



**ESPE**  
UNIVERSIDAD DE LAS FUERZAS ARMADAS  
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y  
TELECOMUNICACIONES**

**CARRERA DE INGENIERÍA EN ELECTRÓNICA Y  
TELECOMUNICACIONES**

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL  
TÍTULO DE INGENIEROS EN ELECTRÓNICA Y  
TELECOMUNICACIONES**

**TEMA: “DIAGNÓSTICO Y DESARROLLO DEL SISTEMA DE  
JAMMING PARA LA AGRUCOMGE”**

**AUTORES: ACEVEDO HEREDIA, LUIS MIGUEL**

**RECALDE CHÁVEZ, CHRISTIAN OSWALDO**

**DIRECTOR: M.Sc. LEÓN VÁSQUEZ, RUBÉN DARÍO**

**APOYO: Dr. TINOCO SALAZAR, ALEXIS FABRICIO**

**SANGOLQUÍ**

**2019**

**CERTIFICACIÓN****DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y  
TELECOMUNICACIONES****CARRERA DE INGENIERÍA EN ELECTRÓNICA Y  
TELECOMUNICACIONES****CERTIFICACIÓN**

Certifico que el trabajo de titulación, “**DIAGNÓSTICO Y DESARROLLO DEL SISTEMA DE JAMMING PARA LA AGRUCOMGE**” realizado por los señores **LUIS MIGUEL ACEVEDO HEREDIA Y CHRISTIAN OSWALDO RECALDE CHÁVEZ**, ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la **UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE**, razón por la cual me permito acreditar y autorizar para que sustenten públicamente.

Sangolquí, 09 de julio del 2019

Firma

Rubén Darío León Vásquez, M.Sc.

**DIRECTOR DE PROYECTO**

## ACTA DE RESPONSABILIDAD



### DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

### CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

#### AUTORÍA DE RESPONSABILIDAD

Nosotros, LUIS MIGUEL ACEVEDO HEREDIA con cedula de identidad N° 1716592579 y CHRISTIAN OSWALDO RECALDE CHÁVEZ con cedula de identidad N° 1720737822 declaramos que el contenido, ideas y criterios del trabajo de titulación, “**DIAGNÓSTICO Y DESARROLLO DEL SISTEMA DE JAMMING PARA LA AGRUCOMGE**” es de nuestra autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente declaramos que este trabajo es de nuestra autoría, en virtud de ello nos declaramos responsables del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 09 de julio del 2019

Firma

Luis Miguel Acevedo Heredia

C.C: 1716592579

Christian Oswaldo Recalde Chávez

C.C: 1720737822

## AUTORIZACIÓN

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y  
TELECOMUNICACIONESCARRERA DE INGENIERÍA EN ELECTRÓNICA Y  
TELECOMUNICACIONES

## AUTORIZACIÓN

Nosotros, **LUIS MIGUEL ACEVEDO HEREDIA** y **CHRISTIAN OSWALDO RECALDE CHÁVEZ**, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca virtual de la institución el presente trabajo de titulación, “**DIAGNÓSTICO Y DESARROLLO DEL SISTEMA DE JAMMING PARA LA AGRUCOMGE**” cuyo contenido, ideas y criterios son de nuestra autoría y responsabilidad.

Sangolquí, 09 de julio del 2019

Luis Miguel Acevedo Heredia

C.C: 1716592579

Christian Oswaldo Recalde Chávez

C.C: 1720737822

## DEDICATORIA

*Queremos dedicar el trabajo de investigación presente a nuestras familias, quienes nos han acompañado siempre en cada etapa de la vida.*

*A nuestros queridos padres quienes supieron darnos siempre su apoyo, guía y ánimo en cualquier circunstancia, y también por todo el amor y los buenos consejos que nos han sabido dar para poder seguir adelante en cada situación a lo largo de los estudios, este proyecto es la cúspide de una etapa de trabajo duro, el cual mediante dedicación y esfuerzo se ha logrado alcanzar.*

*A nuestros amigos y amigas, los cuales durante todos los años de carrera siempre nos hemos apoyado para seguir adelante y no desfallecer y que ahora son profesionales de calidad.*

## AGRADECIMIENTO

Agradecemos a todos los docentes que durante cada fase de nuestra etapa universitaria nos han proporcionado desinteresadamente y con mucha paciencia sus conocimientos y habilidades, las cuales nos serán de gran utilidad para la vida profesional y nos permitirán construir un futuro mejor para nuestra sociedad.

