIO-2 is allowed to make the call.
- Step 3. Force RADIO-2 to scan to SITE 1, and then set SITE 2 to be a non-valid site for TALKGROUP 1 through the UCM.
- Step 4. Force RADIO-2 to scan back to SITE 2. Verify that RADIO-2 is allowed to affiliate to SITE 2 since the individual Radio user record determines site access.
- Step 5. Initiate a call from RADIO-2 on TALKGROUP 1. Verify that RADIO-2 is not allowed to make the call from SITE 2 since TALKGROUP 1 is no longer valid at SITE 2.
- Step 6. Change RADIO-2 to TALKGROUP 2 and attempt to make a call at SITE 2. Verify that the Talkgroup Call occurs because TALKGROUP 2 is valid at SITE 2.
- Step 7. Initiate a Private Call from RADIO-2 to RADIO-1. Verify that the Private Call occurs since RADIO-2 is valid at SITE 2.
- Step 8. Force RADIO-2 to scan to SITE 1.
- Step 9. Set SITE 2 to be a non-valid site for RADIO-2 through the UCM.
- Step 10. Force RADIO-2 to scan to SITE 2. Verify that RADIO-2 can no longer affiliate to SITE 2 and that RADIO-2 will scan to other valid sites.

Pass _____ Fail _____

Wide-Area Trunking Features

Site Access Control/"Talkgroup Only" Site Access Denial

1. DESCRIPTION

The User Configuration Manager (UCM) can be used to limit radio or talkgroup access to selected valid sites. Control can be exercised to restrict radio users or talkgroups to certain sites, or to steer radio activity away from smaller sites in an effort to avoid busies. UCM flags establish which sites are valid for each individual radio user, talkgroup and multigroup. An overall Site Access Denial flag for the system governs how these radio and talkgroup settings affect the affiliation or rejection of radios to individual sites. Four possible values for the Site Access Denial flag exist: Individual Only, Talkgroup Only, Either, or Both.

"Talkgroup (TG) Only" Site Access Denial dictates that a radio will not be allowed to affiliate to a particular site if its affiliated talkgroup does not have access to that site. In this case, the individual radio user setting for valid sites is not used in the determination of actual site affiliation permissions.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1.04

2. TEST

- Step 1. Set the Site Access Denial Flag to Talkgroup Only via the User Configuration Manager (UCM).
- Step 2. Set SITE 2 to be a valid site for RADIO-2 through the UCM. Set SITE 2 to be a non-valid site for TALKGROUP 1 through the UCM.
- Step 3. Force RADIO-2 to scan to SITE 2. Verify that RADIO-2 cannot affiliate to SITE 2 since TALKGROUP 1 is a non-valid talkgroup for SITE 2.
- Step 4. Set SITE 2 to be a valid site for TALKGROUP 1 through the UCM. Set SITE 2 to be a non-valid site for RADIO-2 through the UCM.
- Step 5. Force RADIO-2 to scan to SITE 2. Verify that RADIO-2 is now allowed to affiliate to SITE 2 since the talkgroup record determines site access.
- Step 6. Initiate a call from RADIO-2. Verify that RADIO-2 is allowed to make the call from SITE 2 since TALKGROUP 1 is valid at SITE 2.

Pass ____ Fail ____

Wide-Area Trunking Features

Site Access Control/"Either" Site Access Denial

1. DESCRIPTION

The User Configuration Manager (UCM) can be used to limit radio or talkgroup access to selected valid sites. Control can be exercised to restrict radio users or talkgroups to certain sites, or to steer radio activity away from smaller sites in an effort to avoid busies. UCM flags establish which sites are valid for each individual radio user, talkgroup and multigroup. An overall Site Access Denial flag for the system governs how these radio and talkgroup settings affect the affiliation or rejection of radios to individual sites. Four possible values for the Site Access Denial flag exist: Individual Only, Talkgroup Only, Either, or Both.

"Either" Site Access Denial indicates that a radio will not be allowed to affiliate to a site if either the radio user or affiliated talkgroup does not have access to that site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1.04

2. TEST

- Step 1. Set the Site Access Denial Flag to Either via the User Configuration Manager (UCM).
- Step 2. Set SITE 2 to be a non-valid site for RADIO-2 through the UCM. Set SITE 2 to be a valid site for TALKGROUP 1 through the UCM.
- Step 3. Force RADIO-2 to scan to SITE 2. Verify that RADIO-2 cannot affiliate to SITE 2 since SITE 2 is a non-valid site for RADIO-2.
- Step 4. Set SITE 2 to be a non-valid site for TALKGROUP 1 through the UCM. Set SITE 2 to be a valid site for RADIO-2 through the UCM.
- Step 5. Force RADIO-2 to scan to SITE 2. Verify that RADIO-2 is still not permitted to affiliate to SITE 2 since now the selected talkgroup is non-valid at SITE 2.
- Step 6. Set SITE 2 to be a valid site for TALKGROUP 1 through the UCM. Force RADIO-2 to scan to SITE 2. Verify that RADIO-2 can now affiliate to SITE 2.
- Step 7. Initiate a call from RADIO-2 on TALKGROUP 1. Verify that RADIO-2 is allowed to make the call from SITE 2 since both TALKGROUP 1 and RADIO-2 are valid at SITE 2.

Pass _____ Fail _____

Wide-Area Trunking Features

Site Access Control/"Both" Site Access Denial

1. DESCRIPTION

The User Configuration Manager (UCM) can be used to limit radio or talkgroup access to selected valid sites. Control can be exercised to restrict radio users or talkgroups to certain sites, or to steer radio activity away from smaller sites in an effort to avoid busies. UCM flags establish which sites are valid for each individual radio user, talkgroup and multigroup. An overall Site Access Denial flag for the system governs how these radio and talkgroup settings affect the affiliation or rejection of radios to individual sites. Four possible values for the Site Access Denial flag exist: Individual Only, Talkgroup Only, Either, or Both.

"Both" Site Access Denial indicates that a radio will not be allowed to affiliate to a site only if both the radio user and affiliated talkgroup do not have access to the site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

VERSION #1.05

2. TEST

- Step 1. Set the Site Access Denial Flag to Both via the User Configuration Manager (UCM).
- Step 2. Set SITE 2 to be a valid site for RADIO-2 through the UCM. Set SITE 2 to be a non-valid site for TALKGROUP 1 through the UCM.
- Step 3. Force RADIO-2 to scan to SITE 2. Verify that RADIO-2 can affiliate to SITE 2 since both TALKGROUP 1 and RADIO-2 records are not set as "non-valid" for SITE 2.
- Step 4. Initiate a call from RADIO-2 on TALKGROUP 1. Verify that RADIO-2 is allowed to make the call from SITE 2 since only TALKGROUP 1 is non-valid at SITE 2.
- Step 5. Force RADIO-2 to scan to SITE 1.
- Step 6. Set SITE 2 to be a non-valid site for RADIO-2 through the UCM.
- Step 7. Force RADIO-2 to scan to SITE 2. Verify that RADIO-2 cannot affiliate to SITE 2 since both TALKGROUP 1 and RADIO-2 records are set as "non-valid" for SITE 2.
- Step 8. Reset all Talkgroup and Radio User flags in the UCM.

Pass ____ Fail ____

Wide-Area Trunking Features

All Start Talkgroups

1. DESCRIPTION

Talkgroups can be set up as either All Start or Fast Start.

"AllStart" is the default Talkgroup Call setup approach that requires that all sites with affiliated talkgroup members and other required resources be available before the call begins. Otherwise, the system returns a busy response to the subscriber who initiated the Talkgroup Call. Once the required resources become available, the call is granted.

NOTE: This feature only works on a multi-site system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 2
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 1

VERSION #1.07

2. TEST

- Step 1. Verify TALKGROUP 1's template is setup as an All Start Talkgroup in the User Configuration Manager (UCM).
- Step 2. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 3. Key RADIO-3 and busy out the only voice channel available at SITE 1.
- Step 4. Initiate a Talkgroup Call from RADIO-1 and observe a busy indication is received due to no available voice channel at SITE 1 where RADIO-2 is affiliated.
- Step 5. Dekey RADIO-3. Verify that the call from RADIO-1 is now granted and RADIO-2 can hear the audio.

Pass____ Fail____

Wide-Area Trunking Features

Fast Start Talkgroup without Critical Site

1. DESCRIPTION

Talkgroups can be set up as either All Start or Fast Start.

"FastStart" is the Talkgroup Call setup approach that allows a group call setup whether or not all affiliated Talkgroup members are available. This "Automatic Busy Override by Talkgroup" call setup method still requires the participation of all affiliated consoles, LOMIs (i.e. logging recorders) before the call can begin. As channels at the affiliated talkgroup members' sites become available, they are added to the call in progress.

NOTE: This feature only works on a multi-site system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 2
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 1

VERSION #1.08

2. TEST

- Step 1. Verify that TALKGROUP 1's template is set up as Fast Start through the User Configuration Manager (UCM) with no critical sites specified.
- Step 2. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 3. Key RADIO-3 and busy out the only voice channel available at SITE 1.
- Step 4. Initiate a Talkgroup Call from RADIO-1 and observe the call is granted even with no voice channel available at SITE 2 for RADIO-2.
- Step 5. Dekey RADIO-3. Verify that RADIO-2 can now hear RADIO-1.

Pass ____ Fail ____

Wide-Area Trunking Features

Fast Start Talkgroup with Critical Site

1. DESCRIPTION

Talkgroups can be set up as either All Start or Fast Start.

"FastStart" is the Talkgroup Call setup approach that allows a group call setup whether or not all affiliated Talkgroup members are available. This "Automatic Busy Override by Talkgroup" call setup method still requires the participation of all affiliated consoles, LOMIs (i.e. logging recorders) and critical sites before the call can begin. As channels at the affiliated talkgroup members' sites become available, they are added to the call in progress.

NOTE: This feature only works on a multi-site system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 2
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 1

VERSION #1.07

2. TEST

- Step 1. Verify that TALKGROUP 1's template is set up as Fast Start through the User Configuration Manager (UCM) and specify SITE 1 as a Critical Site.
- Step 2. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 3. Key RADIO-3 and busy out the only voice channel available at SITE 1.
- Step 4. Initiate a Talkgroup Call from RADIO-1 and observe the call is busied as no voice channel is available at SITE 1 for RADIO-2.
- Step 5. Dekey RADIO-3. Verify that the call from RADIO-1 is now granted and RADIO-2 can hear the audio.

Pass____ Fail____

Wide-Area Trunking Features

Subscriber To Landline Telephone Interconnect

1. DESCRIPTION

This test verifies the capability to make or receive phone calls on a radio. Two types of interconnect calls can be initiated: subscriber-to-landline and landline-to-subscriber.

The subscriber-to-landline call feature enables a radio user to dial a land telephone user directly.

Some radios feature phone list capability with programmable alias names which may be assigned. Radios with keypad operation may also be programmed for unlimited dialing capability.

Since the telephone interconnect functionality depends upon the telephone interconnect Private Branch Exchange (PBX) unit, sites must be Wide Area Trunking in order to support this telephone interconnect function. In addition, radios cannot be site-locked to a specific site before initiating a telephone interconnect call.

Note : No specific site affiliation is required to begin this test, although the radios can not be "Site Locked."

Note : A radio can be set up to use either the Private Branch Exchange (PBX) in the zone it is affiliated with or a PBX in a default zone.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1.03

2. TEST

- Step 1. Using RADIO-1, initiate a telephone call to a test telephone phone number.
- Step 2. Verify the telephone rings.
- Step 3. Pickup the phone and verify that RADIO-1 and the landline user can communicate.
- Step 4. Verify that the landline user hears a tone after each radio transmission signifying the half-duplex nature of the interconnect call.
- Step 5. Verify that RADIO-2 is not involved in the call.
- Step 6. Hang up the interconnect call.

Pass _____ Fail _____

Wide-Area Trunking Features

Subscriber To Landline Telephone Interconnect - Overdial Mode

1. DESCRIPTION

This test verifies the capability to make or receive phone calls on a radio. Two types of interconnect calls can be initiated: subscriber-to-landline and landline-to-subscriber.

The subscriber-to-landline call feature enables a radio user to dial a land telephone user directly. If calling a automated voice system or a paging system, the user can enter more dial keys.

Some radios feature phone list capability with programmable alias names which may be assigned. Radios with keypad operation may also be programmed for unlimited dialing capability.

Since the telephone interconnect functionality depends upon the telephone interconnect PBX unit, sites must be Wide Area Trunking in order to support this telephone interconnect function. In addition, radios cannot be site-locked to a specific site before initiating a telephone interconnect call.

Note : No specific site affiliation is required to begin this test, although the radios can not be "Site Locked."

Note : A radio can be setup to use either the Private Branch Exchange (PBX) in the zone it is affiliated with or a PBX in a default zone.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1.03

2. TEST

- Step 1. Using RADIO-1, initiate a telephone call to the RAM Page phone number.
- Step 2. Verify the telephone rings.
- Step 3. Enter the pager number of the party to be paged when asked.
- Step 4. Enter a telephone number when asked.
- Step 5. Hang up the interconnect call on RADIO-1.
- Step 6. Verify the line is dropped.
- Step 7. Verify the page goes through.

Pass ____ Fail ____

Wide-Area Trunking Features

Landline to Subscriber Telephone Interconnect

1. DESCRIPTION

This test verifies the capability to make or receive phone calls on a radio. Two types of interconnect calls can be initiated: subscriber-to-landline and landline-to-subscriber.

The landline-to-subscriber call feature enables a land telephone user to dial a radio user directly.

Some radios feature phone list capability with programmable alias names which may be assigned. Radios with keypad operation may also be programmed for unlimited dialing capability.

Since the telephone interconnect functionality depends upon the telephone interconnect PBX unit, sites must be Wide Area Trunking in order to support this telephone interconnect function. In addition, radios cannot be site-locked to a specific site before initiating a telephone interconnect call.

Note : No specific site affiliation is required to begin this test, although the radios can not be "Site Locked."

Note : A radio can be setup to use either the Private Branch Exchange (PBX) in the zone it is affiliated with or a PBX in a default zone.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1.04

2. TEST

- Step 1. From the test telephone line, dial the telephone number of a phone line connected to the PBX.
- Step 2. Verify that a tone is heard in the telephone prompting the landline caller to enter the eight-digit unit ID of the target radio.
- Step 3. Enter the eight-digit radio ID of RADIO-1.
- Step 4. Verify that ringing is heard on RADIO-1 only and that the display indicates a phone call is being received.
- Step 5. Press the Telephone Interconnect button on RADIO-1 to answer the landline-to-subscriber interconnect call.
- Step 6. Verify that the landline-to-subscriber call can be completed, and the radio and landline users can communicate.
- Step 7. Verify that RADIO-2 does not listen to the call.
- Step 8. Hang up the interconnect call.
- Step 9. Perform a test to indicate a busy on the mobile being contacted.

Pass ____ Fail ____

Wide-Area Trunking Features

Audio Interrupt/Interrupt Never Mode

1. DESCRIPTION

A radio PTT request may be received for a group already active and currently being sourced by another radio unit. The talkgroup can be flagged in the User Configuration Manager (UCM) to either allow or disallow the new PTT. If allowed, the latest PTT request will be granted and become the source of the call. If both Radios are at the same site, RF contention may prevent either call from working.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 3 (SITE 2 if only 2 Sites)

VERSION #1.04

2. TEST

- Step 1. Set up TALKGROUP 1's template to be Audio Interrupt Never through the UCM.
- Step 2. Using RADIO-1, initiate a call on TALKGROUP 1.
- Step 3. Verify both RADIO-2 and RADIO-3 monitor the audio.
- Step 4. Using RADIO-3, initiate a call on TALKGROUP 1.
- Step 5. Verify that RADIO-3 receives a reject and that RADIO-2 continues to listen to RADIO-1.
- Step 6. Dekey both Radios.

Pass _____ Fail _____

Wide-Area Trunking Features

Audio Interrupt/Interrupt Always Mode

1. DESCRIPTION

A radio PTT request may be received for a group already active and currently being sourced by another radio unit. The talkgroup can be flagged in the User Configuration Manager (UCM) to either allow or disallow the new PTT. If allowed, the latest PTT request will be granted and become the source of the call. If both Radios are at the same site, RF contention may prevent either call from working.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 3 (SITE 2 if only 2 Sites)

VERSION #1.04

2. TEST

- Step 1. Set up TALKGROUP 1's template to be Audio Interrupt Always through the UCM.
- Step 2. Using RADIO-1, initiate a call on TALKGROUP 1.
- Step 3. Verify both RADIO-2 and 3 monitor the audio.
- Step 4. Using RADIO-3, initiate a call on TALKGROUP 1.
- Step 5. Verify that RADIO-2 now listens to RADIO-3.
- Step 6. Dekey both Radios.

Pass _____ Fail _____

Wide-Area Trunking Features

Sub-band Restricted Operation

1. DESCRIPTION

This feature will allow radios limited to one sub-band to operate at sites set up with resources to handle both sub-band and full band range radios.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 2

* SITE 1 and SITE 2 should support sub-band channels.

VERSION #1.04

2. TEST

- Step 1. Verify that TALKGROUP 1 is set up in the User Configuration Manager (UCM) to be a sub-band restricted talkgroup.
- Step 2. Verify TALKGROUP 2 is set up in the UCM to be a non-sub-band restricted talkgroup.
- Step 3. Using RADIO-1, initiate a call on TALKGROUP 1.
- Step 4. Verify that a sub-band restricted channel is granted at both sites and that only RADIO-3 is able to monitor and respond to the call.
- Step 5. Dekey RADIO-1.
- Step 6. Using RADIO-2, initiate a call on TALKGROUP 2.
- Step 7. Verify that a non-sub-band restricted channel is granted at both sites and that only RADIO-4 is able to monitor and respond to the call.

Pass____ Fail____

Wide-Area Trunking Features

Priority Monitor/Non-Priority Scan

1. DESCRIPTION

This test verifies that a subscriber unit can scan a pre-programmed list (in the radio) to find any Priority and Non-priority Talkgroups with assigned voice channels at that site. To accomplish this, a call will be initiated from a portable at a remote site on a talkgroup monitored by a portable at the same site as the scanning radio. The scanning radio will scan from its selected talkgroup to the active talkgroup. The test will be repeated with an additional radio transmitting on the Priority Talkgroup while the scanning radio is scanning. This third radio will be on a remote site with a fourth radio on the Priority Talkgroup at the same site as the scanning radio.

SETUP

RADIO-1 - SCANNING
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 3
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 3
RADIO-4 - SITE - SITE 2

* RADIO-1 needs to be set to a dial position configured to scan.

VERSION #1.04

2. TEST

- Step 1. Verify that RADIO-1 is set to the scan mode of operation and programmed to scan all TALKGROUP 1, TALKGROUP 2, and TALKGROUP 3.
- Step 2. Initiate a Talkgroup Call with RADIO-4 and observe that RADIO-1 scans to the talkgroup and receives the call. Keep the call in progress until completion of the following step.
- Step 3. Initiate a Talkgroup Call with RADIO-2 and observe that RADIO-1 does not receive the call since RADIO-1 is listening to TALKGROUP 3.

Pass____ Fail____

Wide-Area Trunking Features

Priority Monitor/Priority Scan

1. DESCRIPTION

This test verifies that a subscriber unit can scan a pre-programmed list (in the radio) to find any Priority and Non-priority Talkgroups with assigned voice channels at that site. To accomplish this, a call will be initiated from a portable at a remote site on a talkgroup monitored by a portable at the same site as the scanning radio. The scanning radio will scan from its selected talkgroup to the active talkgroup. The test will be repeated with an additional radio transmitting on the Priority Talkgroup while the scanning radio is scanning. This third radio will be on a remote site with a fourth radio on the Priority Talkgroup at the same site as the scanning radio.

SETUP

RADIO-1 - SCANNING
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 2
RADIO-5 - TALKGROUP 2
RADIO-5 - SITE - SITE 1

* RADIO-1 needs to be set to a dial position configured to scan.

VERSION #1.05

2. TEST

- Step 1. Verify that RADIO-1 is set to the scan mode of operation and programmed to scan TALKGROUP 1 and TALKGROUP 2 with TALKGROUP 1 as its Priority Monitor Talkgroup.
- Step 2. Verify that in the User Configuration Manager (UCM) under Talkgroup Configuration, Priority Monitor and the Valid Site setting is set to yes for SITE 2.
- Step 3. Initiate a Talkgroup Call with RADIO-4 and observe that RADIO-1 scans to the talkgroup and receives the call. Keep the call in progress until the completion of the following step.
- Step 4. Initiate a Talkgroup Call with RADIO-3 and observe that RADIO-1 reverts to the TALKGROUP 1 and receives the call.

Pass _____ Fail _____

Wide-Area Trunking Features

Receive Only Radio

1. DESCRIPTION

This test verifies that a subscriber can be set up for receive operation only.

Setting a portable for "dispatch enabled" equal to false in the Radio User record allows the radio to receive, but not initiate group calls.

Setting a portable for "user enabled" equal to false in the Radio User profile allows the user to receive dispatch calls, but not originate or receive Unit-to-Unit or call alerts.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

VERSION #1.05

2. TEST

- Step 1. Set RADIO-1's template for "dispatch enabled" equal to false in the Radio User record. This allows the radio to receive, but not initiate group calls.
- Step 2. Set RADIO-1 for "user enabled" equal to false in the Radio User profile. This allows the user to receive dispatch calls, but not originate or receive Unit-to-Unit or call alerts.
- Step 3. Verify that the Site Access denial flag is set to either "Both" or "TG Only".
- Step 4. Make a call from any Console in the system with the Talkgroup. Verify both Radios can hear the audio.
- Step 5. Make a call from RADIO-2 and verify that both RADIO-1 and the Console hear the call.
- Step 6. Verify that RADIO-1 is not granted a channel when it is keyed up.
- Step 7. Verify that the Console can not make a Private Call to RADIO-1 but can Private Call RADIO-2.
- Step 8. Verify that RADIO-2 can not make a Private Call to RADIO-1 but can Private Call the Console.

Pass____ Fail____

Wide-Area Trunking Features

Site Access Control/"Individual Only" Site Access Denial (Single Site)

1. DESCRIPTION

The User Configuration Manager (UCM) can be used to limit radio or talkgroup access to selected valid sites. Control can be exercised to restrict radio users or talkgroups to certain sites, or to steer radio activity away from smaller sites in an effort to avoid busies. UCM flags establish which sites are valid for each individual radio user, talkgroup and multigroup. An overall Site Access Denial flag for the system governs how these radio and talkgroup settings affect the affiliation or rejection of radios to individual sites. Four possible values for the Site Access Denial flag exist: Individual Only, Talkgroup Only, Either, or Both.

