INCREMENTO EN LA FIABILIDAD DE UN SISTEMA DE ENLACE DE DATOS TÁCTICOS MEDIANTE EL DISEÑO Y LA IMPLEMENTACIÓN DE MECANISMOS DE RECUPERACIÓN AUTOMÁTICA ANTE FALLAS.

Stefany del Pilar Marrugo Llorente

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

PROGRAMA: Maestría en Ingeniería.

ÉNFASIS: Ingeniería Electrónica

CARTAGENA, COLOMBIA

Noviembre de 2015.

INCREMENTO EN LA FIABILIDAD DE UN SISTEMA DE ENLACE DE DATOS TÁCTICOS MEDIANTE EL DISEÑO Y LA IMPLEMENTACIÓN DE MECANISMOS DE RECUPERACIÓN AUTOMÁTICA ANTE FALLAS.

Stefany del Pilar Marrugo Llorente

Proyecto de grado - como requisito final para optar por el título de Magister en Ingeniería, énfasis en Ingeniería Electrónica.

Director:

Gustavo Pérez Valdes, MSc.
Investigador– COTECMAR

Codirector:

Eduardo Gómez Vásquez, MSc.
Profesor tiempo completo Programa de ingeniería Electrónica.

Asesor:

Silvia Moreno Trillos, MSc.

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
PROGRAMA: Maestría en Ingeniería
ENFASIS: Ingeniería Electrónica
CARTAGENA, COLOMBIA
Noviembre de 2015.

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Jurado.

_____

Firma del Jurado.

Cartagena, 30/11/2015

DEDICATORIA

A Dios y a mi familia, por su apoyo y amorosa paciencia durante el proceso de elaboración del presente proyecto.

AGRADECIMIENTOS

La autora expresa sus agradecimientos a:

Dios, por darme la vida y el tiempo para realizar este proyecto.

Mis padres, por su apoyo incondicional y esfuerzo constante al educarme como mujer de investigación.

A mi familia por su ayuda y apoyo constante en el desarrollo de la investigación.

MSc, Gustavo Pérez Valdes, Ingeniero Naval Electrónico e Investigador de COTECMAR, por su invaluable colaboración y orientación en la realización del presente proyecto en calidad de Director del mismo.

MSc. Eduardo Gómez Vasquez, Ingeniero electrónico y profesor tiempo completo Universidad Tecnológica de Bolívar, por su colaboración en la realización del presente proyecto como Co-director del mismo.

MSc. Silvia Carolina Moreno Trillos, Ingeniera de sistemas, por su amable orientación en la implementación de este proyecto.

A todas esas personas y entidades, en especial a COTECMAR, que de manera directa o indirecta dieron su apoyo y colaboración para lograr el desarrollo de este proyecto.

CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

GLOSARIO DE SIGLAS Y ABREVIATURAS

ARC	Armada República de Colombia
COTECMAR	Corporación de Ciencia y tecnología para el desarrollo de la Industria Naval Marítima y fluvial.
ECR	Estación Controladora de Red
EW	Electronic Warfare
HF	High Frequency
OTAN	Organización del Tratado del Atlántico Norte
OTC	Oficial Táctico de Comunicaciones
TDL	Tactical Data Link
UC	Unidad Controladora = ECR
UHF	Ultra High Frequency
UP	Unidad Participante
VHF	Very High Frequency

RESUMEN

Este documento presenta el proceso de análisis de un sistema de enlace de datos tácticos, con el fin de identificar sus principales fuentes de falla y posteriormente, proponer e implementar mecanismos de recuperación automática, que permitan hacer más fiable el sistema bajo estudio. Se evalúa el tiempo de recuperación del sistema frente a fallas inducidas al mismo (*MTTR – Mean Time To Recovery*) y el cumplimiento de la especificación de diseño del sistema a partir de un aspecto: cantidad de veces en las que fue posible transmitir/recibir exitosamente mensajes entre unidades de la red.

Se estudian los documentos de diseño del sistema, en los cuales se describe la arquitectura empleada para la construcción del componente de software del sistema, el protocolo de comunicaciones (mensajería y reglas de intercambio de esa mensajería), esquema de seguridad administrativa y criptográfica del sistema, componentes de hardware y modos de operación de la red. Posteriormente, se analizan los estados del sistema a partir de la diagramación de su funcionamiento y se identifican estados muertos (en los cuales el sistema no es capaz de recuperarse y volver a un estado operativo) o potenciales amenazas del entorno operacional, que pueden ser originadoras de fallos.

Empleando la herramienta computacional Extend Sim 8, se simula el sistema y los mecanismos de recuperación diseñados para cada caso, con el fin de verificar su funcionamiento. Posteriormente, se implementan los mecanismos de recuperación en el sistema Data Link bajo estudio, empleando lenguaje de programación C++ en entorno Visual Studio 2010 y se procede a diseñar y ejecutar el protocolo de pruebas en laboratorio del sistema con los mecanismos de recuperación implementados.

Se mide, para cada caso de fallo, el tiempo de recuperación del sistema y se compara con los datos resultantes a partir de la recuperación manual, obteniéndose como resultado una reducción superior al 50% del tiempo promedio de recuperación de cada falla.

INTRODUCCIÓN

Para la coordinación de las operaciones en fuerzas o grupos de tarea que actualmente realiza la Armada Nacional de Colombia, es necesario que exista un intercambio de información que permita generar un panorama táctico común en tiempo real y que además incorpore herramientas que apoyen la toma de decisiones.

Si bien el mercado internacional ofrece sistemas comerciales de enlace de datos tácticos en el ambiente naval, en su mayoría se orientan principalmente hacia la generación de un panorama táctico que permita un uso efectivo de las armas y no ofrecen funcionalidades relacionadas con operaciones navales en tiempo de paz y de aplicación de la ley, funcionalidades que corresponden al tipo de operaciones que realizan constantemente las fuerzas navales de Latinoamérica y el Caribe.

Es por ello que cobra especial importancia, en el entorno regional, el desarrollo e implementación de herramientas que faciliten las actividades de mando y control relacionadas con la conducción de las operaciones en el nivel táctico, en especial de las operaciones navales en tiempo de paz.

El sistema Data Link bajo análisis, diseñado por COTECMAR para la Armada Colombiana, cumple con las características descritas previamente y se diferencia de los demás sistemas comerciales porque se encuentra diseñado exclusivamente para el tipo de operaciones que ejecutan países de nuestra región, sin embargo, es necesario mejorar la fiabilidad del sistema existente, garantizando al operador que el sistema estará en operación la mayor cantidad de tiempo posible.

La principal razón por la cual un sistema sale de funcionamiento, es por la presencia de fallas. Para detectarlas y poder diseñar mecanismos de recuperación automática, que reduzcan el tiempo "*off line*" del sistema, se hace necesario efectuar un análisis detallado de los estados del sistema y verificar en qué punto se llega a estado muertos, en los cuales el sistema no tiene forma de reanudar su operación. Con su identificación y el estudio de las características de arquitectura, protocolo y control de acceso al medio del sistema, es posible diseñar mecanismos de recuperación automática.

Como principales restricciones a la solución propuesta, se encuentra el costo (ya que al ser un sistema en estado de prototipo, los costos asociados a su desarrollo provienen de recursos destinados a investigación, los cuales son limitados) y el empleo obligatorio de la infraestructura de comunicaciones disponible (no está autorizado el empleo de hardware o software adicional al existente).

Lo anterior implica que es necesario diseñar mecanismos de recuperación que puedan ser implementados como módulos de software que se desarrollen en la herramienta de programación con que cuenta COTECMAR (Visual Studio C++) y que no afecte las prestaciones de la red. Es importante resaltar que el código desarrollado como resultado de este proyecto, será de propiedad exclusiva de COTECMAR y la Armada Nacional Colombiana, por lo que no está permitida su publicación.

El CAPÍTULO I de este documento tiene como objeto contextualizar al lector en el marco operacional mediante la presentación de la descripción del problema bajo estudio y los principales objetivos a alcanzar con el desarrollo de este trabajo.

El CAPITULO II pretende familiarizar al lector con el concepto de algunos de los términos que encontrará durante el desarrollo del proyecto. En esta sección del documento se describen aspectos fundamentales de los enlaces de datos tácticos, su entorno y posibles amenazas.

El CAPITULO III tiene como finalidad presentar al lector el estado del arte relacionado con técnicas de recuperación ante fallos en sistemas distribuidos, los cuales tienen gran similitud con los sistemas de enlace de datos tácticos bajo estudio.

El CAPÍTULO IV presentan las principales características del sistema bajo estudio. En esta sección del documento se hace un enfoque especial en el mecanismo de control de acceso al medio que utiliza el sistema, ya que de ello dependerá en gran medida el mecanismo de recuperación empleado.

El CAPITULO V contiene la descripción general de funcionamiento del sistema, a partir de la cual se detectan las situaciones de falla y se proponen mecanismos de recuperación basados en el análisis de los caminos más cortos para devolver el sistema a un estado operativo.

El CAPÍTULO VI presenta la descripción general del modelo de simulación elaborado para cada mecanismo de recuperación implementado en el sistema. Estas simulaciones fueron elaboradas empleando la herramienta computacional ExtendSim 8, que es un simulador de eventos discretos, con que cuenta COTECMAR. A partir de cada modelo se evalúa la efectividad de la solución propuesta en cada caso, teniendo en cuenta el porcentaje en el que se reduce e tiempo de recuperación de cada falla.

El CAPÍTULO VII contiene el plan de pruebas que permita verificar el correcto funcionamiento de los mecanismos de recuperación propuestos para el sistema Data Link bajo estudio. Las pruebas evalúan tanto la recuperación de la falla, como el tiempo que tarda el sistema en volver a un estado operativo. Este

resultado temporal es comparado con los resultados obtenidos en las pruebas de recuperación manual del sistema.

El CAPÍTULO VIII presenta la discusión a partir de la comparación de los resultados experimentales obtenidos Vs. los obtenidos a partir de simulaciones y los obtenidos a partir de implementación de recuperación manual del sistema. Se muestra numéricamente en cuánto fue posible disminuir los tiempos de recuperación del sistema para cada tipo de fallo y el consiguiente incremento en la fiabilidad del sistema bajo estudio.

Finalmente, el CAPÍTULO IX presenta las principales conclusiones y recomendaciones del trabajo desarrollado.

CAPITULO I. GENERALIDADES

Esta sección tiene como finalidad contextualizar al lector con el problema a resolver. Para ello, se presenta una breve descripción del problema, la situación actual y los objetivos fundamentales que se pretenden alcanzar.

1.1 DESCRIPCIÓN DEL PROBLEMA

Hoy en día, cuando las unidades de algunos componentes militares operan en grupos/fuerzas de tarea, es fundamental que todas puedan trasferir información táctica entre ellas, con la finalidad de proporcionar un panorama táctico común que facilite la coordinación en tiempo real de las operaciones.

Este intercambio de información debe hacerse a través de un sistema que garantice la privacidad, que sea fiable, transparente al usuario y que, debido a la restricción de ancho de banda de los medios de comunicaciones disponibles (HF - V/UHF), no incremente exageradamente el tamaño de los mensajes.

Sin embargo, es posible que se presenten fallas durante la operación, que disminuyan la fiabilidad del sistema. Estas fallas pueden ser debidas a aspectos de diseño del sistema (estados muertos), problemas físicos en la red (fallas en equipos, desconexión de unidades) o tecnologías de guerra electrónica, empleadas para interferir y anular sistemas de este tipo.

Para poder garantizar la fiabilidad de este tipo de sistemas es necesario estudiar a fondo el mecanismo de control de acceso al medio y los estados del sistema e identificar las posibles situaciones de falla. Lo anterior, con el fin de poder hacer un diseño de mecanismos de recuperación automática adecuados al sistema bajo análisis, procurando hacer una inversión mínima en hardware especializado y aplicando soluciones desde el componente de software, tomando como punto de partida la sincronización del sistema.

La mayor parte de los estudios desarrollados en esa materia se orientan hacia su aplicación y prueba en sistemas distribuidos tradicionales cuyas prestaciones de ancho de banda e infraestructura de hardware son altas, pero no se encontró información de la aplicación de este tipo de mecanismos en sistemas de enlace de datos tácticos, donde además de errores en las tramas de mensajes, es frecuente que se presenten interferencias debido a mecanismos de ataque de guerra electrónica.

Debido a los costos de implementación, no es posible proponer una solución basada en redundancia, como mecanismo de solución ante fallas, pero si es posible determinar, según los requerimientos del sistema, un mecanismo de recuperación que se base en el análisis de los estados del sistema y el manejo de sincronía, que utilice la infraestructura disponible y que además constituya una alternativa de bajo costo para la implementación en sus sistemas.

El principal problema a resolver cosiste entonces en la identificación, clasificación y recuperación automática de fallas permanentes en un sistema de enlace de datos tácticos, de forma oportuna, con miras a incrementar la fiabilidad del sistema.

1.2 SITUACIÓN ACTUAL

El sistema de enlace de datos (Data Link) que se tomará como base para el diseño e implementación de los mecanismos de recuperación automáticos ante fallas no es un link OTAN, debido a que Colombia no hace parte del grupo de naciones que conforman dicha organización.

Colombia cuenta solamente con unos pocos sistemas de enlace de datos tácticos, utilizados únicamente en algunos buques Militares, dejando por fuera unidades menores que también participan en grupos de tarea, motivo por el cual es necesario que se conecten a este tipo de sistemas, permitiendo tener un mejor mando y control de las operaciones.

Con el desarrollo de un nuevo sistema de enlace de datos tácticos diseñado por COTECMAR para las necesidades operativas y económicas de países como el nuestro (este será el sistema tomado como base para desarrollar este proyecto), se abre el horizonte de investigación en este campo y se reduce la dependencia tecnológica que en estos momentos se tiene en materia de sistemas Data Link. Garantizar la fiabilidad de un sistema de este tipo no es tarea fácil, ya que requiere mucha investigación para conocer en detalle el funcionamiento del sistema, sus potenciales falencias y amenazas.

Actualmente, el sistema presenta una fiabilidad cercana al 90%. Lo anterior ha sido determinado después de varios años de pruebas en laboratorio y a bordo de plataformas. Sin embargo, y a pesar que es poco común que se presenten fallas en el sistema, las veces que se han presentado situaciones de este tipo, la recuperación ante la falla se hace de forma manual, por lo que los tiempos que dura el sistema fuera de servicio tienden a ser prolongados y dependientes de la experticia que tenga el operador del sistema para detectar la falla.

Diseñar e implementar mecanismos de recuperación de un sistema de este tipo, constituye un aporte significativo al campo del diseño de sistemas de comunicación RF y contribuye metodológicamente al diseño e implementación de Data Links, ya que se pretende dar solución por software a todas las fallas que se identifiquen, en vista que se cuenta con un hardware de características limitadas.

En general, la recuperación oportuna y automática de fallas en un sistema Data Link, es necesaria porque permite incrementar la eficiencia en el mando y control de las operaciones, incrementa los índices de fiabilidad del sistema y mejora la calidad del producto/servicio prestado.

1.3 OBJETIVOS

1.3.1 Objetivo General

Diseñar e implementar mecanismos de recuperación para un sistema de enlace de datos tácticos, basado en técnicas de sincronía, con el fin de incrementar su fiabilidad durante las operaciones.

1.3.2 Objetivos Específicos

- Identificar las características de hardware y software del sistema Data Link bajo estudio, a partir del análisis de sus funcionalidades y propiedades, de tal forma que sea posible determinar y clasificar las posibles fallas.
- Analizar las posibles fallas en el sistema debidas al entorno operacional o estados muertos, mediante el estudio de técnicas de guerra electrónica que se podrían aplicar y la identificación de los estados del sistema, con el fin de diseñar los mecanismos de recuperación adecuados.
- Validar los mecanismos de recuperación propuestos, mediante simulación de cada situación.
- Implementar los mecanismos de recuperación apropiados a cada tipo de falla identificada, a través del componente de software del sistema bajo estudio, con el fin de garantizar su fiabilidad.
- Verificar el funcionamiento del mecanismo de recuperación del sistema, mediante la realización de pruebas en laboratorio

CAPITULO II. MARCOTEÓRICO

Esta sección del documento pretende familiarizar al lector con el concepto de algunos de los términos que encontrará durante el desarrollo del proyecto. Se describen aspectos fundamentales de los enlaces de datos tácticos, su entorno y posibles amenazas.

2.1 DEFINICIONES GENERALES

2.1.1 Enlaces de Datos Tácticos (TDL) o Data Links

Un enlace de datos tácticos, es un sistema de comunicaciones tácticas, basado en radio comunicaciones, que permite gestionar la información táctica de una fuerza o grupo de tarea y mediante herramientas de explotación de información, mejorar la toma de decisiones y las funciones de mando y control. (COTECMAR, 2011)

Los Enlaces de Datos Tácticos (TDL) habilitan el intercambio de datos a través de radio entre plataformas, con el objeto de evitar o minimizar las comunicaciones de voz que pueden ser críticas en ambientes de acción o combate (CPT/CIA, 2008). El principio básico de su operación es enlazar las unidades subordinadas con el respectivo comando operativo en tiempo real. Actualmente, gran parte de las comunicaciones militares (voz y no-voz) son transmitidas en forma de datos, facilitando a las fuerzas militares la coordinación de sus acciones en tierra, mar y aire (Asenstorfer, Cox, & Wilksch, 2004). Los TDL han sido estandarizados por la OTAN (STANAG) desde 1991.

Técnicamente, los TDL definen una familia de protocolos conocidos como Links, que han ampliado la cobertura de las comunicaciones militares a través de redes inalámbricas que interconectan buques, submarinos, tanques, bases en tierra, etc. Estos protocolos se enmarcan dentro de las capas física y enlace (uno y dos respectivamente) del modelo de referencia OSI, definiendo aspectos relacionados con el acceso al medio y la transmisión de la información sobre los enlaces de radio (Benavides & Montañez, 2008).

2.1.2 Fallos.

Los fallos (faults) son las causas mecánicas o algorítmicas de los errores en un sistema (Burns & Wellings, 2001).

Estos fallos pueden ser de tres (3) tipos:

- Fallos transitorios
  Desaparecen solos al cabo de un tiempo

Ejemplo: interferencias en comunicaciones

- Fallos permanentes
  Permanecen hasta que se reparan
  Ejemplo: roturas de hardware, errores de diseño de software
- Fallos intermitentes
  Fallos transitorios que ocurren de vez en cuando
  Ejemplo: calentamiento de un componente de hardware (De la Puente, 2001).

2.1.3 Fiabilidad.

La fiabilidad (reliability) de un sistema es una medida de su conformidad con una especificación autorizada de su comportamiento. En otras palabras, es la capacidad que tiene un sistema para comportarse de acuerdo con su especificación. En muchos casos es medido de forma similar a la disponibilidad del sistema (Burns & Wellings, 2001).

2.1.4 Guerra Electrónica.

La guerra electrónica o EW, por sus siglas en inglés (Electronic Warfare), es el nombre que se le da a todas aquellas acciones que tienen por objeto bloquear, interceptar o negar las comunicaciones de un punto transmisor a otro receptor. (Poisel, 2004)

2.1.5 Ataque Electrónico.

Puede ser efectuado por medio de tres tipos de acciones o técnicas (Nocedal, 2006):

- Jamming:
  Actividad que afecta la línea de tiempo en alguna comunicación. Es decir, logra que la información no llegue al receptor en el momento que debía hacerlo. Al afectar esto se afecta también la relevancia de la información. Esto se debe a que la información solamente es útil en determinado instante. No es útil si se recibe antes o después del tiempo establecido.(Poisel, 2004)(Xu, Wade & Yanyong, 2006).

- Engaño:
  Esta técnica tiene como objetivo formar una nueva ruta de comunicación (Poisel, 2004). En este caso, en lugar de que la información llegue al receptor deseado, ésta sufre un cambio de ruta y es recibida por otro receptor. De igual forma, el engaño puede consistir en la sustitución del

sistema transmisor. En este caso, el receptor original está recibiendo una señal que proviene de un segundo sistema transmisor. Cuando el receptor está ocupado no puede recibir la señal emitida por el transmisor original.

- Radiación directa de energía:
  La radiación directa de energía es la manera más fácil de atacar a un sistema de comunicación. Sin embargo, es la mas fácil de detectar y poder evitar. Consiste en enviar una determinada señal con determinada potencia para dañar o destruir completamente la comunicación entre transmisor y receptor. La potencia emitida debe ser mayor a la que emplea el transmisor del sistema que está sobre ataque. (Xu, Wade & Yanyong, 2006)

Un dispositivo capaz de emplear cualquiera de las tres técnicas o una combinación de ellas para interferir, dañar o destruir la transmisión de información dentro de un sistema electrónico de comunicaciones es llamado *Jammer*. (Xu, Wade & Yanyong, 2006).

2.2 ENLACES DE DATOS TÁCTICOS

Con el fin de proporcionar un mejor contexto respecto a los distintos enlaces de datos que existen, a continuación se describirán las características más relevantes de los tipos de TDL más significativos en la actualidad.

2.2.1 Link 11

Link 11 es un enlace de datos táctico basado en tecnología de los años sesenta, por lo tanto su velocidad de transmisión es relativamente baja y oscila entre los 2250 y 1364 bps. Igualmente, la capacidad de una red Link 11 es limitada, admitiendo un máximo de 20 participantes. Este tipo de enlace puede operar en la banda de HF con un alcance de hasta 300 NM y en UHF con un alcance aproximado de 25 NM (Publishing-Integrated, 2007).

A través de una red Link 11, se intercambian mensajes pertenecientes a la serie “M” para representar información relacionada con trazas aéreas, de superficie, submarinas, guerra electrónica (EW) y un número limitado de órdenes de mando.

En cuanto a la técnica de acceso al medio empleada, Link 11 opera a través de un mecanismo de sondeo denominado “Roll Call”, en el cual las unidades participantes (UPs) transmiten la información cuando son interrogadas por una Unidad de Control de Red (NCS); cuando se completa el envío de los datos, las unidades pasan a modo recepción al tiempo que otra unidad transmite sus datos. El tiempo requerido para que todos los participantes de la red transmitan sus datos se denomina “Net Cycle Time”. De esta forma, en un momento

determinado una PU está transmitiendo o recibiendo datos en una red Link 11 simple.

Como complemento al modo “Roll Call”, Link 11 puede operar en modo Radiodifusión, permitiendo a un participante efectuar una o varias transmisiones sobre la red. De esta manera, el Link 11 se comporta como un enlace semiduplex es decir, utiliza el mismo medio para transmitir y recibir pero no al mismo tiempo.

Con respecto a la transmisión de la señal, actualmente existen dos formas de onda distintas e incompatibles para transmitir la información en Link 11: CLEW (Conventional Link Eleven Waveform) y SLEW (Single Tone Link Eleven Waveform). CLEW está compuesta por 16 tonos de audio multiplexados (entre 600 y 3000 Hz), de los cuales 15 son portadores de información (2 bits cada uno). El tiempo empleado para transmitir una trama Link 11 puede variar entre 13,33 o 22 ms, configurables como opción de operación de red. Sin embargo, CLEW no ofrece las garantías suficientes para el intercambio de información ya que produce una señal fácil de detectar y perturbar, con altas tasas de pérdidas de datos.

Este fue uno de los aspectos negativos del Link 11 que promovieron la formación del grupo NILE (NATO Improvement Link Eleven) con el objeto de diseñar un enlace que superara los inconvenientes encontrados, iniciativa que daría origen al Link 22, el cual se describirá más adelante. Sin embargo, ante la necesidad de una solución inmediata a los problemas asociados con la transmisión de la información, Link 11 SLEW hizo su aparición como un desarrollo transitorio. A diferencia de CLEW, la forma de onda de la señal SLEW sufre un proceso complejo de transformación y modulación en la que la información va contenida en un solo tono al cual se le varía la fase, con ocho posibles desfases.

A pesar de las mejoras introducidas, la dependencia de la red de una unidad NCS y la ausencia de mecanismos de contramedidas electrónicas (ECM), hacen que una red Link 11 se considere vulnerable.

2.2.2 Link 11B

En términos simples, Link 11B es la implementación terrestre de los mensajes de la serie “M”; ésta difiere ligeramente con respecto a Link 11, en aspectos como la inclusión de un mensaje exclusivo de control del estado de la conexión punto a punto, y la supresión de algunos mensajes.

A diferencia de Link 11, emplea un esquema de transmisión punto a punto, es dúplex y opera a una velocidad de transmisión de 1200 bits por segundo o 2400 bits por segundo, opcionalmente (CPT/CIA, Sumario de Data Link, 2008).

2.2.3 Link 16

Link 16 es un enlace de datos táctico basado en tecnología de los años setenta. Su capacidad de transferencia es superior a la del Link 11 (normalmente 57,6 Kbps), es resistente a las perturbaciones y está diseñado para cubrir una amplia gama de operaciones militares (navales, aéreas y terrestres), brindando soporte a las unidades requeridas. No obstante, sólo opera en la banda de UHF lo cual restringe su alcance, haciendo necesario el uso de repetidores para ampliar la cobertura del enlace (Asenstorfer, Cox, & Wilksch, 2004).

La capacidad de este enlace se incrementa sustancialmente con respecto al Link 11 (1000 participantes), gracias al uso de una técnica de acceso al medio más eficiente conocida como TDMA (Time Division Multiple Access). Esta técnica, intercala la información de las unidades en periodos de tiempo (time slots), dando la apariencia de disponibilidad de múltiples redes de comunicaciones. A cada participante JU ("JTIDS Unit") se le asignan varios conjuntos de intervalos de tiempo, para funciones de transmisión y recepción de información. Cada intervalo de tiempo tiene una duración fija de 7,8125 milisegundos.

Adicionalmente, Link 16 ofrece la posibilidad de configurar múltiples redes simultáneas a través del uso redundante de los intervalos de tiempo, transmitiendo datos en cada red utilizando una frecuencia distinta de las 51 disponibles para tal fin. Esta frecuencia no permanece constante y durante un intervalo de tiempo, cambia cada 13 microsegundos de acuerdo con un patrón pseudo aleatorio predeterminado, técnica conocida como salto de frecuencia (frecuency hopping). Adicionalmente, a cada red se le asigna un identificador que representa un patrón de salto determinado; existen 128 identificadores posibles (0-127), de los cuales uno (127) es reservado para identificar una configuración de red apilada (stacked net); el concepto de red apilada permite que la misma secuencia de intervalos de tiempo pueda ser utilizado por más de una red, asignando un patrón de salto de frecuencia distinto a cada una. De esta forma, durante un intervalo de tiempo específico, una unidad se encuentra transmitiendo o recibiendo información en cualquiera de las 127 redes posibles.

En cuanto a la estructura de mensajes, Link-16 define tres tipos:

a. Formato fijo (serie “J”): Generalmente, un mensaje de este tipo está formado por un número variable de palabras (normalmente 1, 2 ó 3), con un máximo de 40. Cada palabra contiene 70 bits de datos, equivalente a una trama Link-11. En un intervalo de tiempo de 7.8125 milisegundos se pueden transmitir 3, 6 ó 12 palabras, dependiendo del tipo de estructura utilizada (Standard, Packed-2 ó Packed-4), alcanzando una velocidad efectiva de transferencia de datos de 26880, 53760 ó 107520 bps. Si se incluyen los 5 bits de paridad a cada palabra la velocidad aumenta a 28800, 57600 ó 115200 bps.

b. Formato variable: Este tipo de mensajes utiliza la misma estructura del tipo anterior, pero con formato distinto (menor o mayor a una palabra). Se diseñaron para mantener la compatibilidad con Link 11B.

c. Texto libre: Estos mensajes no tienen un formato específico y se utilizan para transmisión de voz, video o texto.

Gracias a la técnica TDMA definida por Link 16, una de las novedades más importantes de este tipo de enlace para el intercambio de mensajes es la definición de Grupos de Participación NPG (Network Participation Groups). Cada NPG tiene una función específica y por lo tanto, un intercambio de mensajes distinto; esto permite que cada JU participe únicamente en los grupos que tienen correspondencia con las tareas que desarrollan. Algunos de los grupos definidos son los siguientes:

a) Vigilancia
b) EW
c) Gestión de la Misión.
d) Coordinación de Armas.
e) Control Aéreo.
f) Enlace entre cazas.
g) Voz segura.
h) Localización e Identificación Precisa de Participantes (PPLI).

Áreas funcionales de Link 16

Las funciones técnicas de Link 16 abarcan la gestión de la Red y el intercambio de información táctica relativa a las siguientes 12 áreas funcionales (CPT/CIA, Introducción a Link 16, 2008):

a. Intercambio de Información del Sistema y de Gestión de Red: Esta función facilita el intercambio de información requerido para el establecimiento y mantenimiento de la interfaz a través de Link 16. Comprende mensajes de sincronización, temporización, asignación de capacidad, control de relés y otros datos destinados a asegurar la interoperabilidad entre los participantes.

b. Identificación y Localización Precisa de Participantes (PPLI): La función PPLI habilita a los participantes para informar de manera exacta y actualizada su identificación y estado de participación en la red.

c. Vigilancia Aérea: Consiste en la detección, seguimiento, identificación e informe de las trazas aéreas. Esta función incluye el cálculo de rumbo, velocidad, posición y determinación de la identidad de la traza. De esta manera, los participantes son capaces de desplegar avisos de alerta temprana, amenaza, correlación de trazas e información de tráfico aéreo.

d. Vigilancia de Superficie (Marítima): Consiste en la detección, seguimiento, identificación e informe de trazas de superficie. Esta función incluye el cálculo de rumbo, velocidad y posición de trazas. De esta manera, los participantes son capaces de desplegar avisos de alerta temprana, amenaza, correlación de trazas y recopilar datos sobre la situación de superficie.

e. Vigilancia Antisubmarina (Marítima): Consiste en la detección, seguimiento, identificación e informe de trazas submarinas. Esta función incluye el cálculo de rumbo, velocidad y posición de trazas. De esta manera, los participantes son capaces de desplegar avisos de alerta temprana, amenaza, correlación de trazas y recopilar datos sobre la situación submarina.

f. Vigilancia Terrestre: Consiste en la detección, seguimiento, identificación e informe de trazas y puntos terrestres. De esta manera, los participantes son capaces de desplegar avisos de alerta temprana, amenaza, correlación de trazas y recopilar datos sobre la situación terrestre.

g. Vigilancia Espacial: Consiste en la detección, seguimiento, identificación e informe de trazas del espacio, incluyendo misiles balísticos. Esta función Incluye el cálculo del rumbo de la trayectoria, velocidad y posición. De esta manera, los participantes son capaces de desplegar avisos de alerta temprana, amenaza, correlación de trazas y recopilar datos sobre la situación espacial.

h. Vigilancia Electrónica: Consiste en la detección, seguimiento e identificación de emisores y perturbadores.

i. EW/Inteligencia: Esta función técnica permite ampliar la información de vigilancia y entregar información de inteligencia táctica.

j. Gestión de la misión: Facilita el intercambio de información para la gestión y planeación de la misión. Entre las funciones que se deben llevar a cabo, se destaca el control de la ubicación actual de la fuerza de combate para satisfacer las necesidades de apoyo inmediato a la misión. Esto incluye, informes requeridos por el mando táctico para llevar a cabo los requerimientos de la misión; órdenes de operaciones aéreas, terrestres, de superficie y antisubmarinas; reparto de salidas e informes en vuelo y de misión. Normalmente, el nivel de mando que implementa esta función técnica no controla directamente los sistemas de armas, pero es responsable de la asignación oportuna de los recursos de las unidades subordinadas de mando y control (C2). Esta función, sin embargo, permite la interacción entre unidades tácticas tanto al mismo nivel como entre mandos y unidades subordinadas.

k. Gestión y coordinación de armas: Consiste en el intercambio de órdenes y de información necesaria para llevar a cabo un uso óptimo de todas las armas y prevenir interferencias mutuas durante las operaciones tácticas.

Esta función técnica facilita el intercambio de información entre unidades C2 que manejan o tienen bajo su control sistemas-de-armas/plataformas-de-apoyo (Por ejemplo: unidades de reconocimiento, buques logísticos, etc.). Las misiones de interceptación, reconocimiento, apoyo aéreo cercano, control de misiles/RPV, guerra antisubmarina, y otras misiones son apoyadas por esta función técnica.

l. Control: Son las acciones en tiempo real, entre sistemas de control y sistemas de armas/apoyo, necesarias para dirigir los sistemas-de-armas/plataformas-de-apoyo en el cumplimiento de la misión asignada. La función técnica del control facilita el intercambio de información entre unidades C2 y sistemas de armas/plataformas para llevar a cabo el control de aeronaves, control de superficie, control antisubmarino y control terrestre. Además, facilita el intercambio de información de coordinación entre sistemas de armas/plataformas de apoyo, tales como datos de EW o blancos entre unidades. Se incluyen en esta función las misiones de reabastecimiento, maniobras terrestres, vigilancia en el combate, adquisición de blancos, reabastecimiento en vuelo, control del tráfico aéreo, control de desembarco, control EW, control de aeronaves antisubmarinas, etc.

m. Gestión de información: Corresponde a los procedimientos e intercambio de información necesarios para asegurar que las plataformas/sistemas llevan a cabo un efectivo intercambio de datos cuando están interconectadas. Esto hace referencia a la gestión de seguimiento de trazas, solicitudes de información, correlación, identificación de trazas, gestión de filtros, etc. Los datos de gestión de información deben ser los mismos en las funciones de vigilancia aérea, de superficie, antisubmarina, terrestre y electrónica.

JTIDS (Joint Tactical Information Distribution System)

JTIDS hace referencia al componente de comunicaciones de Link 16, lo cual incluye el software, hardware, equipo RF y el *waveform* del terminal. La primera generación de terminales JTIDS fueron el resultado de veinte años de desarrollo del hardware y software de Link 16; estas versiones eran limitadas en capacidad y no fueron ampliamente distribuidas en unidades operacionales. Su implementación inicial fue dirigida a la fuerza aérea de Estados Unidos y la aeronave E-3 Sentry AWACS (Airborne Warning and Control System) de la OTAN, desarrollando un prototipo general de mensajes denominado IJMS (Interim JTIDS Messaging System) (Asenstorfer, Cox, & Wilksch, 2004).

Los terminales de segunda generación (JTIDS Class 2), proporcionan soporte para la implementación de mensajes serie J Link 16; éstos fueron producidos a principios de los 90 para el ejército, armada y fuerza aérea de Estados Unidos, con algunos inconvenientes: alto porcentaje de fallas de terminal, tiempo de vida reducido para componentes clave y problemas de confiablidad del software. Por otro lado, la amplia diversidad de requerimientos no permite que exista una configuración única que reúna la totalidad de los mismos lo cual ha generado el

desarrollo de una amplia variedad de implementaciones hardware y software (Minges, 2001).

MIDS (Multi-function Information Distribution)

A partir de la guerra del Golfo, las comunicaciones de datos para la transferencia de información como detección de blancos y amenazas cobraron más relevancia; en este sentido varios desarrollos exitosos se llevaron a cabo usando JTIDS. Sin embargo, casi al mismo tiempo Estados Unidos y al OTAN iniciaron el desarrollo del programa internacional MIDS, el cual implementa terminales de comunicaciones de datos compatibles con Link 16. Por esta razón, es posible establecer que MIDS es el término equivalente a JTIDS entre los países miembros de la OTAN (Asenstorfer, Cox, & Wilksch, 2004).

En general, MIDS provee comunicaciones de datos interoperables para conectar aviones y controladores aéreos, nodos de comando y control aéreos y terrestres, y demás relacionados con acciones de inteligencia, vigilancia y reconocimiento. Específicamente, los objetivos del programa son los siguientes:

a. Interoperabilidad operacional de capacidades de vigilancia y comando y control.

b. Interoperabilidad de centros terrestres aéreos y marítimos.

c. El uso de capacidades de posicionamiento y localización de participantes, para funciones de identificación de fuerzas amigas o enemigas (Identification Friend or Foe - IFF).

d. Disponibilidad de información precisa e información de estado de todos los participantes en una coalición, que supere las barreras del lenguaje y ayude a integrar las fuerzas.

e. Facilidad para el intercambio tecnológico entre Estados Unidos y los países de la OTAN.

f. Incrementar los niveles de interoperabilidad entre las fuerzas de los Estados Unidos.

2.2.4 Link 22

Originalmente, Link 22 fue conocido con el nombre de NILE (NATO Improvement Link Eleven), un programa que fue creado con el objeto de reemplazar a Link 11. Link 22 retoma algunos elementos de la técnica de acceso TDMA de Link 16 tanto en frecuencia fija como en salto de frecuencia, pero a diferencia de éste opera en las bandas de UHF (225-400 MHz) y HF (3-30 MHz), lo cual permite incrementar la cobertura hasta 300 MN en el segundo caso. Todos los participantes (NU) de la red, tienen la capacidad de participar en una sola red

Link 22 o ejecutar una operación multi-red estableciendo más de una conexión de forma simultánea (4 redes como máximo) (CPT/CIA, Sumario de Data Link, 2008); un conjunto de redes interconectadas recibe el nombre de Superred (Super Network). Las diferentes redes pueden usar el mismo medio (por ejemplo una frecuencia fija en HF o UHF) o una combinación de medios (frecuencias UHF y HF) (Joint-staff, Joint multi-tactical data link (TDL) operating procedures, 2002).

Link 22 es un enlace seguro resistente a la perturbación (ECM-resistant) que ha sido desarrollado para satisfacer los requisitos operativos de intercambio de información táctica entre Sistemas de Combate e intercambio de datos relacionados con la gestión de la red.

En cuanto al intercambio de información, Link 22 transporta datos tácticos desde un participante hacia uno o más destinos usando mensajes de la serie F. Por otro lado, el intercambio de datos operacionales usa mensajes relacionados con la identificación y localización del participante, vigilancia, guerra electrónica (EW), inteligencia, control de armas, gestión de la misión y estado de los participantes. Existe la posibilidad que un mensaje Link 22 pueda ser incluido en la estructura de un mensaje de la serie J Link 16 (mensaje FJ); aunque los mensajes de la serie F y la serie J usan el mismo diccionario de elementos de datos (DED) (Northrop-Grumman, 2002), los mensajes de la serie FJ son más adecuados cuando se busca interoperabilidad entre estos dos tipos de data links.

Mejoras de Link 22 con respecto a Link 11

A continuación se describen las principales mejoras introducidas por Link 22 como evolución de Link 11 (Asenstorfer, Cox, & Wilksch, 2004).

a. *Medidas de protección electrónica*: Link 22 usa técnicas de cifrado modernas, soporte opcional de control de potencia y salto de frecuencia para disminuir la posibilidad de interceptación de la comunicación y uso alternativo de arreglos de antenas adaptativas que proporciona capacidades adicionales para supresión de interferencia y jamming.

b. *Ampliación de la capacidad de los mensajes tácticos*: Link 22 proporciona un incremento significativo sobre la capacidad de transferencia original de Link 11. Usando el modo de frecuencia fija en HF, es posible alcanzar velocidades de 4.053 Kbps, mientras que con UHF la tasa de transferencia puede llegar a los 12.667 Kbps. Considerando el hecho que una unidad puede conectarse simultáneamente con cuatro redes como máximo, una configuración típica usando tres frecuencias fijas en HF y una frecuencia fija en UHF, permitiría alcanzar una velocidad de 24.826 Kbps. Alternativamente, una configuración de dos frecuencias fijas en HF y dos en UHF permitiría alcanzar los 33.440 kbps. Por otro lado, Link 22 facilita el intercambio simultáneo de diversos tipos de mensajes relacionados con guerra anti-aérea (anti-air warfare AAW), guerra anti-submarina (anti-submarine warfare ASUW), guerra anti-superficie (anti-surface warfare ASW), guerra electrónica (electronic warfare EW), etc,

mientras que Link 11 generalmente se concentra en una de estas plataformas.

c. *Ampliación de la capacidad de unidades participantes*: Link 22 puede soportar más unidades por frecuencia operativa que Link11, cuando opera con tasas de transferencia más altas. Adicionalmente, Link 22 brinda soporte de hasta 4 redes diferentes por unidad y hasta 8 redes en un área de responsabilidad extendida con un total de 125 unidades.

d. *Mejora en la eficiencia*: Gracias el uso de la técnica TDMA, Link 22 elimina la dependencia de la conectividad que debe existir entre cada unidad y la Estación de Control de Red (NCS). Esta característica mejora la eficiencia, confiabilidad y cobertura de la red. Igualmente, Link 22 provee capacidades de redundancia a las unidades participantes a través de mecanismos de diversidad en tiempo, frecuencia y patrones de antena; el receptor Link 22 puede operar en diferentes frecuencias y redes.

e. *Mejora en los procesos de detección y corrección de errores*: Link 22 usa técnicas más avanzadas de detección y corrección de errores con respecto a Link 16 (chequeo de paridad CRC-16). Dependiendo de la forma de onda (waveform) se utiliza Reed-Solomon o codificación convolucional.

f. *Flexibilidad y mayor rapidez en los procedimientos*: Link 22 ofrece procedimientos de gestión de red automatizados y más flexibles. Soporta reasignación dinámica de intervalos de tiempo y una optimización automatizada de este proceso.

g. *Conjunto de mensajes más robusto*: Link 22 amplía el conjunto de mensajes para soportar datos relacionados con la posición e identificación de fuerzas amigas y terrestres, mejorando la granularidad de los mismos. El formato de datos es compatible con Link 16, haciendo más simple el proceso de transmisión de datos de un enlace táctico a otro (data forwarding).

h. *Reuso de la infraestructura existente*: Una de las ventajas de Link 22 es el reuso de los módems, radios y demás equipos requeridos para la operación en frecuencia fija de Link 11, al tiempo que permite la utilización de computadores comerciales (COTS).

Link 22 como complemento a Link 16

Aunque Link 22 y Link 16 hacen parte de la familia J de enlaces de datos tácticos, tiene características distintas que los hace complementarios. En principio, Link 16 es un data Link AAW (Anti Air Warfare) que frecuentemente depende de repetidores aerotransportados para lograr el rango de cobertura requerido. Por otro lado, Link 22 es principalmente un data link marítimo (ASW/ASUW) menos dependiente de repetidores aerotransportados, gracias a su capacidad de operar en HF y mecanismos de retransmisión barco a barco, que permiten ampliar la

cobertura. En este sentido, Link 22 es capaz de liberar capacidad adicional para Link 16 particularmente en conflictos de alta intensidad (Asenstorfer, Cox, & Wilksch, 2004).

En concordancia con su aplicación, Link 16 ofrece tasas de transferencia más altas que Link 22. Mientras que el primero tiene una capacidad promedio de 57.6 Kbps, el segundo tiene una capacidad máxima de 33.44 Kbps (usando dos redes UHF y dos redes HF). Sin embargo, la capacidad de transferencia real depende de la configuración de la red; si se utiliza la estructura de paquetes ECM más resistente, la tasa ofrecida por Link 16 es de sólo 28.8 kbps, mientras que el uso de la menos resistente incrementa la capacidad a 238.08 Kbps.

Con respecto a la estructura de red, durante un periodo de tiempo corto ésta es esencialmente fija en Link 16. Por su parte, Link 22 es más flexible y puede reconfigurarse más fácilmente ante los cambios gracias a operaciones de gestión de red automatizadas en unidades especializadas.

Finalmente, aunque Link 16 y Link 22 usan formas de onda diferentes comparten características similares. Son seguros y usan mecanismos de detección y corrección de errores. Adicionalmente, estos enlaces de datos pueden transmitir los mensajes con el mismo nivel de granularidad.

STDL (Satellite Tactical Data Link)

En principio, los Enlaces de Datos Tácticos no han sido diseñados para operar usando comunicaciones satelitales. Sin embargo, la principal motivación para la utilización de este tipo de enlaces es la posibilidad de ampliación de cobertura que éstos ofrecen. A continuación se describen algunas consideraciones relevantes sobre la operación de data links sobre enlaces satelitales (CPT/CIA, Sumario de Data Link, 2008).

a. *Link 11 sobre satélite*. La tecnología de los DTS modernos permite la transmisión de mensajes de la serie “M” sobre satélite, para ampliar la cobertura de Link 11. De esta manera, grupos de combate que operan fuera del alcance normal pueden unirse a la red; un barco de cada grupo debe designarse como unidad de radiodifusión satelital, para habilitar el intercambio de trazas entre las PUs radio y las PUs satélite.

b. *Link 16 sobre satélite*. Link 16 a través de satélite es una alternativa interesante para superar las limitaciones que impone el alcance visual requerido para este tipo de enlaces. El acceso al satélite se efectúa a través de TDMA usando un solo canal, generando tres modos posibles de funcionamiento; en red, radiodifusión e inter-grupo.

   La radiodifusión consiste en la transmisión de datos por parte de una sola unidad, al tiempo que el resto escuchan; en red, cada participante transmite los datos en los intervalos de tiempo asignados; en el modo inter-grupo, un

barco de cada grupo transmite los datos en representación de los participantes que lo componen.