Agradecemos de manera especial al Ingeniero Rubén León y al Ingeniero Alexis Tinoco ya que, sin sus colaboraciones, sin sus saberes y sin sus experiencias la realización de este proyecto no hubiese llegado a buen puerto ni se hubiese alcanzado los objetivos del mismo.

Agradecemos a su vez también al personal militar y civil que conforman el Centro de Investigación de Aplicaciones Militares (CICTE), así como al Agrupamiento de Comunicaciones y Guerra Electrónica (AGRUCOMGE), que contribuyeron para que el presente proyecto pueda haberse llevado a cabo con éxito.

Miguel Acevedo y Christian Recalde

## ÍNDICE DE CONTENIDOS

CERTIFICACIÓN.....	i
ACTA DE RESPONSABILIDAD.....	ii
AUTORIZACIÓN.....	iii
DEDICATORIA.....	iv
AGRADECIMIENTO.....	v
ÍNDICE DE CONTENIDOS.....	vi
ÍNDICE DE TABLAS.....	viii
ÍNDICE DE FIGURAS.....	ix
RESUMEN.....	xii
ABSTRACT.....	xiii
CAPÍTULO 1.....	1
1.1. Antecedentes.....	1
1.2. Justificación e Importancia.....	2
1.3. Alcance del Proyecto.....	2
1.5. Objetivos.....	3
1.5.1. Objetivo General.....	3
1.5.2. Objetivos Específicos.....	3
CAPÍTULO 2.....	5
2. FUNDAMENTO TEÓRICO.....	5
2.1 Propagación de RF.....	5
2.2.1 Clasificación por ancho de banda.....	7
2.2.1.1 Interferencia del tipo barrera (Barrage Jamming).....	7
2.2.1.2 Interferencia puntual (Spot Jamming).....	7

2.2.1.3 Interferencia tipo barradura (Sweep Jamming).....	7
2.2.2 Métodos de interferencia.....	8
2.2.2.1 Interferencia constante (Jamming Constante).....	8
2.2.2.2 Interferencia reactiva o Jamming reactivo.....	8
2.2.3 Tipos de antenas.....	9
2.2.3.1 Antenas Omni-direccionales.....	9
2.2.3.2 Antenas Direccionales.....	10
CAPÍTULO 3.....	12
3. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA.....	12
3.1 Diseño general del sistema.....	13
3.2 Revisión y puesta en marcha del <i>Amplifier Research</i> de 500 watt para la banda de 10 kHz a 100 MHz.....	16
3.2.1 Fuentes de Alimentación.....	17
3.2.3 Etapa de amplificación de potencia.....	28
3.3 Revisión y reparación del amplificador de 200 (W) de 80 – 1000MHz.....	35
3.3.1 Etapa de pre amplificación.....	36
3.3.1.1 Fuente de alimentación:.....	36
3.3.1.2. Circuito de Control.....	37
3.3.1.3. Driver y amplificador:.....	39
3.3.1.4. Etapa final de potencia:.....	40
3.3.2. Fuentes de alimentación:.....	41
3.3.3. Amplificador de potencia:.....	42
3.4. Utilización del Generador de señales Rohde&Schwarz.....	44
3.5. Utilización de una interfaz gráfica.....	46

3.5. Verificación de las antenas de 20 – 100 MHz y de 80 – 1000MHz.....	48
CAPÍTULO 4.....	51
4. PRUEBAS DE FUNCIONAMIENTO.....	51
CAPÍTULO 5.....	73
5. CONCLUSIONES Y RECOMENDACIONES.....	73
6. BIBLIOGRAFÍA.....	74