"Individual Only" Site Access Denial dictates that a radio will not be allowed to affiliate to a particular site if the radio user does not have access to that site. If the Site Access Denial flag is set to "Individual Only", the talkgroup record for valid sites is not used in the determination of actual site affiliation permissions.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1

2. TEST

- Step 1. Set the Site Access Denial Flag to Individual Only via the User Configuration Manager (UCM).
- Step 2. Initiate a call from RADIO-2 on TALKGROUP 1. Verify that RADIO-2 is allowed to make the call.
- Step 3. Set SITE 1 to be a non-valid site for TALKGROUP 1 through the UCM.
- Step 4. Verify that RADIO-2 is still affiliated to SITE 1 since the individual Radio user record determines site access.
- Step 5. Initiate a call from RADIO-2 on TALKGROUP 1. Verify that RADIO-2 is not allowed to make the call from SITE 1 since TALKGROUP 1 is no longer valid at SITE 1.
- Step 6. Change RADIO-2 to TALKGROUP 2 and attempt to make a call at SITE 1. Verify that the Talkgroup Call occurs because TALKGROUP 2 is valid at SITE 1.
- Step 7. Initiate a Private Call from RADIO-2 to RADIO-1. Verify that the Private Call occurs since RADIO-2 is valid at SITE 1.
- Step 8. Set SITE 1 to be a valid site for TALKGROUP 1 through the UCM.
- Step 9. Set SITE 1 to be a non-valid site for RADIO-2 through the UCM.
- Step 10. Verify that RADIO-2 can no longer affiliate to SITE 1 and that RADIO-2 will display "Out of Range."

Pass____ Fail____

Wide-Area Trunking Features

Site Access Control/"Talkgroup Only" Site Access Denial (Single Site)

1. DESCRIPTION

The User Configuration Manager (UCM) can be used to limit radio or talkgroup access to selected valid sites. Control can be exercised to restrict radio users or talkgroups to certain sites, or to steer radio activity away from smaller sites in an effort to avoid busies. UCM flags establish which sites are valid for each individual radio user, talkgroup and multigroup. An overall Site Access Denial flag for the system governs how these radio and talkgroup settings affect the affiliation or rejection of radios to individual sites. Four possible values for the Site Access Denial flag exist: Individual Only, Talkgroup Only, Either, or Both.

"Talkgroup (TG) Only" Site Access Denial dictates that a radio will not be allowed to affiliate to a particular site if its affiliated talkgroup does not have access to that site. In this case, the individual radio user setting for valid sites is not used in the determination of actual site affiliation permissions.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1

2. TEST

- Step 1. Set the Site Access Denial Flag to Talkgroup Only via the User Configuration Manager (UCM).
- Step 2. Set SITE 1 to be a valid site for RADIO-2 through the UCM. Set SITE 1 to be a non-valid site for TALKGROUP 1 through the UCM.
- Step 3. Verify that RADIO-2 cannot affiliate to SITE 1 since TALKGROUP 1 is a non-valid talkgroup for SITE 2. RADIO-2 will display "Out of Range."
- Step 4. Set SITE 1 to be a valid site for TALKGROUP 1 through the UCM. Set SITE 1 to be a non-valid site for RADIO-2 through the UCM.
- Step 5. Verify that RADIO-2 is now allowed to affiliate to SITE 1 since the talkgroup record determines site access.
- Step 6. Initiate a call from RADIO-2. Verify that RADIO-2 is allowed to make the call from SITE 1 since TALKGROUP 1 is valid at SITE 1.

Pass____ Fail____

Wide-Area Trunking Features

Site Access Control/"Either" Site Access Denial (Single Site)

1. DESCRIPTION

The User Configuration Manager (UCM) can be used to limit radio or talkgroup access to selected valid sites. Control can be exercised to restrict radio users or talkgroups to certain sites, or to steer radio activity away from smaller sites in an effort to avoid busies. UCM flags establish which sites are valid for each individual radio user, talkgroup and multigroup. An overall Site Access Denial flag for the system governs how these radio and talkgroup settings affect the affiliation or rejection of radios to individual sites. Four possible values for the Site Access Denial flag exist: Individual Only, Talkgroup Only, Either, or Both.

"Either" Site Access Denial indicates that a radio will not be allowed to affiliate to a site if either the radio user or affiliated talkgroup does not have access to that site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1

2. TEST

- Step 1. Set the Site Access Denial Flag to Either via the User Configuration Manager (UCM).
- Step 2. Set SITE 1 to be a non-valid site for RADIO-2 through the UCM. Set SITE 1 to be a valid site for TALKGROUP 1 through the UCM.
- Step 3. Key-up and verify that RADIO-2 cannot affiliate to SITE 1 since SITE 1 is a non-valid site for RADIO-2. RADIO-2 will display "Out of Range."
- Step 4. Set SITE 1 to be a non-valid site for TALKGROUP 1 through the UCM. Set SITE 1 to be a valid site for RADIO-2 through the UCM.
- Step 5. Force RADIO-2 to scan to SITE 1. Verify that RADIO-2 is still not permitted to affiliate to SITE 1 since now the selected talkgroup is non-valid at SITE 1.
- Step 6. Set SITE 1 to be a valid site for TALKGROUP 1 through the UCM. Verify that after some time, RADIO-2 can now affiliate to SITE 1. Note that power may need to be recycled on RADIO-2 before it can again affiliate to SITE 1.
- Step 7. Initiate a call from RADIO-2 on TALKGROUP 1. Verify that RADIO-2 is allowed to make the call from SITE 1 since both TALKGROUP 1 and RADIO-2 are valid at SITE 1.

Pass____ Fail____

Wide-Area Trunking Features

Site Access Control/"Both" Site Access Denial (Single Site)

1. DESCRIPTION

The User Configuration Manager (UCM) can be used to limit radio or talkgroup access to selected valid sites. Control can be exercised to restrict radio users or talkgroups to certain sites, or to steer radio activity away from smaller sites in an effort to avoid busies. UCM flags establish which sites are valid for each individual radio user, talkgroup and multigroup. An overall Site Access Denial flag for the system governs how these radio and talkgroup settings affect the affiliation or rejection of radios to individual sites. Four possible values for the Site Access Denial flag exist: Individual Only, Talkgroup Only, Either, or Both.

"Both" Site Access Denial indicates that a radio will not be allowed to affiliate to a site only if both the radio user and affiliated talkgroup do not have access to the site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1

2. TEST

- Step 1. Set the Site Access Denial Flag to Both via the User Configuration Manager (UCM).
- Step 2. Set SITE 1 to be a valid site for RADIO-2 through the UCM. Set SITE 1 to be a non-valid site for TALKGROUP 1 through the UCM.
- Step 3. Verify that RADIO-2 can affiliate to SITE 1 since both TALKGROUP 1 and RADIO-2 records are not set as "non-valid" for SITE 1.
- Step 4. Initiate a call from RADIO-2 on TALKGROUP 1. Verify that RADIO-2 is allowed to make the call from SITE 1 since only TALKGROUP 1 is non-valid at SITE 1.
- Step 5. Force RADIO-2 to scan to SITE 1.
- Step 6. Set SITE 1 to be a non-valid site for RADIO-2 through the UCM.
- Step 7. Verify that RADIO-2 cannot affiliate to SITE 1 since both TALKGROUP 1 and RADIO-2 records are set as "non-valid" for SITE 1. RADIO-2 will display "Out of Range."
- Step 8. Reset all Talkgroup and Radio User flags in the UCM.

Pass____ Fail____

Site Trunking Features

Site Trunking Features

Site Trunking Talkgroup Call

1. DESCRIPTION

When a Site goes into Site Trunking, radios with Talkgroup Call capability will be able to communicate with other members of the same talkgroup at that same site. Members of the same talkgroup at other sites will not be able to monitor those conversations.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 1
RADIO-4 - SITE - SITE 2

* All Radios should be "Site Locked"

VERSION #1.03

2. TEST

- Step 1. Place SITE 1 into the Site Trunking mode via the Zone Manager.
- Step 2. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1 at SITE 1.
- Step 3. Observe that only RADIO-2 will be able to monitor and respond to the call.
- Step 4. Initiate a Talkgroup Call with RADIO-3 on TALKGROUP 1 at SITE 2.
- Step 5. Observe that only RADIO-4 will be able to monitor and respond to the call.

Pass____ Fail____

Site Trunking Features

Site Trunking Private Call

1. DESCRIPTION

Private Calls is a selective calling feature that allows a dispatcher or radio user to carry on one-to-one conversation that is only heard by the 2 parties involved. When a site is in Site Trunking, Radios at the site will only be able to Private Call other radios at the same site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 1

* All Radios should be "Site Locked"

VERSION #1.04

2. TEST

- Step 1. Place SITE 1 into the Site Trunking mode via the Zone Manager.
- Step 2. Using RADIO-1, press the Private Call button.
- Step 3. Enter the Unit ID of RADIO-2 with the keypad, or scroll to the location where this ID is stored.
- Step 4. Press the PTT to initiate the call.
- Step 5. Verify that at RADIO-2 only tones are heard and the display indicates that a call has been received.
- Step 6. Answer the call at RADIO-2 by pressing the Private Call button. Verify its display shows the ID number of the calling unit.
- Step 7. Press the PTT switch on RADIO-2 and respond to the call. Note that if you do not press the Private Call button before pressing PTT, your audio will be heard by all members of the talkgroup, and not by the radio initiating the Private Call.
- Step 8. Verify only RADIO-1 hears the audio from RADIO-2.
- Step 9. End the Private Call and return to normal talkgroup operation.

Pass _____ Fail _____

Site Trunking Features

Site Trunking Call Alert

1. DESCRIPTION

Call Alert is a tone page that allows a user to selectively alert another radio unit. When a site is in Site Trunking, Radios at the site will only be able to Call Alert other radios at the same site. The initiating radio will receive notification from the trunked system as to whether or not the page was received by the target radio.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1

* All Radios should be "Site Locked"

VERSION #1.05

2. TEST

- Step 1. Place SITE 1 into the Site Trunking mode via the Zone Manager.
- Step 2. Using RADIO-1, press the page button.
- Step 3. Enter the Unit ID of RADIO-2 with the keypad, or scroll to the location where this ID is stored.
- Step 4. Press the PTT to initiate the Call Alert.
- Step 5. Verify that RADIO-2 received the Call Alert.
- Step 6. Exit the Call Alert mode and return to normal talkgroup mode.

Pass ____ Fail ____

Site Trunking Features

Site Trunking Busy Queuing and Callback

1. DESCRIPTION

If no voice channel resources are available, radios requesting channels for new conversations are placed in a queue. Users of the same priority will move through the queue in a FIFO (first in, first out) sequence; however, users of higher priority will be inserted ahead of lower priority users in the queue. When a voice channel becomes available, the radio at the top of the busy queue gets a channel assignment and generates a callback tone. The callback alerts the user that a channel assignment was made and transmitting is now possible on the selected talkgroup.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 3
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 1
RADIO-4 - SITE - SITE 1

* All Radios should be "Site Locked"

VERSION #1.07

2. TEST

- Step 1. Place SITE 1 into the Site Trunking mode via the Zone Manager.
- Step 2. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 3. Initiate a Talkgroup Call with RADIO-1 and observe that it is received by RADIO-4. Keep this call in progress until instructed to end the call.
- Step 4. Key RADIO-2 and observe that the radio receives a busy.
- Step 5. Key RADIO-3 and observe that the radio receives a busy.
- Step 6. End the Talkgroup Call established in Step 3.
- Step 7. Observe that RADIO-2 receives a callback prior to RADIO-3 receiving a callback.
- Step 8. Return all channels for the site to service.

Pass____ Fail____

Site Trunking Features

Site Trunking Emergency Call and Alarm

1. DESCRIPTION

This test verifies that Emergency Alarms and Calls can be initiated by subscribers when the registered site is in Site Trunking. With all portables registered on the Site Trunking site from the previous test, a portable will initiate an Emergency Alarm by pressing the Emergency button. By pressing the PTT, an Emergency Call will be issued and the ID of the initiator will be displayed with an Emergency indication by the other subscribers on the same talkgroup. Note that for site trunking, Emergency Call operation is always Top of Queue.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 3
RADIO-4 - SITE - SITE 1

* All Radios should be "Site Locked"

VERSION #1.06

2. TEST

- Step 1. Place SITE 1 into the Site Trunking mode via the Zone Manager.
- Step 2. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 3. Press the PTT on RADIO-3 and hold the PTT switch until instructed to release.
- Step 4. Key RADIO-4 and observe that the radio receives a busy.
- Step 5. Using RADIO-1, initiate an emergency alarm followed by an emergency call.
- Step 6. Observe that RADIO-1 cannot transmit due to the voice channel being busy.
- Step 7. Release the PTT switch on RADIO-3.
- Step 8. Observe that RADIO-1 can now proceed with the call and RADIO-2 receives the call. Also observe that the display on RADIO-2 denotes an emergency and the ID of the unit sending the emergency.
- Step 9. End the emergency call and verify that RADIO-4 gets a callback.
- Step 10. Restore all channels to service.

Pass ____ Fail ____

Site Trunking Features

Site Trunking Continuous Assignment Updating

1. DESCRIPTION

When a talkgroup is assigned a voice channel, the site controller continues to transmit the channel assignment on the control channel for the duration of the Talkgroup Call. Radios coming into use on the system are automatically sent to voice channels with conversations in progress involving their selected talkgroups. This is demonstrated for a site in Site Trunking.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 1

* All Radios should be "Site Locked"

VERSION #1.04

2. TEST

- Step 1. Place SITE 1 into the Site Trunking mode via the Zone Manager.
- Step 2. Turn OFF RADIO-1.
- Step 3. Initiate a Talkgroup Call using RADIO-2.
- Step 4. While the Talkgroup Call is in progress, turn ON RADIO-1.
- Step 5. Observe that RADIO-1, which was just brought back into service, joins the Talkgroup Call already in progress.
- Step 6. Release the PTT of RADIO-2.
- Step 7. Switch RADIO-1 to TALKGROUP 2.
- Step 8. Initiate a Talkgroup Call using RADIO-2.
- Step 9. While the Talkgroup Call is in progress, turn RADIO-1 back to TALKGROUP 1.
- Step 10. Observe that RADIO-1, which was just set back to TALKGROUP 1, joins the Talkgroup Call already in progress.

Pass_____ Fail_____

Site Trunking Features

Site Trunking Wide Area Recovery

1. DESCRIPTION

A site in Site Trunking will transition to Wide Area Trunking when all failures have been cleared or when the Zone Manager has set the sites status to Wide Area.

All subscribers should transition from Site Trunking to Wide Area Trunking and continue to process calls.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

* All Radios should be "Site Locked"

VERSION #1

2. TEST

- Step 1. From the Zone Manager set the status of SITE 1 to Wide Area and clear any errors that may have placed SITE 1 into Site Trunking.
- Step 2. Verify that the status of SITE 1 in Zone Watch and FullVision reflect that SITE 1 has transitioned into Wide Area Trunking.
- Step 3. Verify that RADIO-1 and RADIO-2 no longer display Site Trunking.
- Step 4. Verify communications between RADIO-1 and RADIO-2.
- Step 5. Verify that Zone Watch can now monitor the status of SITE 1.

Pass _____ Fail _____

Site Trunking Features

Site Trunking Roaming to Wide Area Sites

1. DESCRIPTION

Radios at a site that goes into Site Trunking will attempt to roam to a site in Wide Area Trunking so it is not stranded at a site with limited system resources available. The parameter adjusted in the test is the Failure Random Holdoff Time setting. This timer is used by the subscribers to set a random timer, which delays subscribers from flooding an adjacent site with registration requests.

NOTE: This feature only works on a multi-site system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

*Start up a ZoneWatch session for the site the radios are affiliated in.

*All sites should be in Wide Area at the start of this test.

*All radios should NOT be "Site Locked"

*The radios should have alternate site control channel frequencies setup in the portable's control channel list.

*The portables should not be configured for "Always Preferred" for this site which would prevent the radios from roaming under site trunking conditions.

VERSION #1.05

2. TEST

- Step 1. Set the Failure Random Holdoff Time (FRHOT) setting for SITE 1 in the Zone Configuration Manager to 1 minute.
- Step 2. Initiate a Talkgroup Call between RADIO-1 and RADIO-2.
- Step 3. Note the site that the radios are affiliated to on the ZoneWatch screen.
- Step 4. Place the site the radios are affiliated to into Site Trunking.
- Step 5. After 1 minute, initiate a Talkgroup Call between RADIO-1 and RADIO-2.
- Step 6. Observe that Radios 1 and 2 have roamed to a wide area site on the Zone Watch screen.
- Step 7. Reset the FRHOT setting of SITE 1 back to the customer's default.
- Step 8. Return SITE 1 back to Wide Area.

Pass____ Fail____

Elite Console Features

Elite Console Features

Console Instant Transmit

1. DESCRIPTION

The instant transmit switch provides immediate operator access to a channel, independent of its select status (selected or unselected). It provides priority over other dispatchers' transmit bars or optional footswitches.

SETUP

RADIO-1 - SITE 1

VERSION #1.03

2. TEST

- Step 1. Click the mouse anywhere in the SITE 1 resource window.
- Step 2. Depress the Instant Transmit button on the SITE 1 resource window.
- Step 3. Verify that the Transmit indicator is lit.
- Step 4. Verify that outbound audio is heard on RADIO-1.

Pass_____ Fail_____

Elite Console Features

Conventional Radio Resource

1. DESCRIPTION

A Radio Resource is selected on Elite Dispatch consoles by placing the cursor over the Radio Resource (Channel Control Window), choosing an area and selecting. The Radio Resource choice area is the region where the name of the Radio Resource is located (Top alphanumeric line of the Radio Resource). When selected, the background of the Radio Resource will turn white and the border will turn green. Choosing the PTT button will send keying commands to the station.

SETUP

RADIO-1 - SITE 1

A VHF base station is configured for conventional operation and connected to a BIM associated with the console under test.

VERSION #1.03

2. TEST

- Step 1. Select the SITE 1 Radio Resource by moving the cursor over the Radio Resource's name and selecting.
- Step 2. Begin an outbound console transmission using the PTT Button on the newly selected Radio Resource, in clear mode.
- Step 3. Verify that console's outbound audio can be monitored by RADIO-1.
- Step 4. Respond to the console outbound transmission from RADIO-1. Verify that RADIO-1 audio can be monitored at the console Select speaker.
- Step 5. Depress any of the other available Radio Resources to "deselect" the present Radio Resource.
- Step 6. Respond to the console outbound transmission from RADIO-1. Verify that RADIO-1's audio can be monitored at the unselect speaker.
- Step 7. Repeat steps 1-6 for a sample of the remaining sites.
- Step 8. Repeat steps 1-7 for a sample of the remaining OPs.

Pass ____ Fail ____

Elite Console Features

Conventional Radio Resource Coded Mode

1. DESCRIPTION

A Radio Resource is selected on Elite Dispatch consoles by placing the cursor over the Radio Resource (Channel Control Window), choosing an area and selecting. The Radio Resource choice area is the region where the name of the Radio Resource is located (Top alphanumeric line of the Radio Resource). When selected, the background of the Radio Resource will turn white and the border will turn green. Choosing the PTT button will send keying commands to the station.

SETUP

RADIO-1 - SITE 1

VERSION #1.02

2. TEST

- Step 1. Select the SITE 1 Radio Resource by moving the cursor over the Radio Resource's name and selecting.
- Step 2. Begin an outbound console transmission using the PTT Button on the newly selected Radio Resource, in coded mode.
- Step 3. Verify that console's outbound audio can be monitored by RADIO-1.
- Step 4. Respond to the console outbound transmission from RADIO-1. Verify that the radio audio can be monitored at the console Select speaker.
- Step 5. Depress any of the other available Radio Resources to "deselect" the present Radio Resource.
- Step 6. Respond to the console outbound transmission from RADIO-1. Verify that RADIO-1 audio can be monitored at the unselect speaker.
- Step 7. Repeat steps 1-6 for a sample of the remaining sites.
- Step 8. Repeat steps 1-7 for a sample of the remaining OPs.

Pass ____ Fail ____

Elite Console Features

Conventional Radio Resource Via Comparator

1. DESCRIPTION

A comparator will vote all receive capable sites and transmit on specified transmit capable sites. Because a comparator will construct a signal from multiple sites, it is necessary to test each site individually.

SETUP

RADIO-1 - SITE 1
RADIO-2 - SITE 1

VERSION #1.02

2. TEST

- Step 1. Disable all sites on the comparator except SITE 1.
- Step 2. Verify communications between RADIO-1, RADIO-2 and the console.
- Step 3. Disable SITE 1 and enable the next site. Change the channel on the subscriber if necessary.
- Step 4. Verify communications between RADIO-1, RADIO-2 and the console.
- Step 5. Repeat steps 3 & 4 until all sites on the comparator have been individually tested.
- Step 6. Enable all sites on the comparator.
- Step 7. Verify communications between RADIO-1, RADIO-2 and the console with all sites enabled.

Pass _____ Fail _____

Elite Console Features

Clear / Coded Receive Indication

1. DESCRIPTION

A call from a subscriber unit to a console is indicated on each dispatch operator position that has a Radio Resource associated with the channel the subscriber unit is transmitting on. When the Radio Resource is receiving secure (CODED) audio, a steady coded pad lock icon is displayed in the Resource window if the current mode of operation for the Radio Resource is clear mode. If the Resource window is selected for coded mode, the coded icon will not be displayed.

SETUP

RADIO-1 - SITE 1

VERSION #1.03

2. TEST

- Step 1. Select the SITE 1 Radio Resource by moving the cursor over the Radio Resource's name and clicking the left mouse button.
- Step 2. Verify that the resource is set for clear. A "pad lock" icon represents the clear/coded option. If the pad lock icon is open the outbound transmission is in the clear mode. If the pad lock icon is in the closed "lock" position, the outbound transmission is in the coded mode.
- Step 3. Initiate a coded call from RADIO-1.
- Step 4. Verify that the call icon, represented by the speaker icon, flashes when the console receives audio. If the Radio Resource is selected, audio is heard through the Select speaker. If the Radio Resource is not selected, audio is heard through the Unselect speaker.
- Step 5. In addition to the call indication, a clear/coded indication, an open or closed 'pad lock' respectively, is displayed. Verify that a coded indication is present.
- Step 6. De-key RADIO-1. Verify that the call indication stops flashing, and that the coded indication ends.
- Step 7. Verify steps 1-6 for an incoming clear call when console is set to coded.
- Step 8. Repeat steps 1-7 for a sample of the remaining sites.
- Step 9. Repeat steps 1-8 for a sample of the remaining OPs.

Pass ____ Fail ____

Elite Console Features

Patch Operation

1. DESCRIPTION

The Patch feature allows more than one Radio Resource to be grouped simultaneously. This can be used for temporarily merging two or more channels/frequencies together to act as one larger group. Telephones and radio resources can be patched together. In a patch group, the members can receive messages from the console and they can transmit to all other members of the patch group.

SETUP

RADIO-1 - SITE 1
RADIO-2 - SITE 2

VERSION #1.02

2. TEST

- Step 1. Select patch 1, 2, or 3 from the Patch/MSEl button.
- Step 2. Select the "Patch Edit" icon. The selected patch will turn blue.
- Step 3. Select the SITE 1 and SITE 2 Radio Resource by moving the cursor over the Radio Resources' names and selecting them.
- Step 4. Verify that the selected Radio Resources display a "Patch Edit" icon.
- Step 5. Press and hold the "Patch Transmit" icon to initiate the patch transmission.
- Step 6. Verify that the RADIO-1 and RADIO-2 monitor the console outbound audio.
- Step 7. Verify that RADIO-1 can communicate with RADIO-2 even though they are on separate channels.
- Step 8. To knock down the patch, select the Radio Resources by moving the mouse cursor over the resource window and clicking over the patch icon. Repeat this process until all the resources have been removed from the Patch window.
- Step 9. Finally, click on the Patch Edit icon and idle the current patch.
- Step 10. Repeat steps 1-9 for a sample of the remaining OPs.