No obstante, para lograr los beneficios asociados a la utilización de enlaces satelitales para Link 16, es necesario superar algunas barreras relacionadas con la capacidad inferior del canal satelital con respecto a la comunicación terrestre y los mayores retardos asociados a este tipo de comunicación.

Una medida efectiva para afrontar la limitación que existe en la capacidad del enlace, es una selección rigurosa de la información a transmitir. Por ejemplo, los datos asociados a la vigilancia aérea de superficie y submarina podrían tener una alta prioridad de transmisión. Sin embargo, pueden existir casos en los cuales se deba tolerar cierta degradación en la actualización de la información. Con respecto al retardo, el receptor debe estar preparado para tolerarlo, ya que éste puede afectar la exactitud de los datos; por otro lado, es importante tener en cuenta que los dispositivos de recepción pueden estar recibiendo la misma información a través del enlace satelital o comunicación terrestre. Otra consideración relevante, tiene que ver con el uso de protocolos de acuerdo ("*handshake*") en algunos mensajes Link 16; éstos fijan un periodo de validez para el mensaje, lo cual admite la posibilidad de ser rechazados por causa del retardo introducido. Por esta razón, es necesario ajustar el periodo de validez de estos mensajes con anterioridad.

2.2.5 Resumen comparativo de Data Links

Luego de realizar una descripción general de cada uno de los tipos de Data Links, la tabla 2 muestra un resumen comparativo con las características más importantes discutidas anteriormente. Adicionalmente, la Tabla 2 muestra la equivalencia entre la nomenclatura de *Links* utilizada por la OTAN y la denominación TADIL, de uso exclusivo en Norteamérica.

Finalmente, la Tabla. 1 muestra la documentación OTAN correspondiente a cada Data Link.

Tabla 1. Cuadro comparativo Data Links OTAN

Característica	LINK 11	LINK 11B	LINK 16	LINK 22
Portadora	UHF/HF	UHF/HF	UHF	UHF/HF
Número de Participantes	20	2	1000	128
Acceso al medio	Sondeo	Punto-punto	TDMA	TDMA
Distribuido	No	N/A	Sí	Sí
Voz	No	No	Sí	No
Velocidad(Kb)	1,8	1,8	57,6 o +	32
Protección a perturbación	No	No	Sí	Sí
Seguro	Sí	Sí	Sí	Sí
Formato de mensajes	M	M	J	F

Fuente: (CPT/CIA, 2008)

Tabla 2. Equivalencia nomenclatura OTAN y Norteamericana para Data Links

OTAN	EE.UU
LINK-11	TADIL A
LINK-11B	TADIL B
LINK-16	TADIL J

Fuente: (CPT/CIA, 2008)

Tabla 3. Data Link - Documentación OTAN

Link	Definición	Procedimientos	Documentos relacionados
LINK 11	STANAG 5511	ADatP 11	STANAG 5601
LINK 11B	STANAG 5511	ADatP 11	STANAG 5601/5616
LINK 16	STANAG 5516	ADatP 16	STANAG 5616/4175/NETMAN D1
LINK 22	STANAG 5522	ADatP 22	STANAG 5616

Fuente: (CPT/CIA, 2008)

2.2.6 CDL (Common Data Link)

El término CDL describe una familia de *Data Links,* diseñados principalmente para soportar tareas de reconocimiento y vigilancia. Estos links proporcionan capacidades *full dúplex*, banda ancha (asimétrica) y enlaces de datos punto a punto entre aviones y barcos o entre aviones y bases terrestres. Esto permite la transmisión de información de radar, imagénes, video y datos de otros sensores desde plataformas aéreas y la transmisión de datos de control hacia este tipo de plataformas (Asenstorfer, Cox, & Wilksch, 2004).

Contrario a otros tipos de *Data Links* como Link 11, Link 16 y Link 22, CDL está diseñado para satisfacer una necesidad específica y no está pensado para ser un enlace de datos genérico. Mientras Link 11, Link 16 y Link 22, tienen la capacidad para enviar varios tipos y tamaños de información para adaptarse de forma flexible a un gran conjunto de requisitos, no ofrecen el ancho de banda proporcionado por CDL. Por otro lado, CDL sólo puede soportar la transmisión de datos a una plataforma de superficie desde una plataforma aérea o un pequeño grupo de plataformas de este tipo, en un intervalo de tiempo corto; la plataforma de superficie procesa los datos y renvía la información apropiada a las otras plataformas, posiblemente a través de alguno de los *Data Links* mencionados.

Con respecto a la operación de CDL, un sistema típico está compuesto por las siguientes partes:

a. Una interface con los sensores aéreos y el sistema de control.

b. Subsistemas de RF y módem aéreo.

c. Procesamiento de *Data Links* en la plataforma de superficie, modem y subsistemas de RF.

d. Interface a los usuarios de datos en la plataforma de superficie.

Los usuarios que requieren datos de sensores en la plataforma de superficie se conectan a la aeronave a través de 10 canales en *uplink* y hasta 25 canales en el *downlink*. El *uplink* o *link* de comando es el enlace con la aeronave y el *downlink* o *link* de retorno corresponde al enlace desde la aeronave hasta la plataforma de superficie. Dentro del *uplink*, existen canales para funciones de gestión y comunicaciones de voz; este enlace seguro y resistente a técnicas de *jamming* opera a una velocidad de 200 Kbps. Dentro del downlink, existe igualmente un canal de voz; este enlace puede operar a velocidades de 10.71 Mbps, 137 Mbps o 274 Mbps y no es resistente a *jamming*.

La seguridad es proporcionada a través de encripción COMSEC y el uso de la modulación de espectro expandido (*Spread Spectrum*) produce resistencia a *jamming*.

El operador del sistema, inicia un *Data Link* entre una plataforma de superficie y una aeronave. Una vez inicializado, el rastreo del enlace de datos es automático y el funcionamiento del *Data Link* es transparente a los usuarios de datos en la plataforma de superficie; este hecho facilita las comunicaciones LOS en la banda Ku. La operación BLOS es posible a través del uso de satélites o plataformas de retransmisión aéreas.

2.2.8 Link Y

Link Y es un data link comercial producido por la compañía THALES, que opera en las bandas HF/VHF/UHF. Link Y ofrece una funcionalidad comparable a la del

Link 11 de la OTAN, pero con mayores capacidades y utilizando criptografía embebida en el software. Link Y soporta operaciones marítimas proporcionando intercambio de información en tiempo cercano al real, facilitando la comunicación entre diferentes tipos de plataformas militares.

Algunas de las ventajas que presenta el Link Y son las siguientes:
Protocolo TDMA (Time Dision Multiple Access), uso de 2 radio frecuencias (HF, VHF y/o UHF) en una misma red, fácil integración con cualquier sistema de gestión del combate, fácil montaje de la red y preparación de la misión, amplias capacidades de gestión de trazas (correlación y responsabilidad de reporte), modulación QPSK.

CAPITULO III. ESTADO DEL ARTE

Este capítulo tiene como finalidad presentar al lector el estado del arte relacionado con técnicas de recuperación ante fallos en sistemas distribuidos, los cuales tienen gran similitud con los sistemas de enlace de datos tácticos bajo estudio.

Los procedimientos de recuperación ante fallas son requeridos para proporcionar alta disponibilidad en sistemas distribuidos. Muchas de las técnicas de recuperación implican un periodo de tiempo considerablemente alto asociados con ellas. Existe entonces, no solo la necesidad de reducir estos tiempos, sino también de automatizar en un alto grado este proceso, con el fin que el sistema pueda retomar uno de sus estados operativos.

Las fallas en sistemas distribuidos pueden ser impredecibles, dejando al sistema en uno de los posibles estado de falla, haciendo incluso posible que existan muchos estados de recuperación aceptables. Esta combinación de posibles estados de falla con varios estados de recuperación, puede complicar el proceso de recuperación del sistema. Por lo que es requerido hacer un estudio cuidadoso y detallado del funcionamiento del sistema bajo estudio antes de proponer un mecanismo de recuperación.

La recuperación de fallas está basada en un gran número de enfoques fundamentales. Además, muchas de las aproximaciones relacionadas con recuperación de fallas se hacen en campo, por lo que se divide esta sección en dos partes: trabajo de fundamentación y trabajo relacionado.

3.1 TRABAJO DE FUNDAMENTACIÓN

El trabajo de fundamentación de recuperación de fallas está basado en muchas áreas de las ciencias de la computación, tales como computación a prueba de fallos, reconfiguración dinámica, análisis de dependencia, entre otros. A continuación se presentan algunos trabajos desarrollados en este sentido.

3.1.1 Reconfiguración dinámica

El propósito de la reconfiguración dinámica es permitirle al sistema evolucionar incrementalmente desde su configuración actual hacia otra configuración sin tener que desconectarse (Almeida, Wegdam, Sinderen & Nieuwenhuis, 2001). Dentro de los enfoques principales de este mecanismo se encuentran:

- Enfoque basado en agente: en este caso, un agente o grupo de agentes son responsables de llevar a cabo la reconfiguración dinámica. Estos agentes pueden ser móviles o estacionarios. Valetto y otros, proponen una aproximación basada en agente móvil para llevar a cabo la reconfiguración dinámica. Ellos afirman que la reconfiguración dinámica basada en procesos resuelve el problema de mantenimiento del sistema de software a un costo menor que la reingeniería. Sus agentes o código móvil fueron llamados "worklets". Estos worklets transportan código en el sistema y llevan la secuencia de reconfiguración. Sin embargo, cuando el sistema se vuelve complejo estos agentes requieren de algunos scripts, previamente construidos (Valetto, Kaiser & Gaurav, 2001). Otra aproximación para implementación de reconfiguración dinámica usando agentes móviles, fue propuesta por Berghoft y otros. De acuerdo con ellos, ambos esquemas, centralizados y descentralizados, para reconfiguración dinámica tienen sus desventajas. La desventaja de los centralizados es la limitación en escalabilidad y la violación de recursos que podría producir atascamientos en la red. En los descentralizados el problema radica en el incremento de tráfico debido a la sincronización y coordinación que es requerida. Por lo tanto, los autores proponen una aproximación basada en agentes móviles. Estos agentes pueden moverse en el sistema con sus estados. Estos agentes desarrollan su tarea de gestión de la red de forma aislada, por lo que no provocan obstrucciones en la red. Pero requieren un servidor de agentes que los genere y un agente principal que los controle (Berghoff, Drobnik, & Otros, 1996).

- Enfoques basados en redundancia: en esta aproximación, el sistema tiene más de una versión de sus componentes trabajando al mismo tiempo. El objetivo de esta aproximación es proteger el sistema de rupturas o fallas debido a inconsistencias desarrolladas como consecuencia de nuevas versiones de componentes. Feiler y Li presentan una técnica llamada Componente de Redundancia Analítica (ARC – por sus siglas en inglés) que proporciona protección ante fallas. Ellos presentan una técnica que representa un análisis de desconexión. Los resultados de este análisis son utilizados por un director de configuración para evitar configuraciones que son inconsistentes. Ellos utilizan una capacidad de tolerancia a fallas simple y la aumenta evitando fallas proactivas a través de la detección y recuperación de reconfiguraciones inconsistentes (Feiler & Li, 1998).

- Enfoques a nivel de sistema operativo (OS): se pueden utilizar para reconfiguración de componentes a nivel de sistema operativo o facilidades en este nivel para manipular e sistema operativo usando comandos de nivel de OS. Soules y otros presentaron una técnica para reconfiguración dinámica de

los componentes del sistema operativo. En su paper presentan dos mecanismos de reconfiguración en línea: interposición e intercambio en caliente. La interposición es una técnica que mantiene oculta una interfaz de componentes activos. El intercambio en caliente reemplaza un componente con una nueva instancia del componente que proporciona la misma interfaz y funcionalidad (Soules, Appavoo & Otros, 2003).

- Enfoque basados en flujo de trabajo: en este enfoque la reconfiguración dinámica es llevada a cabo como una tarea de la red. Kaiser y otros usan un motor de flujo de trabajo llamada Workflakes (un motor de flujo de trabajo descentralizado) para la reconfiguración dinámica de los sistemas basados en componentes. Este sistema ayuda a llevar a cabo adaptaciones locales y reconfiguraciones globales. (Kaiser, Gross & otros, 2002)

3.1.2 Planeamiento

El planeamiento es utilizado para desarrollar una vía para cambiar el estado o configuración del sistema. Dos aspectos son interesantes en este campo de estudio, el primero es cómo representar un sistema de tal forma que se pueda realizar un planeamiento en él y el segundo, el proceso de planeamiento en sí mismo que lleva al sistema de un estado a otro.

- Modelos y marcos: son una de las formas en las que se puede llevar a cabo el planeamiento para reconfiguración dinámica. Un modelo es una abstracción que captura la estructura y las propiedades de rutina del sistema. Un marco es definido como una guía para desarrollar una aplicación de tal forma que sea posible la reconfiguración dinámica en la aplicación. Chen y otros presentan dos requerimientos para los marcos que proporcionan reconfiguración dinámica. El primero, es que se debe tener conocimiento de las interacciones que ocurren en el sistema. en el caso de una reconfiguración, el marco puede bloquear interacciones tal que los componentes alcances un estado reconfigurable. El segundo requerimiento es que el marco debe proporcionar transparencia en la ubicación (Chen & Simons, 2002).

- Lenguajes de reconfiguración dinámica: forma independiente del sistema para representar un sistema de tal forma que la reconfiguración pueda ser planeada y ejecutada en el. Un enfoque fue propuesto por Kramer y Magee, en el que argumentan que los cambios deben ser aplicados a un nivel estructural como oposición al nivel de aplicación (Kramer & Magee, 1990).

3.1.3 Gestión de la dependencia

Los sistemas distribuidos basados en componentes tienen infinidad de dependencias a diferentes niveles. Con el fin de correr tales sistemas, estas dependencias deben ser satisfechas. Incluso, para automatizar el proceso de recuperación de fallas, estas dependencias deben ser representadas de tal forma que el procedimiento de recuperación automático de fallas sea capaz de satisfacer estas dependencias. Manejar estas dependencias es un aspecto importante para manejar las aplicaciones basadas en componente, de hecho, ayuda en la especificación de la estructura de un sistema a partir de un punto de vista funcional (Arshad, 2006).

3.1.4 Tolerancia a fallas

La tolerancia a fallas de un software es el uso de técnicas que permitan la entrega continua de servicios a un nivel aceptable de desempeño y seguridad después de que una falla diseñada se vuelve activa. La tolerancia a fallas es un área que mejora la confiabilidad de un sistema de cómputo. El objetivo de la tolerancia a fallos es reducir el tiempo medio de falla (MTTF) (Torres, 2000).

3.2 TRABAJOS RELACIONADOS

Fueron encontradas varios enfoques en el proceso de recuperación de fallas, los cuales podrían dividirse en tres (3) categorías: técnicas basadas en teoría de control, recuperación basada en arquitectura y recuperación orientada a computación.

3.2.1 Técnicas basadas en teoría de control

Kephart y Chess presentan una idea de computación automática. La computación automática es un paradigma computacional en el que el sistema se maneja a si mismo dando objetivos de alto nivel desde el administrador. Este sistema tiene cuatro propiedades: autoconfiguración, auto-optimización, auto-curación y auto-protección. Estas propiedades están basadas en un lazo de realimentación entre las fases de monitoreo, análisis, planeamiento y ejecución (Kephart & Chess, 2003).

Park y Chandramohan describen dos modelos de recuperación de fallas: estático y dinámico. La principal estrategia detrás del modelo estático es la redundancia.

Un monitor mantiene una lista de servidores disponibles y su estado operativo. Tan pronto como ocurre una falla en un servidor el monitor cambia a otro servidor en un escenario aislado. En el modelo dinámico, el componente que falla es remplazado por un módulo generado dinámicamente que es desplegado sobre la marcha. (Park & Chandramohan, 2004)

3.2.2 Recuperación basada en arquitectura

Tichy y sus colegas presentan una técnica basada en reglas para la recuperación de fallas en sistemas basados en componentes. Ellos desarrollan esta técnica tal que los componentes en sí mismos encuentren acciones para auto-repararse con el fin de minimizar daños y reducir el tiempo de reparación. La función objetivo de una falla es presentada como una desigualdad, las cual es resuelta usando un algoritmo que incluye una fase de pre-solución y una fase de expansión del sub-modelo (Tichy, Giese & otros, 2005).

3.2.3 Computación orientada a recuperación

Es otra área de recuperación de fallas. Su objetivo es reducir el tiempo medio de reparación (MTTR) en vez de reducir el tiempo medio entre fallas (MTTF). Brown y Patterson argumentan que las técnicas de tolerancia a fallos no son lo suficientes para asegurar la disponibilidad de los sistemas. Manifiestan que tanto el software con el hardware y los operadores humanos cometen errores, por lo tanto la recuperación y reparación de fallas debe ser considerado como aspecto vital en un sistema. Como consecuencia de lo anterior, introducen el concepto de computación orientada a recuperación (ROC). En la ROC las fallas en un sistema son aceptadas como hechos inevitables en la operación de los mismos, por lo que los sistemas están diseñados para proporcionar recuperaciones rápidas y eficientes y mecanismos de reparación (Brown & Patterson, 2001).

En los últimos años, las aplicaciones en sistemas distribuidos han incluido redes de computadores empleados para simulaciones de alto nivel, sistemas de servicios en internet como los de google y yahoo, redes inalámbricas de sensores que operan en microondas, sin embargo, no hay evidencia de trabajos realizados en sistemas de enlaces de datos tácticos que cuenten con infraestructura de hardware y ancho de banda limitado y, en donde adicionalmente deban ser tenidas en cuenta fallas debidas a ataques intencionales de guerra electrónica.

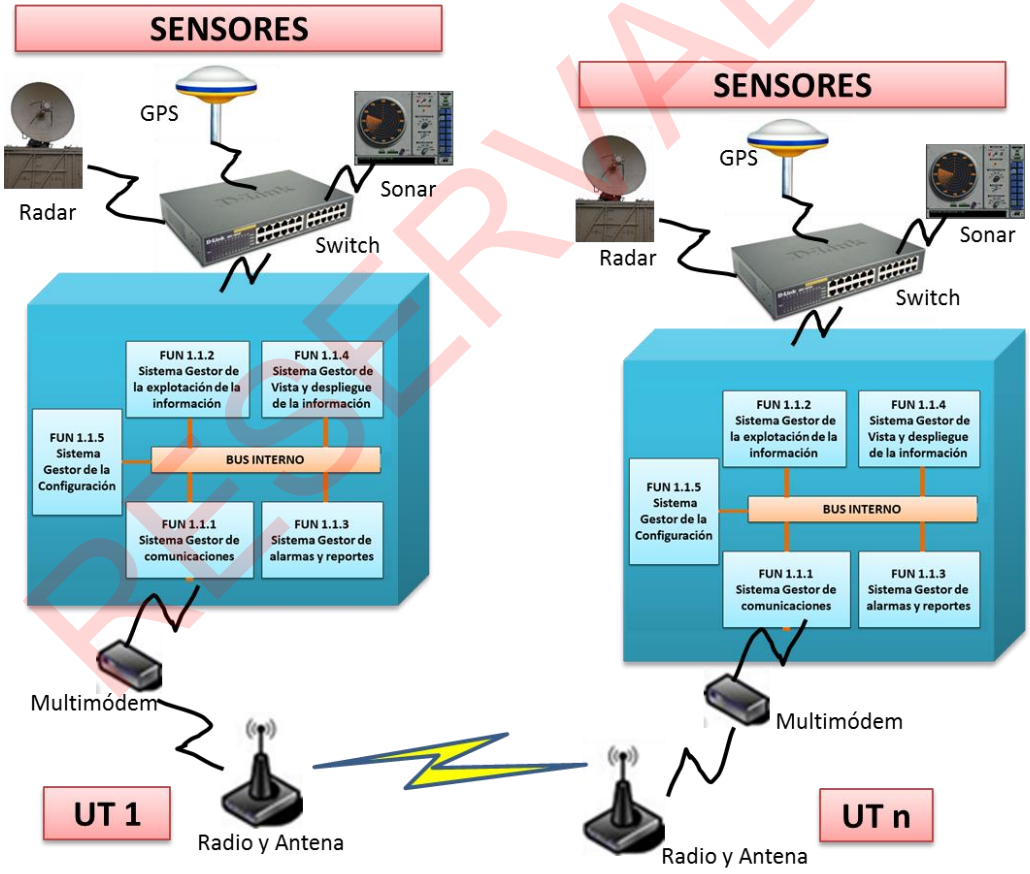
CAPITULO IV. CARACTERÍSTICAS DEL SISTEMA BAJO ESTUDIO

En esta sección del documento se presentan las principales características del sistema bajo estudio. Se hace un enfoque especial en el mecanismo de control de acceso al medio que utiliza, ya que de ello dependerá en gran medida el mecanismo de recuperación empleado.

4.1 DESCRIPCIÓN GENERAL DEL SISTEMA

En la Figura 1 se puede ver el proceso que se sigue en la gestión de la red del sistema.

Figura 1. Vista de despliegue del sistema CDL 1.0.



Fuente: Diseño del protocolo del sistema – COTECMAR - 2011.

En el esquema de la figura 1, se visualiza el DATA LINK como el enlace de datos tácticos entre las unidades participantes en una operación específica.

Durante el proceso de intercambio de información táctica que se realiza para

ayudar a la toma de decisiones en la conducción de la operación, se ven involucrados los siguientes recursos:

- Los sensores con que cuenta cada unidad, que se convierten en fuentes de información de inteligencia de combate que es compartida con todas las unidades.
- Las herramientas de análisis que ayudan a soportar la toma de decisiones.
- El sistema de comunicaciones externas con que cuentan las unidades.
- Los equipos moduladores y demoduladores de datos, para adaptarlos a las radiocomunicaciones.
- Medios de despliegue de la información.
- Sistemas gestores de bases de datos que almacenan la información durante las operaciones.

Figura 2. Esquema táctico del CDL 1.0

Fuente: Diseño del protocolo del sistema – COTECMAR - 2011.

El esquema táctico que se presenta en la Figura 2 es la vista de contexto del sistema. En ella se presentan, a grandes rasgos, las interacciones entre los diferentes tipos de unidades.

Dentro del sistema existirá una estación controladora de red (ECR), la cual hace las veces de unidad central encargada de la comunicación punto-multipunto. A

su vez, la ECR retransmite todos los mensajes, para que todas las unidades puedan tener el “panorama táctico común”.

Cuando se inicia una operación cualquiera, para el funcionamiento del sistema existen los procedimientos detallados y algunos acuerdos respecto a aspectos como: qué unidad será la ECR, definir la tabla de secuencia en los reportes, la tabla de claves criptográficas y su utilización durante la operación.

El primer paso dentro del proceso del diseño del protocolo de este sistema fue el análisis del entorno operacional y llegar a establecer el conjunto de requisitos de comunicaciones. Los requisitos se establecen en términos generales incluyendo los siguientes:

- Entorno operacional global (paz/ejercicio/guerra).
- Número de plataformas (con previsión de participantes adicionales).
- Despliegue de las plataformas.
- Los datos a transmitir y recibir por cada plataforma (o grupo de plataformas si así se facilitan las cosas) y sus características en términos de:
  - Tipo de plataforma.
  - Cantidad.
  - Seguridad, incluyendo requisitos de privacidad, autenticidad, integridad y no repudio.
  - Tipo de mensaje.
  - Mensajes de administración de red

Para una correcta operación de la red es esencial el uso coordinado de la criptografía, por lo tanto la disponibilidad de las claves se hace totalmente indispensable para que sean posibles las comunicaciones.

4.2. REGLAS DE INTERCAMBIO DE MENSAJES

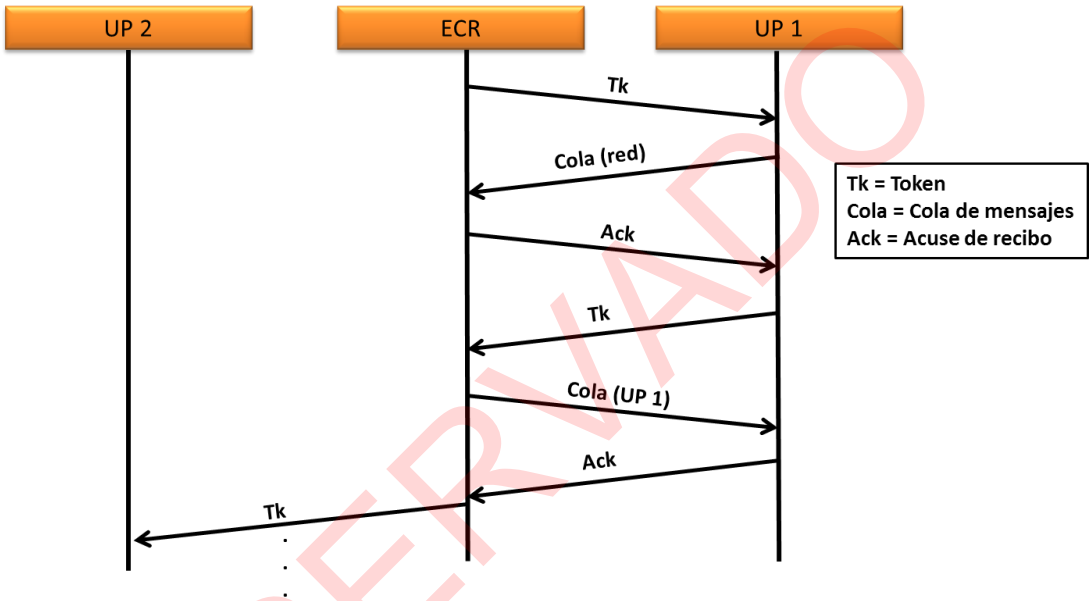
Las reglas de intercambio de mensajes se describen a partir de la representación gráfica (diagramas) de los procesos por medio de diagramas de secuencia que representan con líneas verticales las estaciones o unidades (origen y destinatario) y líneas inclinadas que indican la información que se intercambia en cada proceso. La cabeza de la flecha (línea inclinada) indica quien recibe la información y la cola de la flecha indica quién la envía.

4.2.1 Secuencia de Token

Al inicializar el sistema, la ECR debe enviar el token a la primera unidad participante en su tabla de secuencia, lo anterior, con el fin de permitir que ésta pueda transmitirle los mensajes que tiene pendiente.

El proceso de envío y recepción del token se muestra en la figura 3.

Figura 3. Secuencia del token



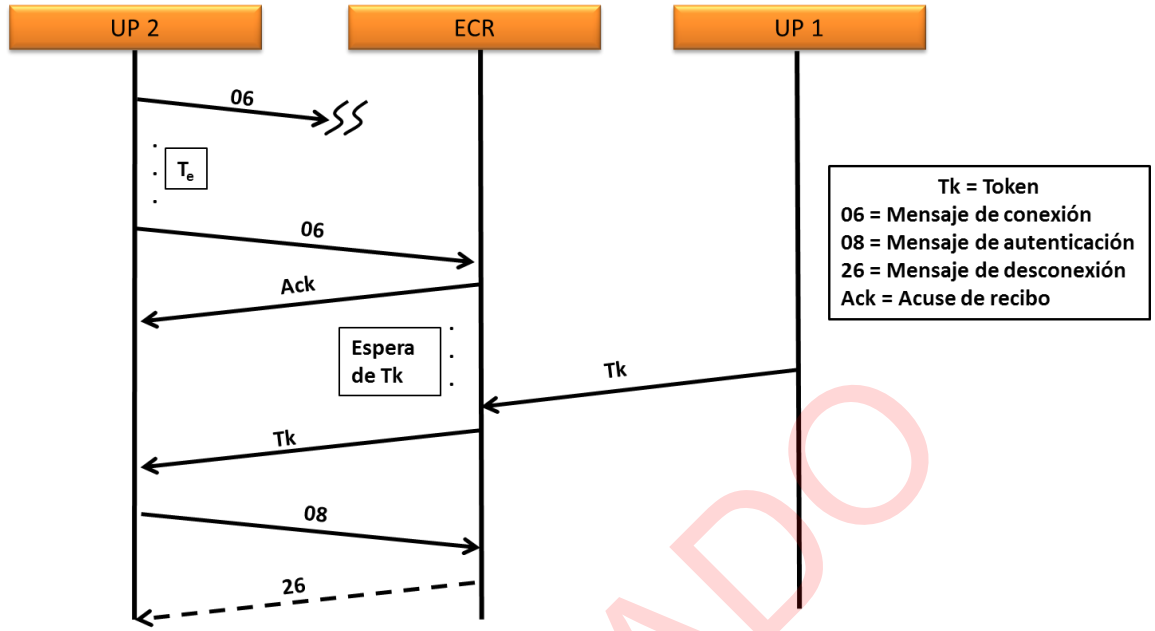
4.2.2 Solicitud de conexión

Cuando una unidad desea a conectarse a la red, debe enviar un mensaje a la ECR este mensaje es el de conexión, seguido del mensaje de autenticación.

Si la unidad no es autenticada correctamente, la ECR lo desconectará automáticamente.

El proceso que se sigue para este caso se presenta en la figura 4.

Figura 4. Solicitud de conexión y autenticación.

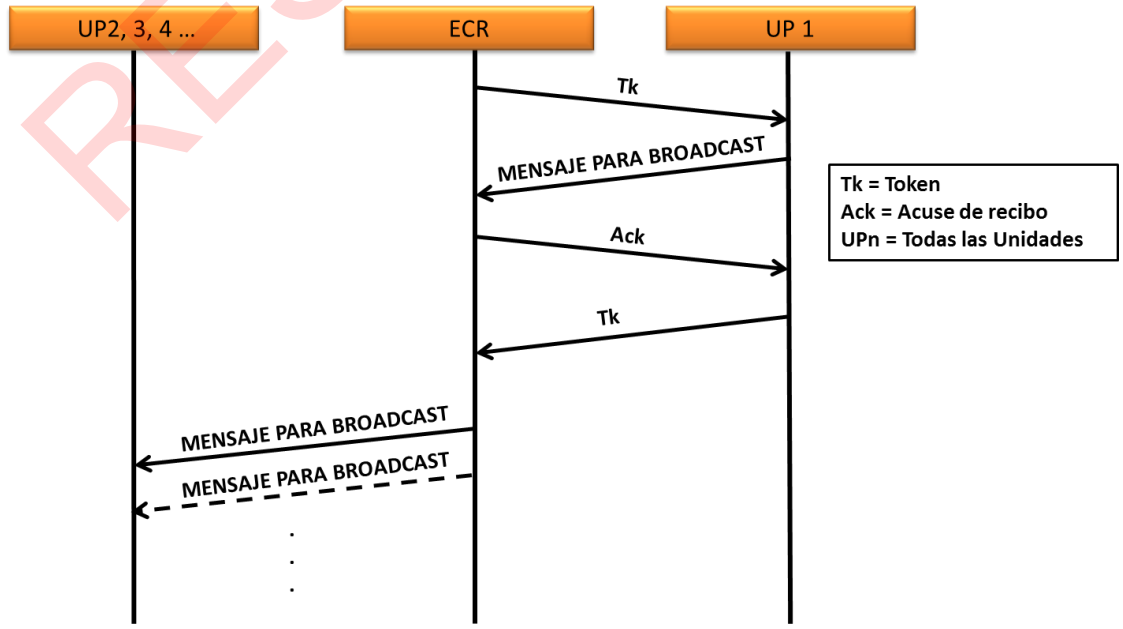


4.2.3 Difusión de mensajes (broadcast)

Ciertos mensajes requieren que la ECR los retransmita a todas las unidades participantes de la red. Estos mensajes son: configuración, posición, contacto, alertas, gestión de armas, modo de red, correlación/decorrelación, entre otros.

El proceso general que siguen estos mensajes es el que se presenta en la figura 5.

Figura 5. Difusión de mensajes (Broadcast)

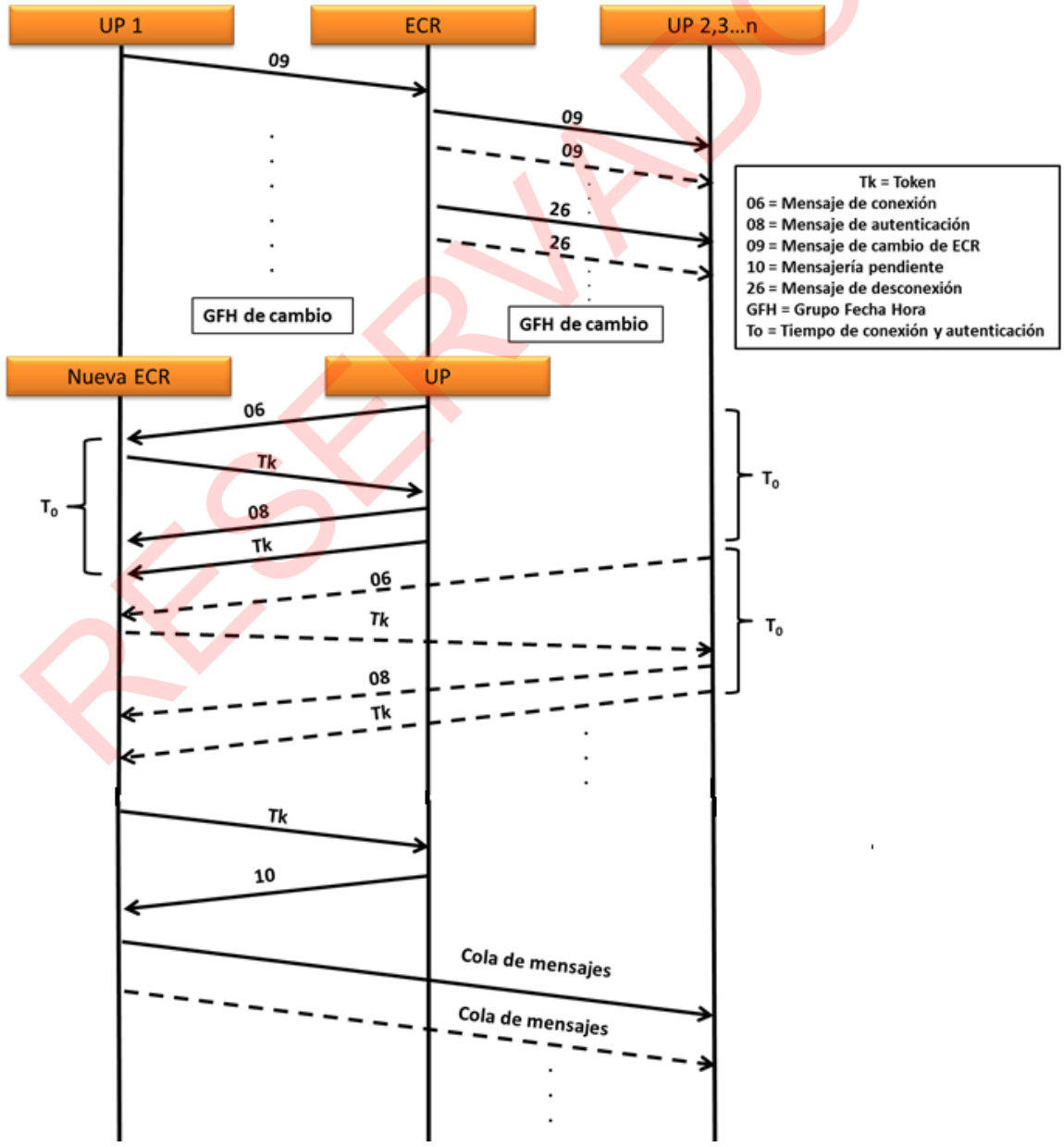


4.2.4 Cambio de estación controladora

En ciertas ocasiones será necesario cambiar la ECR, por motivos que determinará el OTC de la operación. Tan pronto la ECR reciba el mensaje de cambio, deberá retransmitirlo y posteriormente desconectará las UP que se encuentren activas. Cuando llegue el GFH del cambio, la antigua ECR solicitará conexión y posterior autenticación, proceso que tardará un tiempo To. Las demás UPs deberán esperar N veces To (siendo N el número de secuencia de esa UP), para poder realizar el mismo proceso.

El detalle del proceso de cambio de la ECR se presenta en la figura 6.

Figura 6. Cambio de ECR



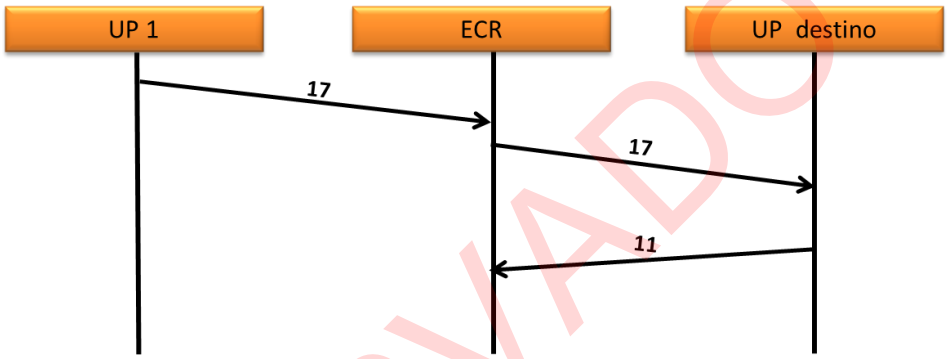
4.2.5 Solicitud de actualización de datos

Una unidad que tenga particular interés en la información de un track, puede solicitar la actualización (mensaje 17) de datos de dicho track, a la unidad que lo reportó.

La unidad interrogada, responderá con un mensaje de actualización de datos (mensaje 11).

El proceso de solicitud de actualización se detalla en la figura 7.

Figura 7. Solicitud de actualización de datos



4.3 MODOS DE RED

Este tipo de mensajes se utilizan para cambiar el modo de la red, con propósitos tácticos, de mantenimiento y de EMCON.

Existen 3 modos de red: normal/operacional, silencio y prueba.

NORMAL: es el que se emplea por defecto para el funcionamiento de la red.

SILENCIO: se emplea por una necesidad táctica de control de emisiones.

PRUEBA: se utiliza con fines de mantenimiento y auditoría del sistema.

El primer modo corresponde al funcionamiento habitual de la red y ha sido detallado en la descripción de los procesos anteriores. El proceso de los otros dos modos de red se presenta en las figuras 8 y 9.

El mensaje 20 corresponde a aquel en que se indica el tipo de modo en el que está la red. El mensaje 19 es el mensaje que contiene la información para prueba de la red.

Figura 8. Modos de red (Silencio)

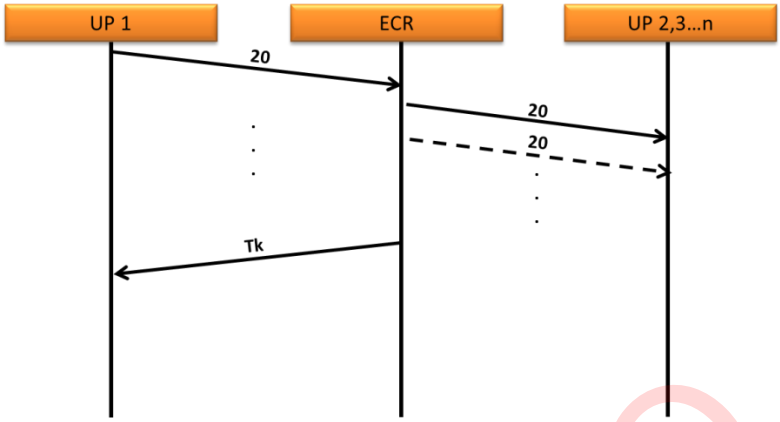
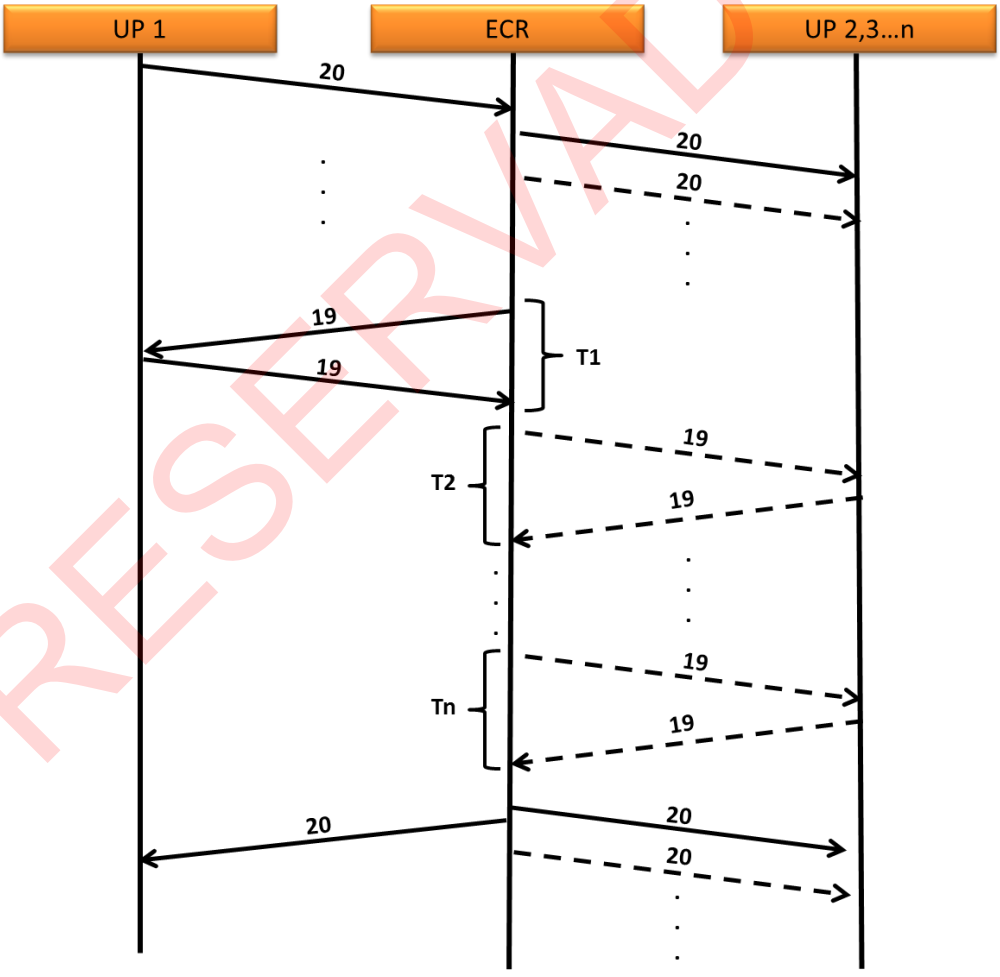


Figura 9. Modos de red (Prueba)



El modo de operación para el cual se evalúa y diseña el mecanismo de recuperación automático ante fallas en el sistema, es modo “Normal”. Lo anterior, por ser el modo en el que opera la red el 90% de las ocasiones, de acuerdo a información suministrada por los usuarios del sistema.

4.4 COMPONENTE DE HARDWARE DEL SISTEMA

El sistema descrito, está acompañado y complementado por un componente de hardware que garantiza la integración de todas las funcionalidades del sistema, a los equipos de radiocomunicación requeridos para el intercambio de información en la red.

El hardware del sistema consiste en una caja integradora de comunicaciones, la cual incorpora componentes COTS[1], dentro de los que se encuentran: una tarjeta multimódem para hacer modulación y demodulación de datos FSK sobre los canales de comunicaciones, una tarjeta switch de 8 puertos para la interconexión con los equipos de a bordo, una fuente interna de 12V y 5V DC para alimentar las tarjetas y los adaptadores para todas las conexiones. La caja tiene alimentación externa 115VAC y 12VDC. Cuenta con puerto USB universal para conexión con el computador y puertos seriales para conexión con el equipo de radio

El anexo 1 contiene información gráfica de la caja integradora de comunicaciones. Los componentes de esta caja serán detallados en el capítulo 7 de este documento.

[1] *Commercial Off-The-Shelf.* Elemento no-desarrollativo (NDI) de suministro, que es a la vez comercial.