## ÍNDICE DE TABLAS

<b>Tabla 1</b> <i>Fuentes de alimentación</i> .....	16
<b>Tabla 2:</b> <i>Verificación del funcionamiento del driver</i> .....	22
<b>Tabla 3:</b> <i>Comprobación de ganancia del driver y el preamplificador</i> .....	22
<b>Tabla 4</b> <i>Verificación del funcionamiento de las etapas de potencia</i> .....	27
<b>Tabla 5</b> <i>Potencia de salida versus frecuencia de operación (0 dBm entrada)</i> .....	42
<b>Tabla 6</b> <i>Potencia de Salida versus Frecuencia de Operación</i> .....	44

## ÍNDICE DE FIGURAS

<b>Figura 1</b> Elementos básicos de un sistema de transmisión de RF.....	7
<b>Figura 2</b> Principales planos de irradiación de una antena monopolo. En a) se ilustra la propagación de las ondas electromagnéticas de forma omni-direccional, en el plano horizontal, y b) el comportamiento direccional en el plano vertical.....	10
<b>Figura 3</b> Ilustración que muestra la capacidad de concentración la energía irradiada por la antena parabólica en el plano horizontal ( $\approx 5^\circ$ ) y en el plano vertical ( $\approx 4^\circ$ ).....	11
<b>Figura 4</b> Diseño general del sistema.....	13
<b>Figura 5</b> Amplificador de potencia de 500 watts para la banda de 10 kHz a 100 MHz marca Amplifier Research.....	14
<b>Figura 6</b> Amplificador de potencia de 200 watts para la banda de 80 MHz a 1000 MHz marca Amplifier Research.....	15
<b>Figura 7</b> Generador de señales.....	15
<b>Figura 8</b> Antenas direccionales de los amplificadores.....	16
<b>Figura 9</b> Aplicación - Interface para el usuario con el generador de señales.....	16
<b>Figura 10</b> Desmontaje de la carcasa protectora de ruido o aisladora de interferencias del Amplifier Research de 500 watts en la banda de 10kHz – 100MHz.....	17
<b>Figura 11</b> Limpieza de los bloques de acondicionamiento, pre amplificación y amplificador de potencia del sistema.....	18
<b>Figura 12</b> Revisión de la Fuente de alimentación.....	19
<b>Figura 13</b> Circuito de activación de la fuente de 36 voltios.....	20
<b>Figura 14</b> Prueba del funcionamiento de la fuente de 28 voltios con una carga de 10 ohm.....	21
<b>Figura 15</b> Prueba del funcionamiento de la fuente de 36 voltios con una carga de 10 ohm.....	22
<b>Figura 16</b> Etapas de funcionamiento del amplificador.....	22
<b>Figura 17</b> Fotografía de la tapa de pre amplificación.....	23
<b>Figura 18</b> Fotografía del circuito del Driver.....	24
<b>Figura 19</b> Gráfica del generador de señales conectado a la entrada del driver.....	25
<b>Figura 20</b> Analizador Espectros a la salida del driver, con un atenuador de 40 dB.....	26
<b>Figura 21</b> Ganancia y potencia de entrada y salida del preamplificador con el driver con atenuador de 40 dB.....	29