Pass____ Fail____

Elite Console Features

Patch Operation Coded Mode

1. DESCRIPTION

The Patch feature allows more than one Radio Resource to be grouped simultaneously. This can be used for temporarily merging two or more channels/frequencies together to act as one larger group. Telephones and radio resources can be patched together. In a patch group, the members can receive messages from the console and they can transmit to all other members of the patch group.

SETUP

RADIO-1 - SITE 1
RADIO-2 - SITE 2

VERSION #1.02

2. TEST

- Step 1. Select patch 1, 2, or 3 from the Patch/MSEL button.
- Step 2. Select the "Patch Edit" icon. The selected patch will turn blue.
- Step 3. Verify that the SITE 1 and SITE 2 Resource windows are set to coded mode.
- Step 4. Select the SITE 1 and SITE 2 Radio Resource by moving the cursor over the Radio Resources' names and selecting them.
- Step 5. Press and hold the "Patch Transmit" icon to initiate the patch transmission.
- Step 6. Verify that the RADIO-1 and RADIO-2 monitor the console outbound audio.
- Step 7. Verify that RADIO-1 can communicate with RADIO-2 even though they are on separate channels.
- Step 8. To knock down the patch, select the Radio Resources by moving the mouse cursor over the resource window and clicking over the patch icon. Repeat this process until all the resources have been removed from the Patch window.
- Step 9. Finally, click on the Patch Edit icon and idle the current patch.
- Step 10. Repeat steps 1-9 for a sample of the remaining OPs.

Pass____ Fail____

Elite Console Features

Multiselect Operation

1. DESCRIPTION

The Multi-select feature allows more than one Radio Resource to be selected simultaneously. This can be used for announcements to two or more channels for general broadcast purposes. In a multi-select, the members can receive messages from the console but they cannot communicate to other members of the multi-select group.

SETUP

RADIO-1 - SITE 1
RADIO-2 - SITE 2

VERSION #1.03

2. TEST

- Step 1. Select MSEL 1, 2, or 3 from the Patch/MSEL button.
- Step 2. Select the "MSEL Edit" button by clicking on it with left mouse. The selected MSEL will turn green.
- Step 3. Select the SITE 1 and SITE 2 Radio Resource by moving the cursor over the Radio Resources' names and selecting them.
- Step 4. Identify that the selected resources display a green border around the resource window.
- Step 5. Press and hold the "general transmit" icon from the toolbar to initiate the multi-select transmission.
- Step 6. Verify that RADIO-1 and RADIO-2 monitor the console outbound audio.
- Step 7. Verify that RADIO-1 and RADIO-2 cannot communicate with each other.
- Step 8. Demonstrate the memory feature by placing the multi-select in idle mode and then returning it to active.
- Step 9. To knock down the multi-select, select the Radio Resources by moving the mouse cursor over the resource window and clicking somewhere in the resource window area. Repeat this process until all the resources have been removed from the Multi-select window. Click on the Multi-select Edit icon and idle the current multi-select. The multi-select window border should turn white with a gray border.
- Step 10. Repeat steps 1-9 for a sample of the remaining OPs.

Pass ____ Fail ____

Elite Console Features

Multiselect Operation Coded Mode

1. DESCRIPTION

The Multi-select feature allows more than one Radio Resource to be selected simultaneously. This can be used for announcements to two or more channels for general broadcast purposes. In a multi-select, the members can receive messages from the console but they cannot communicate to other members of the multi-select group.

SETUP

RADIO-1 - SITE 1
RADIO-2 - SITE 2

VERSION #1.02

2. TEST

- Step 1. Select MSEL 1, 2, or 3 from the Patch/MSEL button.
- Step 2. Select the "MSEL Edit" button by clicking on it with left mouse. The selected MSEL will turn green.
- Step 3. Verify that the SITE 1 and SITE 2 Resources are set to the coded mode.
- Step 4. Select the SITE 1 and SITE 2 Radio Resource by moving the cursor over the Radio Resources' names and selecting them.
- Step 5. Identify that the selected resources display a green border around the resource window.
- Step 6. Press and hold the "general transmit" icon from the toolbar to initiate the multi-select transmission.
- Step 7. Verify that RADIO-1 and RADIO-2 monitor the console outbound audio.
- Step 8. Verify that RADIO-1 and RADIO-2 cannot communicate with each other.
- Step 9. To knock down the multi-select, select the Radio Resources by moving the mouse cursor over the resource window and clicking somewhere in the resource window area. Repeat this process until all the resources have been removed from the Multi-select window. Click on the Multi-select Edit icon and idle the current multi-select. The multi-select window border should turn white with a gray border.
- Step 10. Repeat steps 1-9 for a sample of the remaining Ops .

Pass ____ Fail ____

Elite Console Features

Inbound Telephone Interconnect and Patch

1. DESCRIPTION

The dispatch console has the capabilities of answering communication from landline telephone resources. The console can also patch together a telephone communication to a radio resource.

SETUP

RADIO-1 - SITE 1

VERSION #1.01

2. TEST

- Step 1. From a landline, dial the number connected to the SPI in the CEB.
- Step 2. Verify that OP 1 displays an incoming call indication.
- Step 3. Answer the incoming call and verify communication between landline user and operator.
- Step 4. Patch SITE 1 Resource to the Telephone Resource.
- Step 5. Transmit on RADIO-1, verify communication with landline user. Also verify that Console Operator receives transmission. Console operator presses patch transmit, verify communication with RADIO-1 and landline user
- Step 6. Dissolve the patch.
- Step 7. Repeat steps 1-6 for a sample of the remaining OPs.

Pass____ Fail____

Elite Console Features

Outbound Telephone Interconnect and Patch

1. DESCRIPTION

The dispatch console has the capabilities of initiating communication to landline telephone resources. The console can also patch together a telephone communication to a radio resource.

SETUP

RADIO-1 - SITE 1

VERSION #1.01

2. TEST

- Step 1. Select the Telephone Resource Window. Verify that the Resource Window is highlighted in blue; the On/Off Hook icon displays Off Hook. Verify the dial tone is heard.
- Step 2. Choose the keypad icon and enter a local phone number, verify that operator hears a ringing, close the keypad icon
- Step 3. When the landline answers, verify communication between landline user and operator
- Step 4. Patch the SITE 1 Resource to the Telephone Resource.
- Step 5. Transmit on the RADIO-1, verify communication with landline user.
- Step 6. Verify that Console Operator receives transmission. Console operator presses patch transmit, verify communication with RADIO-1 and landline user.
- Step 7. Dissolve the patch.
- Step 8. Repeat steps 1-7 for a sample of the remaining OPs.

Pass ____ Fail ____

Elite Console Features

ID Stacking

1. DESCRIPTION

During normal call operation radio IDs are displayed in the resource window for a particular resource. These IDs are saved in a "Stack" and can be viewed to determine which radios made the previous calls. Stack size can be up to 10 IDs.

SETUP

RADIO-1 - SITE 1
RADIO-2 - SITE 1
RADIO-3 - SITE 1

VERSION #1.01

2. TEST

- Step 1. View the SITE 1 Resource Window.
- Step 2. Initiate Talkgroup calls from RADIO-1 then RADIO-2 then RADIO-3.
- Step 3. Scroll through the stack to see that the radio IDs are displayed in the order received.
- Step 4. Repeat steps 1-3 for a sample of the remaining OPs.

Pass _____ Fail _____

Elite Console Features

All Mute Operation

1. DESCRIPTION

The All Mute icon allows the dispatcher to mute all audio routed to the UNSELECT speaker, so as not to interfere with the audio from the SELECT speaker.

SETUP

RADIO-1 - SITE 1
RADIO-2 - SITE 2

VERSION #1.01

2. TEST

- Step 1. Select the SITE 1 Resource Window at the console.
- Step 2. Verify that RADIO-1's audio can be heard at the SELECT speaker and that RADIO-2's audio can be heard at the UNSELECT speaker.
- Step 3. Depress the "ALL MUTE" icon, and verify that RADIO-2's audio cannot be heard from the UNSELECT speaker.
- Step 4. Verify that RADIO-1's audio can still be heard out of the SELECT speaker.
- Step 5. Again press the "ALL MUTE" button to un-mute the UNSELECT speaker.
- Step 6. Verify audio at both speakers.

Pass____ Fail____

Elite Console Features

Alert Tones and Channel Markers

1. DESCRIPTION

Alert Tones and Channel Markers are pre-defined tones that can be transmitted on the selected Radio Resource outbound to subscribers.

SETUP

RADIO-1 - SITE 1

VERSION #1

2. TEST

- Step 1. Select the SITE 1 Radio Resource by moving the cursor over the Radio Resource's name and selecting.
- Step 2. Select Tone 1 from the Alert Tone pull down menu.
- Step 3. Transmit Alert Tone 1 by depressing the Alert Tone button. This selected resource will display a red lighting bolt transmit indicator.
- Step 4. Verify the Alert Tone 1 is received by RADIO-1.
- Step 5. Repeat the above procedure for Alert Tone 2 and Alert Tone 3.
- Step 6. Repeat steps 1-5 for a sample of the remaining OPs.
- Step 7. Repeat this test for Channel Marker functionality on selected Radio Resources for a sample of the OPs.

Pass____ Fail____

Elite Console Features

Console Priority

1. DESCRIPTION

Console operator positions have ultimate control of transmitted audio on an assigned voice channel resource. The console position possesses the capability to take control of an assigned voice channel for a talkgroup call so that the operator's audio overrides any subscriber audio. Console priority is a feature that enables dispatchers to gain immediate access to an assigned voice channel so that a central point of audio control exists.

SETUP

RADIO-1 - SITE 1
RADIO-2 - SITE 1

VERSION #1.02

2. TEST

- Step 1. The operator selects the SITE 1 Resource Window.
- Step 2. RADIO-1 transmits on SITE 1.
- Step 3. Verify that RADIO-2 can hear RADIO-1.
- Step 4. While RADIO-1 is transmitting, key SITE 1's Resource Window on the operator.
- Step 5. Verify that RADIO-2 hears the console but not RADIO-1. This shows that the console has priority over the subscriber. Verify that the operator continues to hear received audio from RADIO 1 during this transmission.
- Step 6. De-key the Console.
- Step 7. Verify that RADIO-2 now hears RADIO-1.

Pass____ Fail____

Elite Console Features

Supervisory Control

1. DESCRIPTION

In Motorola Radio Systems, the console operators may override subscriber audio being transmitted on the system. The Console Supervisor position may override all other console positions. The console position overridden will hear side tone, informing them that the Supervisor has exercised control on the channel.

SETUP

RADIO-1 - SITE 1
CONSOLE-1 - Supervisor position
CONSOLE-2 - Non-supervisory position

2. TEST

- Step 1. Set up two dispatch positions on SITE 1. One must be the Supervisor position.
- Step 2. Transmit from the non-Supervisor position.
- Step 3. Verify that RADIO-1 receives the non-Supervisor audio.
- Step 4. While continuing to transmit at the non-supervisory position, transmit on the same channel at the Supervisor's position using Instant Transmit Key.
- Step 5. Verify that RADIO-1 receives the supervisor audio and that the supervisor audio is heard at non-Supervisor position.

Pass ____ Fail ____

VERSION #1.02

Elite Console Features

Console Enable / Disable

1. DESCRIPTION

In an Elite Operator configuration, the Supervisory console position may disable the non-supervisory positions. This will disable all transmit capability from the disabled console.

SETUP

RADIO-1 - SITE 1
CONSOLE-1 - Supervisor position
CONSOLE-2 - Non-supervisory position

VERSION #1.05

2. TEST

- Step 1. Verify that CONSOLE-1 is set up as a Supervisor.
- Step 2. Transmit from the CONSOLE-2 (non-supervisory) and verify communication with RADIO-1.
- Step 3. Select the "Enable/Disable Op Position" button from the tool bar on the Supervisory console.
- Step 4. Disable CONSOLE 2.
- Step 5. Verify that the non-supervisory position is completely disabled from making a call.
- Step 6. Select the "Enable/Disable Op Position" button from the tool bar on the Supervisory console.
- Step 7. Enable CONSOLE 2.
- Step 8. Verify that the non-supervisory position is completely enabled.

Pass ____ Fail ____

Elite Console Features

Emergency Alarm and ID Display

1. DESCRIPTION

When an Emergency Alarm is received at an Elite Dispatch console operator, the Emergency Alarm tone sounds in the select speaker and the border of the resource window that receives an Emergency Alarm flashes red.

SETUP

RADIO-1 - SITE 1

VERSION #1.02

2. TEST

- Step 1. Select the SITE 1 Radio Resource.
- Step 2. Initiate an Emergency Alarm from RADIO-1 by pressing and holding the emergency button.
- Step 3. Verify a continuous emergency tone is generated for each Emergency Alarm.
- Step 4. If the current resource has been set to display status indications, the status line in the resource window will display the text "Emerg Alarm" or "Emerg Call" in the normal color.
- Step 5. Verify the Activity Log displays the text "Emerg Alarm" or "Emerg Call" in red.
- Step 6. Press the emergency button on the resource window. This will cause the Emergency QuickList to appear.
- Step 7. Select the entry in the Emergency Quicklist to acknowledge. Press the Acknowledge button to handle the emergency alarm\call. This ends the tone for that emergency.
- Step 8. Press the Knockdown button to terminate the Emergency on the resource window. This removes the entry from the Emergency QuickList and removes the resource's red border.
- Step 9. Clear the emergency on RADIO-1 by pressing and holding the emergency button.

Pass____ **Fail**____

Elite Console Features

Radio Check

1. DESCRIPTION

Radio Check allows the console operator to determine if a subscriber is operational or within range. The subscriber sends the acknowledgment that it has received the Radio Check.

NOTE: The status/message line must be added to the CCW of the resource in order for the "ACKNOWLEDGED" indication to be visible.

SETUP

RADIO-1 - SITE 1

VERSION #1.02

2. TEST

- Step 1. Select the SITE 1 Radio Resource.
- Step 2. From the active Radio Resource select the Radio Check button. Enter the ID or alias of RADIO-1 in the Radio Check window.
- Step 3. Click the "Send" button from the Radio Check window to initiate the Radio Check.
- Step 4. Verify that "ACKNOWLEDGED" is shown on SITE 1's CCW.
- Step 5. Turn off the selected radio.
- Step 6. Click the "Send" button from the Radio Check window to initiate the Radio Check.
- Step 7. Verify that an error message is logged: "Send Radio Check failed: Target not found."

Pass _____ Fail _____

Elite Console Features

Selective Radio Inhibit

1. DESCRIPTION

The Inhibit command is used to disable radios, preventing them from being used should it be lost or stolen. When a radio is inhibited, all of its functions are disabled. Once inhibited, the radio cannot be used to monitor voice channels or for any other radio user activity.

SETUP

RADIO-1 - SITE 1

VERSION #1.01

2. TEST

- Step 1. Select the SITE 1 Radio Resource.
- Step 2. From the active Radio Resource select the RADIO INHIBIT icon. Enter the ID or alias.
- Step 3. Click the "Send" button to initiate the RADIO INHIBIT.
- Step 4. Verify that target radio has been inhibited.
- Step 5. From the active Radio Resource select the RADIO ENABLE icon. Enter the ID or alias.
- Step 6. Click the "Send" button to initiate the RADIO ENABLE.
- Step 7. Verify that target radio has been enabled.

Pass ____ Fail ____

Elite Console Features

Send Voice Alert

1. DESCRIPTION

Send Voice Alert is used to send a voice selective call to the ID entered or displayed on the Radio Resource display. This unmutes the subscriber's speaker so the call can be heard. The voice alert will sound once on the receiving radio.

SETUP

RADIO-1 - SITE 1
RADIO-2 - SITE 1

VERSION #1.02

2. TEST

- Step 1. Select the SITE 1 Radio Resource.
- Step 2. From the active Radio Resource select the Voice Alert button. Enter the ID or alias of RADIO-1.
- Step 3. Click the "Send" button to initiate the Voice Alert.
- Step 4. Verify that RADIO-1 receives the Voice Alert.
- Step 5. Verify that RADIO-2 does not receive the Voice Alert.

Pass____ Fail____

Elite Console Features

Console Volume

1. DESCRIPTION

In Motorola Elite console, the volume on the Resources window is divided in 8 levels (0-min, 7-max). When there is a Resource window selected, the volume will automatically adjust to maximum level. When the resource is de-selected, the volume will resume back to original level.

SETUP

RADIO-1 - SITE 1

VERSION #1.07

2. TEST

- Step 1. Select the SITE 1 Resource window from the console.
- Step 2. Key up RADIO-1 and talk on SITE 1.
- Step 3. Observe that RADIO-1 audio came out from the SELECT speaker of the console in full volume.
- Step 4. Adjust the SITE 1 volume to a minimum level by means of the mouse.
- Step 5. Note that the audio is muted from the select speaker.

Pass____ Fail____

Elite Console Features

Console Message

1. DESCRIPTION

The purpose of this test is to allow the console operators to be updated with a message from a subscriber unit without the use of a voice conversation. The Console will be updated when the subscriber sends in a Message change. There are sixteen unique Messages in the radio. Each message can have a fourteen-character alias in the subscriber. The Alias Database Manager (ADM) can also alias these different messages. There can be many different folders in the ADM to allow different users different aliases for their particular need.

SETUP

RADIO-1 - SITE 1

VERSION #1.05

2. TEST

- Step 1. From the soft menu on the subscriber select "MSG".
- Step 2. Select each Message from the Radio's list. [Motorola will ensure that the radios are programmed with a list of messages provided by the Commonwealth for this feature.]
- Step 3. Push PTT button.
- Step 4. Verify that all Console Operators receive the message, and that if this chosen message has an alias, verify that the alias appears as well. The Radio will also receive an Acknowledgement that the Console has received the message.

Pass ____ Fail ____

Elite Console Features

Console Status Request

1. DESCRIPTION

The purpose of this test is to allow the console operators to be updated on the status of a subscriber unit without the use of a voice conversation. The Console will be updated when the subscriber sends in a status change or the Console initiates a Status Request form the Resource window. There are sixteen unique statuses in the radio. Each status can have a fourteen-character alias in the subscriber. The Alias Database Manager (ADM) can also alias these different statuses. There can be many different folders in the ADM to allow different users different aliases for their particular status.

SETUP

RADIO-1 - SITE 1

VERSION #1.03

2. TEST

- Step 1. Choose the Status Request button on the resource. This will cause a window to appear.
- Step 2. Select the Radio user from the list that appears.
- Step 3. Push the send button.
- Step 4. The Radio will respond with the last Acknowledged Status
- Step 5. Verify the Status of the Subscriber is displayed in the Resource window.

Pass____ Fail____

Elite Console Features

Console Status

1. DESCRIPTION

The purpose of this test is to allow the console operators to be updated on the status of a subscriber unit without the use of a voice conversation. The Console will be updated when the subscriber sends in a status change or the Console initiates a Status Request form the Resource window. There are sixteen unique statuses in the radio. Each status can have a fourteen-character alias in the subscriber. The Alias Database Manager (ADM) can also alias these different statuses. There can be many different folders in the ADM to allow different users different aliases for their particular status.

SETUP

RADIO-1 - SITE 1

VERSION #1.02

2. TEST

- Step 1. From the soft menu on the subscriber select "STS".
- Step 2. Select a Status Message from Radio's list.
- Step 3. Push PTT button.
- Step 4. Verify that all Console Operators receive the Status message and if this chosen status has an Alias verify this appears. The Radio will also receive an Acknowledgement that the Console has received the Status change.

Pass____ Fail____

Elite Console Features

Monitor Function

1. DESCRIPTION

The Console Monitor function is provided to permit the operator to disable the continuous tone controlled squelch system (CTCSS) of any selected conventional base station receiver, in order to permit monitoring of the communications channel prior to making a transmission.

SETUP

Ensure a conventional channel is setup on the console. At one of the remote site locations, have a service monitor that is capable of generating a RF signal on a conventional channel located at the site, modulated by a 1 KHz tone.

VERSION #1.03

2. TEST

- Step 1. At the remote site, generate the RF signal, modulated by 1 KHz, with no CTCSS tone.
- Step 2. The Console will not hear the 1 KHz tone.
- Step 3. At the Console, press either the Monitor button on the screen, or the Monitor switch on the microphone or the footswitch.
- Step 4. The 1 KHz tone will be heard in the Select Speaker.
- Step 5. Release the Monitor switch.
- Step 6. The Console will not hear the 1 KHz tone.

Pass____ Fail____

Elite Console Features

Acoustic Crossmute

1. DESCRIPTION

Acoustic crossmuting means that selected operator positions will not hear outbound transmissions from operator positions they are cross-muted with.

This feature is used when operator positions are located in the same room.

SETUP

- Two adjacent console positions monitoring the same resource
- Portable monitoring resource

VERSION #1.03

2. TEST

- Step 1. Without an Acoustic Crossmute configured, and the select speakers of each operator position turned to maximum volume, transmit on OP#1.
- Step 2. Confirm feedback is heard on the operator positions and the portable hears feedback on the channel.
- Step 3. With an Acoustic Crossmute configured, and the select speakers of each operator position turned to maximum volume, transmit on OP#1.
- Step 4. Verify no feedback is heard at either operator position and that the portable does not hear feedback on the channel.

Pass____ **Fail**____

Elite Console Features

Talkgroup Selection and Call

1. DESCRIPTION

The Talkgroup Call is the primary level of organization for communications on a trunked radio system. Dispatchers with Talkgroup Call capability will be able to communicate with other members of the same talkgroup. This provides the effect of an assigned channel down to the talkgroup level. When a Talkgroup Call is initiated from a subscriber unit, the call is indicated on each dispatch operator position that has a channel control resource associated with the unit's channel/talkgroup.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 2

VERSION #1.02

2. TEST

- Step 1. Initiate a wide area call from any operator position on TALKGROUP 1.
- Step 2. Observe that RADIO-1 and RADIO-3 will be able to monitor the call. Dekey the console and have either radio respond to the call.
- Step 3. Observe that all Consoles with TALKGROUP 1 can monitor both sides of the conversation.
- Step 4. Initiate a wide area call from any operator position on TALKGROUP 2.
- Step 5. Observe that RADIO-2 and RADIO-4 will be able to monitor the call. Dekey the console and have either radio respond to the call.
- Step 6. Observe that all Consoles with TALKGROUP 2 can monitor both sides of the conversation.

Pass____ Fail____

Elite Console Features

Console ASTRO Secure Talkgroup Call

1. DESCRIPTION

Digital encryption is used to scramble a transmission so only properly equipped radios can monitor the conversation. A "Key" is used to encrypt the transmit audio. Only radios and Consoles/MGEGs with the same "Key" can decrypt the audio and listen to it.

SETUP

RADIO-1 - TALKGROUP 1 (Secure TX Mode)
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1 (Secure TX Mode & No Key)
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1 (Secure TX Mode)
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 1 (Secure TX Mode & No Key)
RADIO-4 - SITE - SITE 2

VERSION #1.04

2. TEST

- Step 1. Initiate a wide area clear call from an operator position on TALKGROUP 1.
- Step 2. Observe that all radios will be able to monitor the call.
- Step 3. Initiate a wide area secure call from an operator position on TALKGROUP 1.
- Step 4. Observe that only RADIO-1 and RADIO-3 will be able to monitor and respond to the call.
- Step 5. If the radios equipped with dual algorithm encryption modules, select a talkgroup using the second algorithm and repeat Steps 3-4.