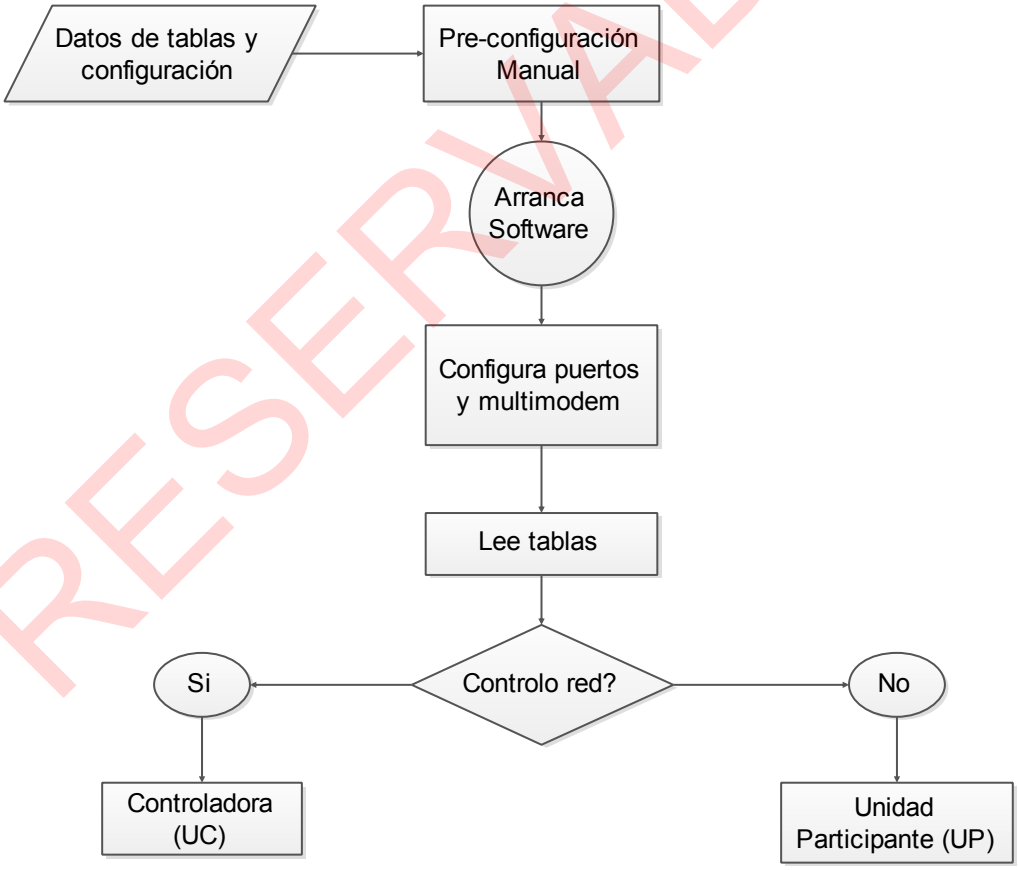
CAPITULO V. IDENTIFICACIÓN DE FALLAS DEL SISTEMA Y DISEÑO DE MECANISMOS DE RECUPERACIÓN

En esta sección del documento se presenta la descripción general de funcionamiento del sistema, a partir de la cual se detectan las situaciones de falla y se proponen mecanismos de recuperación basados en el análisis de los caminos más cortos para devolver el sistema a un estado operativo.

5.1 DIAGRAMA GENERAL DEL SISTEMA

A continuación se presenta el diagrama de flujo general del sistema bajo estudio, para modo de operación “Normal”.

Figura 10. Diagrama de flujo general del sistema



5.2 SITUACIONES DE FALLA

Durante la operación del sistema, es posible que se presenten fallas en alguna unidad participante, debida a factores internos o externos, lo que ocasionaría

que tal unidad pierda la conexión de manera involuntaria o que se perturben significativamente las comunicaciones.

A continuación se presentan las situaciones de este tipo, para las cuales se han considerado procesos de recuperación del sistema.

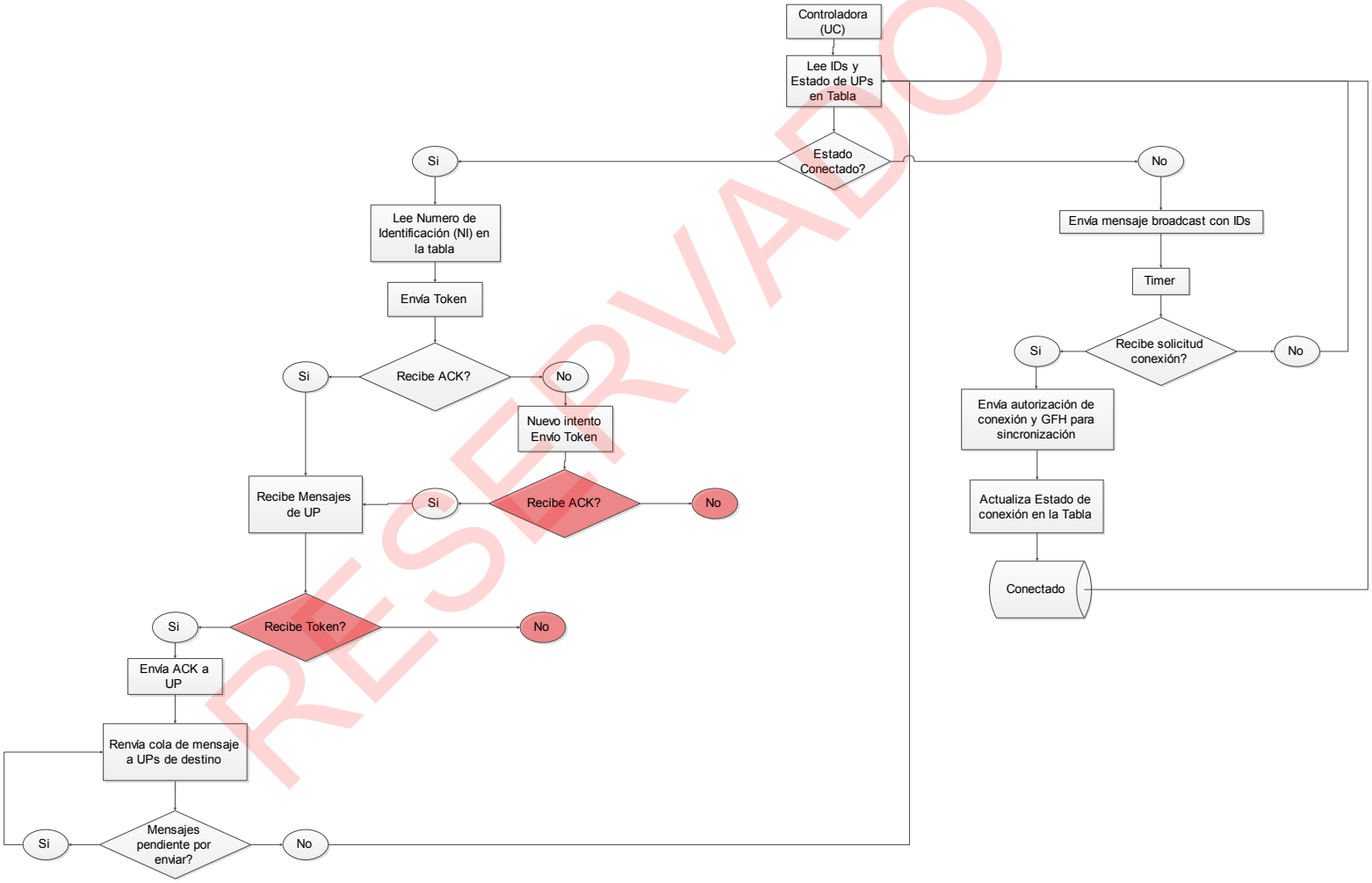
1. Medio perturbado (medidas ECCM).
2. Caida ECR.
3. Caída unidad que tenía el token.
4. Caída de una unidad participante.

Tabla 4. **Identificación de fallas en el sistema**

NOMBRE DE LA FALLA	DESCRIPCIÓN	ORIGEN	AFECTADOS
Medio perturbado	Se bloquea el canal de transmisión con una señal de mayor potencia y como consecuencia de ello no es posible recibir/transmitir información.	Externo	ECR - UPs
Caída de ECR	La unidad que controla la red se desconecta y como consecuencia no es posible efectuar las acciones de coordinación de la red ni retransmisión de información.	Interno – ECR	UPs
Caída UP con Token	La unidad participante que recibe el Token se desconecta y no devuelve el Token a la ECR, como consecuencia se ven afectadas las comunicaciones en la red.	Interno – UP	ECR – UPs
Caída UP	Una unidad participante se desconecta cuando no tiene el Token, como consecuencia de ello, no le es posible recibir/transmitir información.	Interno – UP	UP

La visualización en detalle de estas fallas, dentro de un esquema más detallado del sistema se presenta a continuación en las Figuras 11 – 12, para los roles de UC y UP respectivamente. Las situaciones de falla se presentan en tono rojo dentro de los esquemas.

Figura 11. Diagrama de flujo detallado de la Unidad Controladora de Red.



La figura 11 permite evidenciar dos posibles fallas, vistas desde la UC:

La primera de ellas (de arriba hacia abajo) corresponde a la caída de una UP. La unidad controladora, al enviar el token a la UP y no recibir ACK, intenta enviarlo nuevamente, sin embargo, durante el diseño del sistema sólo se contempló la posibilidad que la UP volviera a conectarse en ese segundo intento, descartando la opción de desconexión accidental o voluntaria de la UP, por lo que al llegar a este punto, el sistema falla y no encuentra un estado en el cual operar, desconfigurando por completo la red.

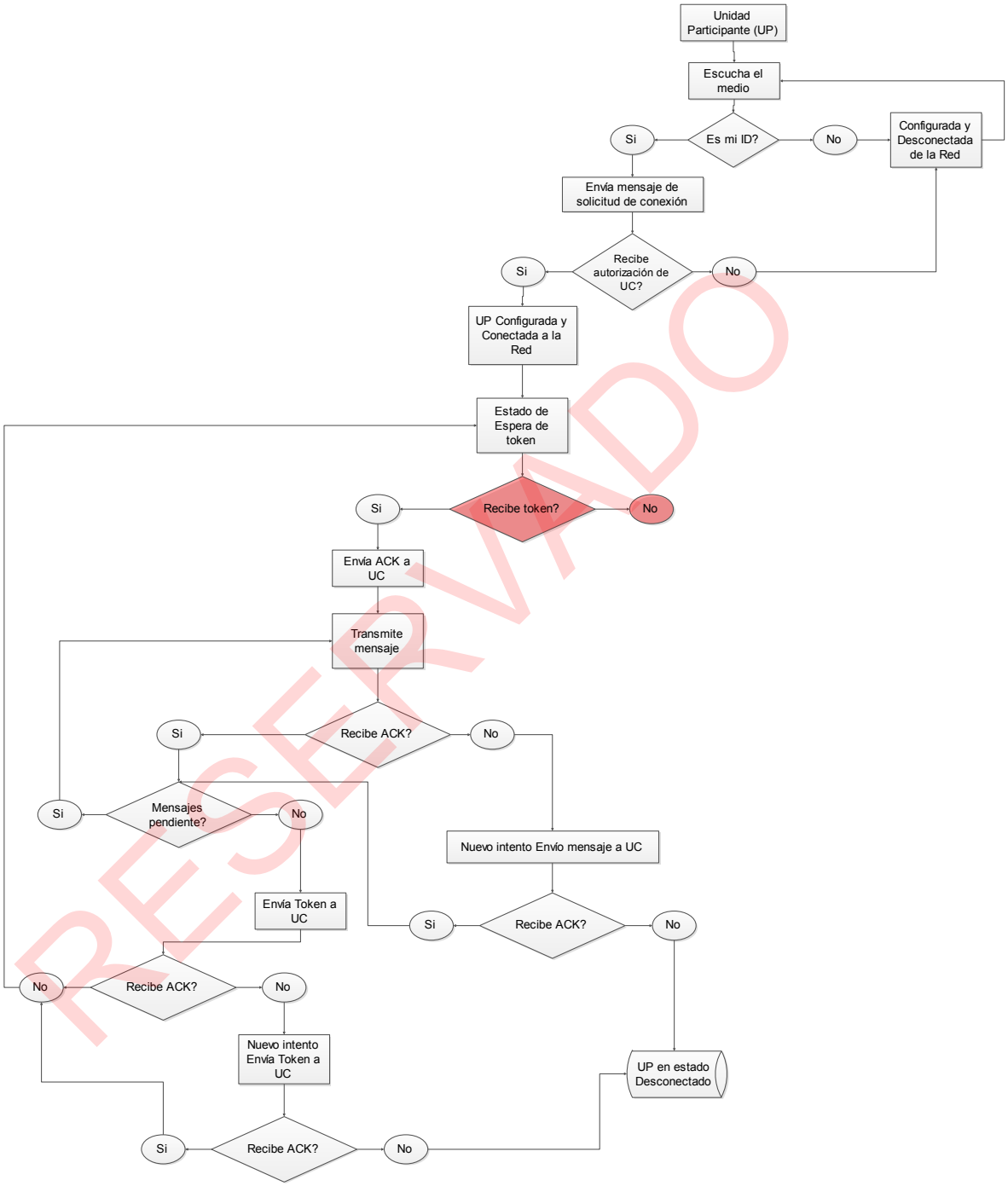
La segunda falla, corresponde a caída de una UP con token. En este caso, la unidad participante recibió el token enviado por la UC, respondió el ACK y por ello la UC envía toda la información que tiene disponible para la UP y también recibe toda la información proveniente de ella, pero al final no recibe de vuelta el token. Esta opción no fue considerada en durante el diseño del sistema, por lo que al llegar a este punto, el sistema falla y no encuentra un estado en el cual operar, desconfigurando la red.

A continuación, en la figura 12, se evidencia el punto (visto desde la UP) que da origen a dos de las situaciones de falla más complejas:

En el diseño del sistema existente, se asume que una vez conectada a la red, la UP siempre deberá recibir el token por parte de la UC, sin embargo, cuando la unidad controladora se desconecta voluntaria o involuntariamente, no hay quien genere token en la red ni quien administre el intercambio de información entre las unidades, por lo que el sistema puede quedar en un silencio infinito o se desconfigura la red al no detectar el ID de la unidad controladora que autorice conexiones.

Ahora bien, dado el entorno naval en el que se emplean este tipo de sistemas, puede suceder que tanto la UP como la UC estén conectadas pero no puedan comunicarse entre ellas porque se encuentra bloqueado o perturbado el canal de comunicación (técnica de guerra electrónica), en este caso, para la UP también parecerá que la UC no se encuentra conectada, motivo por el cual el punto de origen de la falla es asumido como el mismo.

Figura 12. Diagrama de flujo detallado de la Unidad Participante.



5.3 RECUPERACIÓN DE FALLAS

5.3.1 Diseño general

Mediante el empleo de diagramas de secuencia, se presenta de forma general, el mecanismo de recuperación a implementar en cada caso.

Figura 13. Diseño general recuperación para Caída de UP con Token

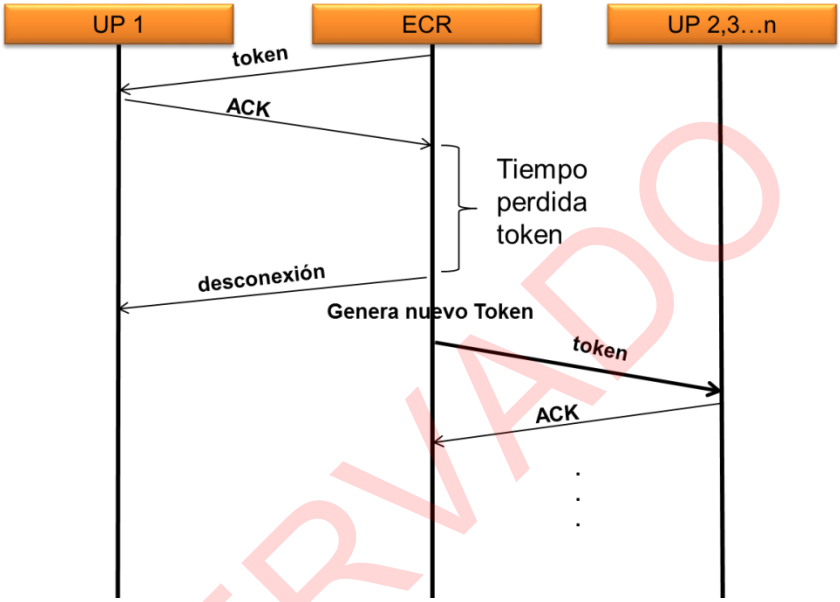


Figura 14. Diseño general recuperación para Caída de UP

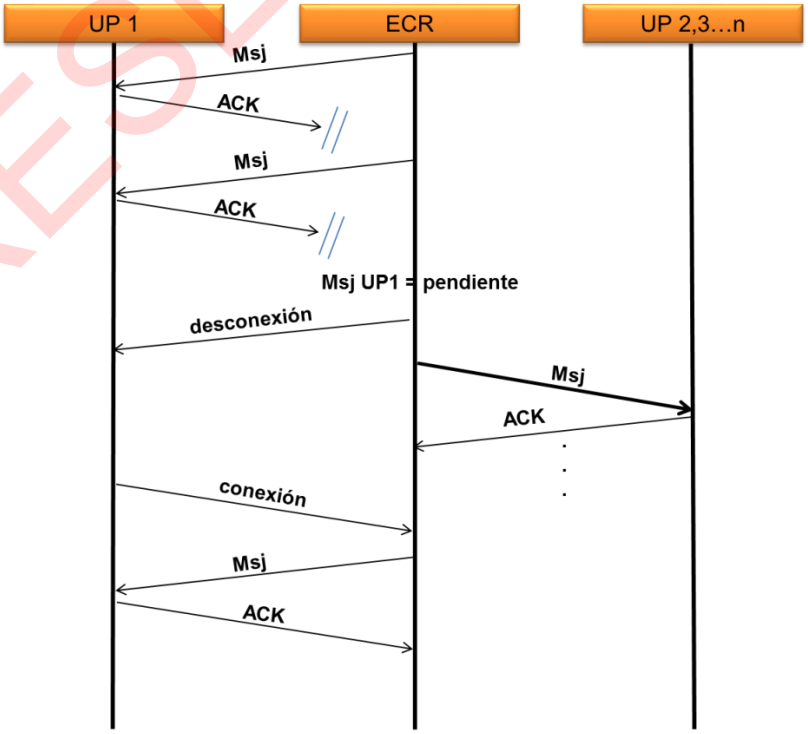
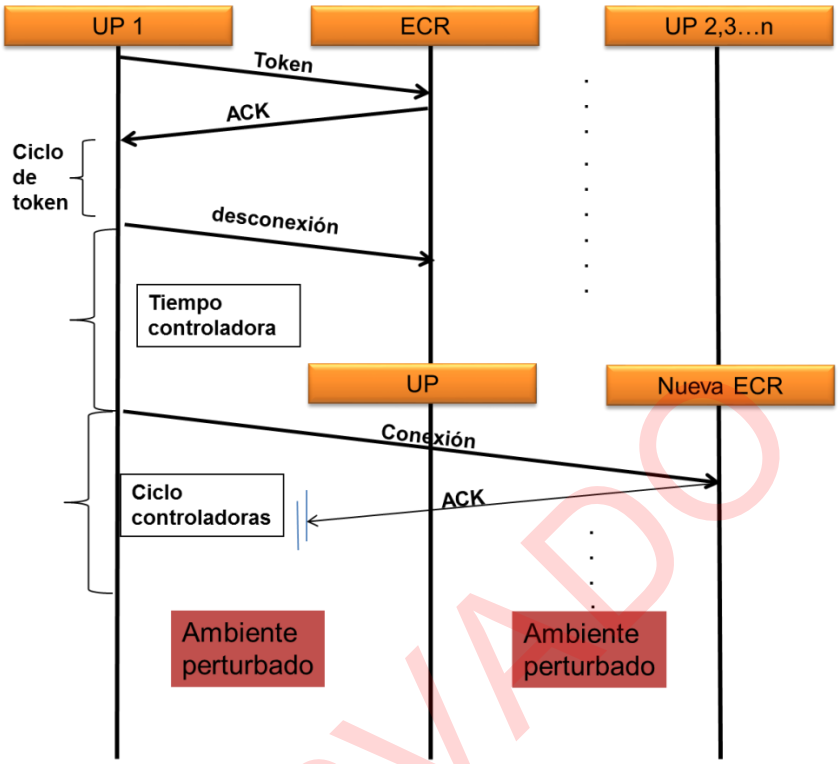


Figura 15. Diseño general recuperación para Caída de ECR y Medio Perturbado



5.3.2 Diseño detallado

Teniendo en cuenta el mecanismo de control de acceso al medio que tiene el sistema, y sabiendo que lo fundamental es disminuir los tiempos de recuperación, se emplearan temporizadores dentro del sistema como mecanismos para accionar las rutas de identificación y recuperación de fallas.

Estos temporizadores tendrán como base los tiempos diseñados para la sincronía del sistema, a continuación se listan y describen estos tiempos:

T_o: Tiempo optimizado de desempeño de la red.

T_e: Tiempo de espera. Se inicia con un silencio en recepción después que una unidad ya tenga el token. Equivale a $2T_o$. Esta medida se resetea cada vez que la ECR reciba un mensaje.

$T_{perturbación}$: Tiempo de espera para recibir conexiones. Permite determinar si se presenta la situación de medio perturbado (ECM). Equivale a NT_o, siendo N el número de unidades en la tabla.

T_{ic}: Tiempo de espera para que las unidades cambien a la nueva frecuencia (ECCM) y sincronizar el proceso de reconexión.

$T_{reconexión}$: Tiempo que inicia con el final del *Tic*, hasta que se cumple el tiempo para conexiones (también es igual a NT_o).

T_{et}: Tiempo entre token. Es el tiempo que tarda un ciclo de token. Está compuesto por un slot de tiempo para cada unidad y esto se multiplica por el número de unidades que aparezcan en la tabla.

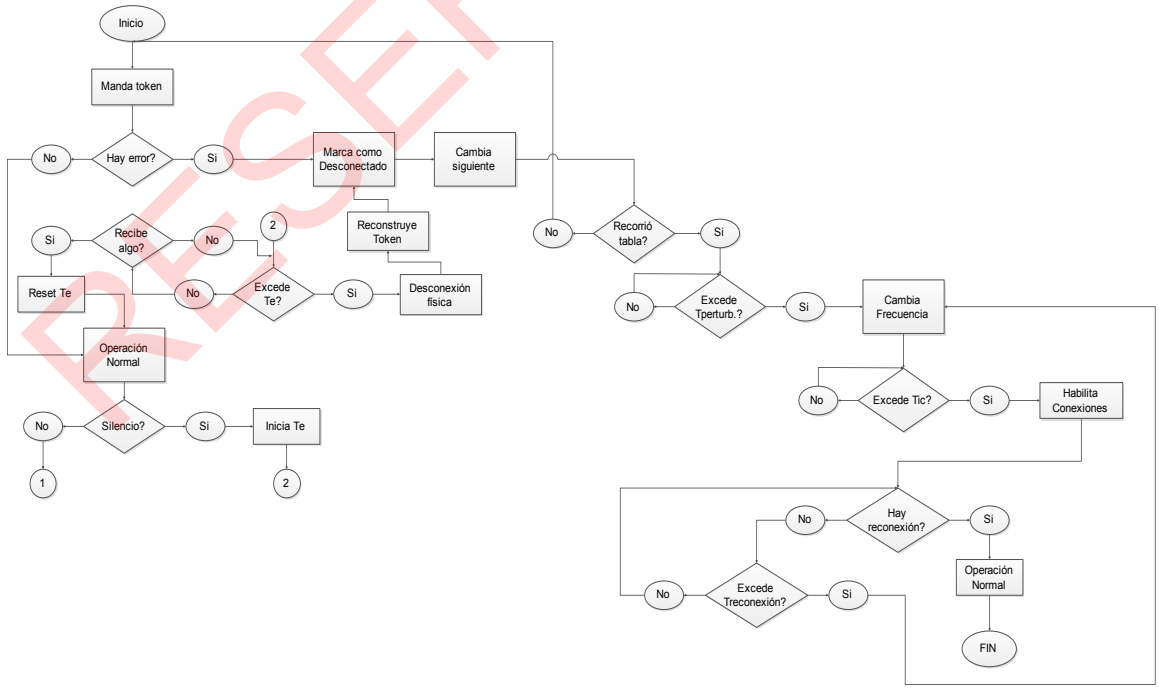
T_{cr}: Tiempo de ciclo de red. Es el tiempo que garantiza que todas las unidades están enteradas de la caída de la ECR.

T_{cm}: Tiempo configuración multimódem. Es el tiempo que tarda en configurarse el multimódem como ECR.

Es necesario mencionar que en el ciclo del token, cuando una unidad está desconectada, la ECR debe esperar un tiempo T_c para que esa unidad pueda tener un espacio para conectarse a la red. Tc equivale a $2T_o$.

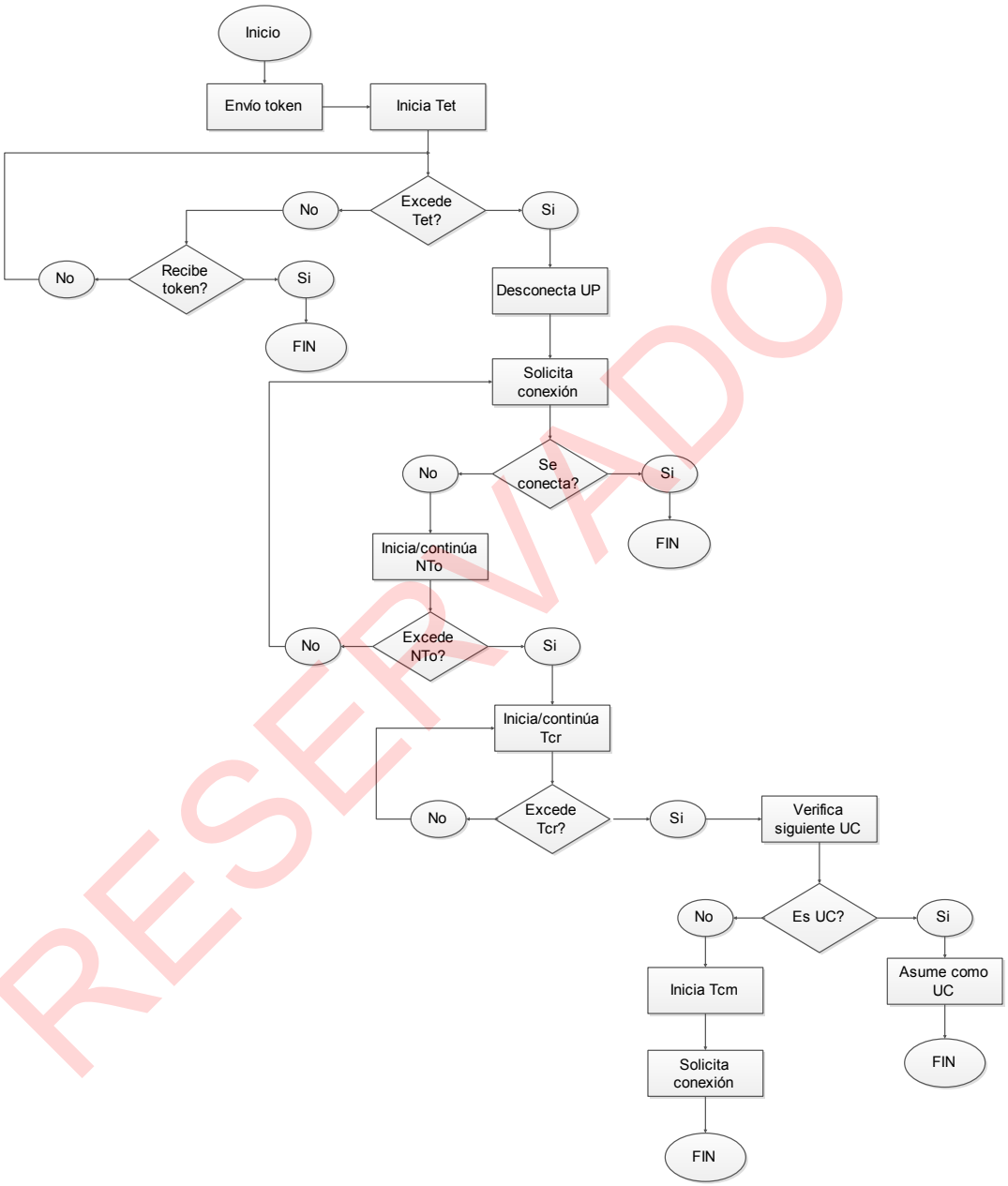
Las situaciones de falla 1, 3 y 4 mencionadas en la tabla 1, tendrán un procedimiento de recuperación de la red visto desde la UC o ECR tal como se presenta en la figura 16.

Figura 16. Recuperación del sistema situaciones 1, 3 y 4.



La situación de falla 2, presentada en la tabla 1, tendrá un procedimiento de recuperación de la red visto desde las UPs tal como se presenta en la figura 17.

Figura 17. Recuperación del sistema situación 2.



La integración de los mecanismos propuestos, al sistema desarrollado se presenta en las Figuras 18 y 19.

Figura 18. Incorporación de mecanismos a UC

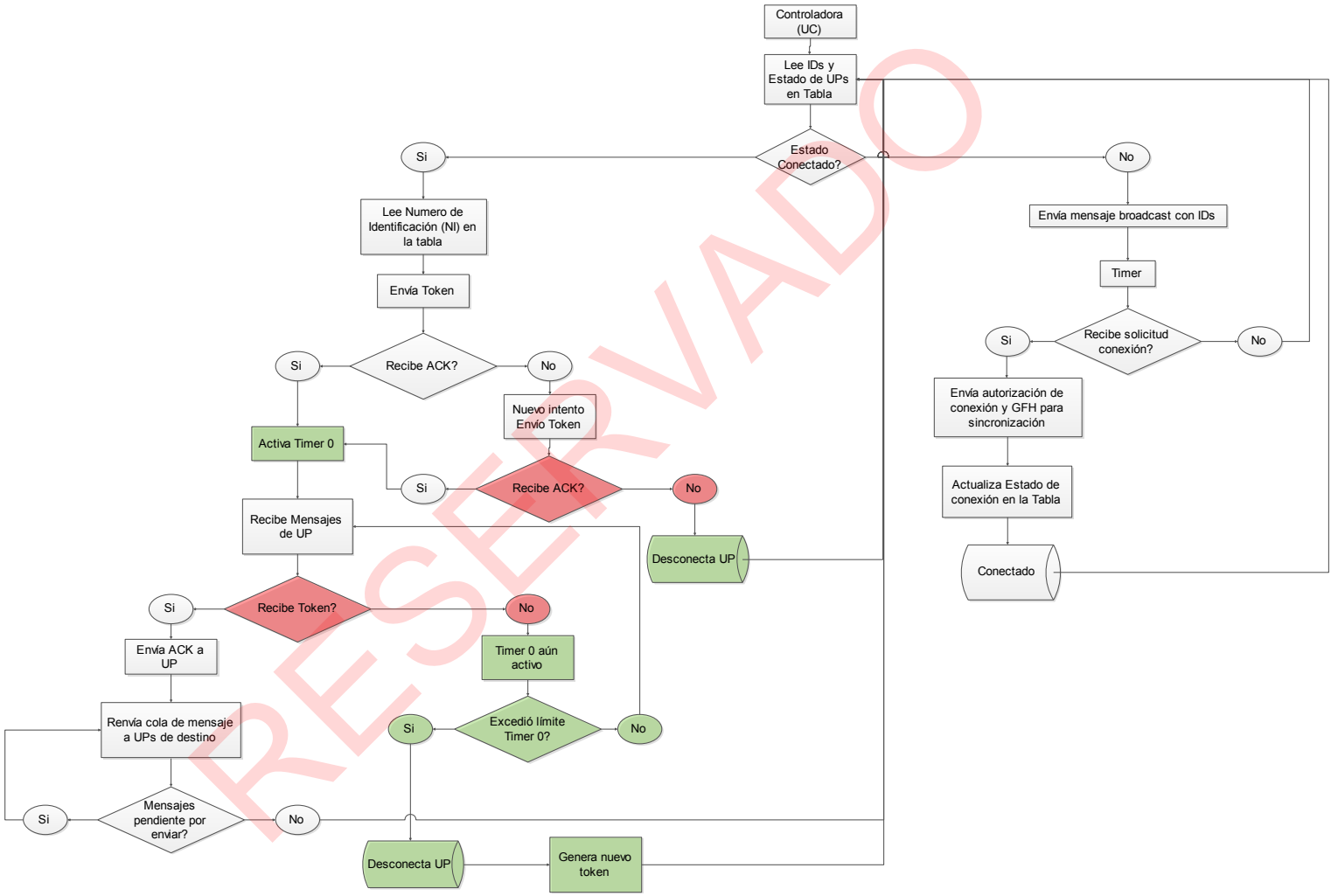
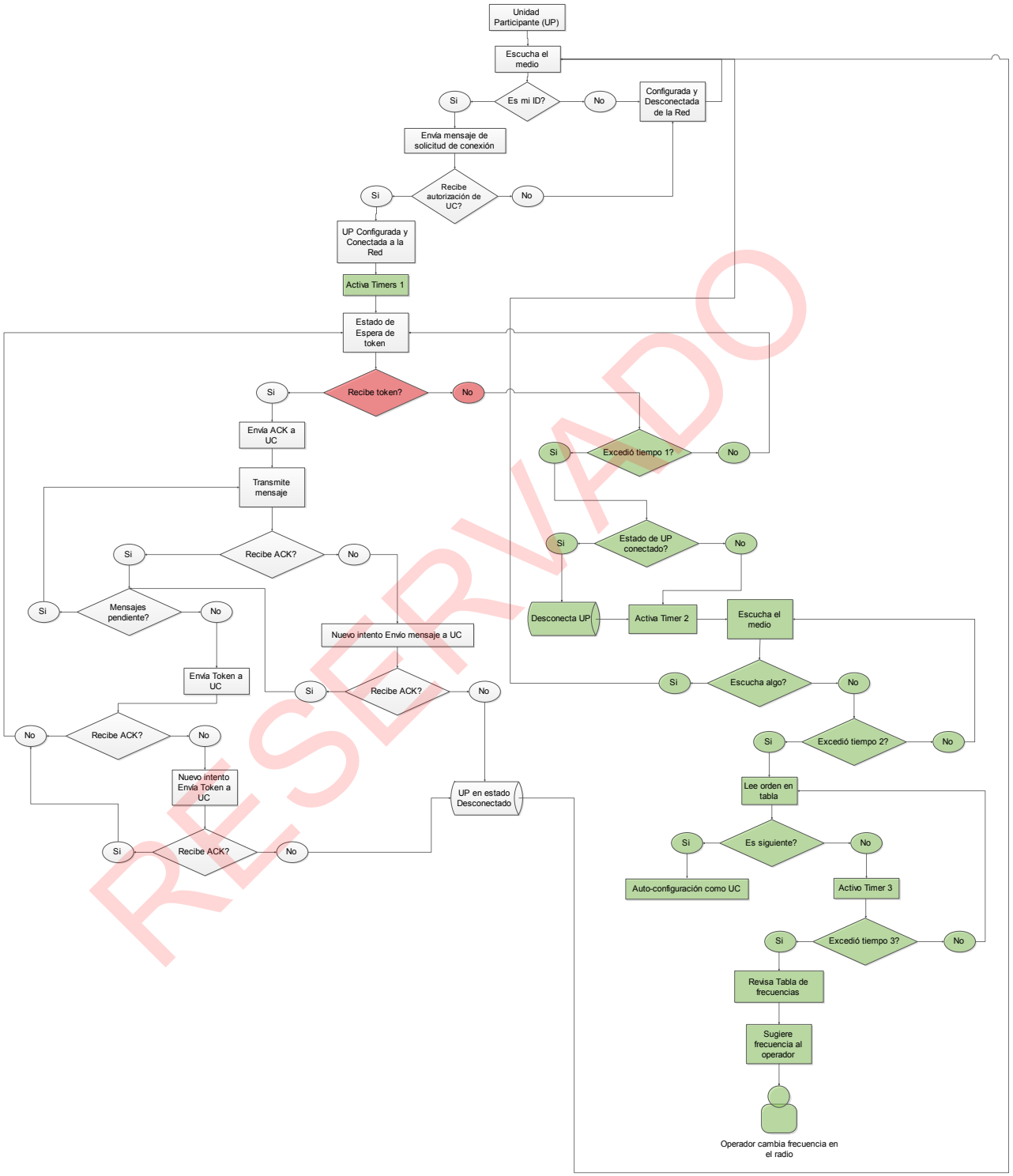
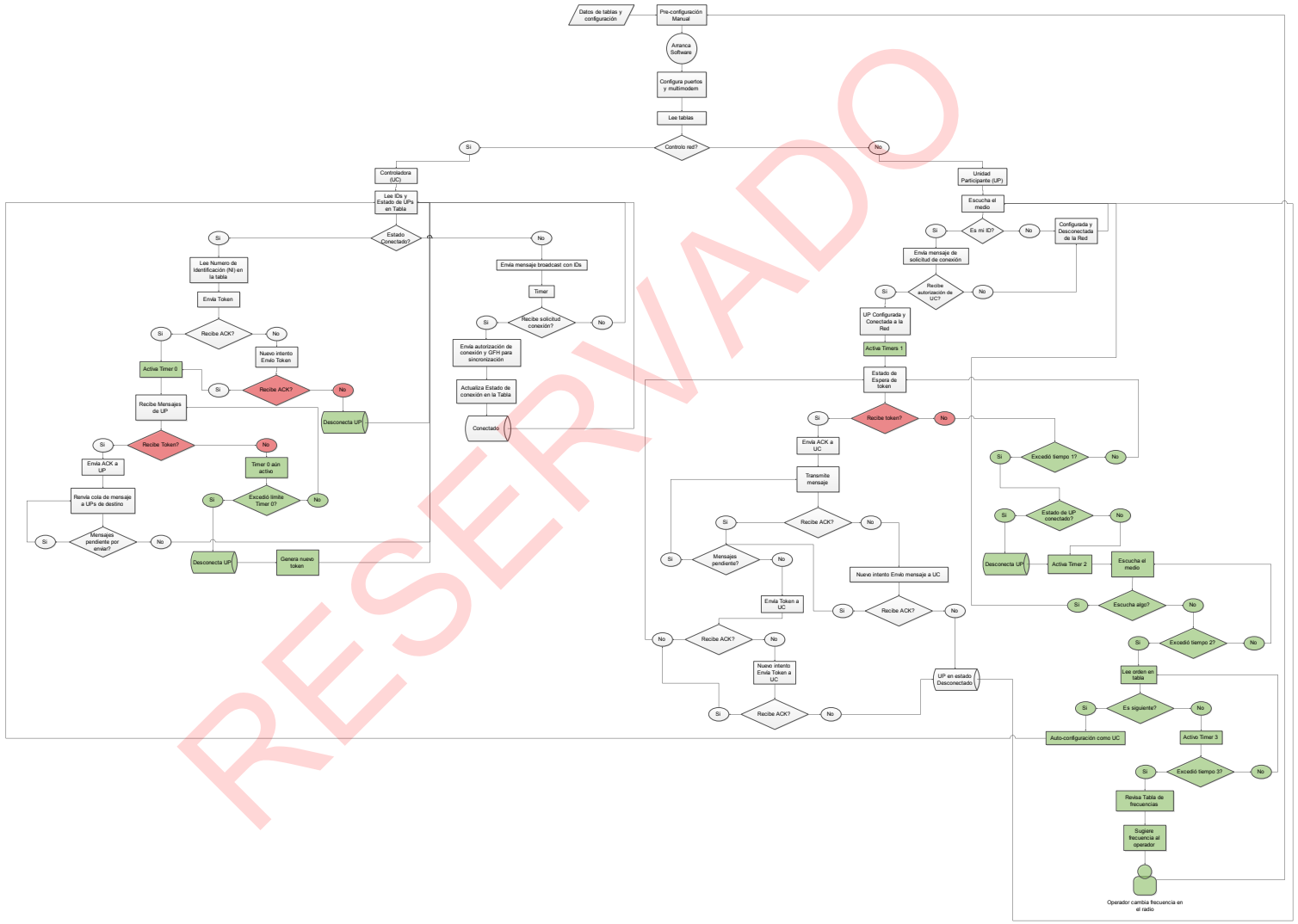


Figura 19. Incorporación de mecanismos a UP



Es importante resaltar que la UC o ECR implementa los procedimientos de recuperación descritos en las figuras 18 y 19. Ya que en el contexto operacional, dentro de la red cumple ambas funciones.

Figura 20. Diagrama del sistema bajo estudio



A continuación se describe de forma breve el esquema presentado en la figura 20, que contiene el diagrama del sistema bajo estudio, con los mecanismos de recuperación diseñados para que el sistema siempre vuelva a un estado operativo.

En la UC se activa un *timer* (t_e) tan pronto ésta recibe mensaje de ACK de token, es decir, tan pronto se ha confirmado la entrega de token a una UP.

Para el caso de la falla de caída de UP, este *timer* no se activa, ya que la UP no alcanza a recibir el mensaje de token. La solución propuesta en esta situación consiste en desconectar la unidad, después del segundo intento de envío del token y continuar revisando la secuencia de UPs conectadas, para hacer envío del token. De esta forma, la UP afectada podrá detectar su inactividad y solicitar nuevamente conexión en un siguiente ciclo de token. Con esta solución, la red no se desconfigura y solo se ve afectada la unidad que presenta problemas.

Para la caída de UP con token, la UC debe verificar el "vencimiento" del tiempo del *timer* (t_e). Lo anterior, con el fin de dar una ventana de tiempo razonable a la UP que tiene el token para que transmita información o bien, para que retorne el token. Una vez excedido este tiempo, la UC procede a desconectar la UP e invalidar el token anterior, generando uno nuevo y continuando con la secuencia de token. De esta forma, no existen dos token en la red y solo se ve afectada la UP caída.

Desde la perspectiva de UPs, los dos procedimientos descritos anteriormente no son detectados, a menos que sea la UP a la que fue necesario desconectar de la red, es decir, la UP que presenta falla. Para este caso, una vez cada unidad se encuentra conectada y configurada en la red, se activa el *timer* (t_{et}) que le permite mantenerse en un estado de espera de token. Si esa ventana de tiempo es excedida, La UP debe verificar si continúa o no en estado de conexión; si es así, deberá desconectarse de la red automáticamente y activar un segundo *timer* (t_{cr}). Durante esta ventana de tiempo la UP estará en modo "escucha" del medio. Si escucha su ID (el cual es emitido por la UC) dentro de esta ventana de tiempo, automáticamente procede a enviar su mensaje de solicitud de conexión nuevamente a la red.

Ahora bien, si dada la condición final expuesta en el párrafo anterior, el medio permanece en silencio y es excedido el *timer* (t_{cr}), automáticamente la UP sabrá que algo sucedió con la UC, por lo que procederá a verificar si es su turno de asumir como controladora de la red. De ser así, la unidad se auto-configura y asume sus funciones como UC. De no ser así, se activa un tercer *timer* ($t_{perturbación}$). Si este *timer* es excedido, la UP interpretará que el medio está siendo perturbado y procederá a revisar la tabla de frecuencias configurada, para sugerir a operador el cambio a una frecuencia segura.

CAPITULO VI. MODELO DE SIMULACIÓN E IMPLEMENTACIÓN DE MECANISMOS PROPUESTOS

En esta sección del documento se presenta la descripción general del modelo de simulación elaborado para cada mecanismo de recuperación implementado en el sistema. Estas simulaciones fueron elaboradas empleando la herramienta computacional ExtendSim 8, que es un simulador de eventos discretos. A partir de cada modelo se evalúa la efectividad de la solución propuesta en cada caso.

6.1 MODELOS DE SIMULACIÓN

A continuación se presenta el modelo de simulación elaborado para el sistema. Las variables de entrada de la simulación son leídas de un documento de Excel que contiene los valores de entrada para la simulación.

El objetivo de este modelo es evaluar cómo la variación de las variables de entrada afecta la salida, con el fin de seleccionar los valores que mejor desempeño presenten, para su implementación en el sistema.

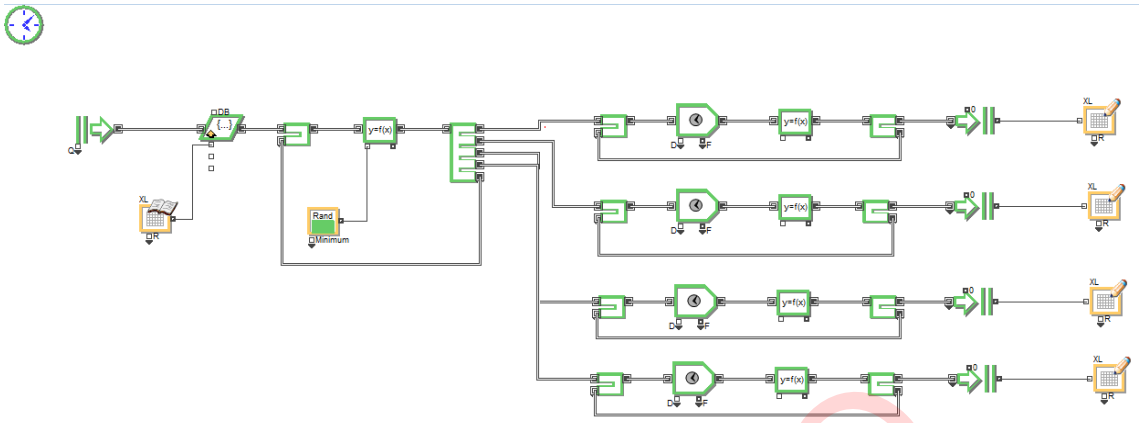
Variables de entrada: Cantidad de Unidades Participantes y Tiempo Optimizado de la Red.
Parámetro de salida: Tiempo de recuperación.