<b>Figura 22</b> Etapa de amplificación de potencia.....	30
<b>Figura 23</b> Etapa de control.....	31
<b>Figura 24</b> Desmontaje del panel de control.....	32
<b>Figura 25</b> Potencia de salida de una etapa de potencia.....	33
<b>Figura 26</b> Fotografías que ilustran la avería del conector de salida tipo N.....	35
<b>Figura 27</b> Conector tipo N nuevo y conectado.....	36
<b>Figura 28</b> Fuente reguladora 24(V).....	37
<b>Figura 29</b> Fuente principal 20 V.....	38
<b>Figura 30</b> Ruptura pin 10.....	39
<b>Figura 31</b> Reparación del pin 10.....	39
<b>Figura 32</b> Etapa final de pre-amplificación.....	41
<b>Figura 33</b> Conector D-sub reemplazado.....	42
<b>Figura 34</b> Fuente regulada deshabilitada.....	43
<b>Figura 35</b> Sub-etapa de amplificación averiada.....	44
<b>Figura 36</b> Señal desconectada en acoplador.....	45
<b>Figura 37</b> Generador conectado con comunicación serial.....	46
<b>Figura 38</b> Generador activado la modulación FM mediante comunicación serial.....	46
<b>Figura 39</b> Generador activado la modulación AM mediante comunicación serial.....	46
<b>Figura 40</b> Conectores para salida e ingreso de señales a ser moduladas.....	47
<b>Figura 41</b> Código de comunicación serial y conexión con el puerto.....	48
<b>Figura 42</b> Esquema de comunicación entre el generador SML01 y el computador.....	49
<b>Figura 43</b> Interfaz de usuario desarrollada para controlar el generador SML01.....	49
<b>Figura 44</b> Dipolos de la antena de VHF.....	50
<b>Figura 45</b> Tornillos de fijación de los dipolos de la antena de HF.....	50
<b>Figura 46</b> Fotografías del conector tipo N de la antena de 20 – 100 MHz. En (a) conector dañado y en (b) conector sustituido.....	51
<b>Figura 47</b> Escenario prueba de funcionamiento amplificador de 10 kHz – 100 MHz.....	52
<b>Figura 48</b> Potencia de Salida amplificador 10 kHz - 100 MHz.....	54
<b>Figura 49</b> Escenario prueba de funcionamiento amplificador de 80 MHz – 1000 MHz.....	54
<b>Figura 50</b> Potencia de Salida amplificador AR 200W1000C.....	56

<b>Figura 51</b> Escenario Jamming a receptor de prueba a 2m de altura.....	57
<b>Figura 52</b> Escenario Jamming a receptor de prueba a 2m de altura.....	58
<b>Figura 53</b> Cobertura del campus prueba a 2m de altura.....	58
<b>Figura 54</b> Escenario Jamming a receptor FM a 5,5m de altura.....	59
<b>Figura 55</b> Antena de transmisión a 5,5m de altura, amplificador de 10 kHz – 100 MHz.....	60
<b>Figura 56</b> Cobertura del campus prueba a 5,5m de altura, banda de 10 – 1000MHz.....	60
<b>Figura 57</b> Escenario Jamming a receptor de prueba a 15 m de altura.....	60
<b>Figura 58</b> Cobertura del campus prueba a 15m de altura.....	61
<b>Figura 59</b> Sistema de monitoreo de señales COMINT.....	62
<b>Figura 60</b> Señal objetivo COMINT prueba 01.....	63
<b>Figura 61</b> Señal objetivo Jamming COMINT prueba 01.....	64
<b>Figura 62</b> Señal objetivo COMINT prueba 02.....	64
<b>Figura 63</b> Señal objetivo Jamming COMINT prueba 02.....	65
<b>Figura 64</b> Parámetros de la señal de jamming.....	66
<b>Figura 65</b> Sistema ELBIT interferido.....	67
<b>Figura 66</b> Capacitación: Escenario de equipos.....	67
<b>Figura 67</b> Capacitación: Secuencia de encendido de equipos.....	69
<b>Figura 68</b> Capacitación: Etapa de conexión entre PC y generador de señales.....	70
<b>Figura 69</b> Capacitación: Etapa de selección de parámetros de la señal.....	71
<b>Figura 70</b> Capacitación: Etapa de selección de parámetros de modulación.....	72
<b>Figura 71</b> Capacitación: Pruebas sistema COMINT.....	72
<b>Figura 72</b> Capacitación: Pruebas sistema Jamming.....	73

## RESUMEN

El proyecto realizó el diagnóstico y el desarrollo del sistema de interferencias de señales en la banda de 1MHz – 1GHz para el Agrupamiento de Comunicaciones y Guerra Electrónica (AGRUCOMGE) del Ejército, enfocado a incrementar la capacidad de respuesta de los sistemas de seguridad y vigilancia públicos; para lo cual se ejecutaron las siguientes actividades generales:

a) Primeramente, se realizó el diagnóstico del sistema de jamming que actualmente dispone la AGRUCOMGE, que al inicio se encontraba no operativo, para reutilizar los dispositivos en buen estado, así como se realizó el estudio y análisis del estado del arte en relación al problema a resolver. b) Luego se trabajó en el desarrollo de técnicas y algoritmos que permitan generar señales de interferencia efectivas, enfocadas a incrementar la capacidad de respuesta de los sistemas de seguridad y vigilancia pública. c) Se realizó la coordinación con el sistema de monitoreo de señales COMINT para obtener la información del objetivo a ser interferido. d) También se asoció los mapas digitales para generar zonas de cobertura efectivas; e) Finalmente, toda la tecnología desarrollada fue evaluada experimentalmente en los sistemas de vigilancia y reconocimiento de la AGRUCOMGE lo que permitirá extender los resultados a bandas de frecuencias superiores a 1GHz, por ejemplo, hasta 6GHz para incluir las bandas WiFi en las que operan drones de reconocimiento.

### **PALABRAS CLAVES:**

- **INTERFERENCIA**
- **JAMMING**
- **DIAGNOSTICO**

## **ABSTRACT**

The project carried out the diagnosis and development of the signal interference system in the 1MHz - 1GHz band for the Army Electronic Communications and Warfare Grouping (AGRUCOMGE), focused on increasing the response capacity of public security and surveillance systems ; for which the following general activities were carried out: a) Firstly, the diagnosis of the jamming system currently available to AGRUCOMGE was made, which at the beginning was not operative, to reuse the devices in good condition, as well as the study and analysis of the state of the art in relation to the problem. to solve. b) Then we worked on the development of techniques and algorithms that allow the generation of effective interference signals, focused on increasing the response capacity of public security and surveillance systems. c) Coordination was carried out with the COMINT signal monitoring system to obtain the information of the objective to be interfered with, complying with all the architecture phases of these systems, that is to say; detection, identification, recognition, monitoring and discrimination of the objective. d) Digital maps were also associated to generate effective coverage areas; e) Finally, all the technology developed was evaluated experimentally in AGRUCOMGE surveillance and recognition systems, which will allow extending the results to bands with frequencies above 1GHz, for example up to 6GHz, to include WiFi bands in which drones operate. recognition.

### **KEY WORDS:**

- **INTERFERENCE**
  
- **JAMMING**
  
- **DIAGNOSE**

## **CAPÍTULO 1**

### **1. INTRODUCCIÓN**

#### **1.1. Antecedentes**

El presente proyecto de investigación tiene como objetivo diagnosticar y poner en funcionamiento equipos tecnológicos del AGRUCOMGE para generar señales de Jamming, usados en la guerra electrónica. La guerra electrónica trata de explotar, reducir o impedir el uso del espectro radioeléctrico por medio de señales de interferencia al enemigo y conservar la comunicación como beneficio.

Se revisó bibliografía sobre el funcionamiento y operación del equipamiento del AGRUCOMGE para este proyecto de investigación, así como el estado del arte para realizar Jamming como se indica en el Capítulo 2.

En segundo lugar, se diagnosticaron los equipos y seleccionaron los elementos necesarios para generar una señal de interferencia y de fácil funcionamiento como se indica en el capítulo 3.

En tercer lugar, se realizaron pruebas de funcionamiento y desempeño del equipamiento acoplado con una interfaz de fácil utilización y portabilidad como se muestra en el capítulo 4.

Finalmente se llegaron a las conclusiones mostradas en el capítulo 5, que mediante el capítulo 3 y 4 demuestran la efectividad y funcionalidad de los equipos utilizados para la realización de este proyecto de investigación.

## **1.2. Justificación e Importancia**

El presente proyecto busca desarrollar un sistema que permita interferir señales de radiofrecuencia de interés para sistemas públicos de seguridad y vigilancia, con tecnología endógena, es decir; cumpliendo con todas las etapas para desarrollar un proceso coherente de I+D+i.