Pass _____ Fail _____

Elite Console Features

Console Repeat Disable

1. DESCRIPTION

This test verifies that any console operator position with a Repeat Disable control can enable and disable the repeat path for a particular talkgroup. This will be accomplished by changing the Repeat Disable status at various console operator positions scattered throughout the system and showing the effects on a radio call.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 1

* Several operator positions with a Repeat Disable control for the selected talkgroup are required.

* For multizone systems, the operator positions should be located in different zones.

VERSION #1.04

2. TEST

- Step 1. Initiate a wide area call with RADIO-1. Keep this call in progress until instructed to end the call.
- Step 2. Verify that the RADIO-1 audio is heard at the other radios and all operator positions with TALKGROUP 1.
- Step 3. Select the Repeat Disable icon for that talkgroup on any operator position.
- Step 4. Verify that RADIO-1 audio is still heard at the operator positions but not at any radio.
- Step 5. Select the Repeat Enable icon for that talkgroup on any operator position.
- Step 6. Verify that RADIO-1 audio is heard at the operator positions and at all radios.
- Step 7. Dekey RADIO-1.

Pass _____ Fail _____

Elite Console Features

Multigroup Call

1. DESCRIPTION

This trunking feature allows an equipped console operator position to transmit an announcement to several different talkgroups simultaneously. As with Talkgroup Calls, multigroup calls operate across sites as well as within the same site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 3
RADIO-3 - SITE - SITE 3 (SITE 1 if only 2 Sites)
RADIO-4 - RANDOM
RADIO-4 - SITE - SITE 4 (SITE 2 if only 2 Sites)

* TALKGROUP 1, TALKGROUP 2, &
TALKGROUP 3 are members of ATG 1.

* RANDOM is any talkgroup not a member of ATG 1.

* Multigroups are set up through both the UCM and the Subscriber Programming software.

VERSION #1.06

2. TEST

- Step 1. Select the ATG 1 resource, which corresponds TALKGROUP 1, TALKGROUP 2, and TALKGROUP 3.
- Step 2. Initiate the Multigroup Call from the operator position.
- Step 3. Observe that RADIO-1, RADIO-2 and RADIO-3 receive the Multigroup Call.
- Step 4. Verify that RADIO-4 does not receive the Multigroup Call because it is not a member of ATG 1.
- Step 5. Answer the Multigroup Call using RADIO-1 and observe the consoles receives the response.
- Step 6. Verify that if the call is answered within the repeater hang time, the console will receive the call on the ATG 1 resource tile, otherwise the console will receive the call on the TALKGROUP 1 tile.
- Step 7. Verify that if the call is answered within the repeater hang time, RADIO-2 and RADIO-3 will monitor that call.

Pass____ Fail____

Elite Console Features

Talkgroup Patch

1. DESCRIPTION

Talkgroup Patch allows a dispatcher to merge several talkgroups together on one voice channel to participate in a single conversation. This can be used for situations involving two or more channels or talkgroups that need to communicate with each other.

Using the Patch feature, the console operator can talk and listen to all of the selected talkgroups grouped; in addition, the members of the individual talkgroups can also talk or listen to members of other talkgroups. Patched talkgroups can communicate with the console dispatcher and other members of different talkgroups because of the "supergroup" nature of the Patch feature.

NOTE : If "secure" and "clear" resources are patched together, one repeater for each mode may be assigned per site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 2

* All 4 Radios must have the same home zone.

VERSION #1.05

2. TEST

- Step 1. Select an operator position for testing which contains TALKGROUP 1 and TALKGROUP 2.
- Step 2. At the desired operator position select one of the Patch tabs in the Patch/Multi-Select window.
- Step 3. Click the button on the patch that allows an operator to setup and edit a patch (note patch window turns blue).
- Step 4. Add TALKGROUP 1 and TALKGROUP 2 to the patch by selecting each resource tile.
- Step 5. Once the talkgroups are added, click the patch setup button again to complete the patch setup.
- Step 6. Initiate several Talkgroup Calls between radios.
- Step 7. Observe that all radios are able to communicate with one another. Also via Zone Watch observe that only one station is assigned at each of the two sites.
- Step 8. Initiate a call from the operator position using the Patch Transmit and observe that all radios are able to receive the call and only one station is assigned at each of the two sites.
- Step 9. Remove TALKGROUP 1 and TALKGROUP 2 from the patch.

Pass____ Fail____

Elite Console Features

Multi-Select/APB

1. DESCRIPTION

A Multi-Select (MSEL) allows a dispatcher to merge several talkgroups together on one voice channel to participate in a single conversation. This can be used for announcements to two or more channels or talkgroups for general broadcast purposes.

Using the Multi-Select feature, the console operator can talk and listen to all of the selected talkgroups grouped; however, the members of the individual talkgroups cannot talk or listen to members of other talkgroups. Multi-selected talkgroups still only communicate with the console dispatcher and other members in the same talkgroup. A predefined multi-select configuration can be saved by the console operator as an All Points Bulletin (APB) for quick broadcast-type transmissions by the dispatcher.

NOTE : If "secure" and "clear" resources are multi-selected, one repeater for each mode may be assigned per site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 3
RADIO-3 - SITE - SITE 3
RADIO-4 - TALKGROUP 4
RADIO-4 - SITE - SITE 4

VERSION #1.04

2. TEST

- Step 1. Select an operator position for testing which contains TALKGROUP 1, TALKGROUP 2, TALKGROUP 3 and TALKGROUP 4.
- Step 2. At the desired operator position select one of the Multi-Select tabs in the Patch/Multi-Select window.
- Step 3. Click the button on the Multi-Select that allows an operator to setup and edit a multiselect (note: MSEL window turns green).
- Step 4. Add TALKGROUP 1, TALKGROUP 2, TALKGROUP 3 and TALKGROUP 4 to the Multi-Select by selecting each resource tile.
- Step 5. Once the talkgroups are added click the Multi-Select Setup button again to complete the Multi-Select setup.
- Step 6. Initiate a call from the operator position using the APB Transmit and observe that all radios are able to receive the call. Also via Zone Watch verify that only one RF resource is assigned at any site where multiple radios are affiliated.
- Step 7. Remove all talkgroups from the Multi-Select.

Pass____ Fail____

Elite Console Features

Console Initiated Private Call

1. DESCRIPTION

Private Conversation is a selective calling feature which allows a dispatcher or radio user to carry on one-to-one conversation that is heard only by the two parties involved. Subscriber units receiving a private call will sound an alert tone. As with other call types, Private Calls operate across sites as well as within the same site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1

VERSION #1.03

2. TEST

- Step 1. Select an operator position for testing.
- Step 2. Select the "PRIVATE-CALL" tile.
- Step 3. Click the button on the tile that provides the Private Call function.
- Step 4. Select the unit to be Private Called, in this case RADIO-1.
- Step 5. Click the Send button.
- Step 6. Answer the Private Call with RADIO-1 and respond to the console.
- Step 7. After completing the Private Call, return to the normal talkgroup mode.

Pass____ **Fail**____

Elite Console Features

Emergency Alarm And Call Display

1. DESCRIPTION

Users in life threatening situations can use the emergency button on the radio to send an audible alarm and a visual alarm signal to a console operator in order to request immediate system access to a voice channel for an emergency call.

An emergency alarm begins after the radio user presses the radio's emergency button. Pressing the emergency button places the radio in "emergency mode". To begin an emergency call, the radio user must press the radio's PTT button while in "emergency mode." The assigned voice channel will be dedicated to the emergency caller's talkgroup for an extended period of time, equal to the Message Hang Time plus the Emergency Hang Time. As with other call types, emergency calls can operate across sites as well as within the same site.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1

VERSION #1.03

2. TEST

- Step 1. Select an operator position in the zone where RADIO-1 is affiliated for the test.
- Step 2. Initiate an Emergency Alarm from RADIO-1.
- Step 3. Observe the Emergency from RADIO-1 is received at the operator position on TALKGROUP 1. Note that if RADIO-1 is programmed for Emergency Revert, the Emergency will be received on the designated revert talkgroup.
- Step 4. Acknowledge the Emergency at the operator position.
- Step 5. Key RADIO-1 to initiate an Emergency call to the operator position and reply to the radio from the operator position. Observe that the call takes place.
- Step 6. Clear the Emergency from the console.
- Step 7. Reset RADIO-1 by holding the Emergency button on the radio.

Pass____ Fail____

Elite Console Features

PTT Unit ID/Alias Display

1. DESCRIPTION

Console operator positions contain various resources such as talkgroup, multigroup and Private Call which enable the operator to communicate with the subscriber units. If activity occurs on one of these operator position resources, the unit ID or associated alias of the initiating radio appears at the console resource. Default operation for the system is to display unit IDs at the console operator resource, but pre-defined aliases can be substituted for each unit ID.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

VERSION #1.04

2. TEST

- Step 1. Select TALKGROUP 1 on any operator position with that Talkgroup.
- Step 2. Initiate a call from RADIO-1 and observe that the portable ID or alias is seen at both consoles in the list in the resource window as well as in the Activity Log window. Note that if the alias for the radio has been downloaded from the User Configuration Subsystem (UCM) to the console, the alias will be displayed in place of the unit ID.
- Step 3. Repeat Step 2 using RADIO-2.

Pass____ Fail____

Elite Console Features

Console Initiated Tactical/Normal Priority

1. DESCRIPTION

The Tactical/Normal Priority feature is initiated at the console operator position and provides the dispatcher with the ability to change the priority for a particular talkgroup. When selected, a higher priority level (level 2) is assigned to the talkgroup. This overrides the priority level set in the UCM.

NOTE: All radios and talkgroups should start with default priorities. Default is 10.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 3
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 3
RADIO-4 - SITE - SITE 2

* The priority level for the talkgroups selected should be the same.

VERSION #1.08

2. TEST

- Step 1. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 2. Enable Tactical Priority for TALKGROUP 3 from any console position with this option.
- Step 3. Initiate a Talkgroup Call with RADIO-1. Keep this call in progress until instructed to end the call.
- Step 4. Key RADIO-2 and observe that the radio receives a busy.
- Step 5. Key RADIO-3 and observe that the radio receives a busy.
- Step 6. End the Talkgroup Call established in Step 3.
- Step 7. Verify RADIO-3 receives the first callback and can communicate with RADIO-4. Note that if TALKGROUP 3 was not set to Tactical, RADIO-2 would receive the first callback.
- Step 8. End the call between RADIO-3 and RADIO-4.
- Step 9. Verify that RADIO-2 receives a call back.
- Step 10. Disable Tactical Priority for TALKGROUP 3.

Pass____ Fail____

Elite Console Features

Alert Tones and Channel Markers

1. DESCRIPTION

To send alert tones or channel markers from a console operator position, the dispatcher must depress an alert tone or channel marker switch which sends a corresponding tone over a selected channel/talkgroup resource.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

VERSION #1.03

2. TEST

- Step 1. Select TALKGROUP 1 on any console position.
- Step 2. Select Alert Tone 1 and depress the Alert Tone button for 5 seconds.
- Step 3. Verify that RADIO-1 and RADIO-2 hear Alert Tone 1.
- Step 4. Repeat Steps 2-3 for Alert Tone 2 and 3.
- Step 5. Repeat this test for Channel Marker functionality on TALKGROUP 1.

Pass____ Fail____

Elite Console Features

Call Alert Page

1. DESCRIPTION

Call Alert Page allows a dispatcher to selectively alert another radio unit. The initiating radio will receive notification as to whether or not the call alert was received. Units receiving a Call Alert will sound an alert tone and show a visual alert indication. The display will also show the individual ID of the initiating radio unit. After receiving the Call Alert, the radio can respond with either a Private Call or normal talkgroup call.

This feature is fully supported on all display portables and mobiles.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1

VERSION #1.02

2. TEST

- Step 1. Select the call alert button in the "Private Call" resource window.
- Step 2. Enter the ID of RADIO-1.
- Step 3. Send the call alert to RADIO-1 by depressing the send button.
- Step 4. Verify that RADIO-1 receives the alert and that the ID of the console is shown.
- Step 5. Turn off RADIO-1.
- Step 6. Send the call alert to RADIO-1 again.
- Step 7. Verify that after trying to page RADIO-1, the console does display "Can not send call alert - target not found" in the summary list.

Pass ____ Fail ____

Elite Console Features

Console Initiated Emergency

1. DESCRIPTION

Emergency Call can be initiated by the console. If the console initiates an emergency call on a Talkgroup, a channel is assigned to that Talkgroup indefinitely. The console initiated emergency call is ended when the call is knocked down, the channel fails, or the last affiliated member in the talkgroup de-affiliates. Any dispatcher may knock down an emergency call, regardless of who initiated it. All the radios in the Talkgroup receive the emergency call.

NOTE : If the subscriber does not have the PTT Display option, the Emergency ID will not be displayed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

* Two console are required for this test.

VERSION #1.03

2. TEST

- Step 1. Click the "Emergency" button on the resource window for TALKGROUP 1 on Console 1 to display the Emergency QuickList and then click on the "Setup" button to initiate a console emergency.
- Step 2. Verify that an emergency indication is shown on Console 2 and on RADIO-1 and RADIO-2 (if they have displays).
- Step 3. Transmit on TALKGROUP 1 from Console 1. Determine which repeaters are keyed at SITE 1.
- Step 4. Verify that the individual ID of the TALKGROUP 1 resource on Console 1 is shown on Console 2 and on both Radios (if they have displays) and all hear Console 1's transmit audio.
- Step 5. Stop transmitting on TALKGROUP 1 from Console 1.
- Step 6. Wait a minute and then key up on RADIO-1.
- Step 7. Verify both consoles and RADIO-2 hear the audio. Verify the same repeaters as determined in step 3 are keyed.
- Step 8. Dekey RADIO-1.
- Step 9. Click the "Emergency" button on the resource window for TALKGROUP 1 on Console 2 to display the Emergency QuickList and then click on the "Knockdown" button.
- Step 10. Verify the emergency is knocked down and the repeaters previously keyed are no longer assigned.

Pass ____ Fail ____

Elite Console Features

Radio Status

1. DESCRIPTION

This optional feature allows the Console to display status information sent in by subscribers. Statuses are used to indicate the Radio operator's operational state (e.g. off duty).

The information that will be displayed in a Resource Tile.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1

* Configure the radio user in the Manager to use a particular status set.

* Configure Status through the Manager to also be routed to the console.

VERSION #1.03

2. TEST

- Step 1. Initiate a Status transmission from RADIO-1.
- Step 2. Verify that RADIO-1 receives an audible indication that the status has been received at the Master Site.
- Step 3. Verify the Console displays the proper Status text.

Pass____ Fail____

Elite Console Features

Console Priority

1. DESCRIPTION

Console Operator Positions have ultimate control of transmitted audio on an assigned voice channel resource. The Console Position has the capability to take control of an assigned voice channel for a talkgroup call so that the operator's audio overrides any subscriber audio. Console priority is a feature that enables dispatchers to gain immediate access to an assigned voice channel so that a central point of audio control exists.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1.07

2. TEST

- Step 1. Initiate a Talkgroup call from RADIO-1 on TALKGROUP 1.
- Step 2. Observe that RADIO-2 receives the call.
- Step 3. While the call is in progress, key up any operator position at the console on TALKGROUP 1.
- Step 4. Observe that RADIO-2 is now receiving audio from the operator position. Also observe that the operator continues to hear the call from RADIO 1 while during this transmission.
- Step 5. De-key the Operator Position.
- Step 6. Verify RADIO-2 now receives RADIO-1 audio.

Pass ____ Fail ____

Elite Console Features

Supervisory Control

1. DESCRIPTION

The Console Operators may override subscriber audio being transmitted on the system. The Console Supervisor position may override all other console positions.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1

VERSION #1.06

2. TEST

- Step 1. Set up two dispatch positions on the same talkgroup; one must be the Supervisor position.
- Step 2. Transmit from the non-Supervisor position.
- Step 3. Verify that RADIO-1 receives the non-Supervisor audio.
- Step 4. While continuing to transmit at the non-supervisory position, transmit on the same channel at the Supervisor's position using the Instant Transmit Key.
- Step 5. Verify that RADIO-1 receives the supervisor audio and that the supervisor audio is heard at non-supervisor position.
- Step 6. Repeat steps 1 through 5 for remaining consoles.

Pass _____ Fail _____

Elite Console Features

Conventional Radio Resource (BIM Only)

1. DESCRIPTION

A conventional station can be integrated into a trunking system by placing a conventional resource on the Elite consoles. This allows the user to patch the conventional station with the desired talkgroups.

SETUP

Connect a transmission test set to the Central Electronics Bank (CEB) interface panel that corresponds to a conventional Base Interface Module (BIM) in the CEB.

VERSION #1.03

2. TEST

- Step 1. Choose a conventional Radio Resource at the console.
- Step 2. Connect a transmission test set to the output of the Base Interface Module corresponding to the selected Radio Resource.
- Step 3. Key up the console Radio Resource and verify Transmit audio for the conventional resource.
- Step 4. Inject a test tone into the input of the Radio Resource selected.
- Step 5. Verify the Radio Resource receives the tone in the select speaker.
- Step 6. Repeat Steps 1-5 for one conventional BIM in each CEB.

Pass ____ Fail ____

Elite Console Features

Alarm Input / Outputs (16 Aux I/O)

1. DESCRIPTION

The alarm inputs of the 16 Aux I/O can be connected to almost any device that requires or can detect a relay closure. These signals can be simulated and monitored with simple test equipment such as a multimeter.

Aux I/O pinout:

Aux I/O 1 - pins 26,1
Aux I/O 2 - pins 27,2
Aux I/O 3 - pins 28,3
Aux I/O 4 - pins 29,4

SETUP

Connect a multi-meter capable of monitoring closures to the proper pins of the punch block cabled to the Aux I/O.

VERSION #1.05

2. TEST

- Step 1. Using a shorting wire, simulate a relay closure on an input via the punch block for the I/O's to be tested.
- Step 2. Verify that the Operator position displays the icon designated for an ON_STATE.
- Step 3. Remove the shorting wire and verify that the Operator position displays the icon designated for an OFF_STATE.
- Step 4. Connect the Multimeter to the pins to monitor a relay output.
- Step 5. Verify that the meter reads an open circuit.
- Step 6. Depress the button on the console to initiate a relay closure.
- Step 7. Verify that the multimeter displays a closed circuit.

Pass_____ Fail_____

Elite Console Features

Logging Recorder

1. DESCRIPTION

The Logging Record Interface (LORI) and Logging Recorder/Operator Interface Module (LOMI) in the Central Electronics Bank (CEB) provide an audio source to an external Logging Recorder used to record console dispatch audio. The LOMI card detrunks the talkgroup audio and sources the talkgroup audio to the AEI/LORI boards which connect to the actual Logging Recorder.

LORI pinouts:

Output Pair #1 - pins 26,1
Output Pair #2 - pins 28,3
Output Pair #3 - pins 30,5
Output Pair #4 - pins 32,7
Output Pair #5 - pins 36,11
Output Pair #6 - pins 38,13
Output Pair #7 - pins 40,15
Output Pair #8 - pins 42,17

SETUP

Use the Console Dispatch Manager (CDM) software to configure a LOMI to detrunk TALKGROUP 1 and TALKGROUP 2 in order to test the audio availability at the LORI card. Connect the LORI card that contains the logging tracks for TALKGROUP 1 and TALKGROUP 2 to a punchblock.

VERSION #1.05

2. TEST

- Step 1. Identify the pins on the designated LORI punchblock that provide the demarcation for the detrunked logging tracks for TALKGROUP 1 and TALKGROUP 2.
- Step 2. Connect a transmission test set to monitor the audio across the punchblock demarcation.
- Step 3. Initiate a Talkgroup Call from the console position.
- Step 4. Monitor audio traffic between the radio user and the console dispatcher on the test set.
- Step 5. Initiate a Talkgroup Call from RADIO-1 on TALKGROUP 1.
- Step 6. Monitor audio traffic between RADIO-1 and the console dispatcher on the test set.
- Step 7. Repeat Steps 2-6 for TALKGROUP 2.

Pass _____ Fail _____

Elite Console Features

Intercom Operation (Console to Console)

1. DESCRIPTION

The intercom function allows console operators to communicate with other console operator positions without using a radio resource.

Motorola will verify inter-zone operation of the Intercom feature by selecting and activating the CCW associated with the dedicated inter-zone intercom BIM.

SETUP

* Two consoles are required

VERSION #1.02

2. TEST

- Step 1. At the console press the "INTERCOM CALL" icon.
- Step 2. Choose the console to be called and press the SEND button.
- Step 3. Answer the call at the destination console by pressing the "INTERCOM CALL" icon and selecting ANSWER.
- Step 4. Verify communications between the two consoles. The answering console will have a hot microphone, and the sending console must press the lightning bolt in the Intercom Window to transmit.
- Step 5. End the intercom call by pressing the HANGUP icon on either console.

Pass ____ Fail ____

Elite Console Features

Console Enable / Disable

1. DESCRIPTION

In an Elite Operator configuration, the Supervisory console position may disable the non-supervisory positions. This will disable all transmit capability from the disabled console.

SETUP

* Two consoles are required

VERSION #1.05

2. TEST

- Step 1. Verify that Console 1 is set up as a Supervisor.
- Step 2. Transmit from the Console 2 (non-supervisory) and verify communication with RADIO-1.
- Step 3. Select the "Enable/Disable Op Position" button from the tool bar on the Supervisory console.
- Step 4. Disable Console 2.
- Step 5. Verify that the non-supervisory position is completely disabled from making a call.
- Step 6. Select the "Enable/Disable Op Position" button from the tool bar on the Supervisory console.
- Step 7. Enable Console 2.
- Step 8. Verify that the non-supervisory position is completely enabled.

Pass____ Fail____

Elite Console Features

Acoustic Crossmute

1. DESCRIPTION

Acoustic crossmuting means that selected operator positions will not hear outbound transmissions from operator positions they are cross-muted with.

This feature is used when operator positions are located in the same room.

The Acoustic Crossmute is configured in the system's Console Database Manager.

SETUP

* Two adjacent console positions monitoring the same talkgroup.

* Portable monitoring talkgroup

VERSION #1.06

2. TEST

- Step 1. Without an Acoustic Crossmute configured, and the select speakers of each operator position turned to maximum volume, transmit on Console 1.
- Step 2. Confirm feedback is heard on the operator positions and the portable hears feedback on the talkgroup.
- Step 3. With an Acoustic Crossmute configured, and the select speakers of each operator position turned to maximum volume, transmit on Console 1.
- Step 4. Verify no feedback is heard at either operator position and that the portable doesn't hear feedback on the talkgroup.

Pass _____ Fail _____

Elite Console Features

Public Address

1. DESCRIPTION

The Public Address (PA) can be accessed through a button on the tool bar of the Elite console. When the PA button is pressed, a relay closure and the microphone audio is routed to the PA board, which in turn is wired to a field installed PA system. These signals can be monitored using test equipment in the factory.

SETUP

* Connect a multi-meter capable of monitoring closures to the proper pins of the PA board.