Para la simulación se parte de la suposición de falla del sistema, para ellos se utiliza un módulo de distribución aleatoria de valores cuyo mínimo es 0 y máximo es 3. Los valores entre 0 y 3 llevan al sistema a una falla (de acuerdo a lo detallado en la tabla 1).

Para cada tipo de fallo se activa un temporizador y se efectúan las acciones requeridas para su recuperación, de acuerdo a lo detallado en los diagramas de la sección anterior.

La figura 21 presenta el esquemático general del modelo de simulación elaborado.

Figura 21. Esquemático general del modelo de simulación.



En la figura 21, la sección inicial corresponde a la lectura de los datos desde el documento de Excel y su respectiva asignación a variables del modelo.

Posteriormente, se procede a indicar el tipo de fallo que se presenta, esto con la ayuda de un módulo “Random”, que adopta valores enteros entre 0 y 3; cada valor está asociado a un tipo de fallo y por consiguiente a su respectivo módulo de recuperación.

Una vez identificado el fallo, se procede a accionar un contador de tiempo y se efectúan las acciones correspondientes a cada mecanismo de recuperación.

Al final del proceso se escriben los resultados obtenidos en una hoja de Excel, con el fin de poder procesarlos más adelante.

Las figuras 22 y 23, presentan algunos de los modelos internos de recuperación para cada tipo de fallo.

Figura 22. Modelo interno para comparación de tiempos internos del sistema.

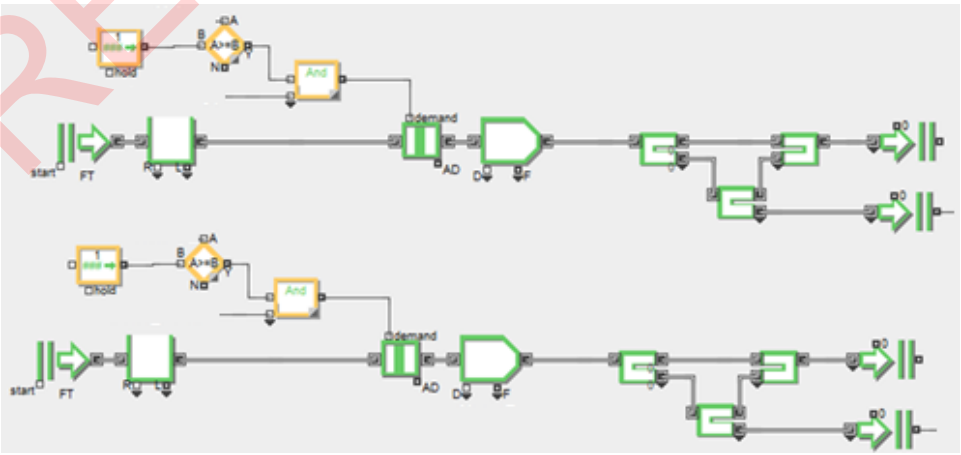
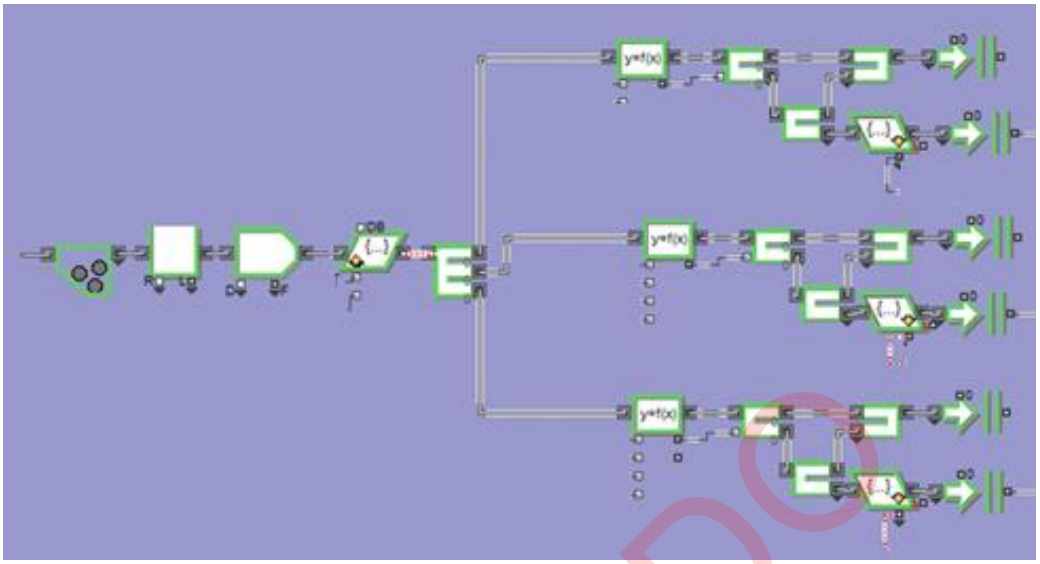


Figura 23. Modelo interno para ejecución y selección de acciones.



Para poder simular los mecanismos de recuperación fue necesario tomar como insumo del modelo los tiempos que tarda experimentalmente el sistema en efectuar ciertas acciones, como lectura de tablas, identificación de ID, entre otras, con el fin de lograr emplear rangos admisibles en el modelo.

La simulación fue corrida 1000 veces, se tomaron como datos de estudio los primeros 100 resultados de tiempo de recuperación de cada tipo de fallo.

6.2 RESULTADOS DE SIMULACIÓN

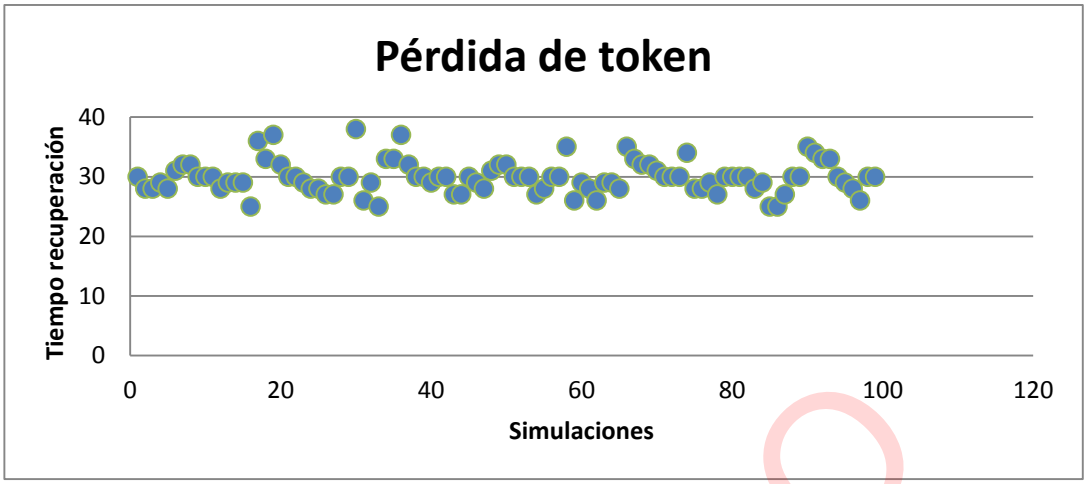
El modelo de simulación se implementó para las siguientes condiciones de entrada:

Cantidad de unidades: 4 (max. Numero unidades que participan en operaciones)
Tiempo de optimización de la red: 3.9 segundos (valor medido)
Cantidad de repeticiones: 100

La figura 24 presenta gráficamente, los tiempos de recuperación medidos para cada una de las 100 simulaciones de la falla “pérdida de token”.

Los resultados numéricos obtenidos a partir de este grupo de simulación se encuentran contenidos en el anexo 2.

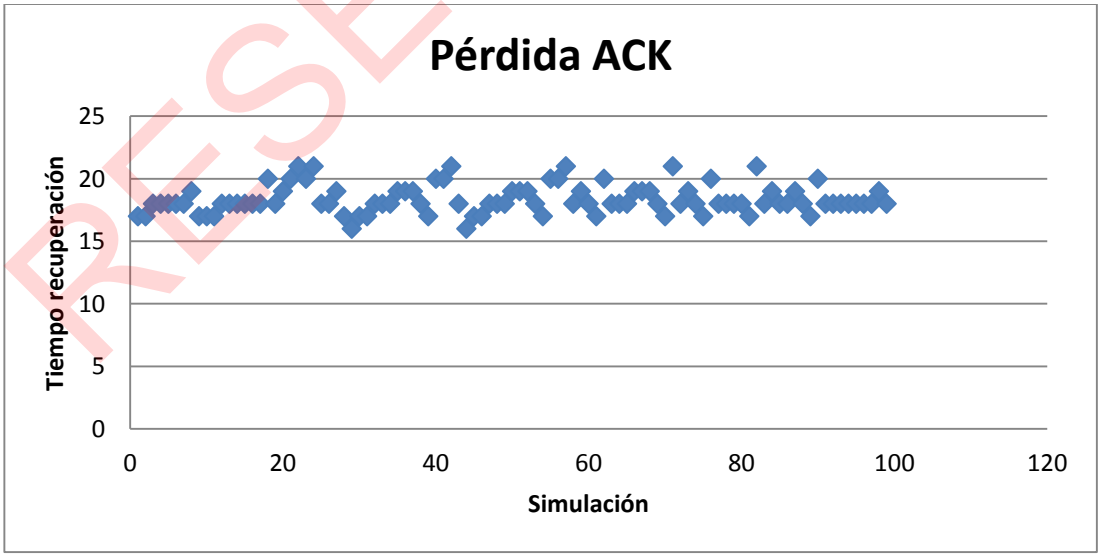
Figura 24. Resultados obtenidos – tiempo recuperación para pérdida de token



El tiempo mínimo de recuperación resultante de la simulación fue de 25 segundos, mientras que el tiempo máximo fue de 38 segundos.
Tiempo promedio de recuperación: 29.9 segundos.
Desviación estándar: 2.65

La figura 25 presenta gráficamente, los tiempos de recuperación medidos para cada una de las 100 simulaciones de la falla "pérdida de ACK".
Los resultados numéricos obtenidos a partir de este grupo de simulación se encuentran contenidos en el anexo 2.

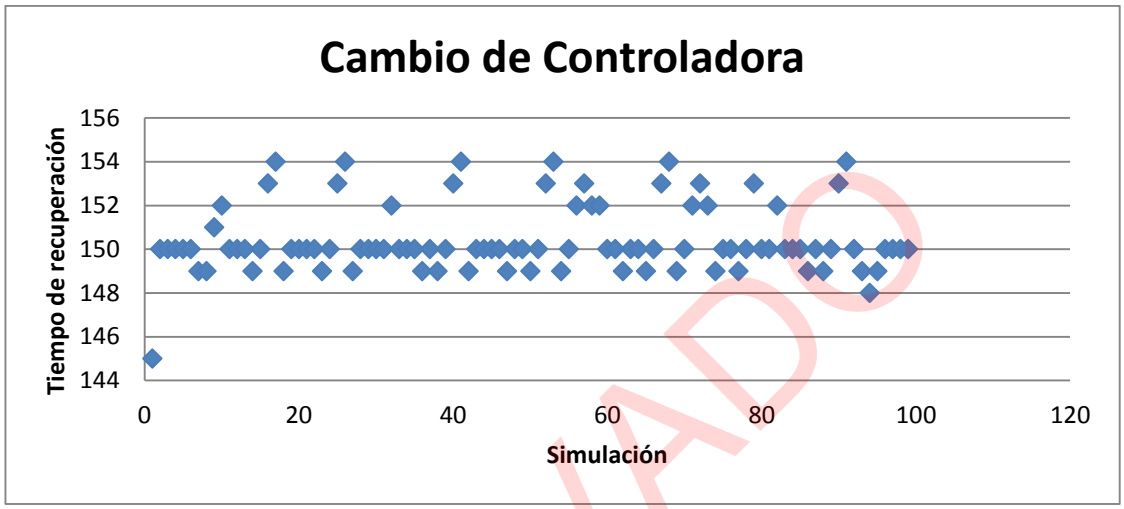
Figura 25. Resultados obtenidos – tiempo recuperación para pérdida de ACK



El tiempo mínimo de recuperación resultante de la simulación fue de 16 segundos, mientras que el tiempo máximo fue de 21 segundos.
Tiempo promedio de recuperación: 18.35 segundos.
Desviación estándar: 1.12

La figura 26 presenta gráficamente, los tiempos de recuperación medidos para cada una de las 100 simulaciones de la falla “caída controladora” (se mide tiempo para cambio controladora).
Los resultados numéricos obtenidos a partir de este grupo de simulación se encuentran contenidos en el anexo 2.

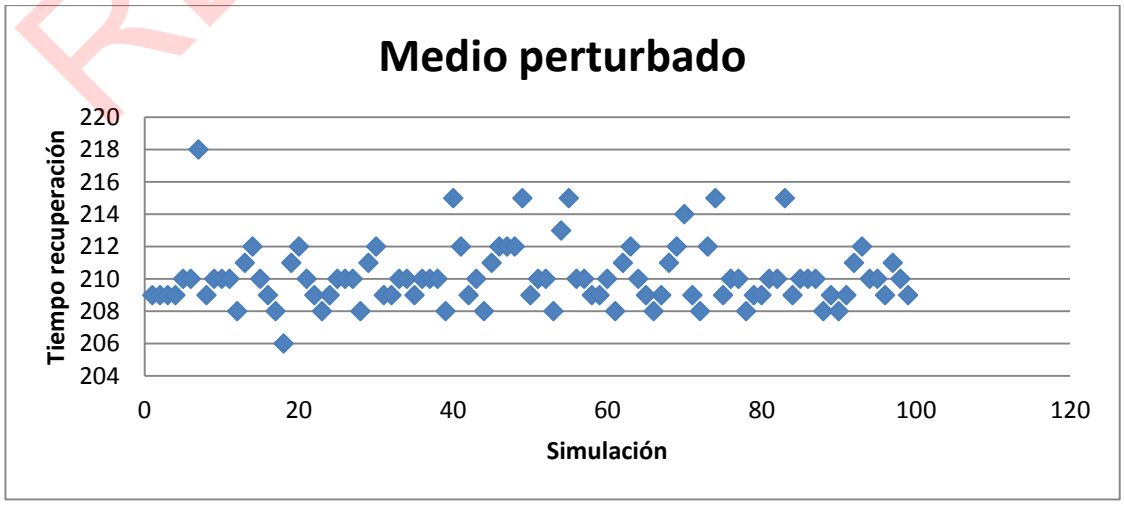
Figura 26. Resultados obtenidos – tiempo recuperación para cambio de controladora



El tiempo mínimo de recuperación resultante de la simulación fue de 145 segundos, mientras que el tiempo máximo fue de 154 segundos.
Tiempo promedio de recuperación: 150.4 segundos.
Desviación estándar: 1.57

La figura 27 presenta gráficamente, los tiempos de recuperación medidos para cada una de las 100 simulaciones de la falla “medio perturbado”.
Los resultados numéricos obtenidos a partir de este grupo de simulación se encuentran contenidos en el anexo 2.

Figura 27. Resultados obtenidos – tiempo recuperación para medio perturbado



El tiempo mínimo de recuperación resultante de la simulación fue de 206 segundos, mientras que el tiempo máximo fue de 218 segundos.
Tiempo promedio de recuperación: 210.13 segundos.
Desviación estándar: 1.91

Tabla 5. Resumen resultados simulaciones

Nombre de prueba	Cantidad de repeticiones	Desviación estándar	Tiempo Promedio
Recuperación del sistema ante pérdida de token	100	2.65	29.9seg
Recuperación del sistema ante pérdida de ACK – caída UP	100	1.13	18.35seg
Recuperación del sistema ante cambio de controladora	100	1.57	150.4seg
Recuperación del sistema ante medio perturbado	100	1.91	210.13seg

6.3 IMPLEMENTACIÓN DE LOS MECANISMOS

Como resultado del proceso de simulación, se verificó que los tiempos de recuperación asociados a cada falla disminuyeron por encima del 50%, con respecto a los tiempos medidos a partir de la recuperación manual del sistema, por lo que se verifica la viabilidad de implementación de los mecanismos propuestos.

El lenguaje de programación empleado para implementar estos mecanismos de recuperación es C++, y el entorno de trabajo fue Visual Studio 2010. Se utiliza una versión licenciada de esta herramienta, propietaria de COTECMAR.

Debido al carácter propietario que tiene COTECMAR sobre el software del sistema DATA LINK (sistema bajo estudio), no es posible presentar públicamente los códigos fuente desarrollados para la implementación de los mecanismos de recuperación, sin embargo, y con el fin que se evidencie en alguna medida el trabajo efectuado, COTECMAR permitió presentar el código desarrollado para el tratamiento de uno de los casos de falla.

A continuación se muestra el código fuente de la implementación del mecanismo de recuperación para el caso de falla “caída de UP”.

```
EN ESTA SECCIÓN SE ARMAN LOS MENSAJES A TRANSMITIR Y BÁSICAMENTE SE DA LA ORDEN DE ACTIVAR
EL TIMER PARA MEDIR LA PÉRDIDA DE ACK, ÉSTA ES LA MEJOR FORMA DE EVALUAR SI UNA UNIDAD
PARTICIPANTE, QUE NO TENÍA EL TOKEN, SUFRIÓ FALLA Y POR ELLO ESTÁ INACTIVA EN EL SISTEMA.

Cola mensajes de tx

(transmitaCola())

        if(Unidades->leerNodo(aquien)->Estado!="0")
        {
                Salida = salioM->TipoMensaje + ","
```

```
                        + salioM->NiOrigen   + ","
                        + salioM->NiDestino  + ","
                        + salioM->Autoridad  + ","
                        + salioM->GFH        + ","
                        + salioM->Prioridad  + ","
                        + salioM->Cuerpo;

                Salida= Unidades->leerNodo(aquien)->Trama +"\x1"+Salida+"\x4"+"\xd";
                this->serialPort1->Write(Salida);
                OnTimerNuestro(2);
                String^ cuerpoEnc = salioM->Cuerpo;
                agregarALogDescifrado(salioM);
                salioM->Cuerpo = cuerpoEnc;

                if(salioM->Prioridad == "01") banderaPrioridad=1;

                setTimer("perdidaACK");
                ack = 0;

        }
```

EN ESTA SECCIÓN SE ASIGNA EL PERIODO DE TIEMPO CORRESPONDIENTE AL TEMPORIZADOR QUE SE EMPLEARÁ COMO COMPARADOR PARA DETERMINAR EL INICIO DEL RESPECTIVO MECANISMO DE RECUPERACIÓN.

```
set timer (setTimer(String^ elTimer))


void Form1::setTimer(String^ elTimer)
{
        if(elTimer == "perdidaACK")
        {
                perdidaACK->Interval = 2.5*To*1000;
                perdidaACK->Enabled = true;
        }
        if(elTimer == "esperaToken")
        {
                esperaToken->Interval = (To/2)*1000;
                esperaToken->Enabled = true;
        }
        if(elTimer == "AACK")
        {
                AACK->Interval = 3000;
                AACK->Enabled = true;
        }
        if(elTimer == "DACK")
        {
                DACK->Interval = 1500;
                DACK->Enabled = true;
        }
```

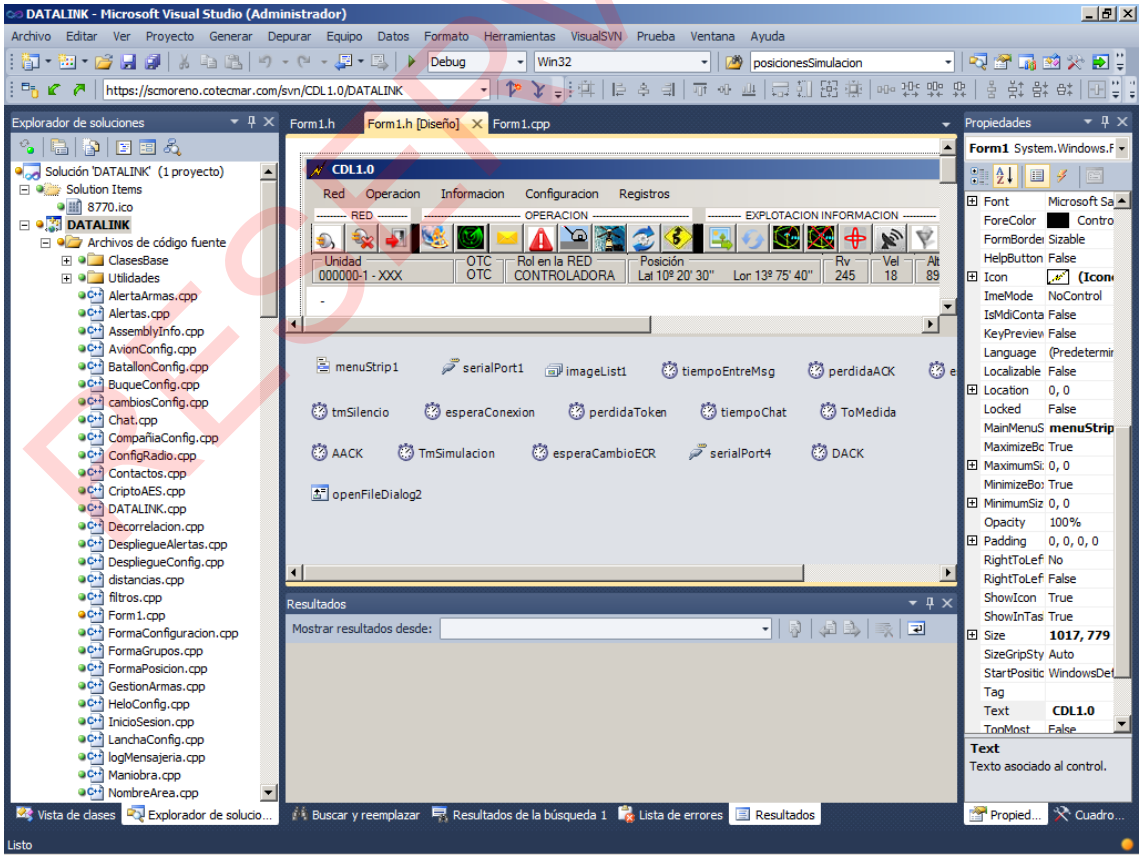
CUMPLIDO EL TIEMPO, SE GENERA EL EVENTO timer112_Tick, ESTE EVENTO DA CABIDA A LA FUNCIÓN "OnPerdidaACK", LA CUAL HABILITA EL MECANISMO DE RECUPERACIÓN.

```
private: System::Void timer112_Tick(System::Object^  sender, System::EventArgs^  e)
        {
                OnPerdidaACK();
        }



void Form1::OnPerdidaACK()
{
        this->perdidaACK->Enabled = false;//Resetea el timer perdida ACK
        if(retransmitaMSG == 0)
        {
                retransmitaMSG = 1;
                if(sNI == NIcontroladora)
                {
                        transmitaCola();
```

```
                }
                else
                {
                        transmitaColaP();
                }
        }
        else
        {
                pendiente++;
                retransmitaMSG;
                if(sNI == NIcontroladora)
                {
                        transmitaCola();
                }
                else
                {
                        transmitaColaP();
                }
        }
}
```

Los temporizadores implementados en el sistema, como parte integral del modelo de recuperación de fallas propuesto, son presentados en la figura 23, la cual presenta, en la interfaz gráfica de la herramienta Visual Studio 2010, los íconos correspondientes y nombres asignados a cada uno de ellos en el sistema.

Figura 28. Interfaz de usuario Visual Studio 2010 –temporizadores implementados.



CAPITULO VII. DISEÑO DE PRUEBAS Y RESULTADOS

El objetivo de esta sección del documento es presentar el plan de pruebas que permita verificar el correcto funcionamiento de los mecanismos de recuperación propuestos para el sistema DATALINK bajo estudio.

Las pruebas evalúan tanto la recuperación de la falla, como el tiempo que tarda el sistema en volver a un estado operativo. Este resultado temporal es comparado con los resultados obtenidos en las pruebas de recuperación manual del sistema.

7.1 COMPOSICIÓN FISICA DE LA PRUEBA

Los equipos y/o herramientas consideradas para este Plan de Pruebas están compuesta por:

- ✓ Cuatro computadores, en condiciones de uso y con el sistema operativo Windows, en versión XP o superior, instalado y actualizado. Las características técnicas de los equipos de cómputo empleados en estas pruebas se detalla en el Anexo 3.

- ✓ Equipamiento radio compuesto por:

  - Cuatro radios tácticos con carga de antena, modelo: Motorola Pro 3100 UHF, con fuente. Las características técnicas de los equipos de radio empleados, se presentan en el Anexo 4.

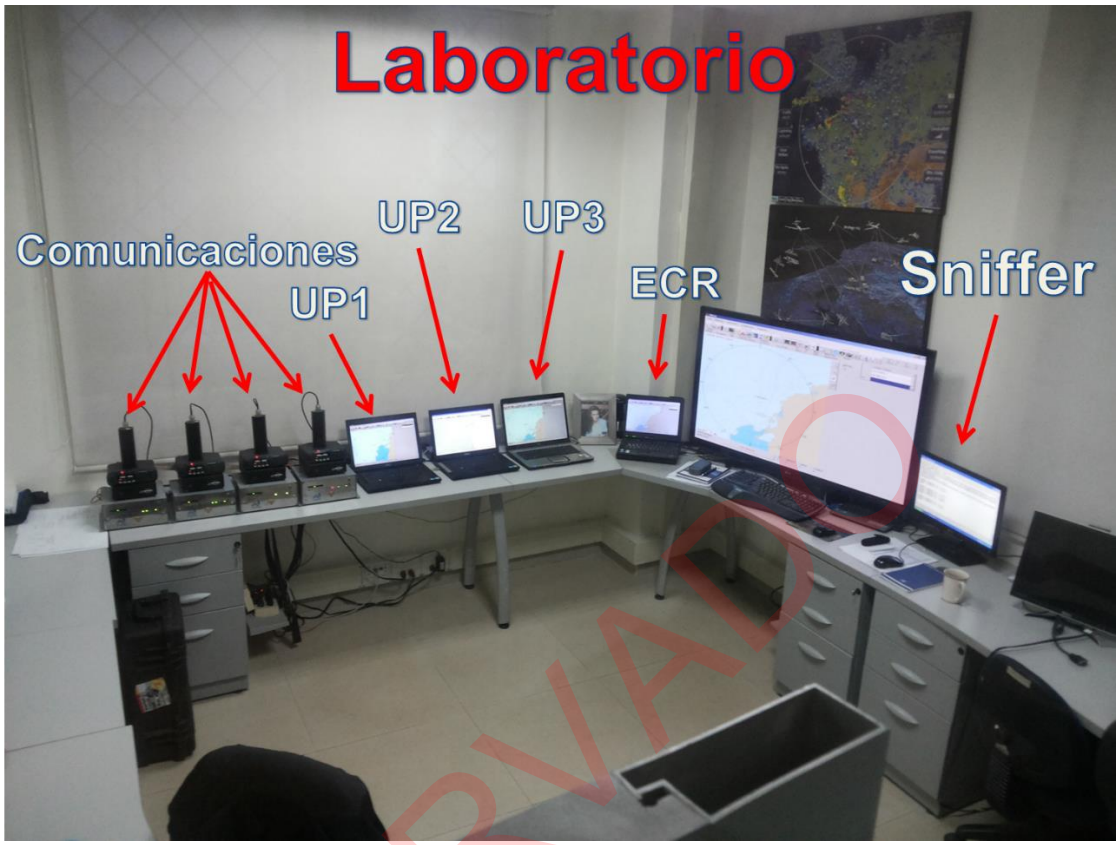
  - Cuatro cajas integradoras de comunicaciones, tal como fueron descritas en la sección 4.4 de este documento. Las características técnicas de los multimódem empleados y de los switch, se detallan en los Anexos 5 y 6.

- Cableado adecuado para conectar computadores, multimódems y radios. Para verificar la configuración de los multimódem y los equipos de radio, remítase los Anexos 7, 8 y 9.

La figura 29 presenta una fotografía del laboratorio donde se efectuaron las pruebas. Este laboratorio se encuentra ubicado en las instalaciones de COTECMAR y fue autorizada su utilización para efectuar el protocolo de pruebas del sistema bajo estudio, con el mecanismo de recuperación automático ante fallas implementado.

La figura también presenta los roles de cada equipo empleado.

Figura 29. Instalaciones Laboratorio donde se efectuaron pruebas



7.2 CONJUNTO DE ESCENARIOS DE PARTIDA

Los conjuntos de escenarios planteados se recogen para establecer los puntos de partida de cada una de las pruebas que se detallan en el presente plan. Se describen a continuación y en cada una de las pruebas se declara cuál de ellos se utiliza en la misma.

7.2.1 Escenario A

Este es el escenario de equipamiento básico que se utilizará en todas las pruebas, para verificar funcionamiento. Está compuesto por:

- Computador para ECR, en condiciones de uso y únicamente con el sistema operativo instalado y actualizado.
- Computador para UP 1, en condiciones de uso y únicamente con el sistema operativo instalado y actualizado.
- Computador para UP 2, en condiciones de uso y únicamente con el sistema operativo instalado y actualizado.
- Computador para SNIFFER, en condiciones de uso y únicamente con el sistema operativo instalado y actualizado.

7.2.2 Escenario B

Este es el escenario de equipamiento básico que se utilizará en todas las pruebas operativas. Está compuesto por:

- Computador para ECR, en condiciones de uso y únicamente con el sistema operativo instalado y actualizado.
- Computador para UP 1, en condiciones de uso y únicamente con el sistema operativo instalado y actualizado.
- Computador para UP 2, en condiciones de uso y únicamente con el sistema operativo instalado y actualizado.
- Computador para UP 3, en condiciones de uso y únicamente con el sistema operativo instalado y actualizado.

Las pruebas constan de un *escenario de partida* descrito, tal como se ha descrito, una *secuencia de acciones* por medio de las cuales se busca evaluar los mecanismos implementados y finalmente una *verificación* de resultados que indica lo que se busca encontrar o evidenciar con cada bloque de pruebas.

7.3 PRUEBAS DE RECUPERACIÓN DEL SISTEMA.

Denominada “recuperación del sistema ante perdida de token, ACK, medio perturbado y cambio de controladora”. Para el caso de pérdida de token, la prueba consistió en simular la caída de una UP que tuviera el token y se verificó que el sistema lo regenerara. Para la situación de pérdida del ACK, la prueba es similar a la realizada para el caso de pérdida de token, con la diferencia que en esta ocasión el mensaje debe ser retransmitido o almacenado como pendiente. Finalmente, para el caso de medio perturbado, las UP detectan la situación y notifican que se debe realizar un cambio de frecuencia.

7.3.1 Secuencia de acciones, para caso Pérdida de token

- Escenario inicial: Escenario A.
- Instalar en tres de los computadores el aplicativo de software para prueba de protocolo.
- Configurar dos de esos aplicativos como UPs.
- Configurar uno de los aplicativos como ECR.
- Instalar el SNIFFER en el cuarto computador.
- Activar el SNIFFER.
- Las UPs intentan conectarse simultáneamente a la red presionando la opción “conectar” del aplicativo.
- La ECR envía mensajes con el identificador de cada UP, indicando el turno de conexión.
- A medida que cada UP identifica su turno, se conecta a la red, de acuerdo a la secuencia establecida en la tabla de unidades del sistema.
- Una vez se encuentre, al menos una UP en la red, la ECR le enviará el token, para que pueda transmitir información. El orden en que la ECR envía el token dependerá de la secuencia de las UPs en la tabla de unidades del sistema.
- Las unidades de la tabla que no estén conectadas no recibirán token, sino que les llegará un mensaje con su número de identificación, para su respectivo turno de conexión.
- Se procede a simular la caída de la UP que tiene el token, apagando el modem de esta unidad una vez que ha recibido el token y enviado el ACK.
- Transcurrido un tiempo, la ECR determina que hubo pérdida de token.
- La ECR marca la unidad que presentó fallas como no conectada, en la tabla de unidades del sistema, despliega la actualización del estado de esta unidad en la ventana del aplicativo, y procede a enviar un nuevo token a la siguiente UP en la secuencia.
- En el ciclo de token, cuando es el turno de la unidad que presentó la falla, la ECR espera un intervalo de tiempo para darle a esta estación la oportunidad de realizar el proceso de reconexión.

- Utilizando el SNIFFER, se monitorea que ocurrió la falla y que la red continua su funcionamiento normal, una vez la ECR ha regenerado el token.

Verificación de resultado escenario A

El resultado deberá ser:

a) Computadores con aplicativo instalado y corriendo correctamente.
b) Computador con SNIFFER corriendo correctamente.
c) Se verifica en el SNIFFER la pérdida de token y la recuperación automática del sistema.

7.3.1.1 Resultados Obtenidos en pruebas de laboratorio – recuperación ante pérdida de token

- ***Prueba escenario A* - Resultados generales.**

Tabla 6. Resultados de la prueba de recuperación ante pérdida de token– escenario A

ACCIÓN	DESCRIPCIÓN	ANOTACIONES	RESULTADO
a)	Equipos encendidos, aplicativos corriendo y configurados.	Aplicativos configurados así: - 040053-1 (ECR) - 070803-1 (UP) - 080130-1 (UP) Las UPs oprimen el botón presentado a continuación:  Para verificación de esta funcionalidad no es necesario oprimir ningún botón. Es automático el proceso.	Ok
b)	Equipo encendido con ventana de SNIFFER abierta.	Estado inicial de la ventana de SNIFFER: pantalla en blanco. Tal como aparece en la Figura 19.	Ok
c)	Verificar pérdida de token y posterior reinicio del sistema	Estado final de la ventana de SNIFFER, como se presenta en la Tabla 6.	Ok

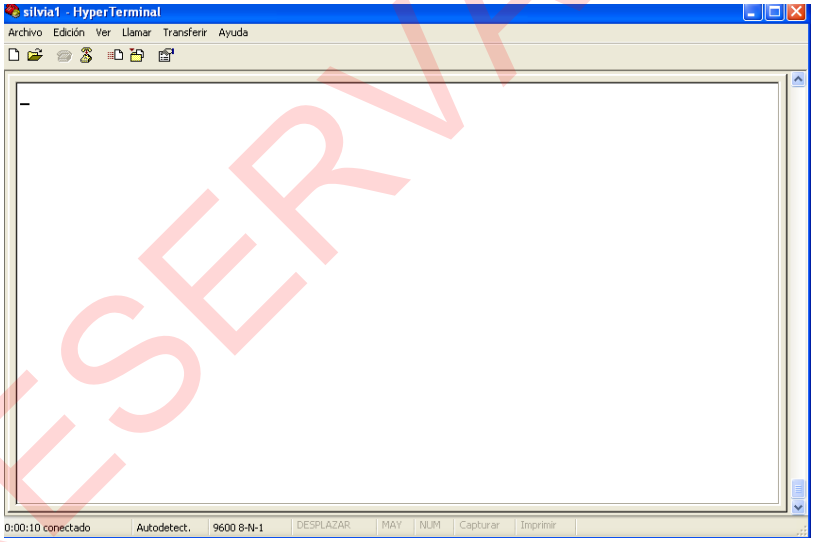
- ***Prueba escenario A* - Resultados detallados.**

a) La configuración de las unidades, respecto a su Rol en la red (ECR o UP), se establecen en la tabla de secuencia. La configuración para esta prueba se presenta a continuación:

Figura 30. Pruebas laboratorio – recuperación ante pérdida de token - Tabla de secuencia configurada para prueba – escenario A.

b) El estado inicial del SNIFFER se presenta a continuación:

Figura 31. Pruebas laboratorio – recuperación ante pérdida de token - Estado inicial ventana de SNIFFER - Escenario A.



c) El estado final del SNIFFER, posterior a la prueba:

Tabla 7. Prueba laboratorio – recuperación ante pérdida de token - Verificación de pérdida de token en SNIFFER –Escenario A.

MENSAJES	DESCRIPCION
040053-1>CQ/1: <UI>: ### 0001	La ECR envía el código con el ID del que tiene el turno para conectarse.
070803-1>040053-1/1: <<C>>: 040053-1>070803-1/1: <<UA>>:	Solicitud de conexión del 803 ACK de conexión de la ECR al 803
040053-1>070803-1/1: <<I00>>: conv	La ECR pasa a modo conv
070803-1>040053-1/1: <<rr1>>: 040053-1>070803-1/1: <<I10>>:	ACK de módem Mensaje de sincronía de la ECR para el 803

08,144021	
070803-1>040053-1/1: <<rr2>>:	ACK de módem
040053-1>070803-1/1: <<I20>>: ### 0002	La ECR envía el código con el ID del que tiene el turno para conectarse.
070803-1>040053-1/1: <<rr3>>: 080130-1>040053-1/1: <<C>>: 040053-1>080130-1/1: <<UA>>:	ACK de módem Solicitud de conexión del 130 ACK de conexión de la ECR para el 130
040053-1>070803-1/1: <<I30>>: conv	La ECR pasa a modo conv
070803-1>040053-1/1: <<rr4>>: 040053-1>080130-1/1: <<I00>>: 08,144034	ACK de módem Mensaje de sincronía de la ECR para el 130
080130-1>040053-1/1: <<rr1>>: 040053-1>070803-1/1: <<I40>>: 01	ACK de módem La ECR envía el token al 803
070803-1>040053-1/1: <<rr5>>: 070803-1>040053-1/1: <<I05>>: 28	ACK de módem Mensaje de ACK del 803 para la ECR
040053-1>070803-1/1: <<rr1>>: 070803-1>040053-1/1: <<I15>>: 01	ACK de módem El 803 envía el token a la ECR
040053-1>070803-1/1: <<rr2>>: 040053-1>070803-1/1: <<I52>>: 28	ACK de módem Mensaje de ACK de la ECR para el 803
070803-1>040053-1/1: <<rr6>>: 040053-1>080130-1/1: <<I10>>: 01	ACK de módem La ECR envía el token al 130
080130-1>040053-1/1: <<rr2>>: 080130-1>040053-1/1: <<I02>>: 28	ACK de módem Mensaje de ACK del 130 a la ECR
040053-1>080130-1/1: <<rr1>>: 080130-1>040053-1/1: <<I12>>: 01	ACK de módem El 130 envía el token a la ECR
040053-1>080130-1/1: <<rr2>>: 040053-1>080130-1/1: <<I22>>: 28	ACK de módem Mensaje de ACK de la ECR al 130
080130-1>040053-1/1: <<rr3>>: 040053-1>070803-1/1: <<I62>>: 01	ACK de módem La ECR envía el token al 803
070803-1>040053-1/1: <<rr7>>: 070803-1>040053-1/1: <<I27>>: 28	ACK de módem Mensaje de ACK del 803 a la ECR
040053-1>070803-1/1: <<rr3>>:	ACK de módem
	(Aquí se simula la pérdida del token)

040053-1>070803-1/1: <<D>>: 040053-1>080130-1/1: <<I32>>: 01	La ECR desconecta al 803 La ECR envía el token al 130
080130-1>040053-1/1: <<rr4>>: 080130-1>040053-1/1: <<I24>>: 28	ACK de módem Mensaje de ACK del 130 a la ECR
040053-1>080130-1/1: <<rr3>>: 080130-1>040053-1/1: <<I34>>: 01	ACK de módem El 130 envía el token a la ECR
040053-1>080130-1/1: <<rr4>>: 040053-1>080130-1/1: <<I44>>: 28	ACK de módem Mensaje de ACK de la ECR al 130
080130-1>040053-1/1: <<rr5>>: 040053-1>080130-1/1: <<I54>>: ### 0001	ACK de módem La ECR envía el código con el ID del que tiene el turno para conectarse.

7.3.2 Secuencia de acciones, para caso Pérdida de ACK

- Escenario inicial: Escenario A.
- Instalar en tres de los computadores el aplicativo de software para prueba de protocolo.
- Configurar dos de esos aplicativos como UPs.
- Configurar uno de los aplicativos como ECR.
- Instalar el SNIFFER en el cuarto computador.
- Activar el SNIFFER.
- Las UPs intentan conectarse simultáneamente a la red presionando la opción “conectar” del aplicativo.
- La ECR envía mensajes con el identificador de cada UP, indicando el turno de conexión.
- A medida que cada UP identifica su turno, se conecta a la red, de acuerdo a la secuencia establecida en la tabla de unidades del sistema.
- Una vez se encuentre, al menos una UP en la red, la ECR le enviará el token, para que pueda transmitir información. El orden en que la ECR envía el token dependerá de la secuencia de las UPs en la tabla de unidades del sistema.
- Las unidades de la tabla que no estén conectadas no recibirán token, sino que les llegará un mensaje con su número de identificación, para su respectivo turno de conexión.
- Todas las UPs que están conectadas envían mensajes a la ECR, la cual los almacena en una cola de mensajes.
- La ECR, cuando tiene el token, retransmite a la siguiente UP de la secuencia el mensaje.

- Antes que la UP envíe el ACK (confirmación de recepción del mensaje) a la ECR, se simula la caída de la unidad apagando el modem de esta estación.
- La ECR, al no recibir el ACK, intenta reenviar el mensaje a esa UP (solo reintenta 1 vez).
- Si no recibe ACK, almacena el mensaje y lo marca como “pendiente” en la cola de mensajes.
- La ECR procede, entonces, a enviar el mensaje a la siguiente UP en la secuencia.
- Se procede a simular la reconexión de la UP que falló y se comprueba que la ECR le envíe el mensaje que tenía pendiente.

Verificación de resultado escenario A

El resultado deberá ser:

a) Computadores con aplicativo instalado y corriendo correctamente.
b) Computador con SNIFFER corriendo correctamente.
c) Se verifica en el SNIFFER la pérdida de ACK y la recuperación automática del sistema.

7.3.2.1 Resultados Obtenidos en pruebas de laboratorio – recuperación ante pérdida de ACK

- **Prueba escenario A - Resultados generales.**

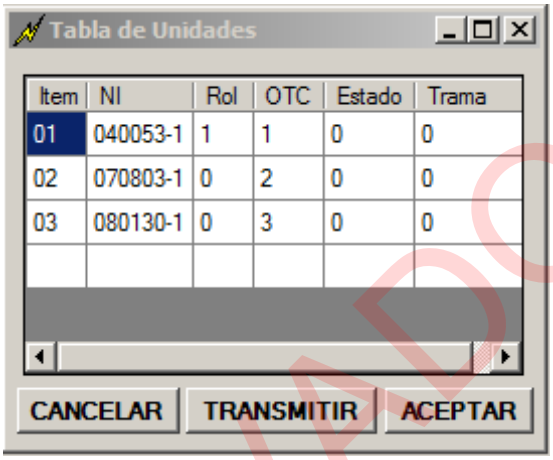
Tabla 8. Resultados de la prueba de recuperación ante pérdida de ACK– escenario A

ACCIÓN	DESCRIPCIÓN	ANOTACIONES	RESULTADO
a)	Equipos encendidos, aplicativos corriendo y configurados.	Aplicativos configurados así: - 040053-1 (ECR) - 070803-1 (UP) - 080130-1 (UP) Las UPs oprimen el botón presentado a continuación:  Para verificación de esta funcionalidad no es necesario oprimir ningún botón. Es automático el proceso.	Ok
b)	Equipo encendido con ventana de SNIFFER abierta.	Estado inicial de la ventana de SNIFFER: pantalla en blanco. Tal como aparece en la Figura 21.	Ok
c)	Verificar pérdida de ACK y posterior recuperación del sistema	Estado final de la ventana de SNIFFER, como se presenta en la Tabla 8.	Ok

- **Prueba escenario A - Resultados detallados.**

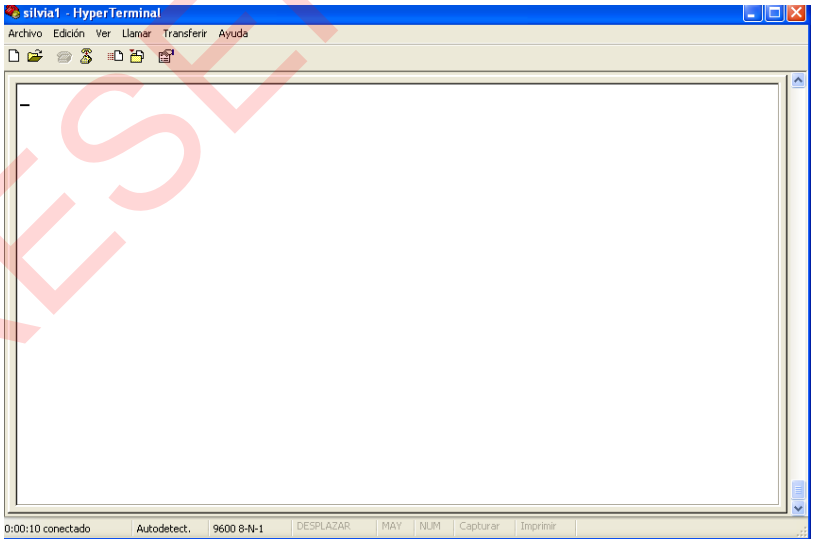
a) La configuración de las unidades, respecto a su Rol en la red (ECR o UP), se establecen en la tabla de secuencia. La configuración para esta prueba se presenta a continuación:

Figura 32. Pruebas laboratorio – recuperación ante pérdida de ACK - Tabla de secuencia configurada para prueba – escenario A.



b) El estado inicial del SNIFFER se presenta a continuación:

Figura 33. Pruebas laboratorio – recuperación ante pérdida de ACK - Estado inicial ventana de SNIFFER - Escenario A.



c) El estado final del SNIFFER, posterior a la prueba:

Tabla 9. Prueba laboratorio – recuperación ante pérdida de ACK - Verificación de pérdida de ACK en SNIFFER –Escenario A.