Los principales problemas que se presentan a la hora de usar sistemas ya existentes en el mercado de Guerra Electrónica, son: i) los altos costos de los existentes y de alta reserva (propietarios de la industria de la defensa mundial), ii) muchas veces la falta de soporte, iii) deficiencia en la transferencia de tecnología por ser sistemas cerrados de producción y iv) la necesidad de obtener permisos de exportación de gobiernos extranjeros como el *DoD-USA* (Departamento de Defensa de los Estados Unidos de Norte América). Contrariamente los sistemas que se desarrollan en base a la investigación aplicada e ingeniería inversa pueden subsanar estos inconvenientes con costos muy reducidos, se tiene la garantía de una transferencia de tecnología real dentro de todos los procesos de implementación y generación de masa crítica para la investigación aplicada confines de seguridad y defensa. Por lo tanto, la generación de señales interferentes efectivas a través de la investigación y propio desarrollo pueden ser solventados dando como resultado mejores herramientas de guerra activa que sobretodo son parte intrínseca y propietaria del sistema general de vigilancia y seguridad.

## **1.3. Alcance del Proyecto**

El plan de trabajo en torno a los objetivos específicos se puede resumir de la siguiente forma:

1. Realizar el diagnóstico exhaustivo del actual sistema del AGRUCOMGE, así como un estudio analítico del estado del arte en relación a las técnicas de interferencia de señales.

2. Desarrollar técnicas y algoritmos que permitan generar señales de interferencia efectivas.
3. Desarrollar procesos interactivos con el COMINT para garantizar el uso de la información con el fin de generar una respuesta inmediata y efectiva.
4. Evaluar los algoritmos y procesos desarrollados.
5. Realizar pruebas en entornos de área local y área extendida de ser el caso y como consecuencia de las pruebas, mejoramiento de los procesos y algoritmos en caso de requerir.
6. Publicar los resultados pertinentes en revistas científicas nacionales o internacionales de impacto
7. Implementar el sistema de jamming en la unidad móvil del AGRUCOMGE.
8. Redactar documentos y manuales relacionados con la tecnología desarrollada y presentación de documentos finales, software y aplicativos.

## **1.5. Objetivos**

### **1.5.1. Objetivo General**

Realizar el diagnóstico del actual sistema de jamming de la AGRUCOMGE y desarrollar un sistema de interferencias de señales en la banda de 1MHz – 1GHz para la Agrupación de Comunicaciones y Guerra Electrónica (AGRUCOMGE) del Ejército, enfocado a incrementar la capacidad de respuesta de los sistemas de seguridad y vigilancia públicos.

### 1.5.2. Objetivos Específicos

Los objetivos específicos estarán en relación al objetivo principal propuesto y formarán parte de cada una de las etapas del desarrollo del presente proyecto. Además, los objetivos específicos se orientan a mejorar continuamente los procesos, la gestión estratégica y la aplicación de tecnologías de información y comunicación para optimizar los servicios de seguridad prestados por el Estado. Los objetivos específicos se pueden resumir de la siguiente forma:

- Diagnosticar el sistema de jamming que actualmente dispone la AGRUCOMGE, que al momento se encuentra no operativo, para reutilizar los dispositivos en buen estado, así como se realizará el estudio y análisis del estado del arte en relación al problema a resolver.
- Desarrollar técnicas y algoritmos que permitan generar señales de interferencia efectivas enfocadas a incrementar la capacidad de respuesta de los sistemas de seguridad y vigilancia pública.
- Coordinar con el sistema de monitoreo de señales COMINT para obtener la información del objetivo a ser interferido, cumpliendo con todas las fases de arquitectura de estos sistemas, es decir; detección, identificación, reconocimiento, seguimiento y discriminación del objetivo.
- Asociar mapas digitales para generar zonas de cobertura efectivas.
- Evaluar experimentalmente las técnicas desarrolladas en los sistemas de vigilancia y reconocimiento del AGRUCOMGE y poder extender los resultados a bandas de

frecuencias superiores a 1GHz, para incluir las bandas WiFi (2.4 GHz y 5.8GHz) en las que operan drones de reconocimiento.