* Connect audio monitoring equipment to the audio output of the PA board.

VERSION #1.03

2. TEST

- Step 1. Press the PA button on the toolbar of the Elite Console.
- Step 2. Verify the multi-meter displays a closure.
- Step 3. Speak into the microphone and verify that the audio is routed to the audio monitoring equipment.
- Step 4. Release the PA Button and verify the console has returned to normal operation.

Pass____ Fail____

System Management Tests

System Management Tests

FullVision Fault Management/Site Path Failure

1. DESCRIPTION

This test verifies that the FullVision (FV) event browser is able to capture information about various failures at the system and zone level.

This test simulates a microwave failure by removing a customer selected site data link and monitoring the alerts.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1

* RADIO-1 should be "Site Locked"

VERSION #1.03

2. TEST

- Step 1. Remove the T1 cable(s) to the site router(s) at the site where RADIO-1 is affiliated.
- Step 2. Observe the appropriate alert appears on the FV Event Browser.
- Step 3. Observe the color for the site turns from Green (normal) to Red (critical) on FV.
- Step 4. In addition, observe that the site is now in the Site Trunking mode.
- Step 5. Reconnect the T1 cable(s) disconnected in Step 1.
- Step 6. Observe the site returns to the Wide Area Trunking mode.
- Step 7. Observe the color for the site changes from Red (critical) to Green (normal) on FV.

Pass_____ Fail_____

System Management Tests

FullVision Fault Management/Ambassador Link Failure

1. DESCRIPTION

This test verifies that the FullVision (FV) event browser is able to capture information about various failures at the system and zone level.

This test simulates a failure by removing one of the links between the Ambassador and MGEG (Motorola Gold Elite Gateway). The alerts will be monitored on FV.

SETUP

No setup is required for this test.

VERSION #1.05

2. TEST

- Step 1. Remove one of the E1 connections from the MGEG line card.
- Step 2. Observe the appropriate alert indicating an Audio Switch slot failure appears on the FV Event Browser.
- Step 3. Observe the color for the associated AMB (Ambassador) slot turns from Green (normal) to Red (critical) on FV.
- Step 4. Replace the link removed in Step 1.
- Step 5. Observe an alert appears at the Manager and on FV indicating the module is restored to service.
- Step 6. Observe the color for the associated AMB slot turns back to Green (normal) on FV.

Pass____ Fail____

System Management Tests

FullVision Fault Management/InterZone Control Path Failure

1. DESCRIPTION

This test verifies that the FullVision (FV) event browser is able to capture information about various failures at the system and zone level.

This test simulates a failure by removing one of the InterZone links. The alerts will be monitored on FV.

NOTE: This feature only works on a multi-zone system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE in Zone 2

VERSION #1.06

2. TEST

- Step 1. Initiate a call with RADIO-1.
- Step 2. Observe that the call is received by both RADIO-2 and RADIO-3.
- Step 3. From any Network Manager workstation, disable a Control Router port to the Zone Controller in the Zone where RADIO-1 is affiliated. Or, disconnect a Control Router link from the Zone Controller in the Zone where RADIO-1 is affiliated.
- Step 4. Observe the color changes for the disconnected link from Green (normal - active) to Cyan (warning - connecting) on FV.
- Step 5. Initiate a call with RADIO-1.
- Step 6. Observe that the call is received by RADIO-2 and RADIO-3 verifying the system remains in interzone trunking since the interzone control paths are redundant.
- Step 7. Enable the Control Router port disabled in Step 3.
- Step 8. Observe the color changes to Green for reconnected link on FV.

Pass ___ Fail ___

System Management Tests

FullVision Fault Management/Station Power Amp Failure

1. DESCRIPTION

This test verifies that the FullVision (FV) event browser is able to capture information about various failures at the system and zone level.

A station will be keyed while the output is unloaded to simulate a power amp failure. The alerts will be monitored on FV.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 1

VERSION #1.06

2. TEST

- Step 1. Simulate a busy system by disabling all channels at SITE 1 with the exception of the control channel and one voice channel.
- Step 2. Verify that the power amp of the station to be tested shows up as Green (normal) on FullVision.
- Step 3. Disconnect the dummy load/antenna from the station.
- Step 4. Simultaneously key up both RADIO-1 and RADIO-2 momentarily.
- Step 5. Observe that an alert indicating a Power Amp failure appears on the FV Event Browser.
- Step 6. Observe the color for the Power Amp turns from Green (normal) to Red (Critical) on FV.
- Step 7. Reconnect the dummy load/antenna disconnected in Step 3.
- Step 8. In approximately 5 minutes, observe that an alert appears on FV indicating the module is restored to service.
- Step 9. Observe that the color for the Power Amp turns back to Green (normal) on FV.

Pass____ Fail____

System Management Tests

FullVision Fault Management/Core Router Failure

1. DESCRIPTION

This test verifies that the FullVision (FV) event browser is able to capture information about various failures at the system and zone level.

A Core Router will be turned off to simulate a failure. The alerts will be monitored on FV.

SETUP

No setup is required for this test.

VERSION #1.04

2. TEST

- Step 1. Verify that the RP Router to be tested shows up as Green (normal) on FullVision. The icon is on the RP Router Submap Window under the Zone Devices Submap for the Zone in which the router is located.
- Step 2. Power down a Core Router.
- Step 3. Observe that an alert indicating a Core Router failure appears on the FV Event Browser.
- Step 4. Observe the color for the Core Router turns from Green (normal) to Red (Critical) on FV.
- Step 5. Restore power to the Core Router.
- Step 6. Observe that an alert appears on FV indicating the Core Router is Enabling.
- Step 7. Observe that the color for the Core Router turns Cyan (warning) on FV.
- Step 8. Observe that an alert appears on FV indicating the Core Router is Enabled.
- Step 9. Observe that the color for the Core Router turns back to Green (normal) on FV.

Pass _____ Fail _____

System Management Tests

Fault Management: Current Status and Diagnostics

1. DESCRIPTION

This test verifies that the Zone Manager can change the trunking state of a site and the status shows up on FullVision. To accomplish this, the current state of a site will be displayed and using Diagnostics, it will be forced into site trunking and back again.

SETUP

Click on the Quick Status Symbol for the Zone with the site to be tested. Click on the appropriate Site Icon to bring up the Alarm browser.

VERSION #1.01

2. TEST

- Step 1. Through the Zone Manager, choose a zone and select the site type to be disabled.
- Step 2. Choose a site to be placed into Site Trunking by left clicking the mouse on the site name.
- Step 3. Put the site into Site Trunking by right clicking the mouse, selecting diagnostics and selecting "Site Trunking".
- Step 4. Observe that the FullVision Alarm Browser shows that the site is now in Site Trunking and is User Requested.
- Step 5. Place the site back into Wide Area Trunking by right clicking the mouse, selecting diagnostics and selecting "Wide Trunking".
- Step 6. Observe that the FullVision Alarm Browser now shows Wide Area Trunking.
- Step 7. Close the open windows.

Pass____ Fail____

System Management Tests

ZoneWatch

1. DESCRIPTION

ZoneWatch is an administration tool for monitoring radio traffic on a system. A system manager can use ZoneWatch to analyze traffic patterns for load distribution and troubleshoot radio and site problems. ZoneWatch is used to view current radio traffic activity for the system. This activity is displayed in graphical format, color-coded for easy identification of the type of activity occurring on the system.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - SITE 3
RADIO-4 - TALKGROUP 1
RADIO-4 - SITE - SITE 4

VERSION #1.02

2. TEST

- Step 1. Set up the Zone Watch Window Definitions and Watch Profile through the User Configuration Manager to allow Multi-Site Scroll and Grid Display.
- Step 2. From the PC Application Launcher, select a zone folder.
- Step 3. From within that zone, select ZoneWatch.
- Step 4. Select the profile created in the Setup procedure.
- Step 5. Initiate several calls with the radios and observe that the appropriate channel usage information is displayed.

Pass ____ Fail ____

System Management Tests

Configuration Management - Subscriber Capabilities

1. DESCRIPTION

The User Configuration Manager (UCM) controls the parameters for all radio users and dispatchers on the system.

Within the Subscriber section, the Radio User Configuration Window enables the network manager to tailor ASTRO 25 subscribers' capabilities. Multigroup, Secure, Call Alert, Private Call, and Telephone Interconnect are some of the features that can be enabled or disabled. The features that could be unique to the particular user are configured directly in the Radio User Configuration Window. The features that could be configured the same for a group of users are placed into records called profiles. The network manager references the profile which contains the desired setup for these features from the Radio User Configuration Window.

NOTE: The Radio Configuration Window must be completed before the Radio User Configuration Window because the serial number and unit ID information for each subscriber resides in the Radio Configuration Window. A profile must already exist to be referenced but can be modified later if needed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

* Flag both radios to be capable of Call Alert, Private Call, and Dispatch Calls.

* Set the "User Enabled" flag to YES for both RADIO-1 and RADIO-2.

VERSION #1.03

2. TEST

- Step 1. Initiate a Call Alert from RADIO-1 to RADIO-2. Verify that RADIO-2 receives the Call Alert.
- Step 2. Change the Call Alert Enabled flag to NO for RADIO-1 via the Network Manager.
- Step 3. Initiate a Call Alert from RADIO-2 to RADIO-1. Verify that RADIO-2 receives a reject when attempting to Call Alert RADIO-1.
- Step 4. Change the Call Alert Enabled flag back to YES for RADIO-1 via the Network Manager.
- Step 5. Initiate a Call Alert from RADIO-2 to RADIO-1. Verify that RADIO-1 now receives the Call Alert.
- Step 6. Initiate a Private Call from RADIO-1 to RADIO-2. Verify that RADIO-2 receives the Private Call.
- Step 7. Change the Private Call Enabled flag to NO for RADIO-1 via the Network Manager.
- Step 8. Initiate a Private Call from RADIO-2 to RADIO-1. Verify that RADIO-2 receives a reject when attempting to Private Call RADIO-1.
- Step 9. Change the Private Call Enabled flag back to YES for RADIO-1 via the Network Manager.
- Step 10. Initiate a Private Call from RADIO-2 to RADIO-1. Verify that RADIO-1 now receives the Private Call.

Pass _____ Fail _____

System Management Tests

Configuration Management - Talkgroup Capabilities

1. DESCRIPTION

The User Configuration Manager (UCM) controls the parameters for all radio users and dispatchers on the system.

Within the Subscriber section, the Talkgroup Configuration Window enables the network manager to tailor ASTRO 25 Talkgroup Capabilities. Emergency, Secure and Priority Monitor are some of the features that can be enabled or disabled. The features that could be unique to the particular user are configured directly in the Talkgroup Configuration Window. The features that could be configured the same for a group of users are placed into records called profiles. The network manager references the profile which contains the desired setup for these features from the Talkgroup Configuration Window.

NOTE: A profile must already exist to be referenced through the Talkgroup Configuration Window but can be modified later if needed.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

* Set the "Group Enabled" flag to YES for TALKGROUP 1 in the UCM.

VERSION #1.03

2. TEST

- Step 1. Initiate a call from RADIO-1 on TALKGROUP 1. Verify that RADIO-2 hears the RADIO-1 audio.
- Step 2. Change the Group Enabled flag to NO for TALKGROUP 1 via the UCM.
- Step 3. Initiate a call from RADIO-1 or RADIO-2 on TALKGROUP 1. Verify that neither radio can initiate a call because of the change in status of the Group Enabled Flag of TALKGROUP 1.
- Step 4. Initiate an Emergency call from RADIO-1. Verify that both the console and RADIO-2 can hear the transmission.
- Step 5. Dekey RADIO-1.
- Step 6. Change the Group Enabled flag back to YES for TALKGROUP 1 via the UCM.
- Step 7. Initiate a call from RADIO-1 on TALKGROUP 1. Verify that both the console and RADIO-2 hear RADIO-1.

Pass____ Fail____

System Management Tests

Configuration Management - Access Permissions

1. DESCRIPTION

The Radio System Infrastructure Configuration Management section of the Zone Configuration Manager (ZCM) application sets the parameters for each of the system devices in the ASTRO 25 system.

Configuration parameters such as Individual and Talkgroup Default Access Permission, and Site Access Denial Type can be manipulated from the Zone Configuration Window.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1.06

2. TEST

- Step 1. Delete the database record for RADIO-1 in both the Radio and Radio User Configuration Windows so that the ASTRO 25 system does not have any knowledge of RADIO-1.
- Step 2. Set the "Individual Default Access Permission" flag to NO in the Zone Configuration Window.
- Step 3. Initiate a call from RADIO-1 on TALKGROUP 1. Verify that the ASTRO 25 system rejects the RADIO-1 call request because RADIO-1 has not been defined in the ASTRO 25 Radio User database.
- Step 4. Change the Individual Default Access Permission flag to YES via the Network Manager.
- Step 5. Initiate a call from RADIO-1. Verify that the ASTRO 25 system permits the RADIO-1 call request because the system grants radio access using default settings.
- Step 6. Configure the RADIO-1 records that were automatically created in the Radio and Radio User Configuration Windows as a result of the radio's PTT.
- Step 7. Reset the "Individual Default Access Permission" flag to NO in the Zone Configuration Window.
- Step 8. Initiate a call from RADIO-1. Verify that the ASTRO 25 system permits the RADIO-1 call request because the RADIO-1 is now a valid user.

Pass _____ Fail _____

System Management Tests

Configuration Management - General Timeout Parameters

1. DESCRIPTION

The Radio System Infrastructure Configuration Management section of the Zone Configuration Manager (ZCM) application sets the parameters for each of the system devices in the ASTRO 25 system.

Within the Radio System Infrastructure section, the Zone Configuration Window enables the network manager to tailor the general timeout and call parameters for each zone in the ASTRO 25 system.

System and call timeout parameters such as Carrier, Message Trunk, Fade, Dispatch Call, and Emergency Call can also be manipulated from the Zone Configuration Window.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

VERSION #1.05

2. TEST

- Step 1. Set the "Private Call Maximum Call Duration," in the System settings of the UCM, to be 1 minute.
- Step 2. Initiate a Private Call from RADIO-1 to RADIO-2. Keep the Private Call active.
- Step 3. Verify that after one minute elapses, the system disconnects the Private Call because the maximum call duration has been exceeded.
- Step 4. Reset the Private Call Maximum Call Duration setting to be 10 minutes.
- Step 5. Repeat steps 1 through 4 for testing Carrier, Message Trunk, Fade, Dispatch Call, and Emergency Call.

Pass ____ Fail ____

Report Generation Tests

Report Generation Tests

Historical Reports

1. DESCRIPTION

Performance reports can be created automatically for dynamic statistical information about the air traffic activity on the system. These reports provide assistance with system management, resource planning, usage allocation, and monitoring. All reports are preformatted and summarize air traffic activity for a configured time span.

SETUP

No prior setup is required for this test.

VERSION #1.07

2. TEST

- Step 1. From the PC Application Launcher, select a zone.
- Step 2. From that zone's menu, choose Zone Historical Reports.
- Step 3. From the Historical Reports Player window that opens, select a report.
- Step 4. Using the left mouse button, click on the view button.
- Step 5. Observe a window opens allowing a user enter report parameters.
- Step 6. Enter all desired data for the report and Generate Report.
- Step 7. Observe a window appears showing the requested report.
- Step 8. Close the report window.
- Step 9. Run the following reports during testing:
Talkgroup at Zone Summary; Radio User at Zone Summary; Site Summary.

Pass____ Fail____

Report Generation Tests

Zone Configuration Manager Reports: Infrastructure

1. DESCRIPTION

The Zone Configuration Manager report window allow the user to generate data summaries to view information from the database in a Web browser or to export the information as a file. The Zone Configuration Manager report window shows the users all of the fields that can be included in the report. By selecting which fields are wanted in the report and entering selection criteria for each field, the user can restrict the data that is retrieved.

SETUP

No prior setup is required for this test.

VERSION #1.06

2. TEST

- Step 1. From the PC Application Launcher, select a zone.
- Step 2. From that zone's menu, select Zone Configuration Manager.
- Step 3. Navigate through the folders on the left side to the object for which a report is to be generated.
- Step 4. Under the toolbar FILE pulldown menu, select Reports.
- Step 5. Observe a window opens allowing a user to create a report.
- Step 6. Enter sorting data for the report and click Generate Report.
- Step 7. Observe a window appears showing the requested report.
- Step 8. Close the report window.
- Step 9. Run one or all of the following reports: MEGEG Application; Zone Controller Configuration; Core RP (Rendezvous Point) Router.

Pass _____ Fail _____

Report Generation Tests

User Configuration Subsystem (UCM) Reports

1. DESCRIPTION

The User Configuration Manager report window allow the user to generate data summaries to view information from the database in a Web browser or to export the information as a file. The User Configuration Manager report window shows the users all of the fields that can be included in the report. By selecting which fields are wanted in the report and entering selection criteria for each field, the user can restrict the data that is retrieved.

SETUP

No prior setup is required for this test.

VERSION #1.04

2. TEST

- Step 1. From the PC Application Launcher, select User Configuration Manager.
- Step 2. Click on the appropriate folder to list its contents if it is not already open.
- Step 3. Select the object for which a report is to be generated.
- Step 4. Under the toolbar FILE pulldown menu, select Reports.
- Step 5. Observe a window opens allowing a user to create a report.
- Step 6. Enter all sorting data for the report and click Generate Report.
- Step 7. Observe a window appears showing the requested report.
- Step 8. Close the report window.
- Step 9. Reports available to an operator under the UCM User Configuration Reports section are arranged in three categories: Subscribers, Security and System Configuration. Run the following reports : Under Subscribers folder, select Radio User; Under Security, select User; Under System Configuration , select System.

Pass____ Fail____

Radio Control Manager (RCM) Tests

Radio Control Manager (RCM) Tests

Emergency Alarm Display

1. DESCRIPTION

The emergency call information that is displayed on the ASTRO 25 RCM includes the radio alias of the radio that initiated the Emergency Alarm, the talkgroup that the radio was affiliated to at the time the alarm was sent, and the time the alarm was received.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 2
RADIO-2 - SITE - SITE 2

VERSION #1.04

2. TEST

- Step 1. Open the Radio Control Manager (RCM) windows and verify that the Emergency Alarm window is visible. If it is not, go the View menu and select it bringing it into the RCM viewable area.
- Step 2. Initiate an Emergency Alarm from RADIO-1.
- Step 3. Observe that the RCM receives the Emergency Alarm.
- Step 4. Acknowledge the Emergency by selecting the Emergency in the window and clicking on the Respond button.
- Step 5. Again select the displayed Emergency and click the Delete button to clear the emergency.
- Step 6. Reset the radio by holding the Emergency button until the radio clears.
- Step 7. Repeat Steps 1-6 using RADIO-2.

Pass____ Fail____

Radio Control Manager (RCM) Tests

Dynamic Regrouping

1. DESCRIPTION

Dynamic Regrouping allows the RCM to assign individual radios operating in different talkgroups to a temporary talkgroup via the Regroup command. Network managers or supervisors can override individual radio talkgroup selections by steering regrouped subscribers to a new talkgroup containing users which need to communicate on a temporary basis. After receiving a Regroup command, a radio will ignore the current setting of the talkgroup selector and move to the target talkgroup specified in the Regroup command. Unless the supervisor issues a LOCK command, the radio user can deselect the target talkgroup by selecting another talkgroup using the radio selector. A unique location on the radio selector is reserved for the target talkgroup following a Regroup command.

Regrouped radios receiving a second Regroup command will move to the new target talkgroup specified in the second command. When a regrouped radio receives a Regroup command, all information pertaining to the previous Regroup command is lost. A Cancel Regroup command or a Revert returns an individual radio to its normal operation.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 3
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 4

VERSION #1.03

2. TEST

- Step 1. With the RCM open from the Commands menu item select the Radio Commands item to open the command window.
- Step 2. Enter TALKGROUP 3 in the target field.
- Step 3. Enter the IDs or aliases of RADIO-1, RADIO-2, RADIO-3 and RADIO-4.
- Step 4. Once all desired radio information is entered and appears in the command window click the Regroup button to initiate the command.
- Step 5. Observe all radios are regrouped and are able to communicate on TALKGROUP 3.
- Step 6. Switch the Subscriber to the Dynamic Regroup channel to acknowledge the group request.
- Step 7. Observe that the radios are able to select different talkgroups and are not locked onto the regrouped mode. Note- The Talkgroup selector knob has to be set to the dynamic regroup position before switching to any other talkgroup.
- Step 8. Observe that the Regroup task appears in the Command Monitor window.
- Step 9. Issue a Selector Lock command all four radios and verify their selectors have been locked.
- Step 10. Revert both commands and verify the radios have returned to normal operation.

Pass____ Fail____

Radio Control Manager (RCM) Tests

Storm Plans

1. DESCRIPTION

Storm Plans represent any number of preprogrammed Dynamic Regrouping combinations constructed in advance to anticipate a unique need, such as a disaster, or to make a needed adjustment for an infrequent yet repeated event, like a parade or election. When implemented, a Storm Plan will automatically assign individual radios operating in different talkgroups to a temporary talkgroups, containing the radios specified by the stored Dynamic Regrouping command. Storm Plans are deactivated by selecting the revert option in the Command window.

Note - Radios are not required to be locked to a specific site for this test.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 3
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 4

Create a storm plan in the UCM that regroups RADIO-1 and RADIO-2 to TALKGROUP 2.

VERSION #1.02

2. TEST

- Step 1. With the RCM open from the Commands menu item select the Storm Plan item to open the Storm Plan Window.
- Step 2. Select the Storm Plan.
- Step 3. Click on OK or Apply to invoke the Storm Plan.
- Step 4. Observe that the Storm Plan appears in the Command Monitor window.
- Step 5. Observe RADIO-1 and RADIO-2 are regrouped.
- Step 6. Initiate a call from RADIO-1.
- Step 7. Observe that RADIO-2, RADIO-3 and RADIO-4 are able to communicate with one another.
- Step 8. Un-regroup the radios by selecting the task in the Command Monitor window and clicking on the Revert button to submit the task.
- Step 9. Observe that the regrouping of the radios is now dissolved.

Pass _____ Fail _____

Radio Control Manager (RCM) Tests

Selective Radio Inhibit

1. DESCRIPTION

The INHIBIT command issued by the RCM disables a radio, preventing it from transmitting or receiving any audio. All of the radio's functionality ceases while a radio is inhibited by the ASTRO 25 RCM. Once inhibited, the radio cannot be used to monitor voice channels or for any other radio user initiated activity. Note that an inhibited radio still monitors the control channel so that it can be re-enabled with the Cancel Inhibit command. Upon receiving the Cancel Inhibit command from the SZ RCM, the radio returns to its normal operation.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1

VERSION #1.03

2. TEST

- Step 1. Select the Commands menu and then select the Radio Commands item in the menu to open the Command Window.
- Step 2. Enter the IDs or aliases of RADIO-1.
- Step 3. Once all desired radio information is entered and appears in the command window click the Inhibit button to initiate the command.
- Step 4. Observe RADIO-1 is inhibited and appears to be dead.
- Step 5. Observe that the Inhibit task appears in the Command Monitor window.
- Step 6. Cancel the Inhibit by selecting the task in the Command Monitor window and clicking the Revert button to submit the task.
- Step 7. Observe that the Cancel Inhibit task appears in the Command Monitor window and that RADIO-1 is returned to normal operation.