MENSAJES	DESCRIPCION
040053-1>CQ/1: <UI>: ### 0001	La ECR (040053-1) envía el código con el ID del que tiene el turno para conectarse
070803-1>040053-1/1: <<C>>:	El 070803-1 solicita conexión
040053-1>070803-1/1: <<UA>>:	ACK de conexión de la ECR
040053-1>070803-1/1: <<I00>>: conv	La ECR pasa a modo conv
070803-1>040053-1/1: <<rr1>>:	ACK de módem
040053-1>070803-1/1: <<I10>>: 08,145250	La ECR envía el mensaje de sincronía
070803-1>040053-1/1: <<rr2>>:	ACK de módem
040053-1>070803-1/1: <<I20>>: ### 0002	La ECR envía el código con el ID del que tiene el turno para conectarse
070803-1>040053-1/1: <<rr3>>:	ACK de módem
080130-1>040053-1/1: <<C>>:	Solicitud de conexión del 080130-1
040053-1>080130-1/1: <<UA>>:	ACK de conexión de la ECR
040053-1>070803-1/1: <<I30>>: conv	La ECR pasa a modo conv
070803-1>040053-1/1: <<rr4>>: 040053-1>080130-1/1: <<I00>>: 08,145303	ACK de módem La ECR envía el mensaje de sincronía
080130-1>040053-1/1: <<rr1>>: 040053-1>070803-1/1: <<I40>>: 01	ACK de módem La ECR envía el token al 803
070803-1>040053-1/1: <<rr5>>: 070803-1>040053-1/1: <<I05>>: 28	ACK de módem Mensaje de ACK del 803
040053-1>070803-1/1: <<rr1>>: 070803-1>040053-1/1: <<I15>>: 01	ACK de módem El 803 envía el token a la ECR
040053-1>070803-1/1: <<rr2>>: 040053-1>070803-1/1: <<I52>>: 28	ACK de módem Mensaje de ACK de la ECR
070803-1>040053-1/1: <<rr6>>:	ACK de módem
040053-1>070803-1/1: <<I62>>: 25,040053-1,070803-1,OCT,031453R DIC/13,03,qPRc17tqUh5AxR1TCQLAEg==	La ECR envía mensaje de chat al 803
	(Aquí ocurre la pérdida del ACK)

070803-1>040053-1/1: <<rr7>>: 040053-1>070803-1/1: <<I72>>: 25,040053-1,070803-1,OCT,031453R DIC/13,03,qPRc17tqUh5AxR1TCQLAEg==	ACK de módem La ECR envía mensaje de chat al 803
040053-1>070803-1/1: <<D>>: 040053-1>080130-1/1: <<I10>>: 01	La ECR desconecta al 803 La ECR envía el token al 130
080130-1>040053-1/1: <<rr2>>: 080130-1>040053-1/1: <<I02>>: 28	ACK de módem El 130 envía mensaje de ACK a la ECR
040053-1>080130-1/1: <<rr1>>: 080130-1>040053-1/1: <<I12>>: 01	ACK de módem El 130 envía el token a la ECR
040053-1>080130-1/1: <<rr2>>: 040053-1>080130-1/1: <<I22>>: 28	ACK de módem Mensaje de ACK de la ECR al 130
080130-1>040053-1/1: <<rr3>>: 040053-1>080130-1/1: <<I32>>: ### 0001 080130-1>040053-1/1: <<rr4>>: 070803-1>040053-1/1: <<C>>: 040053-1>070803-1/1: <<UA>>: 040053-1>080130-1/1: <<I42>>: conv 040053-1>070803-1/1: <<I00>>: 08,145416	ACK de módem La ECR envía el código con el ID del que tiene el turno de conectarse. ACK de módem Solicitud de conexión del 803 ACK de conexión de la ECR La ECR pasa a modo conv Mensaje de sincronía para el 803
070803-1>040053-1/1: <<rr1>>: 040053-1>080130-1/1: <<I10>>: 01	ACK de módem La ECR envía el token al 130
080130-1>040053-1/1: <<rr2>>: 080130-1>040053-1/1: <<I02>>: 28	ACK de módem El 130 envía mensaje de ACK a la ECR
040053-1>080130-1/1: <<rr1>>: 080130-1>040053-1/1: <<I12>>: 01	ACK de módem El 130 envía el token a la ECR
040053-1>080130-1/1: <<rr2>>: 040053-1>080130-1/1: <<I22>>: 28	ACK de módem Mensaje de ACK de la ECR al 130
080130-1>040053-1/1: <<rr3>>: 040053-1>070803-1/1: <<I10>>: 01	ACK de módem La ECR envía el token al 803
070803-1>040053-1/1: <<rr2>>: 070803-1>040053-1/1: <<I02>>: 28	ACK de módem El 803 envía mensaje de ACK a la ECR
040053-1>070803-1/1: <<rr1>>: 070803-1>040053-1/1: <<I12>>:	ACK de módem EL 803 envía el token a la ECR

01	
040053-1>070803-1/1: <<rr2>>: 040053-1>070803-1/1: <<l22>>: 28	ACK de módem La ECR envía mensaje de ACK al 803
070803-1>040053-1/1: <<rr3>>:	ACK módem
040053-1>070803-1/1: <<l32>>: 25,040053-1,070803-1,OCT,031453R DIC/13,03,qPRc17tqUh5AxR1TCQLAEg==	La ECR envía mensaje de chat al 803
070803-1>040053-1/1: <<rr4>>: 070803-1>040053-1/1: <<l24>>: 28	ACK de módem El 803 envía mensaje de ACK a la ECR
040053-1>070803-1/1: <<rr3>>:	ACK de módem

7.3.3 Secuencia de acciones para caso cambio de controladora

- Escenario inicial: Escenario A.
- Instalar en tres de los computadores el aplicativo de software para prueba de protocolo.
- Configurar dos de esos aplicativos como UPs.
- Configurar uno de los aplicativos como ECR.
- Instalar el SNIFFER en el cuarto computador.
- Activar el SNIFFER.
- Las UPs intentan conectarse simultáneamente a la red presionando la opción “conectar” del aplicativo.
- La ECR envía mensajes con el identificador de cada UP, indicando el turno de conexión.
- A medida que cada UP identifica su turno, se conecta a la red, de acuerdo a la secuencia establecida en la tabla de unidades del sistema.
- Una vez se encuentre, al menos una UP en la red, la ECR le enviará el token, para que pueda transmitir información. El orden en que la ECR envía el token dependerá de la secuencia de las UPs en la tabla de unidades del sistema.
- Las unidades de la tabla que no estén conectadas no recibirán token, sino que les llegará un mensaje con su número de identificación, para su respectivo turno de conexión.
- Se apaga intencionalmente la ECR actual, simulando su caída.
- Después de un periodo de tiempo determinado (establecido en función del desempeño de la red) sin que las UPs reciban mensajes de token, las unidades se desconectan.
- La unidad siguiente a la ECR en el orden de la tabla de identificación del sistema, activa un temporizador para dar tiempo a que todas las unidades participantes terminen el proceso de desconexión de la ECR anterior.
- Una vez se cumple este tiempo, la UP asume su nuevo rol de ECR e inicia el envío de mensajes con los identificadores de cada unidad y espera que soliciten conexión.

Verificación de resultado escenario A

El resultado deberá ser:

a) Computadores con aplicativo instalado y corriendo correctamente.
b) Computador con SNIFFER corriendo correctamente.
c) Se verifica en el SNIFFER la secuencia de cambio de controladora y el restablecimiento del sistema.

7.3.3.1 Resultados Obtenidos en pruebas de laboratorio – recuperación ante cambio de controladora

- ***Prueba escenario A*** **- Resultados generales.**

Tabla 10. Resultados de la prueba de recuperación ante cambio de controladora– escenario A

ACCIÓN	DESCRIPCIÓN	ANOTACIONES	RESULTADO
a)	Equipos encendidos, aplicativos corriendo y configurados.	Aplicativos configurados así: - 040053-1 (ECR) - 070803-1 (UP) - 080130-1 (UP) Las UPs oprimen el botón presentado a continuación:  Para verificación de esta funcionalidad no es necesario oprimir ningún botón. Es automático el proceso.	Ok
b)	Equipo encendido con ventana de SNIFFER abierta.	Estado inicial de la ventana de SNIFFER: pantalla en blanco. Tal como aparece en la Figura 23.	Ok
c)	Verificar cambio de controladora y posterior recuperación del sistema	Estado final de la ventana de SNIFFER, como se presenta en la Tabla 10.	Ok

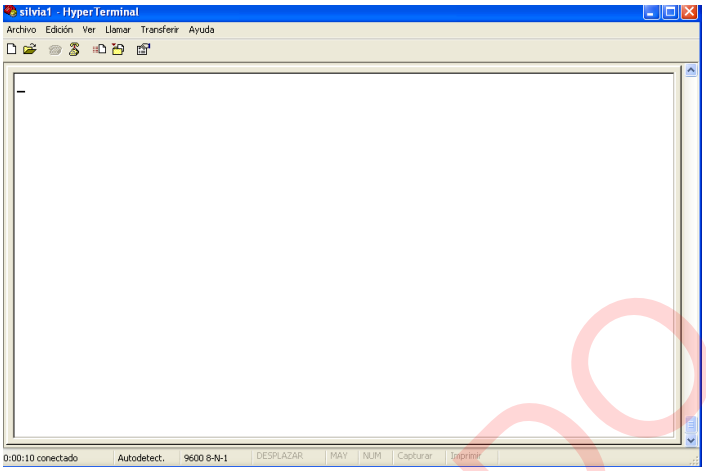
- **Resultados detallados.**

a) La configuración de las unidades, respecto a su Rol en la red (ECR o UP), se establecen en la tabla de secuencia. La configuración para esta prueba se presenta a continuación:

Figura 34. Pruebas laboratorio – recuperación ante cambio de controladora - Tabla de secuencia configurada para prueba – escenario A.

b) El estado inicial del SNIFFER se presenta a continuación:

Figura 35. Pruebas laboratorio – recuperación ante cambio de controladora - Estado inicial ventana de SNIFFER - Escenario A.



c) El estado final del SNIFFER, posterior a la prueba:

Tabla 11. Prueba laboratorio – recuperación ante cambio de controladora - Verificación de secuencia de acciones en SNIFFER –Escenario A.

MENSAJES	DESCRIPCION
040053-1>CQ/1: <UI>: ### 0001	La ECR (040053-1) envía el código con el ID del que tiene el turno para conectarse
070803-1>040053-1/1: <<C>>:	El 070803-1 solicita conexión
040053-1>070803-1/1: <<UA>>:	ACK de conexión de la ECR
040053-1>070803-1/1: <<I00>>: conv	La ECR pasa a modo conv
070803-1>040053-1/1: <<rr1>>:	ACK de módem
040053-1>070803-1/1: <<I10>>: 08,150100	La ECR envía el mensaje de sincronía
070803-1>040053-1/1: <<rr2>>:	ACK de módem
040053-1>070803-1/1: <<I20>>: ### 0002	La ECR envía el código con el ID del que tiene el turno para conectarse
070803-1>040053-1/1: <<rr3>>:	ACK de módem
080130-1>040053-1/1: <<C>>:	Solicitud de conexión del 080130-1
040053-1>080130-1/1: <<UA>>:	ACK de conexión de la ECR
040053-1>070803-1/1: <<I30>>: conv	La ECR pasa a modo conv
070803-1>040053-1/1: <<rr4>>:	ACK de módem
040053-1>080130-1/1: <<I00>>:	La ECR envía el mensaje de sincronía

08,150124	
080130-1>040053-1/1: <<rr1>>: 040053-1>070803-1/1: <<I40>>: 01	ACK de módem La ECR envía el token al 803
070803-1>040053-1/1: <<rr5>>: 070803-1>040053-1/1: <<I05>>: 28	ACK de módem Mensaje de ACK del 803
040053-1>070803-1/1: <<rr1>>: 070803-1>040053-1/1: <<I15>>: 01	ACK de módem El 803 envía el token a la ECR
040053-1>070803-1/1: <<rr2>>:	ACK de módem (Aquí ocurre la caída de la ECR)
080130-1>040053-1/1: <<D>>: 070803-1>040053-1/1: <<D>>:	Desconexión del 130 de la ECR Desconexión del 803 de la ECR
070803-1>CQ/1: <UI>: ### 0100	La nueva ECR (070803-1) envía el código con el ID del que tiene el turno para conectarse
070803-1>CQ/1: <UI>: ### 0102	La nueva ECR envía el código con el ID del que tiene el turno para conectarse. Solicitud de conexión del 130
080130-1>070803-1/1: <<C>>: 070803-1>080130-1/1: <<UA>>:	ACK de conexión de la nueva ECR
070803-1>080130-1/1: <<I00>>: conv	La nueva ECR pasa a modo conv
080130-1>070803-1/1: <<rr1>>:	ACK de módem
070803-1>CQ/1: <UI>: 08,150441	La nueva ECR envía el mensaje de sincronía

7.3.4 Secuencia de acciones, para caso medio perturbado

- Escenario inicial: Escenario B.
- Instalar en los computadores el aplicativo de software para prueba de protocolo.
- Configurar tres de esos aplicativos como UPs.
- Configurar uno de los aplicativos como ECR.
- Las UPs intentan conectarse simultáneamente a la red presionando la opción “conectar” del aplicativo.
- La ECR envía mensajes con el identificador de cada UP, indicando el turno de conexión.
- A medida que cada UP identifica su turno, se conecta a la red, de acuerdo a la secuencia establecida en la tabla de unidades del sistema.
- Una vez se encuentre al menos una UP en la red, la ECR le enviará el token, para que pueda transmitir información. El orden en que la ECR envía el token dependerá de la secuencia de las UPs en la tabla de unidades del sistema.
- Las unidades de la tabla que no estén conectadas no recibirán el token, sino que les llegará un mensaje con su número de identificación, para su respectivo turno de conexión.
- Se genera intencionalmente un ruido en la red, que bloquea la recepción de todas las unidades, y se mantiene hasta que se termine la prueba.
- Después de un periodo de tiempo determinado (establecido en función del desempeño de la red) sin que las UPs reciban mensajes de token, las unidades se desconectan.
- A medida que transcurre el tiempo, la ECR original va desconectando a todas las unidades de la red al no poder comunicarse con ellas. Luego continúa enviando los códigos de identificación de manera secuencial de acuerdo con la Tabla de Unidades. Finalmente una vez que ha pasado un tiempo A, en el aplicativo de la ECR se desplegará una notificación de que el medio está posiblemente perturbado y se pedirá cambio a la siguiente frecuencia en la tabla.
- La unidad siguiente a la ECR en el orden de la tabla de identificación del sistema activa un temporizador para dar tiempo a que todas las unidades participantes terminen el proceso de desconexión de la ECR anterior. Una vez se cumple este tiempo, la UP asume su nuevo rol de ECR e inicia el envío de mensajes con los identificadores de cada unidad y espera que soliciten conexión.
- Una vez que ha pasado un tiempo A sin que ocurran conexiones ni transmisiones, en el aplicativo de la nueva ECR se desplegará una

notificación de que el medio está posiblemente perturbado y se pedirá cambio a la siguiente frecuencia en la tabla.

- El proceso de convertirse en ECR ocurre de manera secuencial para todas las UPs de la red de acuerdo con el orden especificado en la Tabla de Unidades, y para todas tras cumplirse el tiempo A sin que se presenten transmisiones se despliega en el aplicativo la notificación de medio perturbado.

Verificación de resultado escenario B

El resultado deberá ser:

a) Computadores con aplicativo instalado y corriendo correctamente.
b) Se verifica en el aplicativo un mensaje indicando la perturbación del medio y las acciones de recuperación a implementar.

7.3.4.1 Resultados Obtenidos en pruebas de laboratorio – recuperación ante medio perturbado

- ***Prueba escenario B* - Resultados generales.**

Tabla 12. Resultados de la prueba de medio perturbado– escenario B

ACCIÓN	DESCRIPCIÓN	ANOTACIONES	RESULTADO
a)	Equipos encendidos, aplicativos corriendo y configurados.	Aplicativos configurados así: - 040053-1 (ECR) - 070803-1 (UP) - 080130-1 (UP) Las UPs oprimen el botón presentado a continuación:  Para verificación de esta funcionalidad no es necesario oprimir ningún botón. Es automático el proceso.	Ok
b)	Verificar medio perturbado y acciones a seguir para restablecer el sistema	En la barra de estado del aplicativo se despliegan mensajes indicando perturbación de medio y acciones a seguir, tanto en la ECR como en la UP, tal como se presenta en las Figuras 25 y 26 .	Ok

- **Resultados detallados.**

a) La configuración de las unidades, respecto a su Rol en la red (ECR o UP), se establecen en la tabla de secuencia. La configuración para esta prueba se presenta a continuación:

Figura 36. Pruebas laboratorio – recuperación ante medio perturbado - Tabla de secuencia configurada para prueba – escenario B.

b) En la ventana principal del aplicativo, en la barra de estado, se despliega la información correspondiente a esta prueba.

Figura 37. Pruebas laboratorio – recuperación ante medio perturbado - Notificación de medio perturbado en la ECR – escenario B.

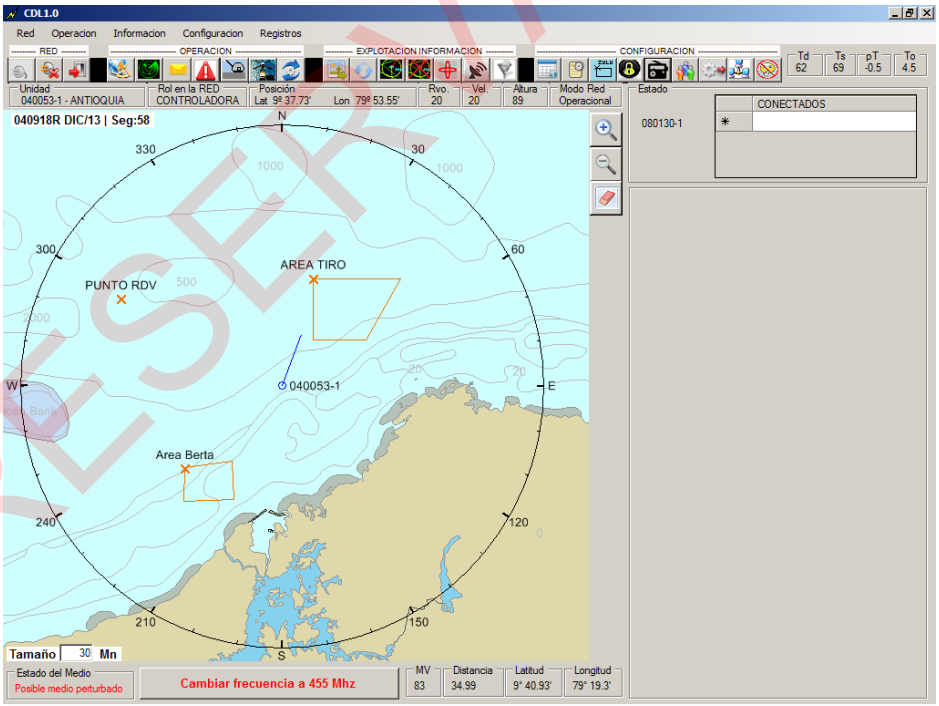
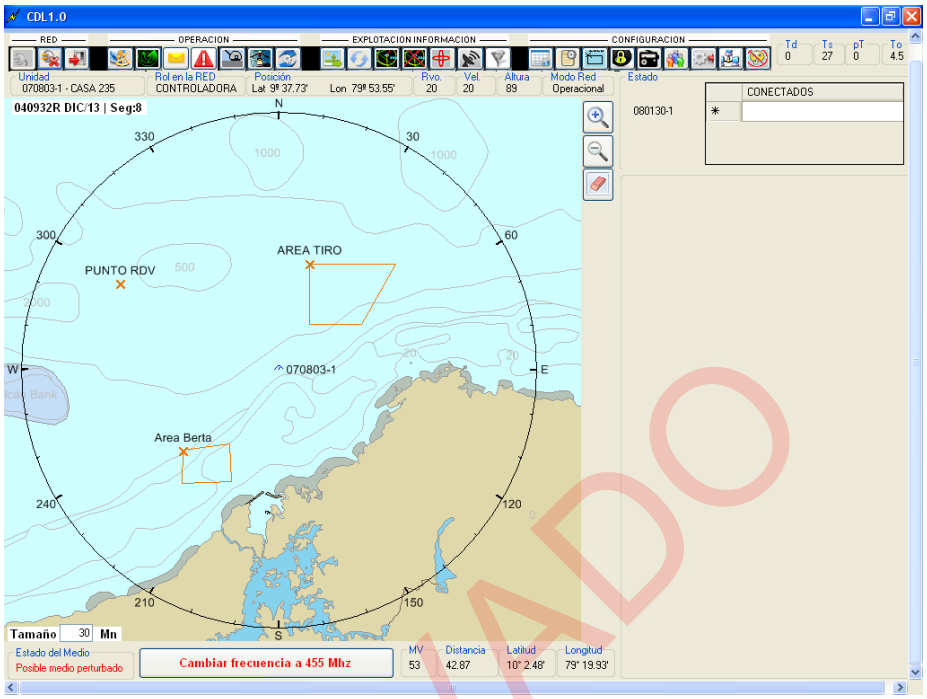


Figura 38. Pruebas laboratorio – recuperación ante medio perturbado - Notificación de medio perturbado en la UP1 – escenario B.



7.4 RESUMEN DE PRUEBAS Y RESULTADOS

A continuación se presenta el resumen de los resultados obtenidos a partir de las pruebas efectuadas en laboratorio.

Tabla 13. Resumen general de pruebas y resultados

Número de prueba	Nombre de prueba	Cantidad de repeticiones	Escenarios	Resultados
7.4.1	Recuperación del sistema ante pérdida de token	50	A	Satisfactorio
7.4.2	Recuperación del sistema ante pérdida de ACK – Caída UP	50	A	Satisfactorio
7.4.3	Recuperación del sistema ante cambio de controladora	50	A	Satisfactorio
7.4.4	Recuperación del sistema ante medio perturbado	50	B	Satisfactorio

Tabla 14. Resumen numérico de pruebas y resultados

Número de prueba	Nombre de prueba	Cantidad de repeticiones	Escenarios	Tiempo Promedio
7.4.1	Recuperación del sistema ante pérdida de token	50	A	30seg
7.4.2	Recuperación del sistema ante pérdida de ACK – caída UP	50	A	18seg
7.4.3	Recuperación del sistema ante cambio de controladora	50	A	149seg
7.4.4	Recuperación del sistema ante medio perturbado	50	B	212seg

CAPÍTULO VIII. DISCUSIÓN DE RESULTADOS

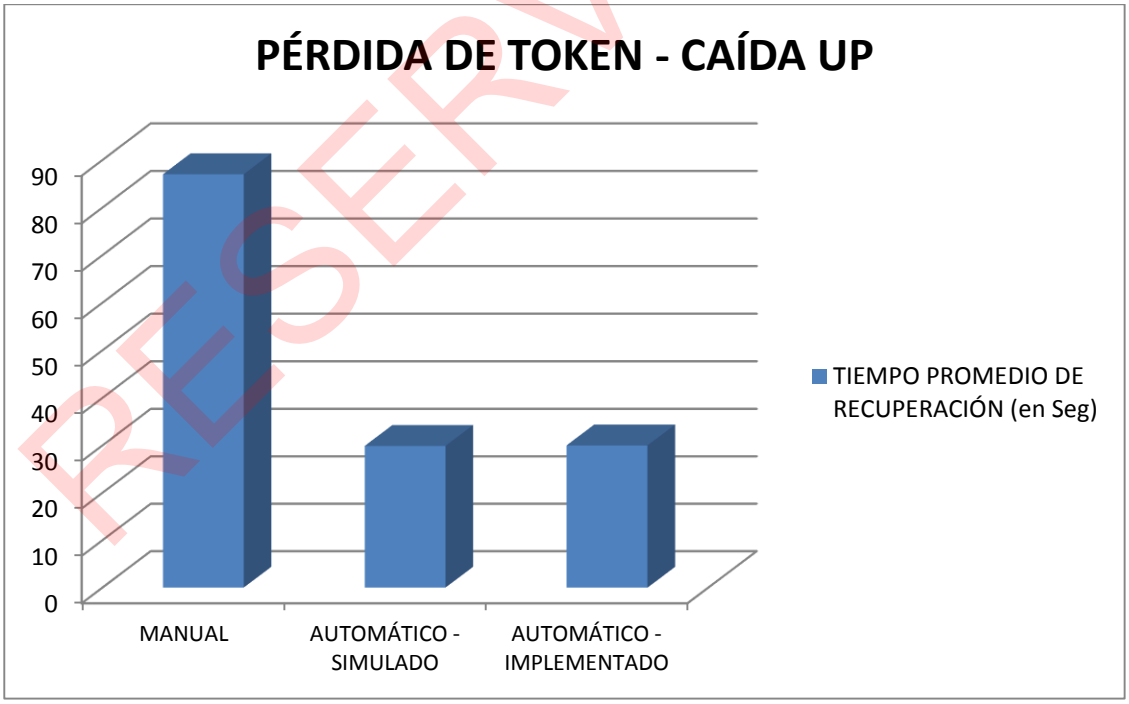
El objetivo de esta sección del documento es presentar el análisis obtenido a partir de la comparación de los resultados experimentales obtenidos Vs. los obtenidos a partir de simulaciones y los obtenidos a partir de implementación de recuperación manual del sistema.

Se muestra numéricamente en cuánto fue posible disminuir los tiempos de recuperación del sistema para cada tipo de fallo y el consiguiente incremento en la fiabilidad del sistema bajo estudio.

8.1 COMPARACIÓN DE RESULTADOS

Las figuras 39 a 42 muestran los resultados obtenidos a partir de la medición del tiempo de recuperación para las condiciones: recuperación manual, recuperación automática simulada y recuperación automática implementada, para cada uno de los fallos identificados.

Figura 39. Comparación resultados obtenidos para fallo: pérdida de token – caída UP

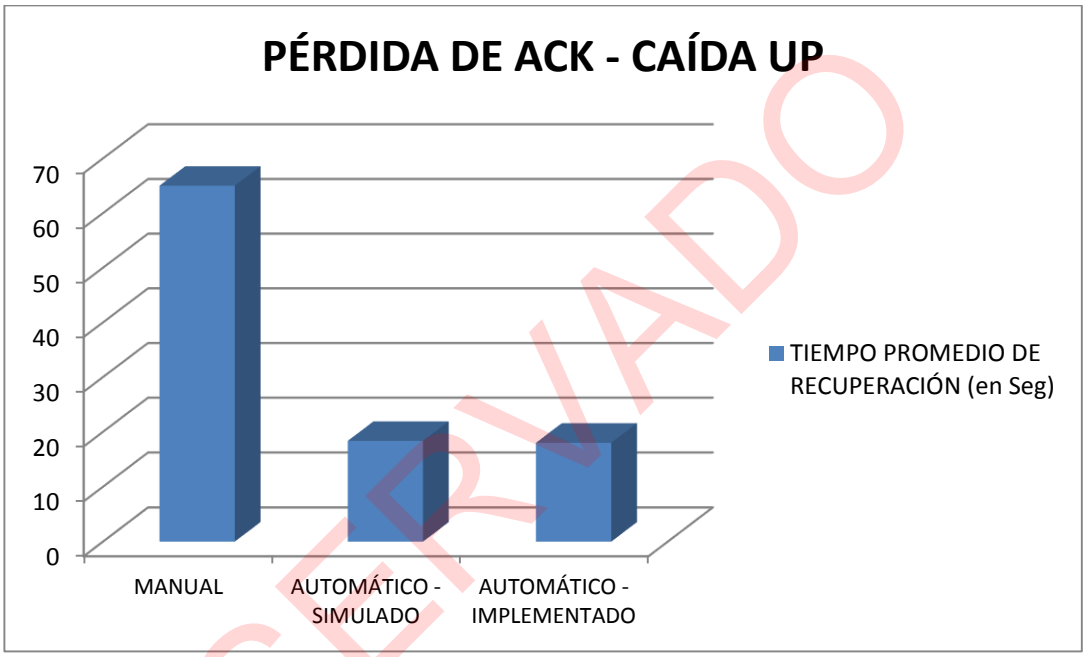


La figura 39 permite evidenciar los siguientes valores promedio de recuperación:

MANUAL	AUTOMÁTICO - SIMULADO	AUTOMÁTICO – IMPLEMENTADO
87seg	29.9seg	30seg

- Para el caso de falla: Caída UP con pérdida de token, se evidencia una reducción promedio del tiempo de recuperación de la falla en un 65%, comparando los valores de tiempo de recuperación manual Vs. recuperación automática implementada.
- Entre los valores de tiempo de recuperación automática simulada Vs. recuperación automática simulada, se obtuvo una diferencia del 0.4%.

Figura 40. Comparación resultados obtenidos para fallo: pérdida de token ACK – caída UP

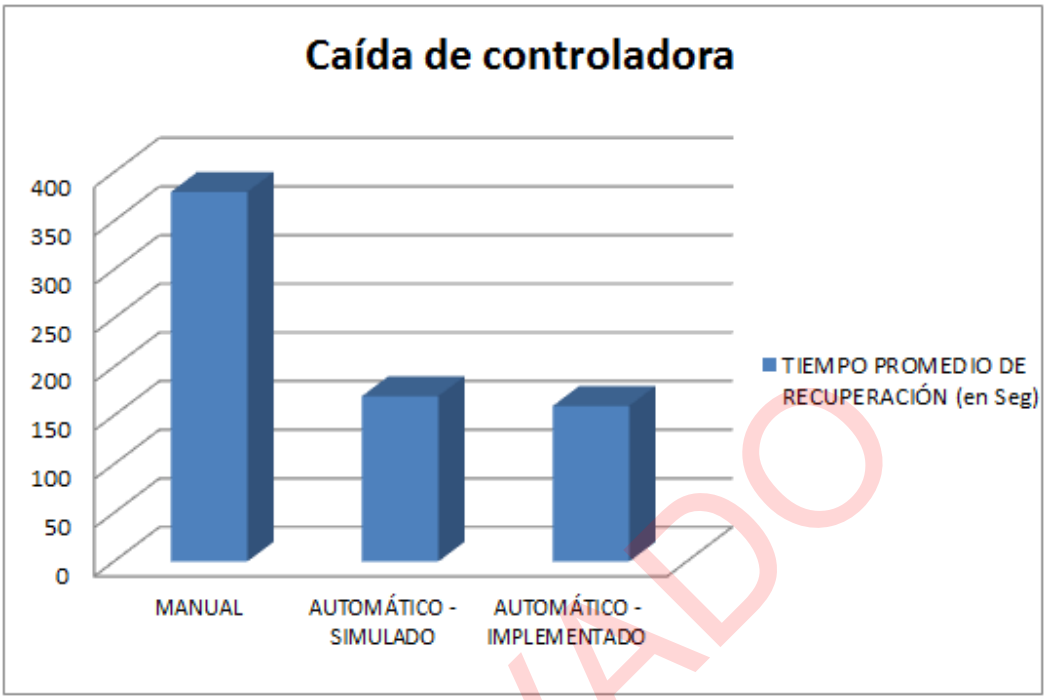


La figura 40 permite evidenciar los siguientes valores promedio de recuperación:

MANUAL	AUTOMÁTICO - SIMULADO	AUTOMÁTICO – IMPLEMENTADO
65seg	18.34seg	18seg

- Para el caso de falla: Caída UP con pérdida de ACK, se evidencia una reducción promedio del tiempo de recuperación de la falla en un 72%, comparando los valores de tiempo de recuperación manual Vs. recuperación automática implementada.
- Entre los valores de tiempo de recuperación automática simulada Vs. recuperación automática simulada, se obtuvo una diferencia del 1.9%.

Figura 41. Comparación resultados obtenidos para fallo: Caída de controladora

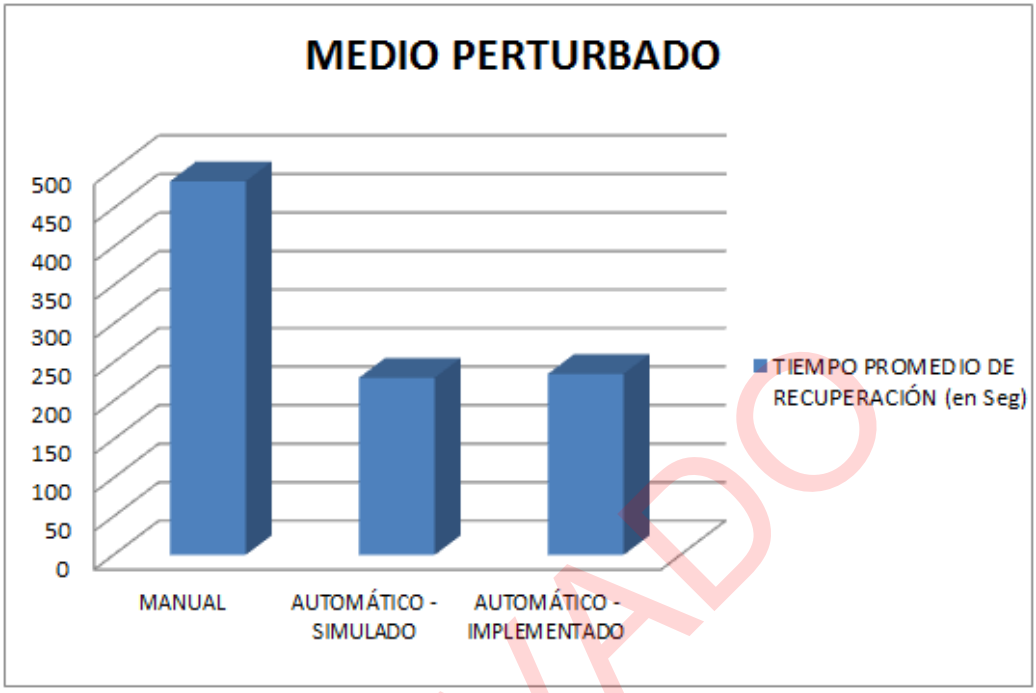


La figura 41 permite evidenciar los siguientes valores promedio de recuperación:

MANUAL	AUTOMÁTICO - SIMULADO	AUTOMÁTICO – IMPLEMENTADO
354seg	150.4seg	149seg

- Para el caso de falla: Caída de controladora, se evidencia una reducción promedio del tiempo de recuperación de la falla en un 57%, comparando los valores de tiempo de recuperación manual Vs. recuperación automática implementada.
- Entre los valores de tiempo de recuperación automática simulada Vs. recuperación automática simulada, se obtuvo una diferencia del 0.9%.

Figura 42. Comparación resultados obtenidos para fallo: Medio perturbado



La figura 42 permite evidenciar los siguientes valores promedio de recuperación:

MANUAL	AUTOMÁTICO - SIMULADO	AUTOMÁTICO – IMPLEMENTADO
458seg	210.14seg	212seg

- Para el caso de falla: medio perturbado, se evidencia una reducción promedio del tiempo de recuperación de la falla en un 53%, comparando los valores de tiempo de recuperación manual Vs. recuperación automática implementada.
- Entre los valores de tiempo de recuperación automática simulada Vs. recuperación automática simulada, se obtuvo una diferencia del 0.8%.

La tabla 15 contiene el resumen de los resultados presentados anteriormente, incluyendo nivel de reducción del tiempo de recuperación (en porcentaje) entre la recuperación manual y la recuperación automática implementada.

Tabla 15. Comparación tiempo promedio de recuperación por fallo

FALLO	TIEMPO PROMEDIO DE RECUPERACIÓN			REDUCCIÓN EN TIEMPO (%)
	MANUAL	AUTOMÁTICO - SIMULADO	AUTOMÁTICO - IMPLEMENTADO	
Pérdida de token - Caída UP	87seg	29.9seg	30seg	65%
Pérdida de ACK – Caída UP	65seg	18.34seg	18seg	72%
Caída de controladora	354seg	150.4seg	149seg	57%
Medio perturbado	458seg	210.14seg	212seg	53%

En términos generales, a partir de los resultados expuestos en la Tabla 15, es posible evidenciar que:

- La reducción promedio del tiempo de recuperación de las fallas detectadas en el sistema es del 61.75%, siendo el fallo "pérdida de ACK – caída de UP", el fallo para el cual se logró mayor reducción en tiempo en un 72% y "medio perturbado" el de menor reducción, con un 53%.

- La diferencia obtenida entre los valores simulados e implementados, no supera el 2% en ninguno de los casos, siendo su valor promedio 1.02%. esto indica que el modelo de simulación (con el nivel de abstracción al que fue elaborado) corresponde en un 98.98% a lo que sucede en la realidad. Este resultado fue posible obtenerlo, gracias a que se tuvieron en cuenta datos medidos (reales) del sistema, durante la elaboración del modelo de simulación.

8.2 FIABILIDAD DEL SISTEMA

De acuerdo a lo especificado en el *Applied R&M Manual for Defence Systems Part D - Supporting Theory, sección 2.6 (página 3)*[2], la fiabilidad de un sistema no tiene una única forma o criterio de medición, pero si puede ser comparable a la disponibilidad del mismo.

Los autores del artículo *Measuring Software Reliaility in Practice: An Industrial Case Study*[3], en su sección 2.3 "*Measurement and tracking practices*", soportan esta afirmación al indicar que "tres (03) parámetros pueden direccionar las

[2] Documento consultado en línea, disponible en: http://www.sars.org.uk/old-site-archive/BOK/Applied%20R&M%20Manual%20for%20Defence%20Systems%20(GR-77)/p4c06.pdf
[3] Tomado de base de datos del IEEE. Elaborado por funcionarios de Alcatel-Lucent – IP Division.

mediciones de disponibilidad/fiabilidad de los servicios: la rata de fallas (Tiempo medio para fallar - MTTF), Cobertura de la falla (para el caso de componentes de hardware – probabilidad de detectar y corregir la falla a nivel hardware) y el tiempo medio de recuperación - MTTR".(Benlarbi y Storte, 2007)

Tal como se definió en la sección 2.1.3 de este documento, la fiabilidad (reliability) de un sistema es la medida de su conformidad con la especificación para la cual fue diseñado. Teniendo en cuenta esto, y las afirmaciones citadas previamente, es posible afirmar que en la medida que un sistema se encuentre operativo y en un estado "normal", su fiabilidad será mayor, ya que cumple con la especificación para la cual fue diseñado, por lo que reducir el tiempo de recuperación ante fallas, permite incrementar el tiempo de operación normal del sistema, contribuyendo a su vez a mejorar su fiabilidad.

Generalmente, de forma simplificada, la fiabilidad de un sistema puede medirse por el Tiempo medio entre fallos MTBF o MTTR, como lo indican compañías como EventHelix[4] y Vinci Consulting[5] quienes emplean medidas de disponibilidad del sistema, para referirse a la fiabilidad del mismo.

Una forma intuitiva de medir la fiabilidad/disponibilidad del sistema es midiendo el tiempo que éste permanece fuera de servicio.

Durante la fase inicial de pruebas del sistema Data Link, se empleó la perspectiva de la compañía EventHelix para determinar la fiabilidad del mismo (cuando la recuperación ante eventos de fallo eran manuales). Con miras a mantener la misma referencia de medición y hacer comparaciones válidas, también se usa la tabla 16 que contiene valores empleados por dicha empresa para medir fiabilidad/disponibilidad del sistema Data Link, incorporando los mecanismos de recuperación automática ante fallos.

Con miras a verificar la validez de la información proporcionada por EventHelix, se comparan los datos presentados en la Tabla 16, con los suministrados por IBM, para el mismo tipo de medición. La tabla 17 contiene la matriz de disponibilidad/fiabilidad proporcionada por IBM[6] en su RedBook "*IBM High Availability Solution for IBM FileNet P8 System*".

[4]Artículo consultado en línea, disponible en: http://www.eventhelix.com/realtimemantra/faulthandling/system_reliability_availability.htm#.VOiMnPmG9e8

[5] Artículo consultado en línea, disponible en: http://vinciconsulting.com/blog/-/blogs/%E2%80%9Cthe-table-of-nines%E2%80%9D-and-high-availability

[6] IBM. High Availability Solution for IBM FileNet P8 System. Libro consultado en linea. Disponible en: http://www.redbooks.ibm.com/redbooks/pdfs/sg247700.pdf

Tabla 16. Fiabilidad/disponibilidad de un sistema según el tiempo fuera de línea del sistema.

Availability/Reliability	Downtime
90% (1-nine)	36.5 days/year
99% (2-nines)	3.65 days/year
99.9% (3-nines)	8.76 hours/year
99.99% (4-nines)	52 minutes/year
99.999% (5-nines)	5 minutes/year
99.9999% (6-nines)	31 seconds/year

Fuente: EventHelix.
http://www.eventhelix.com/realtimemantra/faulthandling/reliability_availability_basics.htm#.VOiORPmG9e8

Tabla 17. Fiabilidad/disponibilidad de un sistema según IBM.

Availability/Reliability	Downtime per year
90% (1-nine)	36 days/year
99% (2-nines)	3.6 days/year
99.9% (3-nines)	8.8 hours/year
99.99% (4-nines)	53 minutes/year
99.999% (5-nines)	5 minutes/year
99.9999% (6-nines)	32 seconds/year

Fuente: RedBook "IBM High Availability Solution for IBM FileNet P8 Systems.
http://www.redbooks.ibm.com/redbooks/pdfs/sg247700.pdf

La información anterior permite corroborar que la empresa EventHelix emplea información válida para efectuar sus mediciones, al no presentar variaciones superiores al 3%, con respecto a la información proporcionada por IBM.

Habiendo validado la información de referencia, para el experimento puntual de medición de fiabilidad del sistema bajo estudio, se consideraron periodos continuos de evaluación durante tres (03) meses (equivalentes a 2160 horas).

La tabla 18 contiene la información de conversión empleada para periodos inferiores a un año, equivalente a los datos contenidos en las Tablas 16 y 17.

Tabla 18. Fiabilidad/disponibilidad de un sistema – equivalencia tiempos fuera de línea del sistema.

	Downtime			
Availability/Reliability	**Year**	**Month**	**Week**	**Day**
90% (1-nine)	36.5 days	3 days	16.8 hours	2.4 hours
99% (2-nines)	3.65 days	7.2 hours	1.68 hours	14.4 mins
99.9% (3-nines)	8.76 hours	43.2mins	10.08 mins	1.44 mins
99.99% (4-nines)	52 mins	4.33 mins	60.48 sec	8.64 sec
99.999% (5-nines)	5 mins	25.9 sec	6.04 sec	864 ms
99.9999% (6-nines)	31 sec	2.59 sec	604.8 ms	86.4 ms

Con la información recolectada durante los tres (03) meses de prueba del sistema, se elaboró la tabla 19, que contiene el resumen de los valores de "tiempo fuera de línea" medidos. Estos valores corresponden al promedio obtenido durante el periodo de prueba.

Las mediciones efectuadas corresponden a dos condiciones: modo recuperación manual (datos tomados entre junio – septiembre de 2012) y modo recuperación

automática implementado (datos tomados entre Octubre de 2014 – Enero de 2015).

Tabla 19. Fiabilidad/disponibilidad del sistema bajo estudio.

Condiciones	Tiempo fuera de línea	Fiabilidad/disponibilidad
Recuperación manual	260500 segundos/mes = 72.36 horas/mes = 3 días/mes	90%
Recuperación automática implementada	26118 segundos/mes = 7.25 horas/mes	99%

Los resultados presentados en la tabla 19 permiten evidenciar que:

- La reducción promedio del tiempo de recuperación de las fallas detectadas en el sistema en un 61.75%, representa un incremento del 9% en la disponibilidad del sistema Data Link bajo estudio, pasando de ser 90% a ser 99%.