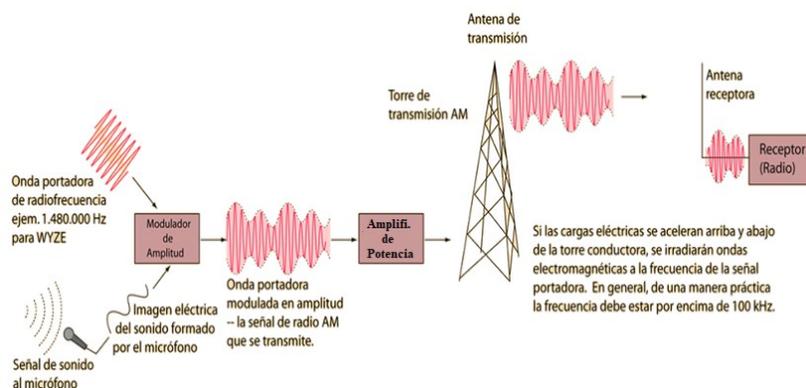
## CAPÍTULO 2

### 2. FUNDAMENTO TEÓRICO

#### 2.1 Propagación de RF

La propagación de las ondas de Radio Frecuencias (RF), se refiere a la transmisión de ondas electromagnéticas por el espacio libre, con el objetivo de establecer y mantener comunicación entre puntos ya sea de manera unidireccional o bidireccional. Estableciendo, de esta forma, una comunicación sin necesidad de cables. Este tipo de comunicación es comúnmente usada para realizar transmisiones entre puntos que se encuentran separados por grandes distancias o cuando el transmisor o receptor, o los dos, se encuentran en movimiento.

En la figura 1 se ilustra, de una forma simplificada, las principales partes de una comunicación de RF. Se puede observar a partir de esa ilustración que esta comunicación es sumamente vulnerable a los obstáculos, ya que la señal al atravesarlos puede sufrir atenuaciones y en algunos casos puede llegar a desvanecerse por completo. Otra de sus desventajas es que resulta muy vulnerable a interferencias intencionales (*Jamming*), es factible de ser interceptada ya que, al encontrarse en un medio abierto, como el espacio libre, cualquier receptor que se encuentre dentro del área de cobertura puede recibir la señal y puede ser identificado su dirección de origen.



**Figura 1** Elementos básicos de un sistema de transmisión de RF.

Fuente: (Nave, 2014)

En el ejemplo de la Fig. 1 una fuente de información, por ejemplo, una señal de sonido, es modulada analógicamente por un modulador en amplitud y posteriormente amplificada por un amplificador de potencia para solo así ser aplicado a la antena de transmisión. La onda modulada y amplificada se propaga por el medio de propagación, que en este caso es el aire libre. Seguidamente, esa onda electromagnética llega al receptor donde varios procesos inversos son aplicado a la señal recibida con el objetivo de recuperar una estimativa de la información que fue originalmente generada. De una forma simplista el proceso ilustrado anteriormente es el que se establece en un enlace de comunicaciones en RF.

## 2.2 Señal intencional de interferencia o *Jamming*

El *jamming*, o interferencia intencional, es considerado como una acción deliberada de ataque a las transmisiones que usan el espacio libre como medio de propagación. Dicho ataque consiste en dificultar el trabajo de los equipos de recepción de la señal a la cual se está atacando. (Zhang Yu, 2014)

La implementación de una estrategia de *jamming* consiste en enviar una señal de ataque dentro de la misma banda de frecuencia que trabaja el sistema a ser interferido. Esta señal, puede

ir desde una señal senoidal común hasta un tipo de señal compuesta por distintos tipos de ruido, obteniendo según el tipo de señal a ser usada diferentes grados de efectividad en el ataque.

### **2.2.1 Clasificación por ancho de banda**

Esta clasificación se refiere a la relación entre el ancho de banda de la señal de interferencia producida por un generador, o *jammer*, con respecto al ancho de banda de la señal a la cual se pretende interferir.

#### **2.2.1.1 Interferencia del tipo barrera (Barrage Jamming)**

Esta técnica consiste en realizar la transmisión de la señal de interferencia en un rango mucho más amplio al comprendido por la señal a la que se busca interferir. Su objetivo es asegurar por completo la interferencia de dicha señal, sin embargo, uno de los inconvenientes de esta técnica es que debido a que la señal de interferencia se encuentra en varios canales a la vez, señales próximas a la señal que se desea atacar también serán afectadas.