Pass____ Fail____

Radio Control Manager (RCM) Tests

Radio Check

1. DESCRIPTION

Radio Check is a RCM command used to verify that a radio is active in the trunking system. The Radio Check command causes the Zone Controller to poll for the radio requesting that the radio re-affiliate. When the radio re-affiliates, the RCM then has the knowledge that the radio is powered on and within system range. If the radio is involved in a conversation, whether group or interconnect, the RCM application displays a message to that effect. The information displayed by the RCM in response to the Radio Check command is: current talkgroup affiliation, the multigroup that the talkgroup is attached to (assuming the talkgroup belongs to a multigroup), and the site where the radio is affiliated. If the radio does not respond to the Radio Check command, a message to that effect displays.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

VERSION #1.04

2. TEST

- Step 1. Select the Command menu and then select the Radio Check item to open the Radio Check window.
- Step 2. Enter the IDs or aliases of RADIO-2 into the entry box and click the Apply button.
- Step 3. Observe the radio is polled and the current radio information is displayed on the RCM.
- Step 4. Turn off RADIO-1.
- Step 5. Enter the ID or alias of the RADIO-1 into the entry box and click the Apply button.
- Step 6. Observe that the RCM displays "Radio Not Found."
- Step 7. Depress and hold the PTT button of RADIO-2 until instructed to release.
- Step 8. Enter the ID or alias of RADIO-2 into the entry box and click the Apply button. Observe that a busy for the radio is displayed on the RCM.
- Step 9. Release the PTT button on RADIO-2.
- Step 10. Observe the radio is polled and the current radio information is displayed on the RCM.

Pass ___ Fail ___

Radio Control Manager (RCM) Tests

Radio Snapshot

1. DESCRIPTION

Snapshot is a RCM command used to retrieve information about an individual radio. Information provided by the RCM application in response to the Snapshot command includes: the serial number of the radio, current talkgroup/multigroup and site affiliations; the Regroup, Inhibit, and Selector Lock state of the radio. Snapshot information is taken from the system databases. The Snapshot command does not initiate any communication with the target radio.

Note - Radios are not required to be locked to a specific site for this test.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 3

VERSION #1.03

2. TEST

- Step 1. Submit a Dynamic Regroup command for RADIO-1 and RADIO-3 to be regrouped to TALKGROUP 3.
- Step 2. At the RCM, initiate the Snapshot command for RADIO-1.
- Step 3. Verify that the dispatcher terminal shows RADIO-1 affiliated to SITE 1 and that its current Regroup state is "Regroup."
- Step 4. At the RCM, revert the dynamic regrouping on RADIO-1 and RADIO-3.
- Step 5. Initiate the Snapshot command for RADIO-1.
- Step 6. Verify RADIO-1 shows an affiliation to SITE 1 and that its current Regroup state is "Cancel Regroup."
- Step 7. At the RCM, inhibit RADIO-2 and then initiate the Snapshot command for RADIO-2.
- Step 8. Verify RADIO-2 shows an affiliation to SITE 2 and that its current Inhibit state is "Selective Inhibit."
- Step 9. At the RCM, revert RADIO-2 and then initiate the Snapshot command for RADIO-2.
- Step 10. Verify RADIO-2 shows an affiliation to SITE 2 and that its current Inhibit state is "Cancel Inhibit."

Pass____ Fail____

Radio Control Manager (RCM) Tests

Radio Status

1. DESCRIPTION

This optional feature allows the Radio Console Manager to view status information sent in by subscribers. Statuses are used to indicate the Radio operator's operational state (e.g. off duty). The information that will be displayed includes the radio alias, talkgroup alias, hour and minute time stamp, status number or message number, and the customer entered translation for the specific status. Status input is displayed in chronological order, independent of the type of status number.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1

* Configure RADIO-1 in the manager to use a particular status set.

* Configure the assigned status set (via the status set manager configuration objects) to include text translations for a few different statuses.

* The RCM user needs to be assigned the dispatch attachment group that matches the radio user's assigned dispatch attachment group.

VERSION #1.02

2. TEST

- Step 1. Initiate a Status transmission from RADIO-1.
- Step 2. Verify the RCM displays the proper Status text.

Pass _____ Fail _____

System Reliability Features

System Reliability Features

AEB to CEB Redundant Link Failure

1. DESCRIPTION

Communication between the AEB (Ambassador Electronics Bank) and each CEB (Central Electronics Bank) can take place over dedicated redundant links. The two links between the AEB and a CEB operate in a hot/standby mode. The system will continue uninterrupted if the main link fails.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1

* Select a CEB with redundant links to the AEB.

* The CEB must have at least one console operator position capable of monitoring TALKGROUP 1.

VERSION #1.02

2. TEST

- Step 1. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1.
- Step 2. Observe that RADIO-2 and the selected console are able to monitor and respond to the call.
- Step 3. Remove the RJ45 AIMI (Ambassador Interface- Mux Interface) link connection between the AEB and the CEB.
- Step 4. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1.
- Step 5. Observe that RADIO-2 and the selected console are able to monitor and respond to the call.
- Step 6. Replace the link connection previously removed in Step 3.
- Step 7. Repeat the above steps for the other AEB to CEB redundant link.

Pass____ **Fail**____

System Reliability Features

AEB to Zone Controller Redundant Link Failure

1. DESCRIPTION

This test verifies that the two communication paths between the Zone Controller and audio switch are hot standby and the system will continue uninterrupted if the main path fails. To accomplish this, each ZAMBI (Zone Ambassador) link in the AEB Ambassador Electronics Bank) will be disconnected individually while verifying that the system remains operational.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 2
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 3

VERSION #1.04

2. TEST

- Step 1. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1.
- Step 2. Observe that only RADIO-2 and the console will be able to monitor and respond to the call.
- Step 3. Initiate a Talkgroup Call with RADIO-3 on TALKGROUP 2.
- Step 4. Observe that only RADIO-4 and the console will be able to monitor and respond to the call.
- Step 5. Remove one of the active ZAMBI cards from the AEB, this will simulate a Zone Controller to AEB Link failure.
- Step 6. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1.
- Step 7. Observe that only RADIO-2 and the console will again be able to monitor and respond to the call.
- Step 8. Initiate a Talkgroup Call with RADIO-3 in TALKGROUP 2.
- Step 9. Observe that only RADIO-4 and the console will again be able to monitor and respond to the call.
- Step 10. Replace the ZAMBI card removed previously in Step 5. Repeat the above steps for the other Zone Controller to AEB link.

Pass____ Fail____

System Reliability Features

Multiple Control Channels

1. DESCRIPTION

A maximum of four channels are eligible for assignment as control channel in each site. In the event that the assigned control channel fails at any remote site, the Zone Controller automatically selects one of the other control capable channels as the active control channel for that site. A Control Channel Preference Level can be used to rank the control capable channels where 1 is the highest ranking and 4 is the lowest.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 2

VERSION #1.03

2. TEST

- Step 1. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1.
- Step 2. Observe that only RADIO-2 will be able to monitor and respond to the call.
- Step 3. Initiate a Talkgroup Call with RADIO-3 on TALKGROUP 2.
- Step 4. Observe that only RADIO-4 will be able to monitor and respond to the call.
- Step 5. Disable the control channel at SITE 1.
- Step 6. Observe that the control channel rotates to the next available channel capable of acting as a control channel.
- Step 7. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1.
- Step 8. Observe that only RADIO-2 will be able to monitor and respond to the call.
- Step 9. Initiate a Talkgroup Call with RADIO-3 on TALKGROUP 2.
- Step 10. Observe that only RADIO-4 will be able to monitor and respond to the call. Enable the channel previously disabled in Step 5.

Pass ___ Fail ___

System Reliability Features

Subsystem Failsoft

1. DESCRIPTION

Failure of all control channels, failure of all voice channels, or failure of the subsystem or site controller will cause a Zone subsystem to enter failsoft operations. Subscribers can be programmed to operate in failsoft by talkgroup; to search its list of control channel frequencies in failsoft; or to disable failsoft altogether. When a system enters failsoft, a radio programmed for failsoft by talkgroup will first look for a specific failsoft channel dictated by the selected talkgroup. Since many systems have different frequencies across sites, if the radio is unable to find the talkgroup's failsoft channel the radio will instead operate in the control channel search failsoft mode. A radio programmed or needing to search control channels for failsoft frequencies will lock onto the first control channel in its control channel list.

Note that radios should not be site locked when in failsoft mode as the radio will not check the full list of 64 control channels programmed into the radio's code plug. All radios should be programmed to have the same sequence of control channel frequencies.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 1
RADIO-3 - TALKGROUP 2
RADIO-3 - SITE - SITE 1
RADIO-4 - TALKGROUP 2
RADIO-4 - SITE - SITE 1

* Program the Radios for failsoft operation by talkgroup. TALKGROUP 1 should use a different channel for failsoft than TALKGROUP 2 and neither should be a control channel.

* Turn off all subsystems except the subsystem under test.

2. TEST

- Step 1. Using the Zone Configuration Manager, place the subsystem into failsoft mode.
- Step 2. Verify that the Radios emits a failsoft tone approximately once every ten seconds.
- Step 3. Initiate a Talkgroup Call from RADIO-1 while in failsoft mode.
- Step 4. Verify that only RADIO-2 can hear RADIO-1.
- Step 5. Dekey RADIO-1 and disable the failsoft channel associated with TALKGROUP 1.
- Step 6. Key RADIO-1 and verify RADIO-2 can still monitor the call but the other radios cannot.
- Step 7. Dekey RADIO-1 and initiate a Talkgroup Call from RADIO-3.
- Step 8. Verify that only RADIO-4 can hear RADIO-3.

Pass____ Fail____

VERSION #1.04

System Reliability Features

Base Station Identification

1. DESCRIPTION

This test verifies that the repeaters programmed for BSI operation at every site broadcasts the FCC Base Station Identification (BSI) every 30 minutes. To accomplish this, a service monitor will be set up to monitor the BSI channel of a random site and note that the Morse Code is heard.

SETUP

A service monitor will be required to perform this test.

VERSION #1.01

2. TEST

- Step 1. Choose one site to test for Base Station Identification.
- Step 2. Set up the service monitor to receive the frequency of the BSI channel for the particular site.
- Step 3. Monitor the service monitor until the system ID is broadcast.

Pass _____ Fail _____

System Reliability Features

Redundant Zone Controller Switching/User Initiated Switchover

1. DESCRIPTION

The Zone Controller subsystem uses two Zone Controllers in a redundant configuration. The backup Zone Controller is made active either upon the loss of the active ZC or upon a user-initiated command from the Zone Configuration Manager.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - Site in Another Zone

* Set the Failure Random Holdoff Time (FRHOT) setting in the Zone Configuration Manager to 1 minute.

VERSION #1.02

2. TEST

- Step 1. Verify in the Zone Configuration Manager (ZCM) that the switchover mode is user-initiated.
- Step 2. Switch the Zone Controllers from the ZCM.
- Step 3. Verify that the backup Zone Controller becomes active and brings all sites back in wide area operations. Wait for the Radios to settle out the site affiliations.
- Step 4. Verify radio 1, radio 2 is affiliated with different sites. Verify radio 3 is affiliated with a site in a different zone. Key RADIO-1 and verify that RADIO-2 and RADIO-3 hear the audio.
- Step 5. End the call from RADIO-1.

Pass ____ Fail ____

System Reliability Features

Redundant Zone Controller Switching/Automatic Switchover

1. DESCRIPTION

The Zone Controller subsystem uses two Zone Controllers in a redundant configuration. The backup Zone Controller is made active either upon the loss of the active ZC or upon a user-initiated command from the Zone Configuration Manager.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2
RADIO-3 - TALKGROUP 1
RADIO-3 - SITE - Site in Another Zone

* Set the Failure Random Holdoff Time (FRHOT) setting in the Zone Configuration Manager to 1 minute.

VERSION #1.02

2. TEST

- Step 1. Set the switchover mode to automatic through the ZCM.
- Step 2. Disable the active Zone Controller via the ZCM diagnostic.
- Step 3. Verify that the backup Zone Controller becomes active and brings all sites back in wide area operations. Wait for the Radios to settle out the site affiliations.
- Step 4. Verify radio 1, radio 2 is affiliated with different sites. Verify radio 3 is affiliated with a site in a different zone. Key RADIO-1 and verifying that RADIO-2 and RADIO-3 hear the audio.
- Step 5. End the call from RADIO-1.

Pass _____ Fail _____

System Reliability Features

WAN Switch CPU Card Failure

1. DESCRIPTION

The WAN switch is equipped with redundant CPU cards, failure of the active or standby will have no effect upon the system. The WAN switch is equipped with redundant CPU cards located in Slots 0 and 15. Either card can be in the active or standby mode. Upon normal operation the switch comes up and the CPU in slot 0 becomes active. In the event of failure the active CPU, slot 15 takes over and becomes active. Upon recovery, the CPU in slot 0 will come up in standby mode and slot 15 will continue to be the active CPU unless it is switched manually to slot 0 or through software. During switchovers between CPU cards, traffic is not affected.

NOTE: This test will cause the Nortel to reboot. All sites will be in Site Trunking during this time.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-2 - SITE - SITE 2

VERSION #1.04

2. TEST

- Step 1. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1.
- Step 2. Observe that RADIO-2 is able to monitor and respond to the call.
- Step 3. Pull the ethernet connection to the active CPU card from the WAN switch in Zone 1.
- Step 4. After the system returns to Wide Area, initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1.
- Step 5. Observe that RADIO-2 is able to monitor and respond to the call.
- Step 6. Verify that FV reports loss of WAN switch CPU in the Alarm Browser.
- Step 7. Reinsert the CPU card from Step 3.

Pass _____ Fail _____

System Reliability Features

Supervisor Module within the Ethernet switch Failure

1. DESCRIPTION

With the high availability feature enabled on the switch, the fail over from the primary to the redundant supervisor card will take place in under 3 seconds. NM users should remain logged in and be unaware of the failure. If fail over takes place in under 1.5 seconds, there is little or no effect on calls in progress, call requests may be delayed by 1 - 2 seconds however. For failures greater than 1.5 seconds but less than 2 seconds, 1 ZC-SCP and 1 IZCP will be lost, sites stay in WA trunking and zone remains in IZ trunking. All MGEs will be lost as Netcom fails and it will take an additional 30 seconds until ZC-MGEG CP recovery timer expires before MGEs will be back in service. Routers will not switch TLANS as Ethernet ports are still considered up.

Two radios are required to perform this test (Radios 1 and 2). Radio 1 should be affiliated at Site 1 and Radio 2 should be affiliated at Site 2. Site 1 and Site 2 may be located in the same or different Zones. Set Radios 1 and 2 to Talkgroup 1.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1
RADIO-2 - TALKGROUP 1
RADIO-1 - SITE - SITE 2

VERSION #1.01

2. TEST

- Step 1. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1.
- Step 2. Verify that all sites are in Wide Area trunking.
- Step 3. Reset active supervisor module on Ethernet switch.
- Step 4. Initiate a Talkgroup Call with RADIO-1 on TALKGROUP 1.
- Step 5. Observe that RADIO-2 is able to monitor and respond to the call.
- Step 6. Verify that all sites are still in Wide Area trunking.

Pass _____ Fail _____

System Reliability Features

Receiver Interference Shutdown

1. DESCRIPTION

Receiver interference occurs when a repeater receives an unauthorized signal. In order to prevent a disruption of communications, the affected channel will be disabled and removed from the system's pool of available channel resources when the undesired carrier is detected for longer than the specified time-out period. Once the interfering carrier disappears, the channel is returned to service within approximately 5 minutes. The channel is then enabled.

SETUP

Set the Carrier Malfunction Timer through the Zone Configuration Manager to 5 seconds.

VERSION #1.02

2. TEST

- Step 1. Using a service monitor, transmit a 1 kHz tone at the receive frequency of any repeater.
- Step 2. Verify the channel is removed from the selection/assignment process.
- Step 3. Continue to transmit the 1 kHz tone until the controller removes the channel from service (timer is configurable at the Site level through the Carrier Malfunction Time parameter).
- Step 4. From FullVision, verify channel malfunction due to interfering carrier is indicated.
- Step 5. Remove the interfering signal. Verify the Channel is returned to service within five minutes and that FullVision indicates that the channel is now enabled.
- Step 6. Return the Carrier Malfunction Timer to the desired system value.

Pass____ Fail____

System Reliability Features

Transmitter Power Failure Shutdown

1. DESCRIPTION

The repeaters can detect a loss or decrease in transmitter output power of all trunked repeaters connected to it. Each trunked repeater contains an internal wattmeter element. Once the forward power has decreased past the threshold set, the repeater instructs the Zone Controller to take the channel out of service. If reflected power increases past the threshold set, the repeater will also instruct the Zone Controller to take the channel out of service.

SETUP

RADIO-1 - TALKGROUP 1
RADIO-1 - SITE - SITE 1

VERSION #1.03

2. TEST

- Step 1. Disconnect the transmit antenna connection to trunked repeater 1. (This will cause a high VSWR condition)
- Step 2. Key RADIO-1 so that channel 1 is assigned, and verify that the channel disables. Verify that this alarm is reported at the Zone Manager.
- Step 3. Restore the transmit antenna connection to trunked repeater 1.
- Step 4. Verify that the channel is put back into service by the Zone Manager within five minutes.
- Step 5. Verify that decreasing the transmitter power will cause transmitter shutdown.

Pass _____ Fail _____

System Reliability Features

Station Failure

1. DESCRIPTION

When a base station repeater at one site fails due to hardware problems, the pending call is lost and the trunking controllers removes the channel from service system wide. This failure can be created by powering down one base station repeater.

SETUP

No set up required.

VERSION #1.02

2. TEST

- Step 1. Power down a voice repeater for any voice channel at one remote site.
- Step 2. Press PTT on a radio several times to step through all available voice channels.
- Step 3. Verify that the disabled channel is not used.

Pass____ Fail____

MOSCAD Fault Management System

MOSCAD Fault Management System

Screen Navigation

1. DESCRIPTION

All MOSCAD alarming tests shall be conducted from the MOSCAD server. The alarms demonstrated are to be made on the actual equipment or punchblock interface, with an exception made for cases where it is not practical to create an actual alarm. The following will provide a brief introduction and description of the main display screens encountered when navigating the MOSCAD GUI (Graphic User Interface).

Login and Password Screen -

This is the first screen displayed after a system startup. It allows a user with the proper login and password to access the MOSCAD alarm system. For system testing the "Login Name" is Administrator and the "Login Password" is Wonderware.

Main Screen -

The "Main" screen contains site name buttons with color status bullets adjacent to the site name buttons. Details of a particular site can be viewed by selecting the site name of interest. If there is an unacknowledged alarm within any given site(s), the color bullet will flash in red and yellow.

Comm Screens -

From the "Main" screen access the "comm" screen tab. The "comm" screen displays unique CPU ID's and communication statuses for each MOSCAD CPU in the system. Should the communications path between the IP Gateway and any CPU in the system be interrupted, it will be indicated by an alarm present on this screen.

Alarm Summary Screens -

Proceed to the Alarm Summary Screen from the "Main" screen. The Alarm Summary Screen provides a text display of all alarms currently present in the system. On this screen, you can select between the alarm summary detail and the alarm history detail by activating the "Alarm Summary / Alarm History"

button. Additionally, the display can be filtered to show only alarms based on site name or acknowledgement status.

Device Monitoring

From the "Main" screen, navigate to each site monitored by MOSCAD in the system. Once a particular site bullet has been selected, a site overview screen will appear that indicates the types and quantities of devices monitored by MOSCAD at that site.

VERSION #1

Pass____ Fail____

MOSCAD Fault Management System

Alarm Processing - Acknowledged Alarm

1. DESCRIPTION

This segment of the test verifies that the bi-state site alarms are processed and communicated to the MOSCAD server. The alarms can originate from a device with "hard wired" physical dry contact interfacing or from a device connected to the MOSCAD CPU by means of an RS232 interface.

VERSION #1.01

2. TEST

- Step 1. Create an alarm condition by simulating an alarm on a device in the system or shorting/opening a status input to any MOSCAD status input module in the system. Navigate to the lowest level screen that depicts the highest degree of alarm detail.
- Step 2. Verify that the colored status bullet for the associated alarm on the server is blinking red and for RS232 interfaces, that the "state" text is red and is displayed for the correct alarm point and site.
- Step 3. If speakers are present, verify that an audible indication is heard at the server.
- Step 4. Verify that the alarm displays in red text on the Alarm Summary window.
- Step 5. Click with the mouse on the "acknowledge" button. Verify that the audible indication is silenced.
- Step 6. Verify that the text on the alarm summary window of the server changes from red to black.
- Step 7. Verify that the colored status bullet for the associated alarm on the server remains red but stops blinking.
- Step 8. Return the alarm point to the normal condition. Verify that the colored status bullet for the associated alarm returns to green.
- Step 9. Verify that the text is removed from the alarm summary window.

Pass _____ Fail _____

MOSCAD Fault Management System

Alarm Processing - Unacknowledged Alarm

1. DESCRIPTION

This segment of the test verifies that the bi-state site alarms are processed and communicated to the MOSCAD server. The alarms can originate from a device with "hard wired" physical dry contact interfacing or from a device connected to the MOSCAD CPU by means of an RS232 interface.

VERSION #1

2. TEST

- Step 1. Create an alarm condition by simulating an alarm on a device in the system or shorting/opening a status input to any MOSCAD status input module in the system.
- Step 2. View the alarm summary window and verify red text for the alarm. Verify that the associated alarm bullet is blinking red and yellow.
- Step 3. Verify the audible alert at the server is present.
- Step 4. Without acknowledging the alarm, return the alarm point to its normal condition.
- Step 5. Verify the text on the alarm summary window of the server has changed from red to blue indicating an unacknowledged alarm that has returned to normal.
- Step 6. Verify that the associated alarm bullet is blinking green and yellow, indicating an unacknowledged alarm that has returned to normal. An audible alert will persist until the alarm is acknowledged.

Pass ____ Fail ____

MOSCAD Fault Management System

Physical Inputs/Outputs - Digital Inputs

1. DESCRIPTION

The purpose of this section is to verify that the physical inputs and outputs that interface to the MOSCAD I/O modules are properly processed by the MOSCAD system. All alarms demonstrated are to be made on the punchblock. Proper processing can be verified by observing I/O module LED indications for DI's.

Digital Inputs – to be defined and tested as part of the final design process.

VERSION #1

2. TEST

- Step 1. Select a site to perform the test.
- Step 2. Short/Open the input point and verify that an alarm indication is received at the server.
- Step 3. Return the input to its normal condition. Verify that the alarm indication on the server returns to normal.

Pass____ Fail____

MOSCAD Fault Management System

Physical Inputs/Outputs - Digital Outputs

1. DESCRIPTION

The purpose of this section is to verify that the physical inputs and outputs that interface to the MOSCAD I/O modules are properly processed by the MOSCAD system. Proper processing can be verified by observing I/O module LED indications for DO's.

Digital Outputs – to be defined and tested as part of the final design process.

2. TEST

- Step 1. Select a site to perform the test.
- Step 2. Trigger a latched state of the output point by selecting the "On" button from the appropriate site's digital output screen, confirming that the screen indication changes from "Off" to "On" for that point.
- Step 3. Verify a change of state by observing the LED on the MOSCAD DI module.
- Step 4. Return the output to its "Off" condition. Verify that the "On" indication on the server returns to "Off" in addition to confirming a change of state of the MOSCAD LED.