CAPÍTULO IX. CONCLUSIONES Y RECOMENDACIONES

Después de efectuar el proceso de análisis del sistema, así como el diseño e implementación del mecanismo de recuperación automática ante fallas descrito en este documento, se concluye que:

1. El sistema Data Link bajo estudio se caracteriza por ser, más que una herramienta para la gestión y control de armas, un mecanismo para el apoyo a la toma de decisiones, durante el proceso de mando y control de las operaciones. Como componente operacional fundamental, se encontró que el sistema fue diseñado para satisfacer los requerimientos funcionales y atributos de calidad establecidos por la ARC, teniendo en cuenta el entorno operacional de países latinoamericanos y sus restricciones presupuestales. A nivel técnico, el sistema se caracteriza por tener un mecanismo de control de acceso al medio por poleo, en el cual una unidad (gracias a sus capacidades operacionales en materia de sensores, armas, personal, etc.) ejerce el rol de gestión y control de la red. Como mecanismo para prevenir interceptaciones o robo de la información, el sistema incorpora un componente criptográfico basado en AES[7]. Su protocolo (mensajería y formato de mensajes intercambiados) es propietario de COTECMAR-ARC y fue diseñado para optimizar el ancho de banda disponible en la actual infraestructura de comunicaciones de la ARC. En materia de hardware, el sistema cuenta con una caja integradora de comunicaciones, basada en componentes COTS, que incluye un modem para modulación en FSK de la señal de información.

2. En general, fueron detectadas cuatro (04) tipos de fallas en el sistema bajo estudio. El 50% de las fallas detectadas se deben a pérdidas del Token[8], bien sea porque la ECR o UC perdió conexión o porque una UP salió de la red mientras tenía el Token. El otro 50% de las fallas se distribuye así: 25% debidas a desconexiones de UP y 25% debidas a factores externos (técnicas de guerra electrónica).

3. El 75% de las fallas detectadas en el sistema, son el resultado de estados muertos en el sistema, mientras que el 25% restante, son debidas a factores externos. En el entorno operacional naval, la radiación directa de energía es

[7] *Advanced Encryption Standard.* Esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.
[8] Mensaje que garantiza el flujo de información en el sistema.

la técnica de guerra electrónica (factor externo – del entorno operacional) más comúnmente empleada[9].

4. El modelo de simulación elaborado, describe en un 98.98% las interacciones que realmente se presentan en el sistema bajo estudio.

5. Con la implementación del sistema, se verifica que:

   - Al comparar los datos obtenidos a partir de las pruebas efectuadas sobre el sistema para el caso de recuperación manual Vs. los datos obtenidos a partir de las pruebas efectuadas sobre el sistema para el caso de recuperación automática, se evidenció una reducción del 61.75% en el tiempo promedio de recuperación de las fallas detectadas en el sistema, permitiendo que se pasara de un tiempo de recuperación promedio de 241 segundos a 102.25 segundos.

   - Se logró incrementar la fiabilidad del sistema data link bajo estudio en un 9%. La reducción del 61.75% en el tiempo promedio de recuperación ante fallas, permitió que la fiabilidad del sistema pasara de ser 90% (equivalente a 72.35 horas/mes en las que el sistema estuvo fuera de línea) a ser 99% (equivalente a 7.25 horas/mes en las que el sistema estuvo fuera de línea).

   - La intervención humana/manual en el proceso de recuperación del sistema, incrementa los tiempos de recuperación entre un 53% - 72% y por consiguiente, reduce la fiabilidad del sistema. Siendo el peor caso “caída UP – Pérdida de ACK”, donde el tiempo pasa de ser 18 segundos a ser 65 segundos.

Finalmente, se recomienda efectuar trabajos futuros asociados al análisis a fondo del modo de operación “silencio” del sistema, con el fin de analizar si los mecanismos desarrollados en este trabajo, para el modo de operación “normal”, son igualmente funcionales.

[9] De acuerdo a la información suministrada por oficiales de la ARC.

REFERENCIAS

ALMEIDA, J.P.A.; M. Wegdam; M. van Sinderen; y L. Nieuwenhuis. Transparent dynamic reconfiguration for corba. En Proceedings of the 3rd International Symposium on Distributed Objects and Applications, páginas 197–207. IEEE Computer Society, 2001.

ARSHAD, N.. A planning-based Approach to Failure Recovery in Distributed Systems. [En Línea]. Disponible en: http://www.doc.ic.ac.uk/~alw/edu/theses/arshad-phd-0506.pdf. Páginas 32 -65. 2006.

ASENSTORFER, J.; T. COX y D. WILKSCH (2004). Tactical Data Link Systems and the Australian Defence Force (ADF), Technology Developments and Interoperability Issues. Edinburgh: DSTO Information Sciences Laboratory.

BENAVIDES, J. y J. MONTAÑEZ (2008). Diseño e implementación de un sistema de multienlace de datos para control y toma de decisiones en redes operativas. Tesis, Escuela Naval de Cadetes Almirante Padilla, Cartagena.

BERGHOFF, J.; Oswald Drobnik, Anselm Lingnau, y Christian Monch. Agent-based configuration management of distributed applications. En Proceedings of Third International Conference on Configurable Distributed Systems, 1996, páginas 52–59. IEEE Computer Society, 1996.

BROWN, A. y Patterson, D. To err is human, 2001.

CHEN, X. y Martin Simons. A component framework for dynamic reconfiguration of distributed systems. En Proceedings of the IFIP/ACM Working Conference on Component Deployment, páginas 82–96. Springer-Verlag, 2002.

CPT/CIA (2008, agosto). Introducción a Link 16. Curso Link 16.

CPT/CIA (2008, agosto). Sumario de Data Link. Curso Link 16 .

FEILER, P. y Jun Li. Consistency in dynamic reconfiguration. En Proceedings of the Fourth International Conference on Configurable Distributed Systems, páginas 189–196, 1998.

JOINT STAFF (2002). Joint Multi-Tactical Data Link (TDL) Operating Procedures. Washington.

JOINT-STAFF (2001). Tactical Data Link Standarization Implementation Plan. Washington.

KAISER, G.; Phil Gross; Gaurav Kc; Janak Parekh; y Giuseppe Valetto. An approach to autonomizing legacy systems, in workshop on self-healing, adaptive

and self-managed systems. In Workshop on Self-Healing, Adaptive and Self-MANaged Systems, June 2002.

KEPHART J. y David M. Chess. The vision of autonomic computing. Computer, 36(1):41–50, 2003.

KRAMER, J. y J. Magee. The evolving philosophers problem: Dynamic change management. IEEE Transactions on Software Engineering, 16(11):1293–1306, nov 1990.

MINGES, M. (2001, junio). Survey of Current Air Force Tactical Data Links and Policy [en línea], disponible en www.afceaeriecanal.org/AFRL.Minges.ppt, recuperado en abril de 2009.

NORTHROP-GRUMMAN (2002). NATO Improved Link 11 NILE [en línea], disponible en http://www.ms.northropgrumman.com/solutions/data_link_processing/data_link_processing.html, recuperado en mayo de 2009.

PARK, J. y Pratheep Chandramohan. Static vs. dynamic recovery models for survivable distributed systems. In HICSS, 2004.

PUBLISHING-INTEGRATED (2007). Fire Controlman, vol. 6, Digital Communications. [en línea], disponible en http://www.tpub.com/content/fc/14103/index.htm, recuperado en abril de 2009.

SOULES, C.; J. Appavoo; K. Hui; D. Silva; G. Ganger; O. Krieger; M. Stumm; R. Wisniewski; M. Auslander; M. Ostrowski; B. Rosenburg; y J. Xenidis. System support for online reconfiguration, 2003.

TICHY, M.; Giese, H.; Schilling, D. y Pauls, W.. Computing optimal self-repair actions: damage minimization versus repair time. En WADS ’05: Proceedings of the 2005 workshop on Architecting dependable systems, páginas 7–6, New York, NY, USA, 2005.

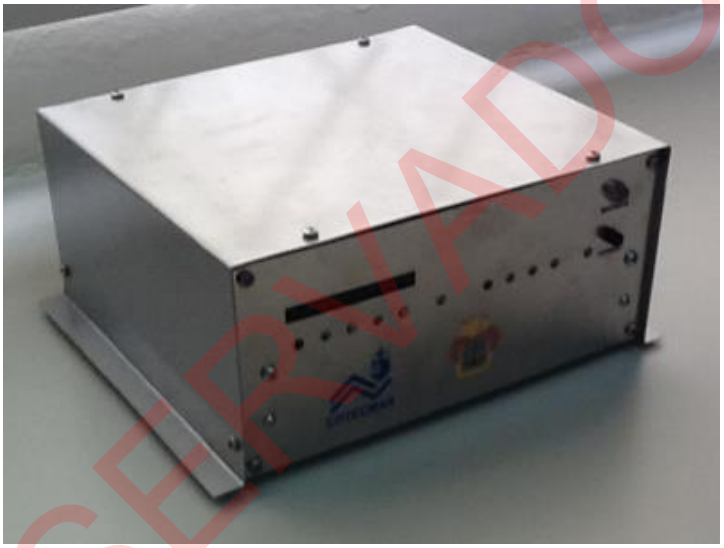
TORRES, W. Software fault tolerance: A tutorial. Technical report, 2000.

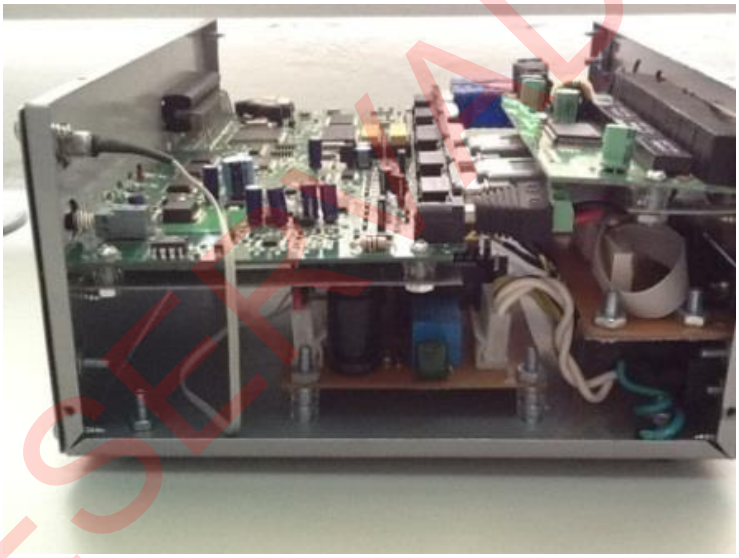
VALETTO, G.; Gail E. Kaiser; y Gaurav S. Kc. A mobile agent approach to process-based dynamic adaptation of complex software systems. En Proceedings of the 8th European Workshop on Software Process Technology, páginas 102–116. Springer- Verlag, 2001.

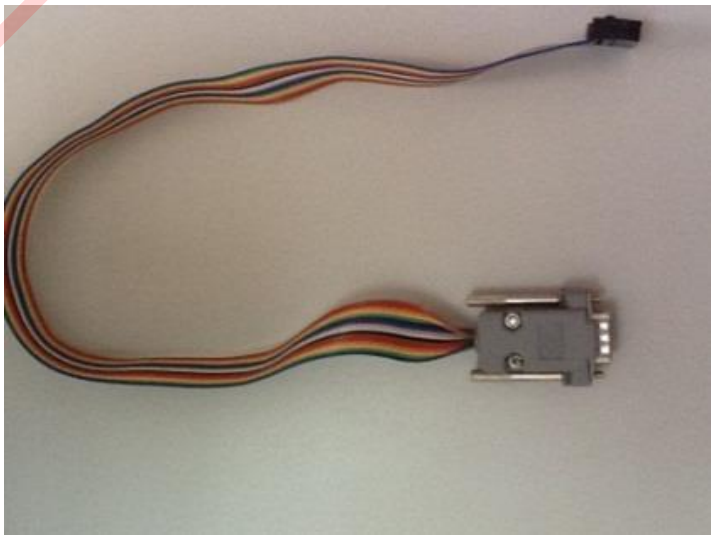
ANEXOS

Anexo 1.

Registro fotográfico - Caja integradora de comunicaciones







Anexo 2.

Resultados simulaciones – Tiempos de recuperación medidos en cada experimento.

Tiempo de recuperación simulado (en segundos)

	Pérdida de token (opción 0)	Pérdida ACK (Opción 1)	Caída ECR (Opción 2)	Medio perturbado (Opción 3)
1	30	17	145	209
2	28	17	150	209
3	28	18	150	209
4	29	18	150	209
5	28	18	150	210
6	31	18	150	210
7	32	18	149	218
8	32	19	149	209
9	30	17	151	210
10	30	17	152	210
11	30	17	150	210
12	28	18	150	208
13	29	18	150	211
14	29	18	149	212
15	29	18	150	210
16	25	18	153	209
17	36	18	154	208
18	33	20	149	206
19	37	18	150	211
20	32	19	150	212
21	30	20	150	210
22	30	21	150	209
23	29	20	149	208
24	28	21	150	209
25	28	18	153	210
26	27	18	154	210
27	27	19	149	210
28	30	17	150	208
29	30	16	150	211
30	38	17	150	212
31	26	17	150	209
32	29	18	152	209
33	25	18	150	210
34	33	18	150	210
35	33	19	150	209
36	37	19	149	210
37	32	19	150	210
38	30	18	149	210
39	30	17	150	208

40	29	20	153	215
41	30	20	154	212
42	30	21	149	209
43	27	18	150	210
44	27	16	150	208
45	30	17	150	211
46	29	17	150	212
47	28	18	149	212
48	31	18	150	212
49	32	18	150	215
50	32	19	149	209
51	30	19	150	210
52	30	19	153	210
53	30	18	154	208
54	27	17	149	213
55	28	20	150	215
56	30	20	152	210
57	30	21	153	210
58	35	18	152	209
59	26	19	152	209
60	29	18	150	210
61	28	17	150	208
62	26	20	149	211
63	29	18	150	212
64	29	18	150	210
65	28	18	149	209
66	35	19	150	208
67	33	19	153	209
68	32	19	154	211
69	32	18	149	212
70	31	17	150	214
71	30	21	152	209
72	30	18	153	208
73	30	19	152	212
74	34	18	149	215
75	28	17	150	209
76	28	20	150	210
77	29	18	149	210
78	27	18	150	208
79	30	18	153	209
80	30	18	150	209

81	30	17	150	210
82	30	21	152	210
83	28	18	150	215
84	29	19	150	209
85	25	18	150	210
86	25	18	149	210
87	27	19	150	210
88	30	18	149	208
89	30	17	150	209
90	35	20	153	208
91	34	18	154	209
92	33	18	150	211
93	33	18	149	212
94	30	18	148	210
95	29	18	149	210
96	28	18	150	209
97	26	18	150	211
98	30	19	150	210
99	30	18	150	209
100	30	18	150	210

Anexo 3.

Equipos de cómputo – características técnicas.

DELL™ LATITUDE™ ESTÁNDAR E6400 Y E6500

CARACTERÍSTICAS	E6400	E6500
Sistema operativo	Windows Vista® Ultimate original Windows Vista® Business original Windows Vista® Business de 64 bits original Windows Vista® Home Basic original Desactualización de Windows Vista® Ultimate o Business originales Windows® XP Professional original cargado[4]	Windows Vista® Ultimate original Windows Vista® Business original Windows Vista® Business de 64 bits original Windows Vista® Home Basic original Desactualización de Windows Vista® Ultimate o Business originales Windows® XP Professional original cargado[4]
Tipo de procesadores	Procesador Intel® Core™ 2 Duo hasta T9600 (2,8 GHz, caché L2 de 6 MB)	Procesador Intel® Core™ 2 Duo hasta T9600 (2,8 GHz, caché L2 de 6 MB)
Chipset	Chipset Intel® 45 Express	Chipset Intel® 45 Express
Gráficos[5]	DDR2 de 256 MB NVIDIA® Quadro® NVS 160M1 Intel® GMA 4500MHD	DDR3 de 256 MB NVIDIA® Quadro® NVS 160M1 Intel® GMA 4500MHD
Pantalla	Pantalla ancha LED WXGA+ (1440 x 900) UltraSharp™ de 14,1" Pantalla ancha WXGA (1280 x 800) con retroiluminación LED. de 14,1", Energy Star Capable.	Pantalla ancha WUXGA (1920 x 1200) UltraSharp™ de 15,4" con ángulo de visión amplio Pantalla ancha LED WXGA+ (1440 x 900) de 15,4" con ángulo de visión amplio Pantalla ancha WXGA (1280 x 800) con retroiluminación LED. de 15,4" Energy Star Capable.
Memoria[5]	Memoria DDR2 de dos canales Dos ranuras de memoria que ofrecen hasta 8 GB[6] Ancho de banda de la memoria: 800 MHz	Memoria DDR3 de dos canales Dos ranuras de memoria que ofrecen hasta 8 GB[6] Ancho de banda de la memoria: 800 MHz
Batería	Batería principal "inteligente" de ion de litio de 4 (duración de 3Hrs) 6 ó 9 celdas con ExpressCharge™; batería secundaria de alta capacidad de 12 celdas	Batería principal "inteligente" de iones de litio de 4 (duración de 3Hrs), 6 ó 9 celdas con ExpressCharge; batería secundaria de alta capacidad de 12 celdas
Fuente de alimentación	Adaptador de CA de 90 vatios con envoltura de cables, adaptador de CA de 65 vatios para automóvil o avión	Adaptador de CA de 90 vatios con envoltura de cables, adaptador de CA de 65 vatios para automóvil o avión
Almacenamiento principal[7]	Disco duro de estado sólido de hasta 64 GB Disco duro de 7200 RPM con sensor de caída libre de hasta 250 GB Disco duro cifrado de 5400 RPM de hasta 120 GB[9] 5400 RPM hasta 250 GB[6]	Disco duro de estado sólido de hasta 64 GB Disco duro de 7200 RPM con sensor de caída libre de hasta 250 GB Disco duro cifrado de 5400 RPM de hasta 120 GB[9] 5400 RPM hasta 250 GB[6]
Opciones de conectividad	Ethernet Gigabit 10/100/1000 Módem interno 56K v924 (opcional) **LAN inalámbrica:** soluciones inalámbricas Dell Wireless 1397 (802.11g) y Dell Wireless 1510 (802.11 a/g/n 2x2), Intel® WiFi Link 5100 [802.11a/g/n (1x2)]; Intel WiFi Link 5300 [802.11a/g/n (3x3)] **Banda ancha móvil[2] y GPS:** Mini Card de banda ancha móvil de la solución inalámbrica Dell Wireless 5720 (EvDO y GPS), Mini Card de la solución inalámbrica Dell Wireless 5530 (HSDPA 7.2/HSUPA 2.0 de tres bandas y GPS) **Bluetooth y banda ultra ancha:** Dell Wireless 370 Bluetooth® 2.1, Dell Wireless 410 Bluetooth® 2.1 con UWB	Ethernet Gigabit 10/100/1000 Módem interno 56K v924 (opcional) **LAN inalámbrica:** soluciones inalámbricas Dell Wireless 1397 (802.11g) y Dell Wireless 1510 (802.11 a/g/n 2x2), Intel® WiFi Link 5100 [802.11a/g/n (1x2)]; Intel WiFi Link 5300 [802.11a/g/n (3x3)] **Banda ancha móvil[2] y GPS:** Mini Card de banda ancha móvil de la solución inalámbrica Dell Wireless 5720 (EvDO y GPS), Mini Card de la solución inalámbrica Dell Wireless 5530 (HSDPA 7.2/HSUPA 2.0 de tres bandas y GPS) **Bluetooth y banda ultra ancha:** Dell Wireless 370 Bluetooth® 2.1, Dell Wireless 410 Bluetooth® 2.1 con UWB
Seguridad	Lector de tarjetas inteligentes y lector de tarjetas inteligentes sin contacto, lector de huellas digitales opcional, administrador de seguridad Dell ControlPoint, Dell ControlVault™, filtro de privacidad opcional, TPM 1.2[9]	Lector de tarjetas inteligentes y lector de tarjetas inteligentes sin contacto, lector de huellas digitales o lector de huellas digitales FIP opcional, administrador de seguridad Dell ControlPoint, Dell ControlVault™, filtro de privacidad opcional, TPM 1.2[9]
Compartimiento de medios	Compartimiento modular de medios de E-Family: DVD-ROM 8X, CDRW/DVD 24X, DVD+/-RW 8X, disco duro secundario o módulo Travel Lite	Compartimiento modular de medios de E-Family: DVD-ROM 8X, CDRW/DVD 24X, DVD+/-RW 8X, disco duro secundario o módulo Travel Lite
Colaboración	2 parlantes con tarjeta interna de audio de 24 bit micrófono digital opcional, cámara VGA opcional	2 parlantes con tarjeta interna de audio de 24 bit micrófono digital opcional, cámara VGA opcional
Ranuras de expansión	1 PCMCIA tipo I/II O Expresscard/54, lector de tarjetas 5 en 1	1 PCMCIA tipo I/II y Expresscard/54, lector de tarjetas 5 en 1
Puertos	IEEE - 1394, conector de acoplamiento, USB 2.0 (x4), VGA, Display Port, RJ-11 (opcional), RJ-45, eSATA, USB PowerShare, salida de auriculares/parlantes y micrófono	IEEE - 1394, conector de acoplamiento, USB 2.0 (x4), VGA, Display Port, RJ-11 (opcional), RJ-45, eSATA, USB PowerShare, salida de auriculares/parlantes y micrófono
Administración de sistemas	Funciones de administración avanzadas de la tecnología Intel vPro™ (opcional, requiere WLAN Intel WiFi® Link), DASH, Dell Client Manager	Funciones de administración avanzadas de la tecnología Intel vPro™ (opcional, requiere WLAN Intel WiFi® Link), DASH, Dell Client Manager
Entrada	Opción de teclado iluminado con doble dispositivo señalador	Opción de teclado iluminado con doble dispositivo señalador
Dimensiones/ peso[8] (inicial)	PRELIMINAR El peso inicial con batería de 4 celdas es de 4,3 libras/1,95 kg [10] 13,2" x 9,4" x 1,0-1,2" (335,0 x 238,3 x 25,4 a 31,0 mm)	PRELIMINAR El peso inicial con batería de 4 celdas es de 5,17 libras/2,34 kg[11] 14,1" x 10,1" x 1,1-1,3" (358,0 x 257,0 x 27,4 a 33,3 mm)
Estaciones de acoplamiento	E-Port, E-Port Plus, E-Legacy Extender, base para monitor plano E-Flat, base para monitor E-Monitor, base para portátil E-View, compartimiento de medios E-Media, CoolSlice™	E-Port, E-Port Plus, E-Legacy Extender, base para monitor plano E-Flat, base para monitor E-Monitor, base para portátil E-View, compartimiento de medios E-Media, CoolSlice™

[1] Resultados preliminares basados en las pruebas de laboratorio de Dell. Varía según la configuración, las condiciones operativas y otros factores. La capacidad máxima de la batería disminuye con el tiempo y el uso.

[2] Sujeta al área de cobertura del proveedor de servicios inalámbricos. Requiere suscripción a un servicio de banda ancha móvil. Pueden aplicarse cargos adicionales; no está disponible en todas las regiones.

[3] Los servicios de movilidad ProSupport de Dell no están disponibles en todos los países. Para obtener los términos de servicio, visite www.dell.com/servicedescriptions.

[4] Las opciones de desactualización de Windows Vista® original se entregan con Windows® XP Professional original preinstalado y con soporte técnico y de medios tanto para Windows® XP original como para Windows Vista® original, de modo que pueda realizar una transición a Windows Vista® original cuando esté preparado.

[5] Es posible que se utilice una cantidad significativa de memoria del sistema para admitir gráficos, en función del tamaño de la memoria del sistema y de otros factores.

[6] Es posible que la opción de hasta 1 GB no esté disponible con sistemas operativos de 32 bits, debido a los requisitos de recursos del sistema.

[7] 1 GB equivale a mil millones de bytes y 1 TB equivale a 1 billón de bytes. La capacidad real dependerá del material que se ha cargado previamente y el entorno operativo, lo cual podrá determinar que dicha capacidad sea menor.

[8] El peso puede cambiar según las configuraciones y la variabilidad de fabricación.

[9] No está disponible en todas las regiones.

[10] El peso inicial preliminar es de 4,3 libras/1,95 kg con batería de 4 celdas, unidad de estado sólido delgada de 2,5", LED de 14,1", gráficos integrados y módulo Travel Lite. El peso puede cambiar según las configuraciones y la variabilidad de fabricación.

[11] El peso inicial preliminar es de 5,17 libras/2,34 kg con batería de 4 celdas, unidad de estado sólido delgada de 2,5", LED de 15,4", gráficos integrados y módulo Travel Lite. El peso puede cambiar según las configuraciones y la variabilidad de fabricación.

Anexo 4.

Características técnicas de equipos de radio empleados en las pruebas.

MOTOROLA

PRO3100™

Radio Móvil
Rádio Móvel
Mobile Radio

contacto

control

Guía del usuario
Manual do usuário
User Guide

Radios Profesionales

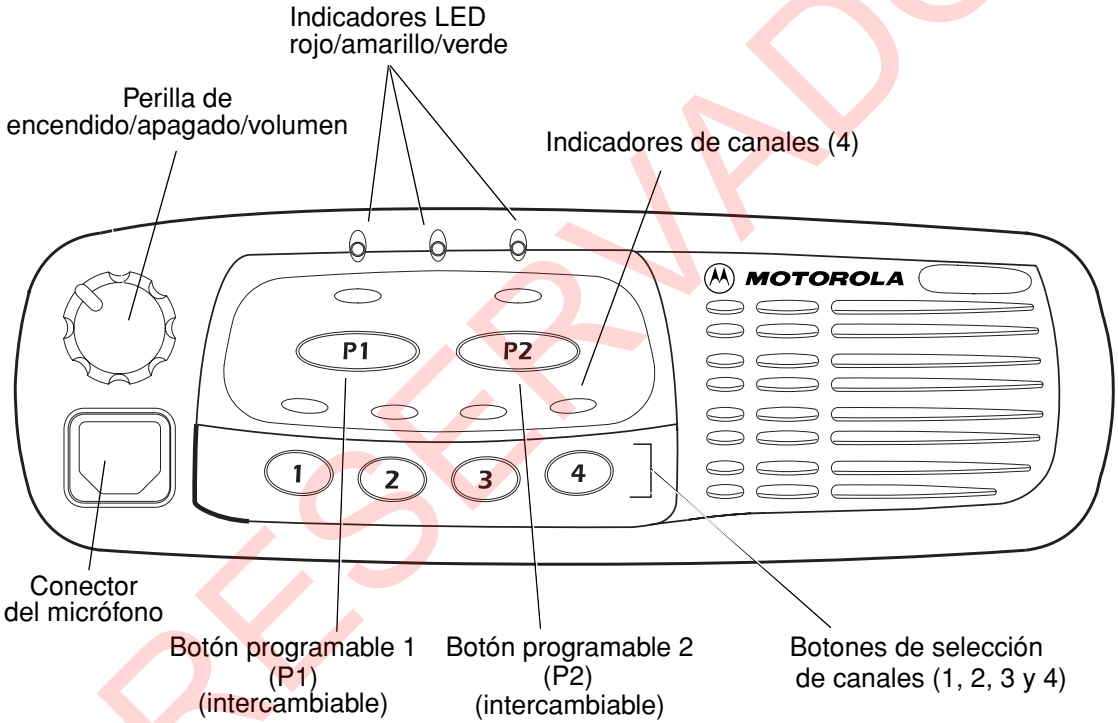
CONTENIDO

DERECHOS DE PROPIEDAD INTELECTUAL DEL SOFTWARE

Los productos Motorola descritos en este manual pueden incluir programas de computación de Motorola protegidos por copyright, almacenados en las memorias semiconductoras u otros medios. Las leyes de los Estados Unidos y otros países protegen ciertos derechos exclusivos de Motorola sobre los programas de computación protegidos por copyright, incluyendo, sin limitarse a, el derecho exclusivo a copiar o reproducir de cualquier manera el programa de computación protegido por copyright. En virtud de lo anterior, no está permitido copiar, reproducir, modificar, decodificar con fines de ingeniería inversa ni distribuir de ninguna manera, sin el permiso expreso por escrito de Motorola, ningún programa de computación de Motorola protegido por copyright que esté incluido en los productos de Motorola descritos en este manual. Además, la compra de los productos de Motorola no implica la concesión, directa, implícita, por omisión o de otra manera, de ninguna clase de licencia en virtud de los copyrights, patentes o solicitudes de patente de Motorola, salvo las licencias normales no exclusivas de uso emergentes por ley de la venta de un producto.

DESCRIPCIÓN GENERAL DEL RADIO

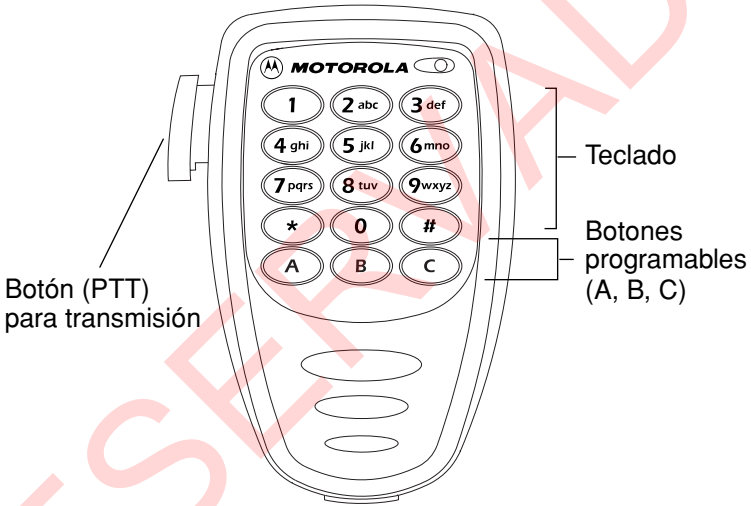
PARTES DEL RADIO



Micrófono con teclado avanzado (RMN4026)

Puede solicitar con su radio un micrófono avanzado con DTMF (multifrecuencia de tono dual), con un teclado de ingreso directo.

Este micrófono con teclado tiene tres botones (A, B, C) debajo del teclado que se pueden programar para activar fácilmente ciertas funciones seleccionadas del radio.



Perilla de encendido/apagado/volumen

Enciende o apaga el radio, y ajusta el volumen.

Indicadores de canales

Cuatro LED (uno por canal) que indican el canal activo o seleccionado.

Botones de selección de canales

1 o 2 o 3 o 4

Se usan para seleccionar los canales. Cuando se presiona un botón de selección de canal (programado), se enciende la luz indicadora de canal correspondiente.

Indicadores LED

Indican el estado del canal, del rastreo y del monitoreo.

Botones programables

Su radio tiene dos botones programables. Su distribuidor puede programar estos botones para que funcionen como accesos directos para varias funciones del radio.

Solicite a su distribuidor una lista completa de las funciones proporcionadas por su radio.

Los botones programables incluyen los botones P1 y P2 (consulte la página 1).

Algunos botones pueden acceder a hasta dos funciones, según el tipo de presión ejercida sobre el botón:

- presión breve—presionar y soltar rápidamente los botones programables
- presión prolongada—presionar y mantener presionados los botones programables durante cierto período de tiempo (predefinido como 1 segundo y medio o el valor programado)
- mantener presionado—presionar y mantener presionados los botones programables mientras se verifica el estado o se realizan los ajustes

A partir de la página 4 presentamos un resumen de las funciones programables del radio y sus referencias de página correspondientes.

Solicite a su distribuidor que anote el nombre del botón programable en la columna “Botón”, junto a la función que se ha programado para ese botón.

El distribuidor puede usar las abreviaturas (P1, P2) que aparecen en la ilustración del radio en la página 1.

Además, de ser aplicable, pida a su distribuidor que indique si se debe aplicar al botón una presión breve o prolongada, o si se debe mantener presionado.

Función	Presión breve	Presión prolongada	Mantener presionado	Página	Botón
Ajuste de volumen	—	—	Emite un tono que lo ayuda a ajustar el nivel de volumen del radio.	7	
PRTT (Permiso para hablar con prioridad)	Envía una solicitud de acceso de prioridad al despachante.		—	8	
Comunicación vía repetidor/directa (radio a radio)	Alterna entre el uso de un repetidor o la transmisión directa a otro radio.†		—	9	
Nivel de potencia	Alterna el nivel de potencia de transmisión entre Alta y Baja.†		—	10	
Eliminación de canal no deseado	Activa y desactiva el rastreo.	Elimina un canal no deseado mientras realiza el rastreo.	—	11	
Teléfono	Modo de acceso de teléfono†		—	13	
Marcación rápida	Accede directamente a su lista telefónica.†		—	13	
Monitoreo	Cambia la operación de monitoreo silencioso (también desactiva el monitoreo con silenciador abierto si está activado).	Activa el monitoreo con silenciador abierto.	—	—	

†Esta función se activa YA SEA con una presión breve O BIEN con una prolongada, pero no con ambas.

Función	Presión breve	Presión prolongada	Mantener presionado	Página	Botón
Tarjeta opcional (si hay una instalada)	Alterna entre activar y desactivar la tarjeta opcional.†		—	—	
Control auxiliar (1/2)	Activa o desactiva una patilla en el conector para accesorios.† (Consulte con su distribuidor).		—	—	

†Esta función se activa YA SEA con una presión breve O BIEN con una prolongada, pero no con ambas.

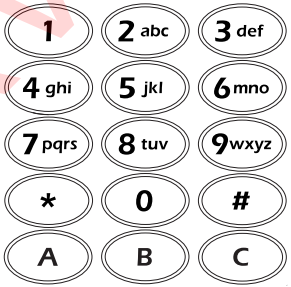
Botón para transmisión (PTT)

Presione y mantenga presionado este botón para hablar, y suéltelo para escuchar.

Micrófono

Sostenga el micrófono a una distancia de entre 2,5 y 5 cm (de 1 a 2 pulgadas) de la boca, y hable claramente en dirección al micrófono.

Uso con el micrófono con teclado avanzado (RMN4026)



Estas teclas se usan para:

- Marcar un número de teléfono
- Acceder directamente a las funciones preprogramadas

INDICADORES DE AUDIO PARA BOTONES PROGRAMABLES

Tono bajo-alto

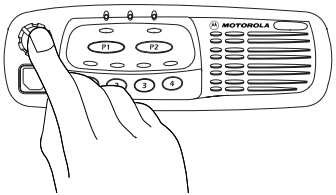
Tono alto-bajo

Algunos de los botones programables usan tonos para indicar uno de los siguientes dos modos:

Botón	Tono bajo-alto	Tono alto-bajo
Rastreo	Iniciar rastreo	Interrumpir rastreo
Nivel Potencia	Potencia alta seleccionada	Potencia baja seleccionada
Tarjeta opcional	Activada	Desactivada
Comunicación vía repetidor/directa (radio a radio)	No usa repetidor	Usa repetidor

OPERACIÓN BÁSICA

ENCENDIDO Y APAGADO DEL RADIO



Encendido	Apagado
Presione la perilla de **encendido**/**apagado**/**volumen** hasta que escuche un “clic”. Si el radio se enciende y si se ha programado el tono de Autoprueba exitoso, se escucha el tono.  Si el radio no se enciende, se escucha el tono de falla de Autoprueba  .	Presione la perilla de **encendido**/**apagado**/**volumen** hasta que se escucha un “clic” y se apagan los indicadores LED.

AJUSTE DEL VOLUMEN

Haga girar la perilla de **encendido**/**apagado**/**volumen** en el sentido de las agujas del reloj para aumentar el volumen, o en el sentido contrario al de las agujas del reloj para bajarlo.

–o–

1. Presione y mantenga presionado el botón de **ajuste de volumen** (consulte la página 4). Se escucha entonces un tono continuo.
2. Haga girar la perilla de **encendido**/**apagado**/**volumen** hasta obtener el nivel de volumen deseado.
3. Suelte el botón de **ajuste de volumen**.

SELECCIÓN DE UN CANAL DE RADIO

El radio ofrece 4 canales.

Nota: En cumplimiento de las normas gubernamentales, algunos canales no pueden programarse. Consulte con su distribuidor para obtener más información.

Para seleccionar un canal:

Presione el botón de **selección de canales** que desee (1, 2, 3 o 4).

TRANSMISIÓN DE UNA LLAMADA

1	Encienda el radio.
2	Seleccione el canal deseado.
3	Sostenga el micrófono en posición vertical a una distancia de entre 2,5 y 5 cm (de 1 a 2 pulgadas) de la boca. Presione el botón **PTT** para hablar; suéltelo para escuchar.

Si su sistema usa la función de “permiso para hablar”, utilice el siguiente procedimiento para transmitir una llamada:

1	Encienda el radio.
2	Seleccione el canal deseado.
3	Presione el botón **PTT** (para obtener permiso para hablar con prioridad, use el botón **PRTT**) y espere el tono de autorización para hablar.
4	Sostenga el micrófono en posición vertical a una distancia de entre 2,5 y 5 cm (de 1 a 2 pulgadas) de la boca. Presione el botón **PTT** para hablar; suéltelo para escuchar.

RECEPCIÓN DE UNA LLAMADA

1	Encienda el radio.
2	De ser necesario, ajuste el volumen del radio (consulte la página 7).
3	Seleccione el canal deseado.
4	Para responder, sostenga el micrófono en posición vertical a una distancia de entre 2,5 y 5 cm (de 1 a 2 pulgadas) de la boca.

LLAMADAS DE RADIO

INHIBICIÓN SELECTIVA DE RADIO

Su radio está equipado con una función de seguridad que puede hacer que la unidad deje de operar temporariamente cuando se recibe una señal de inhibición desde la estación base.

Esta función se usa normalmente para desactivar radios:

- en caso de robo
- mientras se le está realizando un servicio de mantenimiento a su vehículo
- por razones de control del sistema

Nota: Cuando se desactiva la radio mediante una señal emitida desde la estación base, todos los controles dejan de operar, salvo el botón de **encendido**/**apagado**.

COMUNICACIÓN VÍA REPETIDOR O DIRECTA (RADIO A RADIO)

La comunicación directa le permite comunicarse con otro radio en uno de los siguientes casos:

- El repetidor no está operando

–o–

- El radio está fuera del área de cobertura del repetidor pero otro radio se encuentra a una distancia que permite la comunicación. Cuando se cambia de un modo de comunicación a otro, se escucha un indicador audible.

Para seleccionar la comunicación vía repetidor o la directa (radio a radio):

Presione el botón preprogramado de **repetidor**/**radio a radio** (consulte la página 4) para alternar entre la comunicación vía repetidor y la comunicación directa (radio a radio).

NIVEL DE POTENCIA

Cada canal de su radio tiene un nivel de potencia de transmisión predefinido que se puede cambiar.

- Potencia alta
- Potencia baja

Para fijar el nivel de potencia, presione el botón preprogramado de **nivel de potencia** (consulte la página 4) para alternar entre la potencia *alta* y *baja*.

RASTREO

Su radio puede monitorear varios canales enumerados en una lista de rastreo.
El distribuidor puede programar hasta cuatro canales diferentes en cada lista de rastreo.
Cuando el radio detecta actividad en un canal de la lista de rastreo, automáticamente pasa a ese canal.

Nota: Se pueden asignar los mismos canales a diferentes listas de rastreo.

INICIO O INTERRUPCIÓN DEL RASTREO

Durante una operación de rastreo, el indicador LED verde parpadea, y deja de parpadear cuando el radio pasa a un canal.

Puede iniciar o interrumpir una operación de rastreo:

presionando el botón preprogramado de **rastreo** (consulte la página 4).

RESPUESTA EN EL CANAL ACTIVO

La función de respuesta en el canal activo le permite responder a una transmisión mientras realiza un rastreo. Si se detecta una transmisión en un canal mientras se está realizando un rastreo, el radio se detiene en ese canal durante un período de tiempo preprogramado. Durante este “tiempo de espera” se puede responder presionando el botón **PTT**.

Nota: Si la transmisión se detiene/cesa o si el botón **PTT** no se presiona durante un tiempo preprogramado, el radio sigue realizando el rastreo. El indicador LED de rastreo deja de parpadear mientras el radio se encuentra en tiempo de espera.

ELIMINACIÓN DE UN CANAL NO DESEADO

Si un canal genera constantemente llamadas no deseadas o ruido (lo que se define como canal “no deseado”), utilice el botón de **rastreo** para eliminarlo temporariamente de la lista de rastreo.

Nota: No es posible eliminar un canal prioritario, ni el último canal restante en una lista de rastreo.

1 Mientras el radio se encuentra en el canal no deseado, presione y mantenga presionado el botón de **rastreo** hasta escuchar un tono.

2 Suelte el botón de **rastreo**. Se elimina el canal no deseado.

Restitución de un canal a la lista de rastreo

Para volver a introducir un canal eliminado en la lista de rastreo, reinicie la operación de rastreo, o bien, apague el radio y vuélvalo a encender.

TELÉFONO

Si el radio tiene acceso a un sistema telefónico, es posible realizar llamadas telefónicas. Para ello, el radio debe enviar un código de acceso a una estación que lo conecte a una línea telefónica (diríjase al distribuidor para obtener más detalles). Una vez finalizada la llamada, el radio debe enviar un código de desconexión para colgar.

REALIZACIÓN DE UNA LLAMADA TELEFÓNICA

Se puede realizar una llamada telefónica con el botón preprogramado de **teléfono** (consulte la página 4). Para iniciar una llamada telefónica (se requiere un micrófono con teclado avanzado):

1. Presione el botón de **teléfono**.
2. Una serie de tonos indican que el radio envía automáticamente un código de acceso.
   –o–
   introduzca el código de acceso a través del teclado.
3. Cuando escuche el tono para marcar, introduzca el número de teléfono a través del teclado.
   –o–
   Presione y suelte el botón preprogramado de **marcación rápida** (consulte la página 4) para usar la función de marcación rápida.
4. Presione la tecla (de 1 a 8) correspondiente al número al que desea llamar.
   –o–
   Presione “0” si desea llamar al último número marcado.

Nota: Si introdujo el código de acceso por medio del teclado, la función de último número marcado no estará disponible. Si el código de acceso se introdujo automáticamente, simplemente presione el botón de **teléfono**.

Para terminar una llamada telefónica:

1. Si el radio tiene preprogramado el código de desconexión, diríjase al paso 2.
   –o–
   Introduzca el código de desconexión a través del teclado.
2. Presione el botón de **teléfono** para salir de la función de teléfono.

SEGURIDAD Y GARANTÍA

OPERACIÓN SEGURA Y EFICIENTE DE LOS RADIOS BIDIRECCIONALES MOTOROLA

Exposición a la energía de radiofrecuencia

Normas y pautas nacionales e internacionales

Su radio bidireccional Motorola genera y radia energía electromagnética de radiofrecuencia (RF), y ha sido diseñado para que cumpla con las siguientes normas y pautas nacionales e internacionales en torno a la exposición de seres humanos a la energía electromagnética de radiofrecuencia:

- Informe y Ordenanza Nº FCC 96-326 de la Comisión Federal de Comunicaciones de EE.UU. (agosto de 1996)
- Instituto Nacional Americano de Normas de EE.UU. (American National Standards Institute) (C95.1 - 1992)
- Consejo Nacional para la Protección y Medición de Radiación de EE.UU. (NCRP - 1986)
- Comisión Internacional para la Protección contra la Radiación no Ionizante (International Commission on Non-Ionizing Radiation Protection) (ICNRP - 1986)
- Comité Europeo de Normalización Electrotécnica (CENELEC):

ENV. 50166-1 1995 E	Exposición humana a los campos electromagnéticos de baja frecuencia (0Hz a 10kHz)
ENV. 50166-2 1995 E	Exposición humana a los campos electromagnéticos de alta frecuencia (10kHz a 300GHz)

Acta de Sesiones de SC211/8 1996	Consideraciones de seguridad en torno a la exposición humana a los campos electromagnéticos provenientes de equipos de telecomunicaciones móviles (M.T.E.) en la gama de frecuencias de 30MHz - 6GHz (E.M.F. - Campos electromagnéticos)

Para asegurar un funcionamiento óptimo del radio, y para garantizar que la exposición humana a la energía electromagnética de radiofrecuencia se mantenga dentro de los límites establecidos en las normas antes mencionadas, deberán observarse siempre los siguientes procedimientos:

INTERFERENCIA/COMPATIBILIDAD ELECTROMAGNÉTICA

Nota: Casi todos los dispositivos electrónicos son susceptibles a la interferencia electromagnética si no cuentan con el debido blindaje, o si no están diseñados o configurados de manera que sean compatibles con este tipo de señales electromagnéticas.

- Para evitar la interferencia electromagnética y/o problemas de compatibilidad, apague el radio en todo sitio donde haya letreros que así lo establezcan. Por ejemplo, los hospitales y establecimientos de asistencia médica podrían estar usando aparatos sensibles a la energía de radiofrecuencia externa.
- Cuando esté a bordo de un avión, apague el radio cuando se le indique. Si usa el radio, deberá hacerlo de conformidad con las regulaciones de la línea aérea y las instrucciones de la tripulación.

ADVERTENCIAS OPERACIONALES

ADVERTENCIA

Vehículos equipados con bolsas de aire

No coloque un radio móvil sobre una bolsa de aire o en el área de despliegue de la misma. Las bolsas de aire se inflan con gran fuerza. Si un radio móvil se coloca en el área de despliegue de la bolsa de aire y ésta se infla, es posible que el radio salga disparado con gran fuerza y que produzca lesiones a los ocupantes del vehículo.

Atmósferas potencialmente explosivas

Apague el radio bidireccional cuando esté en una atmósfera potencialmente explosiva, a menos que el radio sea del tipo específicamente calificado para uso en tales áreas (por ejemplo, aprobado por Factory Mutual o CENELEC). Las chispas en atmósferas potencialmente explosivas pueden desencadenar una explosión o incendio, y ocasionar lesiones o inclusive la muerte.

Detonadores y áreas de detonación

Para evitar una posible interferencia con las operaciones de detonación, apague el radio cuando esté cerca de detonadores eléctricos, en un área de detonación o donde haya letreros que exijan que se apaguen los radios bidireccionales. Respete todas las señales e instrucciones.

Nota: Las áreas con atmósferas potencialmente explosivas antes mencionadas incluyen áreas de reabastecimiento de combustible, como por ejemplo: debajo de la cubierta de embarcaciones; en instalaciones de transferencia y almacenamiento de combustible y productos químicos, en áreas donde el aire contiene productos químicos o partículas, tales como granos en polvo o polvos metálicos, así como en cualquier otra área donde normalmente se le pediría que apagara el motor de un vehículo. En las áreas con atmósferas potencialmente explosivas hay generalmente señales de precaución, aunque no siempre es así.

Operación de radios móviles y exposición a la energía electromagnética

Para obtener un funcionamiento óptimo del radio y para asegurarse de que la exposición de los seres humanos a la energía electromagnética de radiofrecuencia no exceda las normas mencionadas anteriormente en este documento, realice transmisiones únicamente cuando las personas situadas dentro o fuera del vehículo se encuentren por lo menos a la distancia mínima indicada de una antena de montaje externo debidamente instalada.

En la Tabla 1 se indica la distancia mínima para diversas gamas de energía radiada.

Tabla 1: Energía radiada y distancia

Energía radiada de un radio bidireccional móvil instalado en un vehículo	**Distancia mínima de la antena de transmisión**
7 a 15 Watts	30,5 cm
16 a 50 Watts	61 cm
Más de 50 Watts	91,5 cm

Instalación de una antena móvil

Instale la antena en la parte *externa* del vehículo, teniendo en cuenta:

- Los requisitos del fabricante/distribuidor de la antena
- Las instrucciones del Manual de instalación del radio

OPERACIÓN DE UNA ESTACIÓN DE CONTROL

Cuando se utiliza un equipo de radio como estación de control, es importante que la antena sea instalada en la parte externa del edificio, de tal manera que se evite la posibilidad de que las personas se acerquen a ella.

Nota: Consulte la Tabla 1 en la página 18 para obtener los valores de potencia nominal y de distancia mínima correspondientes a las antenas transmisoras.

GARANTÍA LIMITADA

PRODUCTOS DE COMUNICACIÓN MOTOROLA

I. ALCANCE Y DURACIÓN DE ESTA GARANTÍA:

MOTOROLA INC. (“MOTOROLA”) garantiza los Productos de Comunicación MOTOROLA remanufacturados que se enumeran a continuación (el “Producto”) contra defectos de fabricación y de mano de obra, siempre y cuando los mismos sean operados bajo condiciones de uso y manejo normales, durante los plazos indicados a continuación contados a partir del momento en que el producto fue adquirido:

Unidades móviles PRO3100	Dos (2) años
Accesorios de los productos	Un (1) año

Motorola, a su entera discreción, podrá sin cargo alguno para el consumidor, ya sea reparar el Producto (con partes nuevas o reacondicionadas), reemplazarlo (por un Producto nuevo o reacondicionado), o reembolsar el precio de compra del Producto durante el período de la garantía, siempre y cuando el Producto sea devuelto de conformidad con las condiciones establecidas de la presente Garantía. Las piezas o placas reemplazadas se garantizarán por el resto del período de garantía original. Todas las piezas reemplazadas del Producto pasarán a ser propiedad de MOTOROLA.

Motorola extiende esta garantía limitada explícita únicamente al comprador y usuario original; dicha garantía no se puede asignar o transferir a ninguna otra parte. Esta constituye la garantía completa para el Producto fabricado por MOTOROLA. MOTOROLA no asume ninguna obligación o responsabilidad legal con respecto a enmendaciones o modificaciones de esta garantía, a menos que éstas se hagan por escrito y sean firmadas por un oficial de MOTOROLA. A menos que se especifique en un acuerdo separado que MOTOROLA celebre con el comprador y usuario original, MOTOROLA no garantiza la instalación, el mantenimiento o el servicio del Producto.

MOTOROLA no acepta responsabilidad alguna por equipos auxiliares no suministrados por MOTOROLA que se encuentren conectados al Producto o que se utilicen en conexión con el mismo, ni por el funcionamiento del Producto en conjunto con tales equipos auxiliares; todo equipo de esta clase queda excluido de esta garantía. Debido a las diferencias que existen entre los sistemas en los que puede utilizarse el Producto, MOTOROLA renuncia a cualquier responsabilidad relacionada con el alcance, la cobertura o el funcionamiento del sistema entero bajo esta garantía.

II. DISPOSICIONES GENERALES:

Esta garantía establece la totalidad de la responsabilidad de MOTOROLA con respecto al Producto. La reparación, el reemplazo o el reembolso del precio de compra constituyen los únicos remedios, y éstos quedan a la entera discreción de MOTOROLA. ESTA GARANTÍA SUSTITUYE A CUALQUIER OTRA GARANTÍA EXPRESA. LAS GARANTÍAS IMPLÍCITAS, INCLUYENDO, PERO SIN LIMITARSE A LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O DE IDONEIDAD PARA UN PROPÓSITO EN PARTICULAR, QUEDAN LIMITADAS A LA DURACIÓN DE LA PRESENTE GARANTÍA LIMITADA.

EN NINGÚN CASO MOTOROLA SE HARÁ RESPONSABLE DE DAÑOS O PERJUICIOS QUE EXCEDAN EL PRECIO DE COMPRA DEL PRODUCTO, NI DE NINGUNA PÉRDIDA DE USO, PÉRDIDA DE TIEMPO, INCOMODIDAD, PÉRDIDA COMERCIAL, GANANCIAS O AHORROS PERDIDOS U OTROS DAÑOS CONSECUENTES, ESPECIALES O CONCOMITANTES QUE SURJAN DEL USO, O DE LA INHABILIDAD DE USAR EL PRODUCTO, HASTA EL GRADO EN QUE LA LEY APLICABLE PERMITA LA RENUNCIA DE TALES DAÑOS Y PERJUICIOS.

III. CÓMO OBTENER SERVICIO BAJO LA GARANTÍA:

Se debe presentar alguna prueba de compra (que lleve la fecha de adquisición y el número de serie del Producto) para poder recibir servicio bajo la garantía; además, se debe entregar o enviar el Producto, con porte y seguro prepagados, a un centro de servicio autorizado. Motorola proporcionará el servicio bajo la garantía por medio de un centro de servicio autorizado. El usuario puede facilitar la obtención de servicio bajo la garantía, comunicándose primero con la compañía que le vendió el Producto (p. ej.: el distribuidor o proveedor de servicios de comunicación).

IV. ESTA GARANTÍA NO ES VÁLIDA EN LOS SIGUIENTES CASOS:

A Defectos o daños derivados del uso anormal del Producto.

B Defectos o daños derivados del mal uso, accidente, contacto con el agua o negligencia.

C Defectos o daños derivados de pruebas, operación, mantenimiento, instalación, modificaciones o ajustes inapropiados.

D Rupturas o daños causados a las antenas, a menos que los mismos sean consecuencias de defectos en el material o mano de obra.

E Productos que han sido modificados, desmontados o reparados sin autorización (incluyendo, sin limitación, la adición al Producto de equipos no suministrados por Motorola) de una manera que afecte adversamente el funcionamiento del Producto o que interfiera en los procedimientos normales de inspección y prueba del Producto que Motorola emplea para verificar las reclamaciones bajo la garantía.

F Los Productos a los cuales se les haya retirado el número de serie o en que el mismo sea ilegible.

G Costos de enviar el Producto a un centro de reparación.

H Productos que, debido a una modificación ilícita o no autorizada del software/firmware, no funcionen de acuerdo con las especificaciones publicadas de MOTOROLA o con la etiqueta de aceptación de tipo de la FCC que estaba vigente en el momento en que MOTOROLA fabricó el Producto.

I Rayones u otros defectos superficiales del Producto que no afecten el funcionamiento del mismo.

J Desgaste causado por el uso normal.

V. DISPOSICIONES RELACIONADAS CON PATENTES Y SOFTWARE:

MOTOROLA defenderá, por su propia cuenta, cualquier acción legal que se entable en contra del comprador y usuario final que sea basada en una afirmación de que el Producto o sus componentes violen una patente estadounidense, y MOTOROLA pagará cualquier costo en el que incurra el comprador y usuario final, o indemnización que éste esté obligado a pagar como consecuencia de cualquier demanda de esta clase; sin embargo, dicha defensa y el pago de los costos e indemnizaciones correspondientes dependerá del cumplimiento de los siguientes requisitos:

A que dicho comprador informe a MOTOROLA en forma oportuna y por escrito cuando sea notificado de una acción de este tipo;

B que MOTOROLA tenga el derecho de asumir el control exclusivo de la defensa y pueda conducir todas las negociaciones necesarias para su resolución o para llegar a un acuerdo mutuo; y

C en caso de que el Producto o los componentes de éste se conviertan en el objeto de una acción legal por violación de una patente estadounidense (o en caso de que MOTOROLA considere que tal acción legal sea probable), el comprador permitirá que MOTOROLA, a su discreción y por su propia cuenta, adquiera para dicho comprador el derecho de continuar utilizando el Producto o los componentes, o que reemplace o modifique los mismos para que ya no violen la patente, o que acepte la devolución del Producto o de sus componentes y conceda al comprador un crédito por su valor depreciado.
La depreciación se calculará en línea recta (una cantidad igual cada año) basándose en la vida útil del Producto o de los componentes, según establezca MOTOROLA.

MOTOROLA no aceptará responsabilidad alguna con respecto a ninguna acción por violación de patente que sea basada en una combinación del Producto o de los componentes suministrados bajo el presente acuerdo con otros productos de software, aparatos o dispositivos no suministrados por MOTOROLA, ni tampoco MOTOROLA aceptará responsabilidad alguna por el uso de equipos auxiliares o productos de software no suministrados por MOTOROLA que se encuentren conectados al Producto o que se utilicen en conjunto con el mismo. Lo anterior

constituye una declaración de la responsabilidad total de MOTOROLA con respecto a la violación de patentes por parte del Producto o de los componentes del mismo.

Las leyes de los Estados Unidos y de otros países establecen para MOTOROLA ciertos derechos exclusivos relacionados con el software de MOTOROLA que está protegido por copyright (leyes de propiedad intelectual), como por ejemplo el derecho exclusivo de reproducir y distribuir copias de dicho software de Motorola. Se permite el uso del software de MOTOROLA únicamente en el Producto en el que el software fue incorporado originalmente, y dicho software en dicho Producto no puede ser reemplazado, copiado, distribuido o modificado de ninguna manera, ni tampoco puede ser utilizado para crear productos derivados. Se prohíbe cualquier otro uso, incluyendo, sin limitación, la alteración, modificación, reproducción, distribución o ingeniería inversa de dicho software de MOTOROLA, así como el ejercicio de los derechos que atañen al software de MOTOROLA. No se concede bajo los derechos de patente o de copyright de MOTOROLA, ninguna licencia implícita o basada en el concepto jurídico anglosajón de “estoppel”.

VI. JURISDICCIÓN:

Esta Garantía será regida por las leyes del estado de Illinois de los Estados Unidos.

ACCESORIOS

Motorola ofrece una serie de accesorios destinados a aumentar la productividad del radio bidireccional. En la siguiente lista aparecen algunos de los accesorios disponibles. Para obtener una lista completa, consulte con su distribuidor de Motorola.

AUDIO

RMN4025	Micrófono/parlante externo
RMN4026	Microfono con teclado avanzado
RMN4038	Micrófono para trabajo pesado
RSN4001	Parlante externo 13W
HSN8145	Parlante externo 7,5W

MONTAJE

GLN7324	Soporte de perfil bajo
RLN4780	Soporte de perfil alto
HLN8097	Montaje deslizable removible
RLN4779	Montaje con candado
RLN4782	Kit de montaje
RKN4077	Cable para montaje remoto - 3 m
RKN4078	Cable para montaje remoto - 5 m
RKN4079	Cable para montaje remoto - 7 m

ANTENAS

HAD4006A	Antena de techo de 1/4 de onda, VHF 136-144 MHz
HAD4007A	Antena de techo de 1/4 de onda, VHF 146-150,8 MHz
HAD4008A	Antena de techo de 1/4 de onda, VHF 150,8-162 MHz
HAD4009A	Antena de techo de 1/4 de onda, VHF 162-174 MHz
HAD4014A	Antena de techo de 3,0dB de ganancia, VHF 146-172 MHz
HAE4002A	Antena de techo de 1/4 de onda, UHF 403-430 MHz
HAE4003A	Antena de techo de 1/4 de onda, UHF 450-470 MHz
HAE4010A	Antena de techo de 3,5dB de ganancia, UHF 406-420 MHz
HAE4011A	Antena de techo de 3,5dB de ganancia, UHF 450-470 MHz
HAE4019A	Antena de techo de 5dB de ganancia, UHF 450-470 MHz
HAE4004A	Antena de techo de 1/4 de onda, UHF 470-512 MHz
HAE4012A	Antena de techo de 3,5dB de ganancia, UHF 470-494 MHz
09-02105F01	Conector BNC

ESTACIÓN DE CONTROL

GPN6145	Fuente de alimentación 1-25W (EMC)
HPN4002	Fuente de alimentación 1-25W
GPN6149	Fuente de alimentación 25-45W (EMC)
HPN4001	Fuente de alimentación 25-45W
RMN4030	Micrófono de escritorio
GLN7318	Consola sin parlante
GLN7326	Consola con parlante

Nota: Hay una serie de botones intercambiables disponibles para su uso en las ubicaciones P1-P2 del radio (página 1). Consulte con su distribuidor para más detalles.

Transmisión de una llamada

1. Encienda el radio y seleccione el canal apropiado.
2. Presione **PTT**, sostenga el micrófono a una distancia de entre 2,5 y 5 cm (1 a 2 pulgadas) de la boca, y hable claramente en dirección al micrófono.
3. Suelte el botón **PTT** para escuchar.

Recepción de una llamada

1. Encienda el radio y ajuste el volumen.
2. Seleccione el canal deseado.
3. Para responder a una llamada, presione **PTT**, sostenga el micrófono a una distancia de entre 2,5 y 5 cm (1 a 2 pulgadas) de la boca, y hable claramente en dirección al micrófono.

Eliminación de un canal molesto durante el escaneo

1. Mientras el radio se encuentra en el canal molesto, presione y mantenga presionado el botón preprogramado de **rastreo** hasta escuchar un tono.
2. Suelte el botón de **rastreo**.

Realización de una llamada telefónica

1. Presione el botón de **teléfono**.
2. Si no se escucha el código de acceso, envíe el código de acceso si es necesario.
3. Utilice uno de los siguientes métodos para transmitir el número de teléfono:
   - Presione y suelte **PTT** para enviar el último número marcado.
     —o—
   - Si utiliza solamente el micrófono con teclado avanzado, presione el botón preprogramado de **marcación rápida**, seguida de una de las teclas del teclado (1–8), para acceder a los primeros nueve números de la lista telefónica. (Presione **PTT** para utilizar la marcación almacenada.)
     —o—
   - Si utiliza solamente el micrófono con teclado avanzado, introduzca el número telefónico usando el teclado. (Presione **PTT** para utilizar la marcación almacenada.)
4. Presione **PTT**, sostenga el micrófono a una distancia de entre 2,5 y 5 cm (1 a 2 pulgadas) de la boca, y hable claramente en dirección al micrófono.

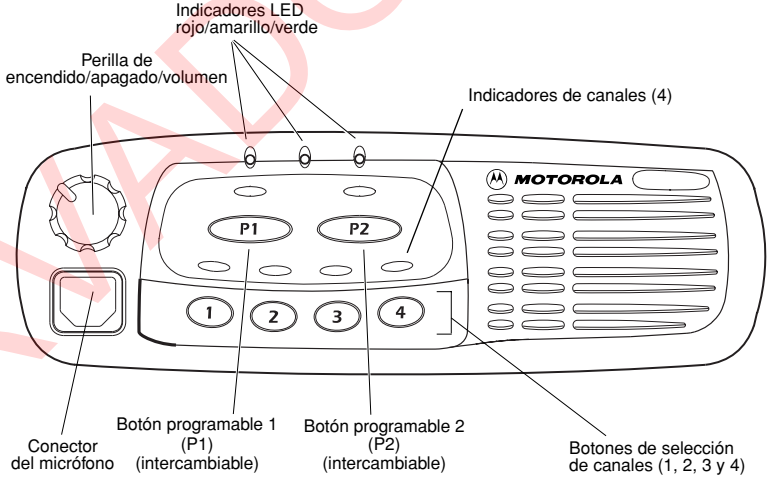
Terminación de una llamada telefónica

1. Envíe el código de desconexión si es necesario.
2. Presione el botón de **teléfono**.

MOTOROLA

PRO3100™ Tarjeta de Consulta Rápida

Utilice la siguiente tabla para registrar las funciones de los botones programables del radio. Para información adicional, consulte la página 4 de esta Guía del usuario.



Botón	Función	Presión breve	Presión prolongada	Mantener presionado	Página

Bird Technologies - The RF Experts

75-T Series

75-T Series

75-T Series, 75 Watt, Convection-Cooled Dry Terminations
Bird's RF terminations are world renowned for their high-quailty, robust construction and conservative power ratings. The use of non-magnetic materials and plating provide safety when used in high magnetic fields such as MRI. **For Aluminum Nitride (BeO free) see model 75-NT-MN**

- Wide variety of connectors
- Rugged Reliability provides years of trouble free use
- Compact size, easily transportable
- Optionally available with Aluminum Nitride ceramic

Request Information

DOWNLOADS:

- 75-NT-MN Drawing
- 75-T-FB Drawing
- 75-T-FE Drawing
- 75-T-FN Drawing
- 75-T-FT Drawing
- 75-T-MB Drawing
- 75-T-ME Drawing
- 75-T-MN Drawing
- 75-T-MT Drawing
- Declaration of Conformity
- 3D Model 75-NT
- 3D Model 75-T

PRODUCT SPECIFICATIONS:

Item No	75-T Series
Item Name	75 Watt, Convection-Cooled Dry Terminations
Power Rating	75 W
Frequency Range and VSWR	DC to 1 GHz @ 1.10:1 max. 1 GHz to 4 GHz @ 1.25:1 max.
Temperture Range	-40 to +40 °C
Product Type	Dry (Convection-Cooled)
Operating Position	Any
Connectors	N, BNC, TNC, SMA, 7/16 DIN
Finish	Black Anodized, Silver or Tri-Alloy Plated Connectors
Dimensions	(with N-type connector):6.7" L x 2.3 Dia. (170.2 x 58.5 mm)
Weight	1.32 lbs. (0.6 kg)

9 Autry
Irvine, CA 92618
(949) 458-7277 | (949) 458-0826

...POWER ON WITH ASTRON

SWITCHING POWER SUPPLIES...

SPECIAL FEATURES:

- HIGH EFFICIENCY SWITCHING TECHNOLOGY SPECIFICALLY FILTERED FOR USE WITH COMMUNICATIONS EQUIPMENT, FOR ALL FREQUENCIES INCLUDING HF
- HEAVY DUTY DESIGN
- LOW PROFILE, LIGHT WEIGHT PACKAGE
- EMI FILTER
- MEETS FCC CLASS B

PROTECTION FEATURES:

- CURRENT LIMITING
- OVERVOLTAGE PROTECTION
- FUSE PROTECTION
- OVER TEMPERATURE SHUTDOWN

SPECIFICATIONS:

INPUT VOLTAGE: 115 VAC 50/60HZ
OR 220 VAC 50/60HZ
SWITCH SELECTABLE

OUTPUT VOLTAGE: 13.8VDC

E151765 E151765

AVAILABLE WITH THE FOLLOWING APPROVALS: UL, CUL, CE, TUV.

MODEL SS-18

DESKTOP SWITCHING POWER SUPPLIES

MODEL	CONT. (Amps)	ICS	SIZE (inches)	Wt.(lbs.)
SS-10	7	10	2⅜ x 6 x 9	3.2
SS-12	10	12	2⅜ x 6 x 9	3.4
SS-18	15	18	2⅜ x 6 x 9	3.6
SS-25	20	25	2⅞ x 7 x 9⅜	4.2
SS-30	25	30	3¾ x 7 x 9⅝	5.0

MODEL SS-25M

DESKTOP SWITCHING POWER SUPPLIES WITH VOLT AND AMP METERS

MODEL	CONT. (Amps)	ICS	SIZE (inches)	Wt.(lbs.)
SS-25M*	20	25	2⅞ x 7 x 9⅜	4.2
SS-30M*	25	30	3¾ x 7 x 9⅝	5.0

MODEL SRM-30

RACKMOUNT SWITCHING POWER SUPPLIES

MODEL	CONT. (Amps)	ICS	SIZE (inches)	Wt.(lbs.)
SRM-10	7	10	3½ x 19 x 9⅜	4.3
SRM-12	10	12	3½ x 19 x 9⅝	4.7
SRM-18	15	18	3½ x 19 x 9⅝	5.0
SRM-25	20	25	3½ x 19 x 9⅜	6.5
SRM-30	25	30	3½ x 19 x 9⅝	7.0

WITH SEPARATE VOLT & AMP METERS

MODEL	CONT. (Amps)	ICS	SIZE (inches)	Wt.(lbs.)
SRM-25M	20	25	3½ x 19 x 9⅜	6.5
SRM-30M	25	30	3½ x 19 x 9⅝	7.0

MODEL SRM-30M-2

2 ea SWITCHING POWER SUPPLIES ON ONE RACK PANEL

MODEL	CONT. (Amps)	ICS	SIZE (inches)	Wt.(lbs.)
SRM-25-2	20	25	3½ x 19 x 9⅜	10.5
SRM-30-2	25	30	3½ x 19 x 9⅝	11.0

WITH SEPARATE VOLT & AMP METERS

MODEL	CONT. (Amps)	ICS	SIZE (inches)	Wt.(lbs.)
SRM-25M-2	20	25	3½ x 19 x 9⅜	10.5
SRM-30M-2	25	30	3½ x 19 x 9⅝	11.0

*ICS – Intermittent Communication Service

Anexo 5.

Características técnicas de multimódems empleados en las pruebas.

KAM-XL All-Mode Wireless Modem

Features | **Specifications** | **App Notes** | **Accessories**

View/Download (PDF format):
KAM-XL **Brochure** (192k) KAM-XL **Manual** (1543k) KAM-XL **Port Pinout** (105k)
KAM-XL **Firmware Update** (ZIP, 225k) (latest rev, 02/19/2007)
(allow arqbbs link if vhf bbs in use, display of rtext through myremote link suppressed, fixes for mheard display and xkiss,changed handling of I and UI frames with no PID)
KAM-XL **Firmware Update** (ZIP, 215k) (latest rev, 12/13/2005)
(Refinements in message forwarding in nonpacket mailbox access)
KAM-XL Firmware Update (ZIP, 218k) (rev 08/11/2004)

Overview

The Kantronics original KAM (Kantronics All Mode) was a global revolution in digital communication. In Kantronics tradition, the KAM Plus evolved through customer suggestions and years of operating experience, making the Kantronics KAM Plus the most popular TNC on the global market. The KAM XL, Kantronics third generation multi-modem TNC is a state-of-the-art design giving the customer operations on both HF and UHF/VHF, while supporting DSP modems and popular new modes of operation.

Kantronics KAM-XL was designed to operate in many different applications as the digital world continues to change. Engineered for years of dependable performance, the KAM-XL also includes room for new modes and upgrades well into the future. Kantronics, the pioneer in digital communications, now offers you 30 years engineering experience in the Kantronics KAM-XL.

KAM-XL Features

Operating modes and functions include:

- Packet (300, 1200 or 9600 bps)
- GTOR™
- PACTOR 1
- AMTOR (ARQ, FEC, SELFEC, CCIR 476 & 625)
- PSK31
- RTTY
- NAVTEX / AMTEX
- ASCII
- WEFAX
- EMWIN
- Dual Port Mailbox
- CW
- GPS NMEA-0183 compatible
- TELEMETRY
- REMOTE CONTROL
- REMOTE SYSOP ACCESS
- Kantronics HOST Mode
- KISS

- **Location Tracking/Announcement**: With a GPS connected to the KAM-XL, you can automatically announce your position to others via HF, UHF, or VHF. Kantronics KAM-XL is engineered to work with APRS® software and supports advanced UI frame digipeating functions
- **HF and/or VHF/UHF Operations**: With dual radio ports, the flexible Kantronics KAM-XL can be used on HF, UHF and VHF bands. The popular Kantronics KAM "gateway" feature between ports 1 and 2 allows for a local packet to be received on VHF or UHF bands, then transmitted over an HF band.
- **Large capacity Internal Mailbox**: 480K personal mailbox is standard. The KAM-XL mailbox can respond to HF on TOR modes, as well as packet modes.
- **Versatile Operations**: The Kantronics KAM-XL may be used at your base, in the field, or as a mobile. Designed for flexibility, the KAM-XL will function with mobile, base, or hand-held radios.
- **Detailed Manual**: The KAM-XL manual is included on CD-ROM, and is available **here** in PDF form (1111k).
- **Made in the USA** -- Limited one year warranty to original purchaser

KAM-XL Specifications

Dimensions (H×W×D)	1.4"×8.5"×4.6" (36 mm × 216 mm × 117 mm)
System Control Processor	HC12 with 512K Flash and 512K Battery-Backed RAM
DSP Chip	ADSP 2185M processor
Power Requirements	DC 10 V - 18 V, 150 ma
Power Plug	2.1 mm coaxial, center pin positive
External Connection Ports	Radio Ports 1 & 2: DB-9 female Computer Port: DB-9 female Aux. Port: DB-9 male Telemetry Port: DB-15 female
PTT Watchdog Timer	Approx. 2.5 minutes
External Carrier Detect	Pulldown to ground
Data Rate, Port 1	45-1200 bps
Data Rate, Port 2	300-9600 bps
PTT Output	Open drain, max +50 V dc
FSK Output	Open drain, max +50 V dc
Audio Output	Continuously adjustable 10 mv - 2 V p-p
Output Impedance	600 Ohm, AC coupled
HF Modulation	Up to 1200 bps AFSK
VHF/UHF Modulation	1200 bps FSK (Bell 202 ~ 1200/2200 Hz standard) 9600 bps GMSK
Audio Input	
Dynamic Range	HF: >75 dB VHF/UHF: >73 dB
Input Impedance	10 kOhm or 620 Ohm
Max input voltage	±12 V dc; 35 v p-p sinusoidal
Operating Modes	Packet, PACTOR, GTOR, AMTOR, RTTY, ASCII, CW, WEFAX, NAVTEX/AMTEX, KISS, HOST, GPS, PSK31
Other Features	HF and VHF PBBS access, KA-Node, Packet Gateway and Cross Connect
LED Indicators	Power, Mail, Port 1 (Xmit, Rcv, Lock/Con, Val/Sta Speed, Tuner Bargraph), Port 2 (Xmit, Rec, Con/Sta)
Remote Control Access	All controller functions, user-defined password
External Reset	Pulldown to ground
Warranty	KAM-XL is protected by a one-year limited warranty to the original owner

Specifications subject to change without notice or obligation.
APRS® is a registered trademark of Bob Bruninga, WB4APR.
All registered trademarks remain the property of their respective owners.

Kantronics • 14830 West 117th Street, • Olathe, Kansas 66062
Phone (913) 839-1470 • Fax (913) 839-8231 • sales@kantronics.com

Kantronics Home | Top of Page

Anexo 6.

Características técnicas de switch empleado en las pruebas.

D-Link®
Building Networks for People

Product Highlights

Eco-Friendly
Innovative design runs quiet, cool, and clean, saving power automatically

Silent Operation
Fanless design provides noise free operation

Intelligent Data Streaming
Quality of Service (QoS) support enables clear VoIP calls

Rugged Metal Product House
Ensures the product can withstand extreme temperatures

Plug & Play
No configurations needed

DES-105 / DES-108

5/8 Port Fast Ethernet Switches

Key Features

- Inexpensive Fast Ethernet solution for businesses.
- Five/Eight 10/100 Mbps Fast Ethernet ports
- Rugged Metal Housing
- Auto MDI/MDIX crossover for all ports
- Full/half-duplex for Ethernet/Fast Ethernet speeds
- IEEE 802.3x Flow Control
- Supports Jumbo Frames
- Supports 802.1p QoS
- RoHS compliant
- Plug-and-play installation
- Slot for Kensington Security lock

The DES-105/DES-108 Fast Ethernet Switches provide a quick, easy and economical way to add high speed networking to home offices, small and medium businesses. With data transfer speeds of up to 200 Mbps the DES-105/DES-108 are ideal for fast file transfers. They provide five or eight ports for easy expansion of your network for connecting printers, scanners, storage, and backup devices to any network.

Robust Design

The DES-105 / DES-108 are designed with durability and performance in mind. Their sturdy metal housing ensures the product can withstand extreme temperatures and can be placed in typical industrial environments such as factories, construction and mining. They help to dissipate heat and reduce stress on internal components.

Effortless High Speed Networking

They are easy access, auto-sensing 10/100 front Ethernet ports with two LED indicators per port to quickly distinguish link status and speed. The DES-105/DES-108 switches also support Auto MDI/MDIX Crossover allowing each port to be plugged directly to a server, hub, router, or switch using regular straight-through twisted-pair Ethernet cables. Support for IEEE 802.1p QoS is included, which organises and prioritises time-sensitive and important data for efficient delivery.

IEEE 802.1p QoS

QoS prioritises network traffic so that time-sensitive data is delivered efficiently, even during bursts of high data traffic. This helps ensure an optimal experience for streaming media and VoIP calls.

DES-105 / DES-108 5/8 Port Fast Ethernet Switches

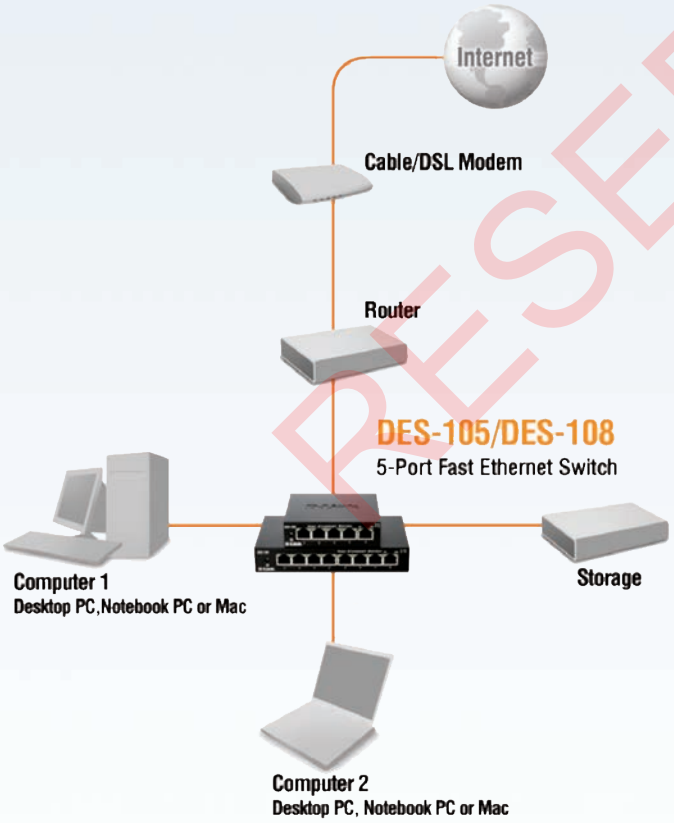
Power-saving technology

The DES-105/DES-108 are part of D-Link Green™, D-Link's eco-friendly technology, providing energy savings, reduced power consumption, and a longer product lifespan without sacrificing operational performance or functionality. These switches support IEEE 802.3az Energy Efficient Ethernet (EEE) standard which detects when a connected computer is shut down or when there is no Ethernet traffic, in which case the switches will proceed to power down the idle port, saving a substantial amount of power. This helps businesses to save money by reducing their electricity bills with no compromise on performance.

Environmentally Friendly

The DES-105/DES-108 switches are designed with the environment in mind. They are compliant with Energy Star Level V, CEC, and MEPS regulations which require the use of energy efficient power adapters. They are built to comply with RoHS standards to minimise use of hazardous materials and is packaged with an EnergyStar Level V qualified power adapter all with recyclable packaging making this product truly environmental friendly.

Your Network Setup



D-Link Assist
Rapid Response Support

If the worst should happen to your network you need the very best support and fast. Downtime costs your business money. D-Link Assist maximises your uptime by solving technical problems quickly and effectively. Our highly trained technicians are on standby around the clock, ensuring that award-winning support is only a phone call away.

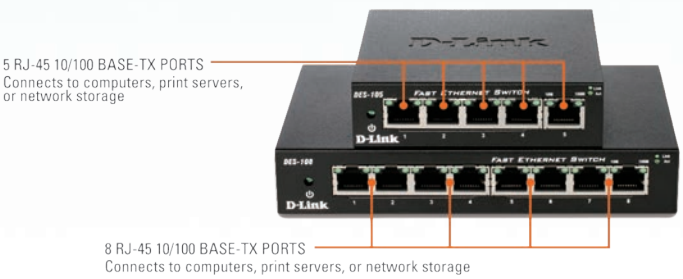
With a choice of three affordable service offerings covering all D-Link business products, you can select the package that suits you best:

D-Link Assist Gold - for comprehensive 24-hour support
D-Link Assist Gold is perfect for mission-critical environments where maximum uptime is a high priority. It guarantees four hour around-the-clock response. Cover applies 24/7 for every day of the year including holidays.

D-Link Assist Silver - for prompt same-day assistance
D-Link Assist Silver is designed for 'high availability' businesses that require rapid response within regular working hours. It provides a four hour response service Monday to Friday from 8am to 5pm, excluding holidays.

D-Link Assist Bronze - for guaranteed response on the next business day
D-Link Assist Bronze is a highly cost-effective support solution for less critical environments. Response is guaranteed within eight business hours Monday to Friday from 8am to 5pm, excluding holidays.

D-Link Assist can be purchased together with any D-Link business product. So whether you're buying switching, wireless, storage, security or IP Surveillance equipment from D-Link, your peace of mind is guaranteed. D-Link Assist also offers installation and configuration services to get your new hardware working quickly and correctly.



D-Link®
Building Networks for People

DES-105 / DES-108 5/8 Port Fast Ethernet Switches

Technical Specifications

	DES-105	DES-108
		
Switching Fabric	• 1.0 Gbps	• 1.6 Gbps
Standards	• IEEE 802.3 10BASE-T Ethernet (twisted-pair copper) • IEEE 802.3u 100BASE-TX Fast Ethernet (twisted-pair copper) • ANSI/IEEE 802.3 NWay auto-negotiation	• IEEE 802.3x Flow Control • IEEE 802.1p QoS • IEEE 802.3az Energy-Efficient Ethernet (EEE)
Protocol	• CSMA/CD	
Data Transfer Rates	• Ethernet: - 10 Mbps (half duplex) - 20 Mbps (full duplex)	• Fast Ethernet: - 100 Mbps (half duplex) - 200 Mbps (full duplex)
Topology	• Star	
Network Cables	• 10BASE-T: - UTP CAT 3, 4, 5/5e (100 m max.) - EIA/TIA-586 100-ohm STP (100 m max.)	• 100BASE-TX: - UTP CAT 5/5e (100 m max.) - EIA/TIA-568 100-ohm STP (100 m max.)
Media Interface Exchange	• Auto MDI/MDIX adjustment for all ports	
LED Indicators	• Per port: Link/Activity	• Per device: Power
Transmission Method	• Store-and-forward	
MAC Address Table	• 2K	• 1K
MAC Address Learning	• Automatic update	
Packet Filtering/Forwarding Rates	• Ethernet: 14,880 pps per port	• Fast Ethernet: 148,800 pps per port
RAM Buffer	• 384 KBytes per device	• 768 KBytes per device
Jumbo Frames	• 2047 Bytes	• 1536 Bytes
QoS	• 2 Queues, strict mode	• 2 Queues, WRR mode

DES-105 / DES-108 5/8 Port Fast Ethernet Switches

General Specifications		
DC Input	• External 5 V/1 A Level "V" Power Adapter	
Power Consumption	• Power On (Standby): - DC input: 0.5 watts - AC input: 1.0 watts • Maximum: - DC input: 2.01 watts - AC input: 3.10 watts	• Power On (Standby): - DC input: 0.55 watts - AC input: 1.0 watts • Maximum: - DC input: 2.8 watts - AC input: 4.5 watts
Heat Dissipation	• Power On (Standby) AC input: 3.41 BTU/h • Maximum DC input: 6.854 BTU/h	• Power On (Standby) AC input: 3.41 BTU/h • Maximum DC input: 9.548 BTU/h
MTBF	• 495,709 hours	• 511,323 hours
Operating Temperature	• 32 to 122 ˚F (0 to 50 ˚C)	
Storage Temperature	• 14 to 158 ˚F (-10 to 70 ˚C)	
Operating Humidity	• 10% to 90% RH non-condensing	
Storage Humidity	• 5% to 90% RH non-condensing	
Dimensions	• 100 x 98 x 28 mm	• 162 x 102 x 28 mm
Weight	• 265 grams	• 412 grams
Certifications	• FCC Class B • ICES-003 Class B • CE Class B • C-Tick Class B	• VCCI Class B • cUL • CB

For more information: www.dlink.eu

Updated 7/2/2012

dlink green

Energy Efficient Ethernet

D-Link®
Building Networks for People

Anexo 7.

Configuración de multimodems y prueba back to back

CONFIGURACIÓN DE MULTIMODEMS Y PRUEBA BACK TO BACK

1.1.1 Descripción

En este experimento se muestra como se deben configurar los TNCs Kantronics 9612 Plus para establecer comunicaciones Back to Back.

1.1.2 Propósito

Lograr la comunicación Back to Back entre TNCs mediante el uso de la interfaz Hyperterminal en un computador.

1.1.3 Descripción Del Experimento

a) Elaboración del cable cruzado para la conexión Back to Back
b) Configuración del Hyperterminal
c) Configuración del TNC
d) Pruebas de comunicaciones Back to Back.

1.1.4 Artefactos Creados

Cable cruzado.

1.1.5 Criterio De Terminación

Logro de las comunicaciones entre dos TNCs para establecer una conversación entre dos computadores.

1.1.6 Recursos Requeridos

Computador con Hyperterminal, Conversor serial DB-25 a DB-9, Conversor serial DB-9 a USB, Fuente de poder, Cable de 5 hilos blindado, Terminales DB-9, TNCs, Manuales, Cautín, Soldadura

1.1.7 Resultados Del Experimento

Las funciones principales del TNC son:

a) Transformar información digital en señales de audio y viceversa.

b) Comunicación digital con la computadora

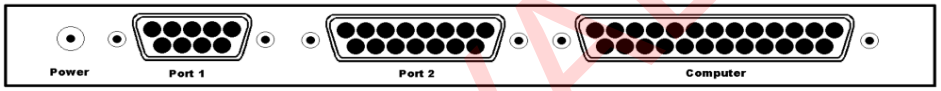
c) Permitir el control de información mediante algunos comandos

d) Soporta el protocolo NMA 0183

Para este experimento se utilizaron los TNCs marca Kantronics modelo 9612 Plus, debido a que cumple con las funciones necesarias para la prueba.

A continuación se muestra la parte trasera del TNC y se detallan los puertos para conectar un computador, radio, GPS u otro TNC y la fuente de poder.

Figura 43 Vista de la parte trasera del TNC Kantronics 9612 Plus



Fuente: Manual TNC Kantronics 9612 Plus

El propósito de cada conector se describe a continuación:

Power jack (2.1 mm interno): Esta destinado para conectar una fuente de poder entre 5.5 y 25Vdc al TNC. El centro del conector es positivo y el exterior es negativo o tierra. El TNC soporta cargas hasta 200mA, Para el experimento se utilizan Adaptadores de 120Vac a 9Vdc con capacidad de carga hasta 300mA.

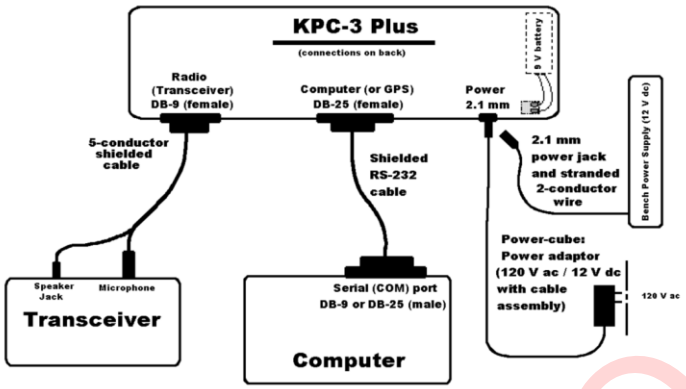
Puerto 1: Posee un conector DB-9 hembra para conexión con radios usando la banda HF para la operación de paquetes a 1200 baudios.

Puerto 2: Posee un conector DB-15 hembra para conexión con radios usando la banda VHF para la operación de paquetes a 4800/9600 baudios.

Computer: Posee un conector DB-25 hembra para conexión RS232 con un computador, usa el estándar de caracteres ASCII para todos los comandos. En esta conexión es necesario un adaptador DB-25 a DB-9 serial y un conversor serial DB-9 a USB ya que los computadores no cuentan con puerto serial.

En seguida se muestra la forma de en que se conectan los dispositivos

Figura 44 Conexión de dispositivos en el TNC Kantronics 9612 Plus



Fuente: Manual TNC Kantronics 9612 Plus

1.1.7.1 Elaboración del cable cruzado para la conexión Back to Back

Para el ensamble del cable se necesitan 2 conectores DB-9 ya que el experimento se realiza utilizando el puerto 1 en los TNCs suministrados con los equipos, 1m de cable blindado con 5 hilos suministrado con los TNCs, cautín y soldadura. La conexión entre los conectores DB-9 se realiza de la siguiente forma:

Figura 45 Conexión de pines en el conector DB9 para el cable Back to Back

TNC A		TNC B
Pin 1	→ Tx Audio →	Pin 5
Pin 3	→ PTT →	Pin 3
Pin 5	→ Rx Audio →	Pin 1
Pin 6	→ Ground Rx →	Pin 6
Pin 9	→ Ground Tx →	Pin 9

Fuente: CINTEL

1.1.7.2 Configuración del Hyperterminal

A continuación se muestra la manera en que debe configurarse la aplicación de Hyperterminal para comunicar el computador con el TNC.

Para ejecutar el Hyperterminal bajo Windows XP se hace clic en Inicio, luego todos los programas, accesorios, comunicaciones e Hyperterminal.

Estando en el programa se asigna un nombre a la conexión

Figura 46 Creación de la sesión de conexión en el Hyperteminal

Fuente: CINTEL

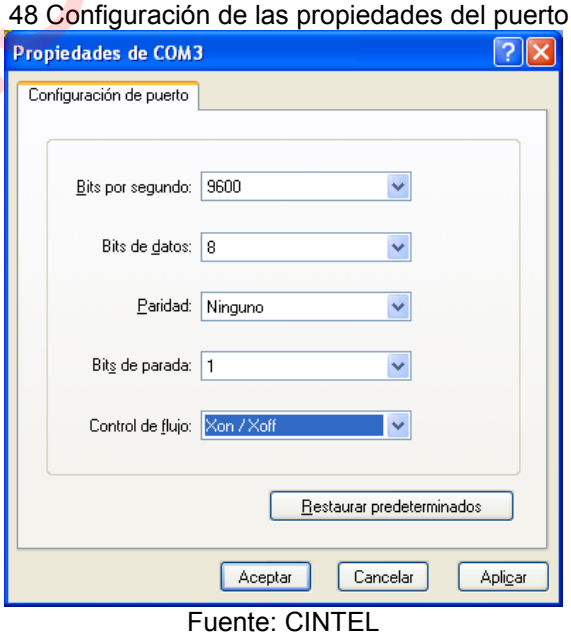
Luego se busca el puerto COM asignado al puerto serial, en nuestro caso utilizamos un adaptador Serial – USB.