VERSION #1

Pass____ Fail____

MOSCAD Fault Management System

Physical Inputs/Outputs - Analog Inputs

1. DESCRIPTION

The purpose of this section is to verify that the physical inputs and outputs that interface to the MOSCAD I/O modules are properly processed by the MOSCAD system. Analog inputs can be tested by comparing GUI needle deflection on-screen (full scale, half scale, 2/3 scale, etc)

Analog Inputs – to be defined and tested as part of the final design process.

2. TEST

- Step 1. Choose the site to perform the test.
- Step 2. At the server, select the Analog Input icon from the testing site overview screen.
- Step 3. Using a test board with a variable resistor, manipulate the AI input voltage by moving the potentiometer to $\frac{1}{4}$, $\frac{1}{2}$, or $\frac{3}{4}$ of the full resistance.
- Step 4. Verify that the needle deflection of the GUI matches, with reasonable accuracy, to that of the potentiometer.

Pass____ Fail____

VERSION #1

MOSCAD Fault Management System

TRAK GPS - GPS Fault

1. DESCRIPTION

The MOSCAD system will connect to each GPS Standard via its RS-232 port mini 9 pin D connector and requires a dedicated MOSCAD CPU RS-232 port (port 2 or 3). The MOSCAD will continuously monitor for any alarm messages that the TRAK sends to the CPU. Alarm messages are then converted to native MOSCAD data format for transmission to the control center.

VERSION #1

2. TEST

- Step 1. Choose the site to perform the test.
- Step 2. Verify there are no current alarms for the chosen TRAK GPS.
- Step 3. Disconnect the antenna cable from the TRAK GPS.
- Step 4. At the server, select the TRAK GPS tab.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. Reconnect the antenna cable to the TRAK GPS standard.
- Step 8. Verify that the GPS status returns to normal.

Pass____ Fail____

MOSCAD Fault Management System

TRAK GPS - Communication Status Fault

1. DESCRIPTION

The MOSCAD system will connect to each GPS Standard via its RS-232 port mini 9 pin D connector and requires a dedicated MOSCAD CPU RS-232 port (port 2 or 3). The MOSCAD will continuously monitor for any alarm messages that the TRAK sends to the CPU. Alarm messages are then converted to native MOSCAD data format for transmission to the control center.

VERSION #1

2. TEST

- Step 1. Choose the site to perform the test.
- Step 2. Verify there are no current alarms for the chosen TRAK GPS.
- Step 3. Disconnect the RJ45 communication cable from the rear of the GPS.
- Step 4. At the server, select the TRAK GPS tab.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. Reconnect the communication cable to the rear of the GPS.
- Step 8. Verify that the GPS status returns to normal.

Pass____ Fail____

MOSCAD Fault Management System

TRAK GPS - Power Supply Fault

1. DESCRIPTION

The MOSCAD system will connect to each GPS Standard via its RS-232 port mini 9 pin D connector and requires a dedicated MOSCAD CPU RS-232 port (port 2 or 3). The MOSCAD will continuously monitor for any alarm messages that the TRAK sends to the CPU. Alarm messages are then converted to native MOSCAD data format for transmission to the control center.

VERSION #1

2. TEST

- Step 1. Choose the site to perform the test.
- Step 2. Verify there are no current alarms for the chosen TRAK GPS.
- Step 3. Disconnect one of the power supply cables from the rear of the GPS.
- Step 4. At the server, select the TRAK GPS tab.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. Reconnect the power supply cable to the rear of the TRAK GPS.
- Step 8. Verify that the GPS status returns to normal.

Pass____ Fail____

MOSCAD Fault Management System

TeNSr Channel Bank - T1 No Signal (NOS)

1. DESCRIPTION

The MOSCAD system will connect to each TeNSr channel bank via its computer port mini 9 pin D connector along the rear of the INF (Interface) module and requires a dedicated MOSCAD CPU RS-232 port (port 2 or 3). The MOSCAD will be in a "listen-only" mode, where it will continuously monitor for any alarm messages that the TeNSr channel bank sends to the CPU. Alarm messages will then be converted to native MOSCAD data format for transmission to the control center. The channel bank can have up to 28 modular circuits monitored, though in most cases it will be a subset of this maximum.

VERSION #1

2. TEST

- Step 1. Choose the TeNSr channel bank to perform test.
- Step 2. Verify that there are no current alarms for the chosen channel bank.
- Step 3. Disconnect the T1 Link.
- Step 4. At the server, select the TeNSr channel bank.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. Reconnect the T1 Link.
- Step 8. Verify that the TeNSr status returns to normal.

Pass____ **Fail**____

MOSCAD Fault Management System

TeNSr Channel Bank - User Card Alarm (OOS)

1. DESCRIPTION

The MOSCAD system will connect to each TeNSr channel bank via its computer port mini 9 pin D connector along the rear of the INF (Interface) module and requires a dedicated MOSCAD CPU RS-232 port (port 2 or 3). The MOSCAD will be in a "listen-only" mode, where it will continuously monitor for any alarm messages that the TeNSr channel bank sends to the CPU. Alarm messages will then be converted to native MOSCAD data format for transmission to the control center. The channel bank can have up to 28 modular circuits monitored, though in most cases it will be a subset of this maximum.

2. TEST

- Step 1. Choose the TeNSr channel bank to perform test.
- Step 2. Verify that there are no current alarms for the chosen channel bank.
- Step 3. Pull a user card other than the INTF card from the rear of the TeNSr.
- Step 4. At the server, select the TeNSr channel bank tab.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. Reinsert the card.
- Step 8. Verify that the TeNSr status returns to normal.

VERSION #1

Pass____ Fail____

MOSCAD Fault Management System

TeNSr Channel Bank - Power Supply Fail

1. DESCRIPTION

The MOSCAD system will connect to each TeNSr channel bank via its computer port mini 9 pin D connector along the rear of the INF (Interface) module and requires a dedicated MOSCAD CPU RS-232 port (port 2 or 3). The MOSCAD will be in a "listen-only" mode, where it will continuously monitor for any alarm messages that the TeNSr channel bank sends to the CPU. Alarm messages will then be converted to native MOSCAD data format for transmission to the control center. The channel bank can have up to 28 modular circuits monitored, though in most cases it will be a subset of this maximum.

VERSION #1

2. TEST

- Step 1. Choose the TeNSr channel bank to perform test.
- Step 2. Verify that there are no current alarms for the chosen channel bank, and that the channel bank contains dual, redundant power supplies.
- Step 3. Remove one of the power supplies and verify it is no longer powered.
- Step 4. At the server, select the TeNSr channel bank tab.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. Reinsert the power supply.
- Step 8. Verify that the TeNSr status returns to normal.

Pass____ Fail____

MOSCAD Fault Management System

TeNSr Channel Bank - Configuration

1. DESCRIPTION

The MOSCAD system will connect to each TeNSr channel bank via its term port along the rear of the INF (Interface) module and requires a dedicated MOSCAD MUX port (port 1, 2, 3 or 4). This connection, made using the TeNSr term port, is used solely for the VT-100 configuration interface. A separate connection to the comp DB9 port is utilized for alarming.

2. TEST

- Step 1. At the server, open the terminal application (VT100 mode) by selecting the configure button on the TeNSr display screen.
- Step 2. A HyperTerminal display should come indicating the channel bank that corresponds to the current site and margin tab.
- Step 3. Verify connection by validating channel bank name.
- Step 4. Close the HyperTerminal display.

Pass____ Fail____

VERSION #1

MOSCAD Fault Management System

Quantar Diagnostics - PA Low/ High
VSWR

1. DESCRIPTION

The MOSCAD system will connect to each Quantar via its RS-232 port mini 9 pin D connector and requires a dedicated MOSCAD MUX port (port 1, 2, 3, or 4). The MOSCAD will continuously poll for any alarm messages present in the Quantar. Alarm messages are then converted to native MOSCAD data format for transmission to the control center.

VERSION #1

2. TEST

- Step 1. Choose the channel and site to perform test.
- Step 2. Verify that there are no current alarms for the chosen station.
- Step 3. Disconnect load from the chosen station and key-up the station.
- Step 4. At the server, select the Quantar tab.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. De-key the station and reconnect the load at the station.
- Step 8. Verify that the station status returns to normal.

Pass____ Fail____

MOSCAD Fault Management System

Quantar Diagnostics - PA Fail Alarm

1. DESCRIPTION

The MOSCAD system will connect to each Quantar via its RS-232 port mini 9 pin D connector and requires a dedicated MOSCAD MUX port (port 1, 2, 3, or 4). The MOSCAD will continuously poll for any alarm messages present in the Quantar. Alarm messages are then converted to native MOSCAD data format for transmission to the control center.

VERSION #1

2. TEST

- Step 1. Choose the channel and site to perform test.
- Step 2. Verify that there are no current alarms for the chosen Quantar.
- Step 3. Disconnect the cable between the Exciter FRU and the PA FRU at the chosen station and key-up the station.
- Step 4. At the server, select the Quantar tab.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. Reconnect the cable at the station.
- Step 8. Verify that the station status returns to normal.

Pass _____ Fail _____

MOSCAD Fault Management System

Quantar Diagnostics - Access Disable

1. DESCRIPTION

The MOSCAD system will connect to each Quantar via its RS-232 port mini 9 pin D connector and requires a dedicated MOSCAD MUX port (port 1, 2, 3, or 4). The MOSCAD will continuously poll for any alarm messages present in the Quantar. Alarm messages are then converted to native MOSCAD data format for transmission to the control center.

VERSION #1

2. TEST

- Step 1. Choose the channel and site to perform test.
- Step 2. Verify that there are no current alarms for the chosen station.
- Step 3. At the server, select the Quantar tab.
- Step 4. Select "Access Disable"
- Step 5. Verify that the station is in Access Disable.
- Step 6. Select "Operate".
- Step 7. Verify that the station is not in Access Disable.

Pass____ Fail____

MOSCAD Fault Management System

Quantar Diagnostics - Configuration

1. DESCRIPTION

The MOSCAD system will connect to each Quantar via its RS-232 port mini 9 pin D connector and requires a dedicated MOSCAD MUX port (port 1, 2, 3, or 4). The MOSCAD will continuously poll for any alarm messages present in the Quantar. Alarm messages are then converted to native MOSCAD data format for transmission to the control center.

VERSION #1

2. TEST

- Step 1. At the Graphic Workstation, open the terminal application (VT100 mode) by selecting the RSS button on the Quantar display screen.
- Step 2. The RSS software main communication screen should then appear.
- Step 3. Within RSS select F2, F6, then F2 to upload front panel display information from the Quantar.
- Step 4. Verify proper operation by validating the Quantar name, serial number, Tx, or Rx operating frequency.

Pass ____ Fail ____

MOSCAD Fault Management System

ISR Diagnostics - PA Fail Alarm

1. DESCRIPTION

The MOSCAD (Motorola Supervisory Control and Data Acquisition) monitors alarms from the base stations via an IP based FSP and SNMP interface. The MOSCAD will report changes reported by the ISR to the MOSCAD alarm manager.

VERSION #1

2. TEST

- Step 1. Choose the channel and site to perform test.
- Step 2. Verify that there are no current alarms for the chosen ISR.
- Step 3. Disconnect the cable between the Exciter FRU and the PA FRU at the chosen station and key-up the station.
- Step 4. At the server, select the ISR tab.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. Reconnect the cable at the station.
- Step 8. Verify that the station status returns to normal.

Pass____ Fail____

MOSCAD Fault Management System

ISR Diagnostics - Reset Station

1. DESCRIPTION

The MOSCAD (Motorola Supervisory Control and Data Acquisition) monitors alarms from the base stations via an IP based FSP and SNMP interface. The MOSCAD will report changes reported by the ISR to the MOSCAD alarm manager.

2. TEST

- Step 1. Choose the channel and site to perform test.
- Step 2. Verify that there are no current alarms for the chosen station.
- Step 3. At the server, select the ISR tab.
- Step 4. Select "Station Reset"
- Step 5. Verify that the station is reset by observing the LED's on the face of the ISR.

VERSION #1

Pass_____ Fail_____

MOSCAD Fault Management System

Central Electronics Bank (CEB) - Power Supply Fault

1. DESCRIPTION

The MOSCAD system will connect to each CEB via its RS232 port mini 9 pin D connector and requires a dedicated MOSCAD CPU RS-232 port (port 2 or 3). The MOSCAD will be in a "listen-only" mode, where it will continuously monitor for any alarm messages that the CEB sends to the CPU. Alarm messages are then converted to native MOSCAD data format for transmission to the control center.

VERSION #1

2. TEST

- Step 1. Choose the CEB to perform test.
- Step 2. Verify that there are no current alarms for the chosen CEB.
- Step 3. At the server, select the CEB tab.
- Step 4. Remove one of the power supply cables from the CEB.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm. Re-insert the power supply cable.
- Step 7. Verify that the CEB status returns to normal.

Pass _____ Fail _____

MOSCAD Fault Management System

Central Electronic Bank (CEB) - TDM Card Missing

1. DESCRIPTION

The MOSCAD system will connect to each CEB via its RS232 port mini 9 pin D connector and requires a dedicated MOSCAD CPU RS-232 port (port 2 or 3). The MOSCAD will be in a "listen-only" mode, where it will continuously monitor for any alarm messages that the CEB sends to the CPU. Alarm messages are then converted to native MOSCAD data format for transmission to the control center.

VERSION #1

2. TEST

- Step 1. Choose the CEB site to perform test.
- Step 2. Verify that there are no current alarms for the chosen CEB.
- Step 3. At the server, select the CEB tab.
- Step 4. Remove a TDM from the CEB.
- Step 5. Verify that the alarm is received at the server.
- Step 6. Acknowledge the alarm. Re-insert the TDM card.
- Step 7. Verify that the CEB status returns to normal.

Pass____ **Fail**____

MOSCAD Fault Management System

PSC - Site Failsoft

1. DESCRIPTION

The MOSCAD (Motorola Supervisory Control and Data Acquisition) monitors alarms from the base stations via an SNMP interface. The MOSCAD will report changes reported by the PSC to the MOSCAD alarm manager.

VERSION #1

2. TEST

- Step 1. Choose the site to perform test.
- Step 2. Verify that there are no current alarms for the chosen PSC.
- Step 3. Power off all but 2 radio channels at the site under consideration.
- Step 4. At the server, select the PSC tab.
- Step 5. Verify that a site failsoft alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. Return the site from failsoft.
- Step 8. Verify that the station status returns to normal.

Pass____ Fail____

MOSCAD Fault Management System

PSC - Station Link

1. DESCRIPTION

The MOSCAD (Motorola Supervisory Control and Data Acquisition) monitors alarms from the base stations via an SNMP interface. The MOSCAD will report changes reported by the PSC to the MOSCAD alarm manager.

VERSION #1.01

2. TEST

- Step 1. Choose the site to perform test.
- Step 2. Verify that there are no current alarms for the chosen PSC.
- Step 3. Remove the cable that provides the site link from the rear of the ISR.
- Step 4. At the server, select the PSC tab.
- Step 5. Verify that an alarm is received at the server.
- Step 6. Acknowledge the alarm.
- Step 7. Replace cable and verify proper operation.
- Step 8. Verify PSC status returns to normal.

Pass____ Fail____

Key Management Facility (KMF)

Key Management Facility (KMF)

Creating The Subscriber Record(s)

1. DESCRIPTION

The KMF (OTAR client station) operator must establish a database of the subscriber(s), which will be allowed to operate under the OTAR system. Those not on the database will not be recognized and will not participate on routine OTAR operations.

The Key Loss Key (KLK) is used in the subscriber if the keys are lost by manually zeroizing by either removing the battery or pressing the zeroize key. This way, a new UKEK is not required. The radio will use the KLK to encrypt the messages between the KVL and the radio.

If a KLK is not present, a Red Store and Forward is required.

VERSION #1.04

2. TEST

- Step 1. From the KMF Client Tool bar, click on Key Management icon. Verify the Key Management screen appears. It has three tabs: i.e.: Keys, Units, and CKRs.
- Step 2. Select the Unit Tab.
- Step 3. Click on Create New Unit Button or select File \ New.
- Step 4. In the Unit box click on the Subscriber icon and press OK.
- Step 5. Enter Subscriber information, such as Unit Name, RSI, and CAI ID. Ascertain the "Service Level" is set to: OTAR-able.
- Step 6. Click on KLK Enabled if desired.
- Step 7. Click on the SAVE button
- Step 8. Verify that the newly created subscriber unit will appear in Italics on the Unit Screen because it doesn't have a UKEK assigned or a CKR.

Pass_____ Fail_____

Key Management Facility (KMF)

Creating The Common Key Reference

1. DESCRIPTION

The KMF (OTAR client station) operator must establish a database of the CKR(s), which will be utilized by the OTAR system subscribers. Those not on the database will not be able to participate on routine OTAR operations.

VERSION #1.03

2. TEST

- Step 1. From the KMF Client Tool bar, click on Key Management icon.
- Step 2. Verify the Key Management screen appears. It has three (3) tabs: i.e.: Keys, Units, and CKRs.
- Step 3. Select the CKR Tab.
- Step 4. Click on Create New CKR icon or select File \ New.
- Step 5. Enter Information for the new CKR; i.e.. CKR Name, etc.
- Step 6. Click on the SAVE button and verify that the newly created CKR appears in Italics on the CKR Screen.

Pass _____ Fail _____

Key Management Facility (KMF)

Creating New User Key(s)

1. DESCRIPTION

The KMF (OTAR client station) operator must create Unique Key Encryption Keys (UKEKs) for all valid OTAR system subscribers. There are two Key sources from which to obtain them.

VERSION #1.04

2. TEST

- Step 1. From the KMF Client Tool bar, click on Key Management icon.
- Step 2. Verify that the Key Management screen appears. It has three (3) tabs: i.e.: Keys, Units, and CKRs.
- Step 3. Select the KEY Tab.
- Step 4. Click on Create New KEY icon or select File \ New.
- Step 5. Enter a KEY Name and then select the KEY type i.e.: UKEK in this case.
- Step 6. Select the KEY algorithm i.e.: AES-OFB in this case.
- Step 7. Choose the method for adding the new KEY: i.e. Keyboard or Key Kettle.
- Step 8. Click on the Keyboard button. The Key data entry screen appears. Type in the Key data.
- Step 9. Verify that the Key data can be up to and including 16 digits.
- Step 10. Click OK then Click Save to finish the task.

Pass ___ Fail ___

Key Management Facility (KMF)

Creating New Traffic Encryption Key(s) For CKRs

1. DESCRIPTION

The KMF (OTAR client station) operator must create Traffic Encryption Keys (TEKs) for all valid OTAR system subscribers. There are two Key sources from which to obtain them.

VERSION #1.04

2. TEST

- Step 1. From the KMF Client Tool bar, click on Key Management icon.
- Step 2. Verify that the Key Management screen appears. It has three (3) tabs: i.e.: Keys, Units, and CKRs.
- Step 3. Select the KEY Tab
- Step 4. Click on Create New KEY icon or select File \ New.
- Step 5. Enter a KEY Name and then select the KEY type i.e.: TEK in this case.
- Step 6. Select the KEY algorithm i.e.: AES-OFB in this case
- Step 7. Choose the method for adding the new KEY: i.e. Keyboard or Key Kettle.
- Step 8. Click on the Keyboard button. The Key data entry screen appears. Type in the Key data.
- Step 9. Verify that the Key data can be up to and including 16 digits.
- Step 10. Click OK then Click Save to finish the task.
- Step 11. Perform test again getting key from key kettle.

Pass____ Fail____

Key Management Facility (KMF)

Association Of Traffic Keys To Common Key References (CKRs)

1. DESCRIPTION

Having created all appropriate Keys, the KMF (OTAR client station) operator must now associate them to the corresponding CKRs.

VERSION #1.03

2. TEST

- Step 1. From the KMF Client Tool bar, click on Key Management icon.
- Step 2. Verify that the Key Management screen appears. It has three (3) tabs: i.e.: Keys, Units, and CKRs.
- Step 3. Select the CKR Tab.
- Step 4. Select the CKR of interest from the CKRs list and Double Click on it. The CKR information screen appears.
- Step 5. Click back on the Key Management window and select Key Tab.
- Step 6. Select the desired TEK for "Key Set 1" and, drag this TEK into the CKR information screen.
- Step 7. Select the desired TEK for "Key Set 2" and, drag this TEK into the CKR information screen.
- Step 8. TEK for Key Set 2 should be different from that of Key Set 1.
- Step 9. Click on the SAVE button to finish the process.
- Step 10. The Key association is complete.

Pass____ Fail____

Key Management Facility (KMF)

Association Of Individual Keys To Subscriber Unit(s)

1. DESCRIPTION

Having created all appropriate Individual Unique Encryption Keys, the KMF (OTAR client station) operator must now associate them to the corresponding subscriber units.

VERSION #1.04

2. TEST

- Step 1. From the KMF Client Tool bar, click on Key Management icon.
- Step 2. Verify that the Key Management screen appears. It has three (3) tabs: i.e.: Keys, Units, and CKRs.
- Step 3. Select the Unit Tab.
- Step 4. Select the Subscriber unit of interest from the Units list and Double Click on it.
- Step 5. Verify that once in the specific subscriber Unit screen, three Tabs appear The Attributes, The CKR assignment and the KVL assignment.
- Step 6. Choose the correct algorithm for the UKEK.
- Step 7. Click back on the Key Management window and select the Key Tab.
- Step 8. Select the desired UKEK and, drag it into the UKEK field of the Subscriber Unit of interest.
- Step 9. Click on the SAVE button to finish the process.
- Step 10. The Key association is complete. The newly created subscriber unit will remain marked with Italics on the Unit Screen because it still needs the CKR association.

Pass____ Fail____

Key Management Facility (KMF)

Association Of Individual CKRs To Subscriber Unit(s)

1. DESCRIPTION

Having created all appropriate Individual CKRs, the KMF (OTAR client station) operator must now associate them to the corresponding subscriber units.

VERSION #1.03

2. TEST

- Step 1. From the KMF Client Tool bar, click on Key Management icon.
- Step 2. Verify that the Key Management screen appears. It has three (3) tabs: i.e.: Keys, Units, and CKRs.
- Step 3. Select the CKR Tab. Double click on the CKR to be associated with a Subscriber Unit.
- Step 4. Verify that the characteristics for that specific CKR tab appears.
- Step 5. From the CKR window, select the Unit Assignment Tab. Verify that the Unit list appears.
- Step 6. Leaving the CKR window open, return to the Key Management function and select the Unit Tab. Click on the Subscriber Unit to be associated with the above CKR.
- Step 7. Using the mouse, drag the Unit icon (selected in step 3) into the CKR's Unit Assignment.
- Step 8. Verify that the new Subscriber Unit name appears within the CKR window.
- Step 9. Click on the SAVE button to finish the process.
- Step 10. Repeat the above operation for all CKRs and Subscriber Units to be associated in the system.

Pass____ Fail____

Key Management Facility (KMF)

Association Of Individual Subscriber Unit(s)
To KVL(s)

1. DESCRIPTION

Having configured all system KVLs, the KMF (OTAR client station) operator must now associate them to the corresponding subscriber units.