Figura 47 Configuración del puerto de comunicaciones

Fuente: CINTEL

Enseguida se configuran los siguientes parámetros de la comunicación serial con el TNC, como son, la tasa de bits por segundo en 1200, 8 bits de datos, paridad ninguna, bits de parada 1, y control de flujo Xon/Xoff.

Figura 48 Configuración de las propiedades del puerto serial



Fuente: CINTEL

1.1.7.3 Configuración del TNC

Al establecer la conexión aparecerá la siguiente pantalla, el TNC enviara una serie de caracteres para luego enviar un mensaje.

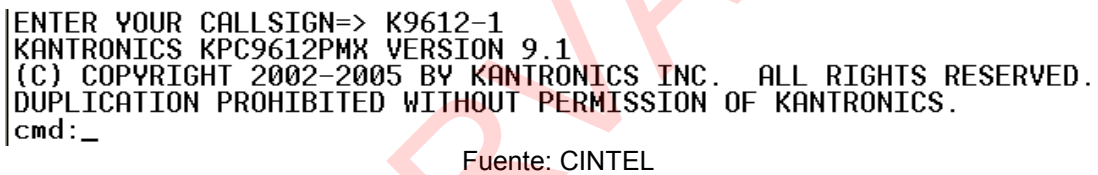
Figura 49 Mensaje de sincronización de tasa de baudios en el TNC

Fuente: CINTEL

Cuando se conecta el TNC por primera vez a un computador, inicia una función automática de sincronización en el TNC para ajustar la tasa de baudios en la comunicación con el PC, en nuestro caso esta velocidad se ajusta a 9600 baudios.

Luego de la sincronización aparecerá un mensaje para asignar el identificador, en nuestro caso se asignó k9612-1 en referencia al modelo del TNC, cabe resaltar que el TNC no distingue entre el uso de caracteres en mayúscula o minúscula al ingresar un comando.

Figura 50 Configuración del Identificador (Callsign) en el TNC



Fuente: CINTEL

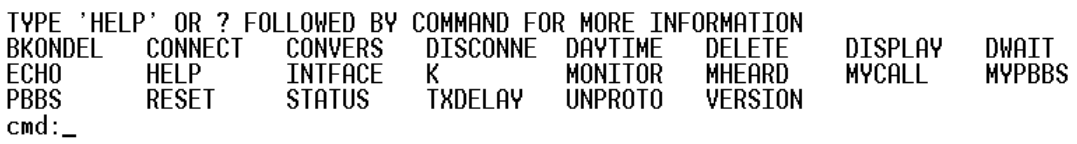
Los TNC Kantronics cuentan con diversas interfaces de comandos en las que se distinguen la cantidad de comandos que el usuario puede utilizar para configurar las diversas funcionalidades que posee, en nuestro caso utilizaremos en este experimento la instrucción INTFACE NEWUSER que cuenta con 22 instrucciones disponibles para configuración, para saber en que interfaz se encuentra trabajando el TNC se ingresa el comando INTFACE.

Figura 51 Verificación de interfaz en el TNC

Fuente: CINTEL

Para ver las instrucciones con las que cuenta el TNC es suficiente con ingresar el signo de interrogación "?" o la instrucción HELP al estar en modo cmd: para desplegar todos los comandos que posee la interfaz.

Figura 52 Comandos de la interfaz NEWUSER en el TNC



Fuente: CINTEL

En este momento se puede establecer una conexión para comunicarse en loopback con el TNC, para ello se ingresa la instrucción CONNECT o en su forma abreviada C seguida del nombre del TNC.

Figura 53 Establecimiento de la conexión con otro TNC

```
cmd:c k9612-1
cmd:*** CONNECTED to K9612-1
_
```

Fuente: CINTEL

Cuando la conexión es satisfactoria aparecerá *** CONNECTED to seguido del identificador del TNC con el que se desea establecer conexión y se entrará en modo de conversación, en el modo de conversación se intercambian datos o mensajes entre TNCs mediante el PC o un repetidor, para salir del modo conversación y entrar en el modo de comandos o cmd:, se pulsa CTRL+C, para volver a entrar en modo conversación se ejecuta la instrucción CONVERS en el modo cmd:. Si la conexión es fallida por alguna razón el TNC inicia una secuencia de reintentos esperando encontrar el dispositivo con el que se desea establecer la conexión, al terminar ese número de reintentos si la conexión es fallida se mostrará el siguiente mensaje:

Figura 54 Desconexión del TNC por reintentos excedidos

```
cmd:*** retry count exceeded
*** DISCONNECTED
```

Fuente: CINTEL

Para desconectarse de un terminal se debe ingresar el comando DISCONNECT o simplemente D, el resultado de la desconexión es el siguiente:

Figura 55 Comando de desconexión del TNC

```
cmd:d
cmd:*** DISCONNECTED
K9612-1>K9612-1/1: <<UA>>:
```

Fuente: CINTEL

Al finalizar una desconexión el TNC queda en modo cmd:.

1.1.7.4 Pruebas de comunicaciones Back to Back

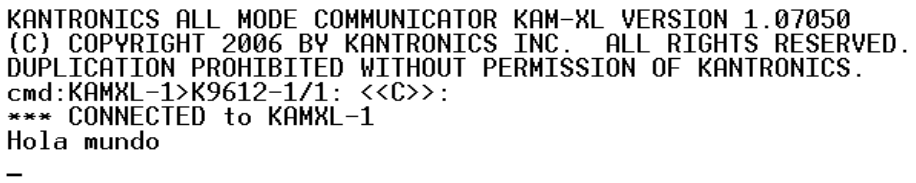
Para las pruebas Back to Back se realiza la configuración anteriormente descrita en un segundo TNC y se establece la conexión entre ellos utilizando la instrucción CONNECT. El resultado es el siguiente:

Figura 56 Establecimiento de la conexión con el TNC B en el TNC A

```
ENTER YOUR CALLSIGN=> kamxl-1
KANTRONICS KPC9612PMX VERSION 9.1
(C) COPYRIGHT 2002-2005 BY KANTRONICS INC.  ALL RIGHTS RESERVED.
DUPLICATION PROHIBITED WITHOUT PERMISSION OF KANTRONICS.
cmd:c k9612-1
cmd:*** CONNECTED to K9612-1
Hola mundo
_
```

Fuente: CINTEL

Figura 57 Establecimiento de la conexión con el TNC A en el TNC B



Fuente: CINTEL

Con este resultado queda concluido el experimento de manera exitosa.

1.1.8 Resumen De Los Resultados

En este experimento se mostró la manera de comunicar un par de TNCs Back to Back para lo que se necesitó elaborar un cable cruzado, también se mostró la manera de configurar el Hyperterminal de Windows para acceder al sistema operativo de los TNC, configurarlos de manera apropiada para poder tener la conexión deseada y transmitir un mensaje entre ellos.

1.1.9 Recomendaciones

En caso de haber ingresado mal el identificador o callsing o necesitar devolver los parámetros de fábrica al TNC se debe ingresar la instrucción RESTORE DEFAULTS con lo cual el TNC inicia la secuencia de sincronización con el PC.

Anexo 8.

Configuración de los radios motorola pro 3100 y pruebas de voz.

CONFIGURACIÓN DE LOS RADIOS MOTOROLA PRO 3100 Y PRUEBAS DE VOZ

1.1.10 Descripción

En este experimento se muestra la forma en que se deben configurar los radios para establecer comunicaciones de voz y datos.

1.1.11 Propósito

Establecer comunicaciones por voz mediante el uso de dos equipos de radio.

1.1.12 Descripción Del Experimento

e. Configuración del radio

f. Pruebas de comunicaciones punto a punto.

1.1.13 Artefactos Creados

Cable TIPO N Macho a mini UHF Macho

1.1.14 Criterio De Terminación

Logro de las comunicaciones por voz entre radios.

1.1.15 Recursos Requeridos

Computador, Radios Motorola Pro 3100, Micrófono, Cable de programación Motorola AARKN4081, Adaptador DB-25 a DB-9, Conversor Serial-USB, Fuente Switchada, cable de poder, Software Professional Radio CPS R06.11.05, Cargas para radio de 50 Ohmios a 75 Watts, Cable TIPO N Macho a mini UHF Macho.

1.1.16 Resultados Del Experimento

Para configurar los radios Motorola Pro 3100 es necesario contar con el cable de programación AARKN4081 que se muestra a continuación:

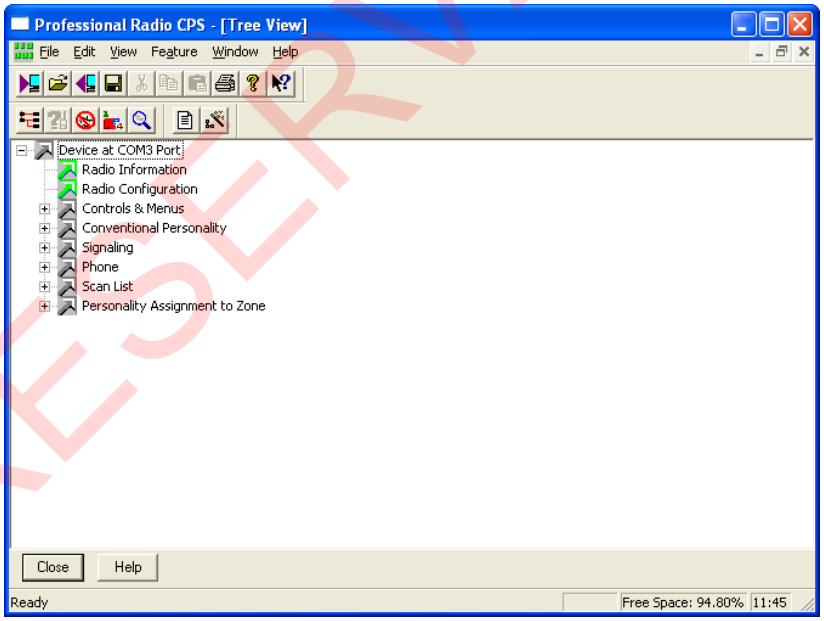
Figura 58 Cable de programación AARKN4081

Fuente: http://cpsmayorista.com/CPS/ACCESORIOS/PRO5100/pro5100%20hardware.htm

El conector RJ-45 se conecta al radio en el puerto del micrófono, el conector DB-25 debe conectarse al adaptador para luego conectar al convertidor serial – USB en el computador.

La configuración de los radios se realiza mediante el programa Professional Radio CPS R06.11.05 suministrado con los radios:

Figura 59 Menú principal en el programa CPS R06.11.05



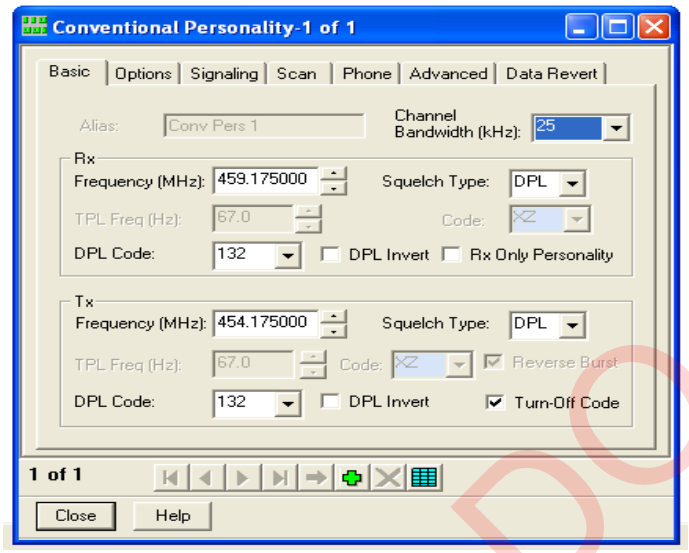
Fuente: CINTEL

Esta pantalla aparecerá luego de dar clic en el icono que tiene una flecha apuntando hacia el computador, el software se encargará de identifica el puerto serial en el computador. A su vez se muestran las diferentes opciones que se pueden modificar para modificar o ingresar valores.

1.1.16.1 Configuración del radio

La configuración de los parámetros básicos se realiza entrando a la opción “Conventional Personality” en donde se encuentran las siguientes opciones:

Figura 60 Configuración de parámetros de transmisión y recepción del radio



Fuente: CINTEL

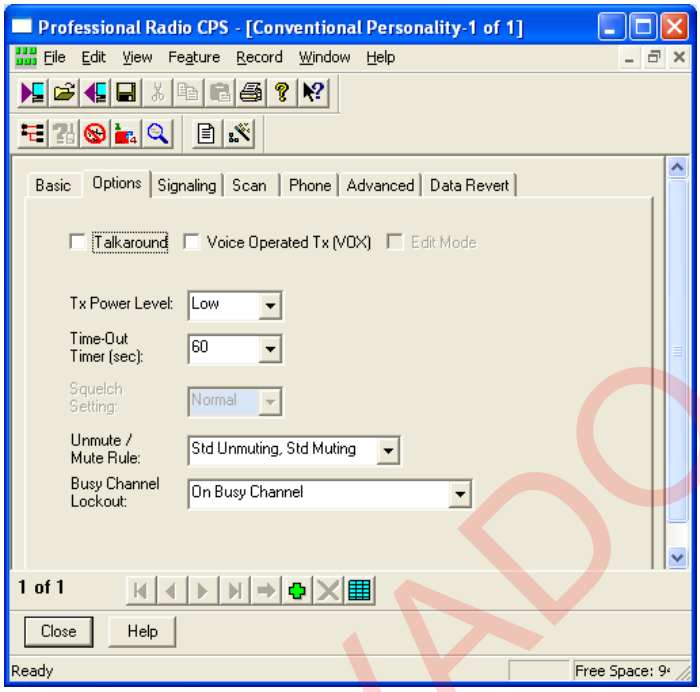
Los parámetros a configurar son los siguientes:

- **Ancho de banda del canal:** 25 kHz.
- **Frecuencia de Recepción:** Habilita la frecuencia de recepción, se establece en 459.175 MHz.
- **Tonos (Squelch Type):** Contiene tres opciones para elegir:
  - ✓ CQS: Trabajar con portadora.
  - ✓ TPL: Tonos Sub-audibles.
  - ✓ DPL: Códigos Digitales.

  Escogemos DPL para nuestro experimento, el código se fija en 132.
- **Frecuencia de Transmisión:** Habilita la frecuencia de transmisión, se establece en 454.175 MHz

En la etiqueta Opciones se muestran los siguientes parámetros:

Figura 61 Configuración de opciones del radio



Fuente: CINTEL

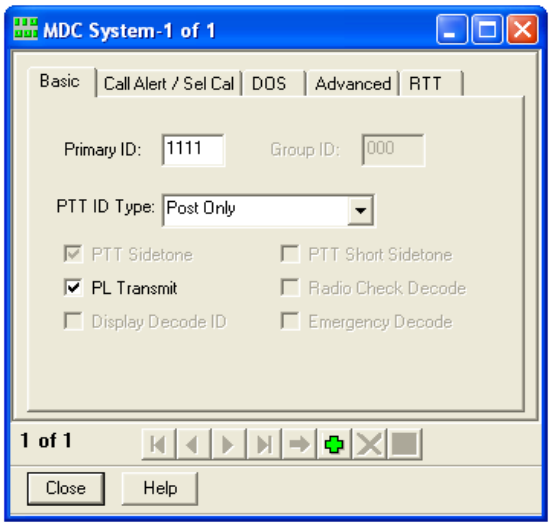
En esta ventana se puede configurar lo siguiente:

Time Out: Este tiempo se configura para evitar que el radio transmita por tiempo indefinido. Se configura en 60 segundos.

Busy Channel Lockout: Este parámetro impide que una conversación sea interrumpida, se elige On Busy Channel.

En el menú principal existe una opción llamada “Señalización”, esta opción se subdivide en MDC System y DTMF System, elegimos MDF System.

Figura 62 Configuración de parámetros MDC



Fuente: CINTEL

En esta ventana se configura los siguientes parámetros:

ID: Selecciona la identificación exclusiva, con uno o cuatro dígitos, que permite reconocer al radio cuando esté en funcionamiento (ya sea transmitiendo o recibiendo llamadas MDC). Se fija en 1111.

PTT ID Type: Selecciona cuándo se envía el ID, existen 4 opciones de configuración:

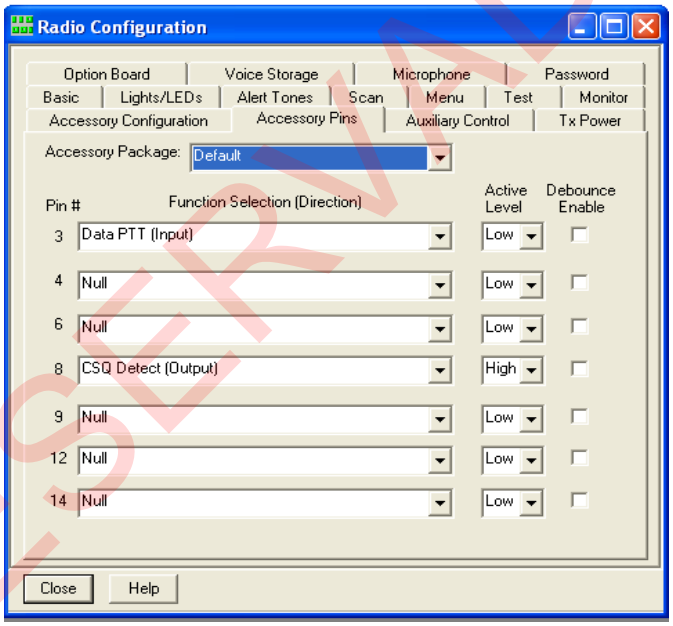
None: No de envía el ID.

Pre Only: Se envía el ID solo al inicio de la cadena de señalización.
Post Only: Se envía el ID solo al final de la cadena de señalización.
Pre & Post: Se envía el ID tanto al inicio como al final de la cadena de señalización.

La señalización se fija en Post Only.

En la pestaña “Accesory Pins”, la configuración consiste en habilitar los pines del puerto auxiliar de la radio, a continuación se describen las opciones de programación de los pines empleados:

Figura 63 Configuración de pines en el puerto de accesorios del radio



Fuente: CINTEL

Pin #3: Corresponde al PTT: Las opciones para configurar este pin son:

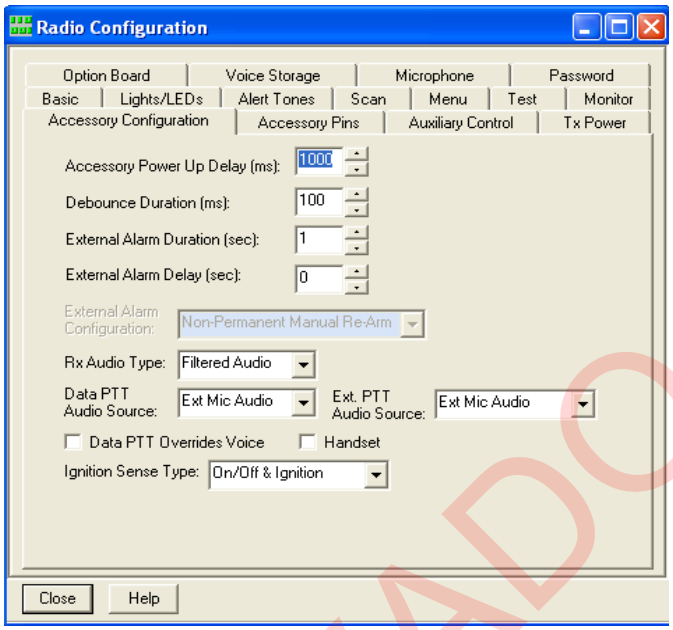
Exterman Mic PTT (input): Habilita al PTT del conector de accesorios (parte posterior de la radio), este parámetro es usadogeneralmente cuando el enlace de radio es solo usaso para transmisión de datos.

Data PTT (input): Esta opción habilita al PTT de la parte posterior de la radio, es usado cuando se necesita pasar datos y voz sobre un mismo enlace de radio.

Este pin se configura como Data PTT.

Por último, en la pestaña “Accesory Configuration”, se debe configurar lo siguiente.

Figura 64 Configuración accesorios del radio



Fuente: CINTEL

Dado que se planea utilizar el radio para transmisión de voz y datos utilizado un TNC se debe configurar el tipo de audio Rx en la opción de filtrado. La fuente de Datos PTT Audio es en este caso Ext Mic Audio al igual que en la opcion Ext PTT Audio Source.

1.1.16.2 Pruebas de comunicaciones punto a punto

Para las pruebas de comunicaciones se configura un segundo radio siguiendo el mismo procedimiento anterior con el único cambio en las frecuencias de transmisión y recepción ya que deben ir cruzadas. Tx = 459.175 MHz y Rx = 454.175 MHz.

Finalmente para poder probar los radios es necesario conectar las cargas de referencia Bird 75-T-FN de 50 Ohmios a 75 Watts que se muestran a continuación:

Figura 65 Carga Bird 75-T-FN

Fuente: Bird Technologies Group

Para esta conexión fue necesario elaborar un cable RG58 con conector TIPO N macho y mini UHF Macho en cada extremo. Teniendo esto en cuenta se procedió a realizar la prueba de voz sin inconvenientes.

1.1.17 Resumen De Los Resultados

Se configuraron los radios Motorola de manera apropiada para el envió de voz y datos de manera compartida.

1.1.18 Recomendaciones

Se debe tener en cuenta si es necesario configurar si el tipo de audio recibido es filtrado o no filtrado al momento de transmitir voz, datos o ambos.

Para la transmisión a grandes distancias se puede ajustar el nivel de potencia de los radios.

Anexo 9.

Enlace de radio para transmisión de voz y datos utilizando TNCs (multimodems)

ENLACE DE RADIO PARA TRANSMISIÓN DE VOZ Y DATOS UTILIZANDO TNCS (MULTIMODEMS)

1.1.19 Descripción

Prueba de transmisión de voz y datos utilizando TNCs y Radios

1.1.20 Propósito

Lograr la transmisión simultánea de voz y datos por medio de un enlace de radio.

1.1.21 Descripción Del Experimento

a) Elaboración del cable de datos para transmisión por radio
b) Configuración del TNC KAM-XL
c) Pruebas de transmisión.

1.1.22 Artefactos Creados

Cables de datos para transmisión por radio.

1.1.23 Criterio De Terminación

Logro de las transmisiones por medio de un enlace de radio.

1.1.24 Recursos Requeridos

Computador, Radios Motorola Pro 3100, Micrófono, Adaptador DB-25 a DB-9, Conversor Serial-USB, Fuente Switchada, cable de poder, Cargas para radio de 50 Ohmios a 75 Watts, Cable TIPO N Macho a mini UHF Macho, TNCs Kantronics 9612 plus y KAM-XL, cables de datos para transmisión por radio.

1.1.25 Resultados Del Experimento

La operación de una estación que forma parte de un sistema de radio paquete es transparente al usuario final, en este caso, lo que el usuario hace es conectarse a la otra estación, seleccionar la información a enviar y la cual se envía automáticamente.

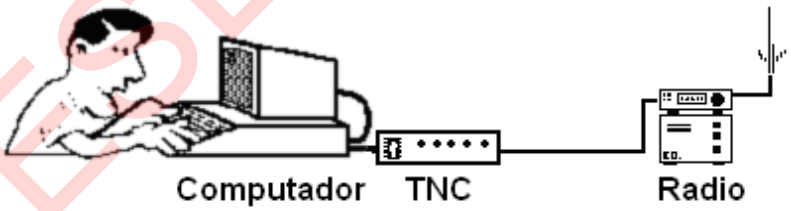
El TNC acepta información proveniente del computador o terminal ASCII y divide los datos en partes más pequeñas llamadas paquetes. Además de la información que proviene del computador, cada paquete contiene direccionamiento, chequeo de errores e información de control. La información de direccionamiento incluye el nombre de la estación origen, así como el nombre de la estación destino del paquete. La dirección puede incluir el nombre de las estaciones que funcionan como repetidoras.

Los datos a ser transmitidos se almacenan en el TNC y se envían como ráfagas o paquetes de información después de ser segmentados. La segmentación de los datos en partes pequeñas permite a algunos usuarios compartir la frecuencia de transmisión. El campo de dirección permite a cada usuario del TNC, separar los paquetes dirigidos hacia ellos, de los paquetes dirigidos hacia otros. La dirección también le permite a los paquetes ser distribuidos a través de varias estaciones antes de que alcancen su destino final.

Al recibir el paquete, el TNC decodifica el mensaje, lo chequea en caso de errores y luego envía un el mensaje recibido (ACK). El sistema de comunicación por Radio paquete provee una transmisión libres de errores debido a los esquemas de detección de errores empleados al construir el mensaje. Un paquete es chequeado al ser recibido y desplegado siempre y cuando no posea errores. Los datos que poseen errores no se pierden, porque son reenviados desde el origen hasta que lleguen sin errores

Los equipos requeridos para la conformación de una estación de comunicación por radio paquetes son un computador o terminal, un TNC y un radio transceptor (Ver Figura 66).

Figura 66 Estación de comunicación por Packet Radio



Fuente: Manual TNC Kantronics KAM-XL

A continuación se describe cada uno de estos componentes:

TNC (*Terminal Node Controller*): Dispositivo ubicado entre el computador y el radio., que funciona tanto en la capa física del Modelo OSI (*Open System Interconnection*), como en la Capa de Enlace de Datos. Este dispositivo ofrece una transferencia libre de errores entre cualquier dispositivo digital: computadores, terminales. Lectoras de códigos de barrar. GPS, etc. Contiene el software para controlar las transmisiones desde y hacia la estación y un módem que convierte los datos provenientes desde el computador en tonos AFSK, para poder transmitirlos. También se encarga de recuperar los datos a partir de los tonos que son recibidos por la radio y enviárselos al computador. Implementa el estándar RS-232 para la comunicación con el computador y el protocolo usado por radio paquete. EL protocolo de radio paquete permite al TNC ensamblar un paquete de datos recibidos desde el computador, realiza un cálculo para chequeos de error (CRC), modularlo en una frecuencia de audio y lo transmite a través del radio. También lleva a cabo el proceso inverso, es decir, demodula las señales

recibidas recuperando los datos del paquete, verifica si existen errores y envía un acuse de recibo si el paquete no contiene errores, caso contrario el paquete es retransmitido por el origen.

Computador o terminal: Es la interfaz con la que interactúa el usuario para transmitir y recibir información. Puede usarse un computador corriendo un programa emulador de terminal, un programa específico para radio paquete u otro tipo de equipos terminales como GPS o sensores.

Radio: medio a través del cual se envía la información.

Radio paquete, a diferencia de las comunicaciones de voz, puede soportar múltiples conversaciones sobre la misma frecuencia al mismo tiempo, ya que se comparte el canal de transmisión en el tiempo. Eso no quiere decir que no se produzcan colisiones, las transmisiones ocurren cuando no existe ninguna conversación en el canal. Radio paquete usa un protocolo llamado AX.25 para compartir el canal. AX.25 especifica que el acceso al canal se basa en el Acceso Múltiple por Sensado de Portadora (CSMA, *Carrier Sense Multiple Access*), por lo cual cuando una estación quiere transmitir, el TNC monitorea el canal para ver si alguien más está transmitiendo; si está libre envía el paquete y todas las demás estaciones lo escuchan y no transmiten hasta que haya completado el envío del paquete a la estación a la cual va dirigido. Si llegase a producirse una colisión, porque 2 estaciones transmiten simultáneamente, ningún TNC recibirá el paquete que envió y cada uno de ellos tendrá que esperar un tiempo aleatorio para reenviarlo.

AX.25 es considerado el protocolo estándar por defecto para radio aficionados. AX.25 fue desarrollado en 1970 y está basado en el protocolo X.25. Debido a las diferencias en el medio de transporte (radio vs. cable) y en los esquemas de direccionamiento, X.25 fue modificado a los requerimientos de los radio aficionados. Una de las ventajas de AX.25 es que cada paquete enviado contiene el nombre de la estación que origina y el nombre de la estación que recibe el paquete, dando identificación a las estaciones con cada transmisión.

Todos los Kantronics TNC pueden operar sin un computador conectado, una vez que han sido configurados. Por ejemplo, el TNC K-9612 Plus puede recibir y almacenar mensajes en un buzón de correo. También TNC K-9612 Plus puede servir como una estación de relevo para otras estaciones. La independencia del computador es posible gracias que e TNC tiene la inteligencia necesaria para realizar estas funciones, una vez que sea apropiadamente configurado y enlazado al transceptor.

CONFORMACIÓN DE UNA ESTACIÓN DE RADIO PAQUETES CON EL TNC K-9612 PLUS

El diagrama de la Figura 44 se muestra como se deben conectar el TNC K-9612 Plus al computador y al transceptor o radio para la conformación de una estación de para la comunicación por radio paquetes. A continuación se describen los conectores y cables usados en esta configuración:

Conexión del TNC al Computador: En la prueba de concepto se usaron los siguientes elementos para la conexión del puerto *Computer* del TNC K-9612 Plus al puerto serial Computador, donde el computador se usa tanto para la configuración del TNC y como Equipo Terminal de Datos (DTE, *Data Terminal Equipment*):

- Conversor DB-25 hembra a DB-9 hembra
- Cable serial directo con conectores DB-9 hembra y macho
- Cable conversor USB a serial DB-9 macho

Conexión del TNC al Radio : En la prueba de concepto se usaron los siguientes elementos para la conexión del puerto de baja velocidad (*Port 1*) del TNC K-9612 Plus al conector de accesorios del radio Motorola PRO 3100, donde el radio se usa como transceptor de los paquetes AX.25 para la comunicación con otras estaciones:

Cable con conector DB-9 macho y con *jack* para micrófono y *plug* para parlante

Cable con conector para el puerto de accesorio del radio Motorola PRO 3100 y *plug* para micrófono y *jack* para parlante.

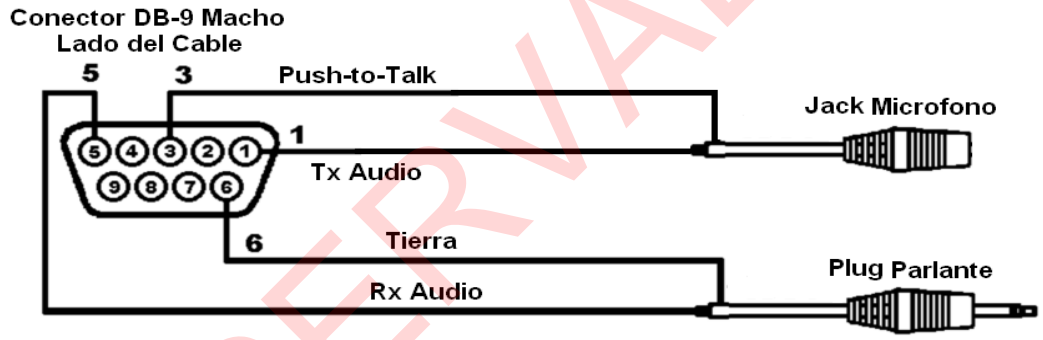
La conexión con el puerto de alta velocidad (*Port 2*) se realiza con los mismos elementos pero cambiando el conector DB-9 macho a DB-15 macho.

1.1.25.1 Elaboración del cable de datos para transmisión por radio

CONEXIÓN DEL TNC K-9612 PLUS POR EL PUERTO DE BAJA VELOCIDAD (Port 1)

Para la elaboración del cable de conexión del TNC K-9612 Plus al radio Motorola PRO 3100 a través del puerto de baja velocidad (*Port 1*) se siguió la disposición de pines del conector DB-9 macho y su conexión con el *jack* del micrófono y el *plug* del parlante como la mostrada en la Figura 67 Cable de conexión del TNC K-9612 Plus al radio Motorola PRO 3100.

Figura 67 Cable de conexión del TNC K-9612 Plus al radio Motorola PRO 3100



Fuente: Manual TNC Kantronics 9612 plus

En la tabla 1 se puede ver la relación de pines entre el conector DB-9 del puerto de baja velocidad (*Port 1*) del TNC K-9612 Plus y el conector de accesorios del radio Motorola PRO 3100

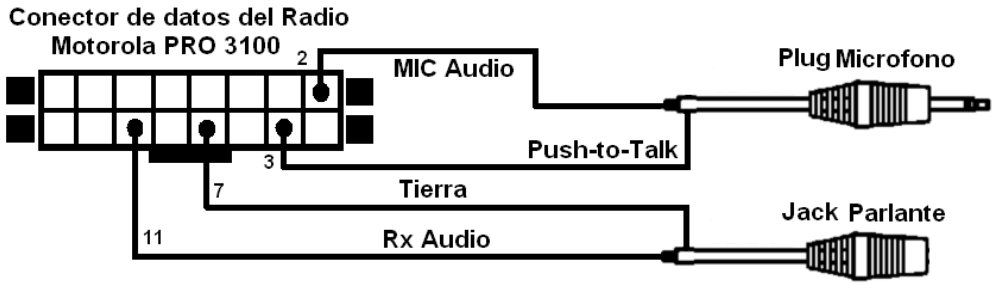
Tabla 20 Conexión entre TNC K-9612 Plus (*Port 1*) y el radio Motorola PRO 3100

Conector DB-9 Macho TNC		**Conector de Accesorios Radio**	
Pin 1	Tx Audio	Pin 2	MIC Audio
Pin 3	Push-to-Talk	Pin 3	Push-to-Talk
Pin 5	Rx Audio	Pin 11	Rx Audio
Pin 6	Tierra	Pin 7	Tierra

Fuente: Manual TNC Kantronics 9612 plus

El radio Motorola PRO 3100 tiene un conector de accesorios de 20 pines, sin embargo las conexiones se realizaron con un conector de 16 pines obviando los 4 pines de los extremos. En la Figura X se puede observar la disposición de pines del conector de accesorios del radio Motorola PRO 3100 y su conexión con el plug del micrófono y el *jack* del parlante.

Figura 68 de conexión del radio Motorola PRO 3100 al TNC K-9612 Plus



Fuente: CINTEL

CONEXIÓN DEL TNC K-9612 PLUS POR EL PUERTO DE ALTA VELOCIDAD (Port 2)

En la tabla X se puede ver la relación de pines entre el conector DB-9 del puerto de alta velocidad (*Port 2*) del TNC K-9612 Plus y el conector de Accesorio del radio Motorola PRO 3100.

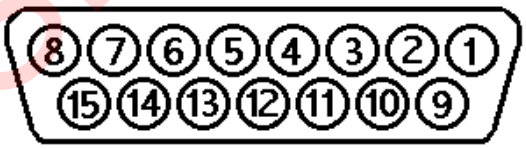
Tabla 21 Conexión entre TNC K-9612 Plus (*Port 2*) y el radio Motorola PRO 3100

Conector DB-15 Macho		**Conector de Accesorios Radio**	
Pin 1	Push-to-Talk	Pin 3	Push-to-Talk
Pin 2	Rx Data	Pin 11	Rx Audio
Pin3	Tx Data	Pin 2	MIC Audio
Pin 11	Tierra	Pin 7	Tierra

Fuente: Manual TNC Kantronics 9612 plus

La disposición de pines del conector DB-15 del puerto de alta velocidad (*Port 2*) del TNC K-9612 Plus se muestra en la figura X.

Figura 69 Cable de conexión del radio Motorola PRO 3100 al TNC K-9612 Plus



Fuente: CINTEL

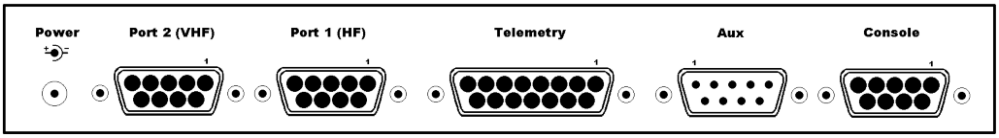
La conexión del puerto de alta velocidad (*Port 2*) del TNC K-9612 Plus y el radio Motorola PRO 3100 se realiza con los mismos elementos del puerto de baja velocidad (*Port 2*) y que presentado en los literales anteriores pero cambiando el conector DB-9 macho a DB-15 macho.

1.1.25.2 Configuración del TNC KAM-XL

PUERTOS DEL TNC KAM-XL

Como se muestra en la Figura 70, el TNC KAM-XL tiene diferentes puertos para conectarlo a un transceptor o radio, al un computador (a un dispositivo GPS), a un dispositivo de telemetría y uno para la fuente de poder.

Figura 70 Puertos del TNC KAM-XL



Fuente: Manual TNC Kantronics KAM-XL

A continuación se describe el propósito de los 6 puertos:

- ***Power jack* (2.1 mm):** Este conector está dispuesto para aplicar una fuente de poder externa (5.5 V a 25 V dc). El centro del conector es positivo y el borde es negativo (tierra).

- ***Port 1* (conector DB-9 hembra):** Para conectar el TNC KAM-XL al conector de accesorios del radio. Soporta una operación de transmisión de paquetes de 4800/9600/19200 baudios.

- ***Port 2* (conector DB-9 hembra):** Para conectar el TNC KAM-XL al conector de accesorios del radio. Soporta una operación de transmisión de paquetes de 1200 baudios.

- ***Telemetry* (conector DB-15 hembra):** Usado como entrada analógica de dispositivos de sensores externos usados para telemetría, y también dos líneas de salida para control.

- ***Aux* (conector DB-9 hembra):** Es un puerto RS-232 de tipo DTE, para entrada de datos de un receptor GPS (o dispositivo similar) o para comunicación RS-232 a otro dispositivo.

- ***Console* (conector DB-25 hembra):** Para conectar el TNC KAM-XL al puerto serial del computador. Este puerto utiliza el estándar RS-232 usando códigos de caracteres ASCII para todos los comandos configuración.

En la conexión del TNC KAM-XL por los puertos *Port 1* y *Port 2* al conector de accesorios del radio Motorola PRO 3100 se usaron los cables descritos para la conexión del puerto de baja velocidad (*Port 1*) del TNC K9612 Plus.

En los TNCs KAM-XL es necesario configurar, aparte de las opciones vistas en el experimento 1, las siguientes opciones al hacer la transmisión de datos utilizando los radios:

Tabla 22 Comandos de configuración del TNC KAM-XL

hbaud	1200/9600
echo	off
port	|1a
paclen	255
maxframe	4
slottime	10
txdelay	50 (500ms)
dwait	18 (180ms)

Fuente: CINTEL

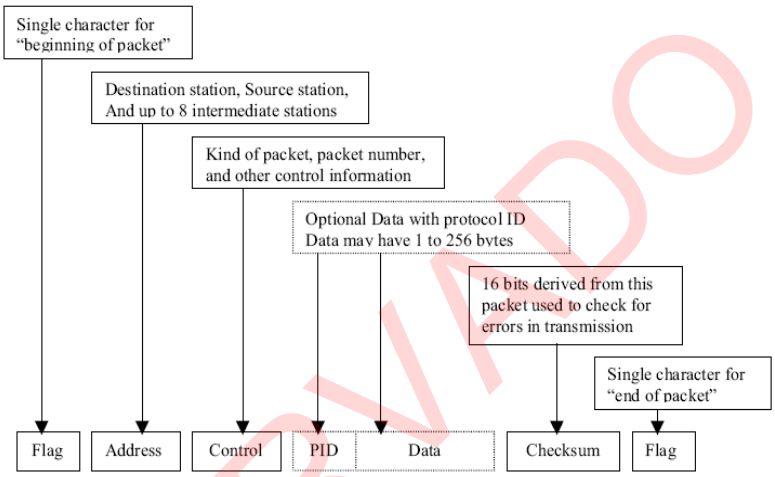
HBAUD: Determina la velocidad con la que se transmiten los datos por el puerto 1 (HF: 1200bps) o puerto 2 (VHF: 4800/9600 baudios).

ECHO: Reenvía los datos que transmite el TNC hacia el terminal al cual este conectado, Se debe desactivar al enviar datos ya que se pueden generar errores en la transmisión.

PORT: |nx donde n corresponde al puerto (1 o 2), x corresponde al canal (en este caso a).

PACLEN: Determina la longitud máxima del paquete. En la siguiente figura se muestra como está compuesto un paquete AX25 en el TNC.

Figura 71 Organización del paquete AX.25



Fuente: Manual TNC Kantronics 9612 plus

MAXFRAME: Determina el número máximo de paquetes en una transmisión sin recibir ACK.

SLOTTIME: Especifica la cantidad de tiempo en incrementos de 10ms entre sucesivos intentos del algoritmo de persistencia.

TXDELAY: Especifica el tiempo que espera el TNC cuando la aplicación envía una solicitud PTT y el inicio de la transmisión, en nuestro caso este es el tiempo que se debe esperar para que el radio energice la antena antes de transmitir.

DWAIT: Define el tiempo de espera tras una colisión de paquetes.

1.1.25.3 Pruebas de transmisión

Finalmente se comprobó el enlace enviando tanto un mensaje de texto por el Hyperterminal de la manera en que se mostró él en experimento 1 como por la interfaz diseñada para el proyecto enviando texto, imágenes y voz.

1.1.26 Resumen De Los Resultados

Se identificaron los pines a utilizar en el puerto de accesorios del radio.

A su vez se elaboró el cable de datos para la transmisión de datos del TNC hacia el radio.

También se configuro el TNC KAM-XL para su funcionamiento en conjunto con los radios.

Finalmente se logró exitosamente la transmisión de voz y datos con la topología sugerida.

1.1.27 Recomendaciones

Dado que se está trabajando a bajas velocidades la transmisión de imágenes de buena calidad es demasiado lenta. Es posible manejar una velocidad mayor en la transmisión de datos configurando los TNCs para tener salida por el puerto VHF y en consecuencia tener mayor ancho de banda.

Anexo 10.

Script elaborado para configuración automática de módems, desde el software del Data Link.

```
void Form1::OnModem()
{
	try
	{
		String^ Salida;
		Salida = "\x03 \x03 \x03 \xd";//modo cmd
		this->serialPort1->Write(Salida);
		Thread::Sleep(1000);

		Salida = "reset \xd"; // reset del modem
		this->serialPort1->Write(Salida);
		Thread::Sleep(1000);

		Salida = "my " + sNI + "\xd";//configura el NI en el modem
		this->serialPort1->Write(Salida);
		Thread::Sleep(1000);

		Salida = "port 2 \xd";//el puerto utilizado es el de VHF
		this->serialPort1->Write(Salida);
		Thread::Sleep(100);

		Salida = "txd 60/60 \xd";// retardo al PTT de (60*30ms= 1800ms)
		this->serialPort1->Write(Salida);
		Thread::Sleep(100);

		Salida = "sl 40/40 \xd";// retardos (40*10ms) entre sucesivos
					//intentos del algoritmo de persistencia
		this->serialPort1->Write(Salida);
		Thread::Sleep(100);

		Salida = "hb "+ sVelocidad + "/" + sVelocidad +"xd";
				// Velocidad del  modem
		this->serialPort1->Write(Salida);
		Thread::Sleep(100);

		Salida = "in T \xd";// interface Terminal
		this->serialPort1->Write(Salida);
		Thread::Sleep(100);

		Salida = "cono on \xd";// ACK automatico
		this->serialPort1->Write(Salida);
		Thread::Sleep(100);

		Salida = "cr on \xd";// envio paquetes con CR
		this->serialPort1->Write(Salida);
		Thread::Sleep(100);

		Salida = "xmitl 50/50 \xd";//nivel de señal de salida modem
		this->serialPort1->Write(Salida);
		Thread::Sleep(100);

		Salida = "ec off \xd";// eco off del modem
		this->serialPort1->Write(Salida);
		Thread::Sleep(100);

		Salida = "maxf 4/4 \xd";// número máximo en que se puede
					//fraccionar un paquete
		this->serialPort1->Write(Salida);
		Thread::Sleep(100);
```

```
                Salida = "pacl 255/255 \xd";// número máximo de caracteres
                                            //en una fracción
                this->serialPort1->Write(Salida);
                Thread::Sleep(100);

                Salida = "retry 1 \xd"; //número que paquetes que
                                        //requieren ACK al transmitir
                this->serialPort1->Write(Salida);
                Thread::Sleep(100);

                if (Unidades->leerNodo(miItem)->Rol == "1")
                {
                       //Código para estación Controladora
                       Salida = "users "+cantidadUnidades+" \xd";// cantidad de
                                                    // Conexiones simultaneas
                       this->serialPort1->Write(Salida);
                       Thread::Sleep(100);
                       this->button4->Enabled = false;
                       this->LB_rol->Text = L"CONTROLADORA";
                }

                else
                {
                       //Código para estación Participante
                       Salida = "users 1 \xd";
                       this->serialPort1->Write(Salida);
                       Thread::Sleep(100);
                       this->button4->Enabled = true;
                       this->LB_rol->Text = L"PARTICIPANTE";
                }

                Salida = " \xd";
                this->serialPort1->Write(Salida);
                Thread::Sleep(100);
        }

         catch (Exception^ e)
        {
                this->BT_mensajesSistema->Text = L"Error: No se pudo configurar el
                modem";
        }
}
```