VERSION #1.04

2. TEST

- Step 1. From the KMF Client Tool bar, click on Key Management icon.
- Step 2. Verify that the Key Management screen appears. It has three (3) tabs: i.e.: Keys, Units, and CKRs.
- Step 3. Select the Unit Tab.
- Step 4. Select the KVL of interest from the units list and Double Click on it.
- Step 5. Verify that three (4) Tabs appear. Select the Unit Assignment Tab.
- Step 6. Go back to the Key Management function and, under the Units Tab, select the chosen Subscriber Unit to be associated.
- Step 7. Using the mouse, drag the Subscriber Unit into the KVL's Unit Assignment Tab.
- Step 8. Verify that the newly chosen Subscriber Unit appears within the KVL window.
- Step 9. Click on the SAVE button to finish the process.

Pass____ Fail____

Key Management Facility (KMF)

OTAR System Subscriber Units Key Initialization

1. DESCRIPTION

Having configured the OTAR system, every field unit must be loaded with the initialization information. This is referred to as "Store and Forward" operation. This method is the same as a standard "OTAR" one except the messages (KMMs) are delivered physically and directly. Prior to performing the S&F function, the KMF manager has associated all Units with CKRs, KVLs, UKEKs, TEKs, etc.

NOTE: A Red Store and Forward is not encrypted, a Black Store and Forward is encrypted. A Red Store and Forward is required if a UKEK or a KLK is not available in the subscriber.

VERSION #1.05

2. TEST

- Step 1. Power up the KVL. Connect the KVL to the KMF server to download KMMs. The connection can be direct or via modem.
- Step 2. Using the KVL controls arrow to "KMF" and select it. Next chose "Direct/RS232" and select it.
- Step 3. Verify that the KVL displays: "Downloading from the KMF". The KVL downloads new KMMs for all OTAR components on the system.
- Step 4. After the download is complete, remove the KVL and power it down.
- Step 5. Disconnect the KVL from the KMF and then connect the KVL to the subscriber unit.
- Step 6. Power up both the KVL and the Subscriber Unit, connect them together and select the Update function.
- Step 7. Verify that the KVL automatically searches for the Unit ID currently connected to it. Upon completion of the download, the KVL collects the Unit's acknowledgement and updates its memory status.
- Step 8. Reconnect the KVL to the KMF Server to return the acknowledgements. Do this by repeating steps 1-3.
- Step 9. Verify that the KMF Server updates the Unit's currency and history.

Pass____ Fail____

Key Management Facility (KMF)

Clear Hello

1. DESCRIPTION

Sending a Clear Hello to a subscriber insures it can receive OTAR messages.

This test requires a data system configured for Over The Air Re-Keying.

SETUP

RADIO-1 - OTAR CHANNEL

VERSION #1.02

2. TEST

- Step 1. From the KMF Client Toolbar screen, click on OTAR Event Display.
- Step 2. On the KMF Client Toolbar, click on Key Management.
- Step 3. Select the Unit Tab in the Key Management Window.
- Step 4. Select RADIO-1 from the list.
- Step 5. From the menu, select Operations/OTAR/Clear Hello or from the toolbar choose Clear Hello.
- Step 6. From the OTAR Event Display, verify an icon for "OTAR Operation Successful" was displayed.

Pass _____ Fail _____

Key Management Facility (KMF)

Encrypted Hello

1. DESCRIPTION

Sending an Encrypted Hello to a subscriber insures it can receive Encrypted OTAR messages.

This test requires a data system configured for Over The Air Re-Keying.

SETUP

RADIO-1 - OTAR CHANNEL

VERSION #1.03

2. TEST

- Step 1. From the KMF Client Toolbar screen, click on OTAR Event Display.
- Step 2. On the KMF Client Toolbar, click on Key Management.
- Step 3. Select the Unit Tab in the Key Management Window.
- Step 4. Select RADIO-1 from the list.
- Step 5. From the menu select Operations/OTAR/Encrypted Hello or from the toolbar choose Encrypted Hello.
- Step 6. From the OTAR Event Display, verify an icon for "OTAR Operation Successful" was displayed.

Pass____ Fail____

Key Management Facility (KMF)

CKR Group Update

1. DESCRIPTION

The following tests exercise operations related to the manipulation of CKRs.

This test requires a data system configured for Over The Air Re-Keying.

VERSION #1.01

2. TEST

- Step 1. From the KMF Client Toolbar screen, click on OTAR Event Display.
- Step 2. On the KMF Client Toolbar, click on Key Management.
- Step 3. Select the CKR Tab in the Key Management Window.
- Step 4. Select the particular CKR to be updated.
- Step 5. From the menu select Operations/OTAR/Group Update or from the toolbar click on the Group Update button.
- Step 6. Verify that all members of the chosen CKR are updated.
- Step 7. From the OTAR Event Display, verify an icon for "CKR Update Complete" was displayed.

Pass_____ Fail_____

Key Management Facility (KMF)

Optimized Unit Update

1. DESCRIPTION

Initiating an Optimized Unit Update will only update the subscriber with the information marked as not current in the KMF database.

This test requires a data system configured for Over The Air Re-Keying.

VERSION #1.02

2. TEST

- Step 1. From the KMF Client Toolbar screen, click on OTAR Event Display.
- Step 2. On the KMF Client Toolbar, click on Key Management.
- Step 3. Select the Unit Tab in the Key Management Window.
- Step 4. Select the particular Unit to be updated.
- Step 5. From the menu select Operations/OTAR/Optimized Unit Update or from the toolbar click on the Optimized Unit Update.
- Step 6. From the OTAR Event Display, verify an icon for "OTAR Operation Successful" was displayed.
- Step 7. Verify that the chosen unit is updated.

Pass_____ Fail_____

Key Management Facility (KMF)

Unit Zeroize

1. DESCRIPTION

The KMF can remotely zeroize a unit. This will remove all Keys from its memory therefore rendering it unable to transmit or receive encrypted messages.

The unit must have a Red Store and Forward performed on it before it can receive or transmit in encrypted mode.

After a Red Store and Forward, the KVL must download to the KMF before any secure functions can be performed on the subscriber.

NOTE: If an Inhibited unit is zeroized, it cannot be enabled via the KMF. It must be re-enabled using RSS.

This test requires a data system configured for Over The Air Re-Keying.

SETUP

RADIO-1 - OTAR CHANNEL

VERSION #1.03

2. TEST

- Step 1. From the KMF Client Toolbar screen, click on OTAR Event Display.
- Step 2. On the KMF Client Toolbar, click on Key Management.
- Step 3. Select the Unit Tab in the Key Management Window.
- Step 4. Select the particular Unit to be zeroized.
- Step 5. From the menu select Operations/OTAR/Zeroize or from the toolbar choose Zeroize.
- Step 6. From the OTAR Event Display, verify an icon for "OTAR Operation Successful" was displayed.
- Step 7. Verify that RADIO-1 can no longer transmit or receive in encrypted mode.

Pass____ Fail____

Key Management Facility (KMF)

Unit Re-Key Request

1. DESCRIPTION

A subscriber has the ability to request a Re-Key by the KMF over the data channel.

This test requires a data system configured for Over The Air Re-Keying.

SETUP

RADIO-1 - OTAR CHANNEL

VERSION #1.02

2. TEST

- Step 1. Verify RADIO-1 is on a Data capable channel and that it is registered with the WNG.
- Step 2. Choose REKY from the subscriber menu.
- Step 3. When the subscriber's display shows "REQUEST REKEY," press the PTT to send the request.
- Step 4. Verify the subscriber shows "PLEASE WAIT"
- Step 5. Verify the activity on the OTAR Event Display and that it displays an icon for "OTAR Operation Successful"
- Step 6. Verify the subscriber display's REKEYED.

Pass ____ Fail ____

Key Management Facility (KMF)

Compromised Unit Parameter

1. DESCRIPTION

A unit can be tagged as Compromised if it has been lost or stolen. This setting will block the ability to perform a Full Unit Update from the KMF or a unit initiated Re-Key Request.

This test requires a data system configured for Over The Air Re-Keying.

SETUP

RADIO-1 - OTAR CHANNEL

VERSION #1.03

2. TEST

- Step 1. From the KMF Client Toolbar screen, click on OTAR Event Display.
- Step 2. On the KMF Client Toolbar, click on Key Management.
- Step 3. Select the Unit Tab in the Key Management Window.
- Step 4. From the list, double click on RADIO-1.
- Step 5. Set the compromised check box and save the unit by pressing the Save button.
- Step 6. Choose REKY from the subscriber menu.
- Step 7. When the subscriber's display shows "REQUEST REKEY," press the PTT to send the request.
- Step 8. From the OTAR Event Display, verify an icon reading "Unit is Compromised so the Full Range of OTAR Operations is not Available" is displayed.
- Step 9. Verify RADIO-1 never receives a "RE-KEYED" acknowledgement.

Pass____ Fail____

Key Management Facility (KMF)

Keyset Change Over

1. DESCRIPTION

KMF has the ability to utilize two sets of keys or "keysets" per CKR. Each CKR can have two keysets that can either be toggled manually on the subscriber using the menu, or toggled remotely via the OTAR system.

This test requires a data system configured for Over The Air Re-Keying.

SETUP

RADIO-1 - OTAR CHANNEL

VERSION #1.03

2. TEST

- Step 1. Check the subscriber's active Keyset by choosing KSET in the subscriber's menu.
- Step 2. From the KMF Client Toolbar screen, click on OTAR Event Display.
- Step 3. On the KMF Client Toolbar, click on Key Management.
- Step 4. From the menu, choose Operations and then Show Keyset. Verify the Keyset popup window is displayed.
- Step 5. Toggle the Active Keyset and press the OK button.
- Step 6. From the menu, choose Operations, OTAR, and then Keyset Changeover.
- Step 7. Verify the system traffic on the OTAR Event Display.
- Step 8. From the OTAR Event Display, verify an icon for "Keyset Update Complete" is displayed. This may take a few seconds depending on the number of units in the database.
- Step 9. Verify the subscriber has switched active Keysets by choosing KSET in the subscriber's menu.

Pass____ Fail____

Key Management Facility (KMF)

Unit Polling

1. DESCRIPTION

When individual commands are sent to a subscriber over the air, the subscriber acknowledges them and the KMF updates its database accordingly.

When group commands are sent over the air, subscribers do not acknowledge the commands immediately so not to busy up the channel. They may send it on their next PTT or after another individual command.

When "Polling" is initiated, the KMF requests updated information from all of the units. The units that respond to the poll will be set to "Current" in the database.

This test requires a data system configured for Over The Air Re-Keying.

SETUP

RADIO-1 - OTAR CHANNEL

VERSION #1.02

2. TEST

- Step 1. From the KMF Client Toolbar screen, click on OTAR Event Display.
- Step 2. On the KMF Client Toolbar, click on Key Management.
- Step 3. From the menu select Operations/OTAR/Initiate Polling
- Step 4. From the OTAR Event Display, verify an icon for each unit is displayed and that "Received Delayed Acknowledgement" is displayed.
- Step 5. In the Key Management Window, press the Refresh button and verify that the units that responded are now set to Current.

Pass _____ Fail _____

Key Management Facility (KMF)

Unit Inhibit

1. DESCRIPTION

KMF has the ability to disable or "Inhibit" a unit over the air.

NOTE: If an Inhibited unit is zeroized, it cannot be enabled via the KMF. It must be re-enabled using RSS.

This test requires a data system configured for Over The Air Re-Keying.

SETUP

RADIO-1 - OTAR CHANNEL

VERSION #1.03

2. TEST

- Step 1. From the KMF Client Toolbar screen, click on OTAR Event Display.
- Step 2. On the KMF Client Toolbar, click on Key Management.
- Step 3. Select the Unit Tab in the Key Management Window.
- Step 4. Select RADIO-1 from the list.
- Step 5. Press the Inhibit button on the toolbar to Inhibit RADIO-1.
- Step 6. From the OTAR Event Display, verify an icon for "OTAR Operation Successful" was displayed.
- Step 7. Verify that RADIO-1 is Inhibited.
- Step 8. Use the same procedure to Enable RADIO-1.
- Step 9. Verify RADIO-1 is fully enabled.

Pass____ Fail____

MDC Signaling Features

MDC Signaling Features

Car-to-Car Messaging

1. DESCRIPTION

This test verifies a Premier MDC Select user is able to send a free-form message to another unit or group of units, specified by unit designator(s) or by ID(s) of the personnel in the vehicle, that message arrival in the vehicle is accompanied by an audible alert, and that all car-to-car messages are logged by the Premier MDC Select Message Switch. (23)

The successful delivery of the following free-form messages will constitute an acceptable test.

- To another unit, specified by unit designator.
Example : U=305
- To another unit, specified by ID of personnel.
- To a group of units, specified by unit designators.
Example : U=305, U=102
- To a group of units, specified by ID of personnel.
- To a unit not in service at time of sending, delivered when brought in service.

NOTE: If a message is sent with the option, "Only If Logged On" checked, the message will only be delivered if the user is currently logged on.

SETUP

UNIT-4 - Initially not in service.

VERSION #1.02

2. TEST

- Step 1. Initiate a free form message to UNIT-2 from UNIT-1 using its unit designator.
- Step 2. Verify that UNIT-2 receives the free form message and an audible alert.
- Step 3. Initiate a free form message to UNIT-2 using its ID of personnel.
- Step 4. Verify that UNIT-2 receives the free form message and an audible alert.
- Step 5. Initiate a free form message to UNIT-2 and UNIT-3 using their ID of personnel.
- Step 6. Verify that UNIT-2 and UNIT-3 receive the free form message and audible alerts.
- Step 7. Initiate a free form message to UNIT-4 using its ID of personnel.
- Step 8. Verify that the message is not successful because UNIT-4 is not in service.
- Step 9. Bring UNIT-4 back into service.
- Step 10. Verify that UNIT-4 now receives the free form message and an audible alert.

Pass ____ Fail ____

MDC Signaling Features

LAN-to-Car Messaging

1. DESCRIPTION

This test verifies a Premier MDC Select user is able to send a free-form message to another unit or group of units, specified by unit designator(s) or by ID(s) of the personnel in the vehicle, that message arrival in the vehicle is accompanied by an audible alert, and that all LAN-to-car messages are logged by the Premier MDC Select Message Switch.

The successful delivery of the following free-form messages from the LAN client will constitute an acceptable test.

- To another unit, specified by unit designator.
Example : U=305
- To another unit, specified by ID of personnel.
- To a group of units, specified by unit designators.
Example : U=305, U=102
- To a group of units, specified by ID of personnel.
- To a unit not in service at time of sending, delivered when brought in service.

NOTE: If a message is sent with the option, "Only If Logged On" checked, the message will only be delivered if the user is currently logged on.

SETUP

UNIT-4 - Initially not in service.

VERSION #1.05

2. TEST

- Step 1. Initiate a free form message from the LAN client to UNIT-2 using its unit designator.
- Step 2. Verify that UNIT-2 receives the free form message and an audible alert.
- Step 3. Initiate a free form message from the LAN client to UNIT-2 using its ID of personnel.
- Step 4. Verify that UNIT-2 receives the free form message and an audible alert.
- Step 5. Initiate a free form message from the LAN client to UNIT-2 and UNIT-3 using their ID of personnel.
- Step 6. Verify that UNIT-2 and UNIT-3 receive the free form message and audible alerts.
- Step 7. Initiate a free form message from the LAN client to UNIT-4 using its ID of personnel.
- Step 8. Verify that the message is not successful because UNIT-4 is not in service.
- Step 9. Bring UNIT-4 back into service.
- Step 10. Verify that UNIT-4 now receives the free form message and an audible alert.

Pass ___ Fail ___

MDC Signaling Features

Additional Messaging Features

1. DESCRIPTION

This test verifies a Premier MDC Select user is able to send a free-form message to another unit or group of units, specified by unit designator(s) or by ID(s) of the personnel in the vehicle, that message arrival in the vehicle is accompanied by an audible alert, and that all car-to-car messages are logged by the Premier MDC Select Message Switch.

The PMDC user has the ability to perform the following standard messaging features:

- Reply
- Forward
- Return Receipts
- File Attachments

The successful delivery of a free-form message using each of the above features will constitute a successful test.

SETUP

UNIT-1, UNIT-2, and UNIT-3 -- In service.

VERSION #1

2. TEST

- Step 1. Send a message from UNIT-1 to UNIT-2. Verify that the "return receipt" option is chosen.
- Step 2. Verify that UNIT-2 receives the message. Open the message.
- Step 3. Verify that when UNIT-2 opens the message, a "Return Receipt" is sent to UNIT-1.
- Step 4. Use the "Reply" button on UNIT-2 to reply to the message sent by UNIT-1.
- Step 5. Verify that UNIT-1 receives the reply from UNIT-2.
- Step 6. Press the "Forward" button on UNIT-1 to forward the message from UNIT-2 to UNIT-3.
- Step 7. Verify that UNIT-3 receives the forwarded message.
- Step 8. Reply to UNIT-1's message and attach a small file to the message.
- Step 9. Verify that UNIT-1 receives the message and the file attachment.
- Step 10. Use the "Paperclip" button to open the file attachment. Verify the attachment opens.

Pass _____ Fail _____

MDC Signaling Features

Who-is-on Button

1. DESCRIPTION

This test verifies that the mobile unit user has the ability display a list of users online status represented by an icon.

The successful display of the online status of registered users will constitute an acceptable test.

2. TEST

- Step 1. On UNIT-1, press the "Who-is-on" button.
- Step 2. Verify that the Address Book is displayed.
- Step 3. Verify that all users are displayed in the list with the proper status icon.

Pass ____ Fail ____

VERSION #1

MDC Signaling Features

Day or Night Mode

1. DESCRIPTION

This test verifies that the mobile unit user has the ability switch between the day mode and night mode of Premier MDC.

The successful switching from day to night mode and back again will constitute acceptance.

2. TEST

- Step 1. On UNIT-1, switch the PMDC to Night Mode.
- Step 2. Verify that UNIT-1 enters Night Mode.
- Step 3. Switch UNIT-1 to Day Mode.
- Step 4. Verify that UNIT-1 enters Day Mode.

Pass____ **Fail**____

VERSION #1.01

MDC Signaling Features

Message Switch Reports

1. DESCRIPTION

The PMDC Message Switch has the ability to archive all messages that are processed on the system.

This information can be retrieved in various reports sorted by time and users.

The following major reports can be printed or displayed:

- Users and Units
- Messages
- Chat Text
- All Queries

The successful display of one of each of the above reports will constitute an acceptable test.

VERSION #1.01

2. TEST

- Step 1. From the PMDC Message Switch computer, start the Message Switch Reports application.
- Step 2. Choose the "User Registry" icon. Select one of the reports in the list and press the "Display" button.
- Step 3. Verify the correct information is displayed.
- Step 4. Choose the "Messaging" icon. Select a Messaging report in the list and press the "Display" button.
- Step 5. Verify the correct information is displayed.
- Step 6. Choose the "Messaging" icon. Select a Chatroom report in the list and press the "Display" button.
- Step 7. Verify the correct information is displayed.
- Step 8. Choose the "State" icon. Select one of the reports in the list and press the "Display" button.
- Step 9. Verify the correct information is displayed.

Pass____ Fail____

NCIC through CAD Interface Functionality

NCIC Interface Features

Wants / Warrants / License Query on Individual

1. DESCRIPTION

This test verifies that the mobile unit user has the ability to "run" an individual by Name / Race / Sex / DOB / SSN or by Drivers License Number through the interface to the State/County/NCIC. The information received from State/County/NCIC in response to the query will be routed back to the inquiring unit.

The successful display of results from two (2) person queries to the State/County/NCIC will constitute an acceptable test.

2. TEST

- Step 1. Run an individual by Name through the interface to the State/County/NCIC.
- Step 2. Verify that the information received from State/County/NCIC in response to the query is routed back to the inquiring unit.
- Step 3. Run a second individual by Drivers License Number through the interface to State/County/NCIC.
- Step 4. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.

Pass____ Fail____

VERSION #1.03

NCIC Interface Features

Vehicle Queries

1. DESCRIPTION

This test verifies that the mobile unit user has the ability to "run" a vehicle by VIN or by License Tag Number (Plate) through the interface to the State/County/NCIC. The information received from the State/County/NCIC in response to the query will be routed back to the inquiring unit.

The successful display of results from two (2) vehicle queries to the State/County/NCIC will constitute an acceptable test.

2. TEST

- Step 1. Run a vehicle by VIN through the interface to the State/County/NCIC.
- Step 2. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.
- Step 3. Run a second vehicle by License Tag Number (Plate) through the interface to the State/County/NCIC.
- Step 4. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.

Pass____ Fail____

VERSION #1.03

NCIC Interface Features

Article Queries

1. DESCRIPTION

This test verifies that the mobile unit user has the ability to "run" an individual article to see if it is listed as stolen through the interface to the State/County/NCIC. The information received from the State/County/NCIC in response to the query will be routed back to the inquiring unit.

The successful display of results from two (2) Property queries to the State/County/NCIC will constitute an acceptable test.

2. TEST

- Step 1. Run an article through the interface to the State/County/NCIC.
- Step 2. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.
- Step 3. Run a second article through the interface to the State/County/NCIC.
- Step 4. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.

Pass____ Fail____

VERSION #1.02

NCIC Interface Features

Gun Queries

1. DESCRIPTION

This test verifies that the mobile unit user has the ability to "run" a firearm by serial number to see if it is "wanted" or stolen, and to determine the owner through the interface to the State/County/NCIC. The information received from the State/County/NCIC in response to the query will be routed back to the inquiring unit.

The successful display of results from two (2) Gun queries to the State/County/NCIC will constitute an acceptable test.

2. TEST

- Step 1. Run a firearm by serial number through the interface to the State/County/NCIC.
- Step 2. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.
- Step 3. Run a second firearm by serial number through the interface to the State/County/NCIC.
- Step 4. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.

Pass____ Fail____

VERSION #1.02

NCIC Interface Features

Boat Query

1. DESCRIPTION

This test verifies that the mobile unit user has the ability to "run" a boat by Registration Number, Name or by Hull Number through the interface to the State/County/NCIC. The information received from the State/County/NCIC in response to the query will be routed back to the inquiring unit.

The successful display of results from two (2) boat queries to the State/County/NCIC will constitute an acceptable test.

2. TEST

- Step 1. Run a boat by Registration Number through the interface to the State/County/NCIC.
- Step 2. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.
- Step 3. Run a second boat by Hull Number through the interface to the State/County/NCIC.
- Step 4. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.

Pass____ Fail____

VERSION #1.02

NCIC Interface Features

Hazmat Query

1. DESCRIPTION

This test verifies that the mobile unit user has the ability to "run" a HAZMAT 4 digit PlaCard number through the interface to the State/County/NCIC.

The information received from the State/County/NCIC in response to the query will be routed back to the inquiring unit.

The successful display of results from two (2) HAZMAT queries to the State/County/NCIC will constitute an acceptable test.

2. TEST

- Step 1. Run a HAZMAT 4 digit PlaCard number through the interface to the State/County/NCIC.
- Step 2. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.
- Step 3. Run a second HAZMAT number through the interface to the State/County/NCIC.
- Step 4. Verify that the information received from the State/County/NCIC in response to the query is routed back to the inquiring unit.

Pass ____ Fail

VERSION #1.01