#### **2.2.1.2 Interferencia puntual (Spot Jamming)**

La interferencia puntual o *spot jamming* consiste en realizar la transmisión únicamente dentro del mismo ancho de banda de la señal a interferir, o en su defecto que el ancho de banda de la señal de interferencia se asemeje lo más posible a la señal a interferir, con el objetivo de evitar el problema del *barrage jamming*, asegurándose que únicamente se ataca al objetivo deseado.

### **2.2.1.3 Interferencia tipo barradura (Sweep Jamming)**

Esta técnica consiste en realizar un barrido dentro de un rango de frecuencias. Este comportamiento se logra mediante el desplazamiento progresivo de la frecuencia de operación, desde una frecuencia inicial a una final, de un generador de RF. El receptor percibirá que la señal está siendo interferida porque, para su punto de vista, existirá una señal que barre todo el ancho de banda del canal.

## **2.2.2 Métodos de interferencia**

Se entiende por métodos de interferencia a los procedimientos o algoritmos que se pueden utilizar para implementar algunas de las interferencias arriba mencionadas. La importancia de la selección del método radica en la maximización de los efectos de la interferencia en el receptor blanco.

### **2.2.2.1 Interferencia constante (Jamming Constante)**

El *jamming* constante genera una señal de ruido dentro de la banda del receptor que se desea interferir por periodos de tiempo muy grandes. Se puede observar que al mantenerse constante resulta fácilmente detectable y factible de ser bloqueado. De igual manera su uso constante genera un alto consumo de potencia por parte del equipo utilizado.

Este tipo de *jamming* suele ser usado, por ejemplo, en locales donde se prestan servicios bancarios, para evitar el uso de celulares dentro de sus instalaciones o en áreas propensas a ataques en las cuales se busca inhibir señales que puedan ser emitidas por dispositivos remotos o personas mal intencionadas.

### **2.2.2.2 Interferencia reactiva o Jamming reactivo**

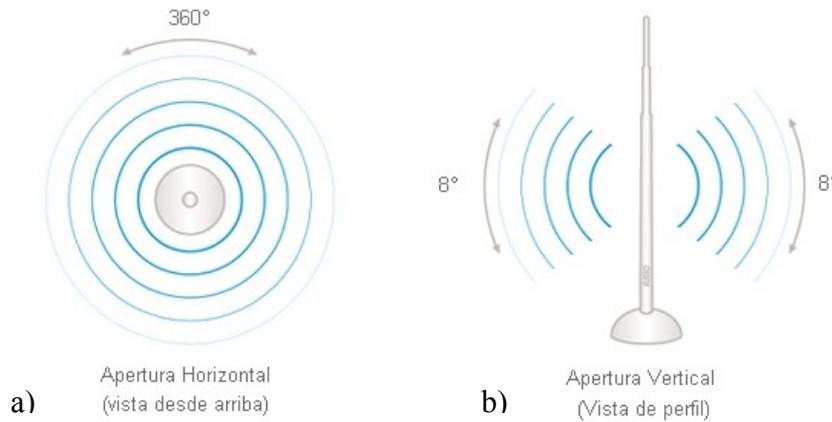
Esta técnica consiste en realizar un monitoreo continuo de la actividad de una red de radiofrecuencias (RF) y determinar el momento idóneo para inhibir la señal del objetivo deseado. Debido a esto el *jamming* reactivo consume una cantidad mínima de potencia, lo cual lo vuelve más eficiente, además de tornarlo más difícil de ser detectado. Generalmente su operación es del tipo *spot* o *sweep jamming*.

### **2.2.3 Tipos de antenas**

La selección de los métodos arriba mencionados y del tipo de antena que será utilizada guarda una estrecha relación con el propósito o misión para la cual el dispositivo de interferencia (o *jammer*) fue diseñado.

#### **2.2.3.1 Antenas Omni-direccionales**

Este tipo de antenas se encarga de emitir energía, en forma de ondas electromagnéticas, todas las direcciones alrededor del *jammer*. Por lo general este tipo de antenas son las que poseen un nivel de ganancia bajo con respecto a otros tipos de antenas más direccionales. Un ejemplo simple de este tipo de elemento es el monopolo y está ilustrado en la figura 2. (Chapaca, 2016)

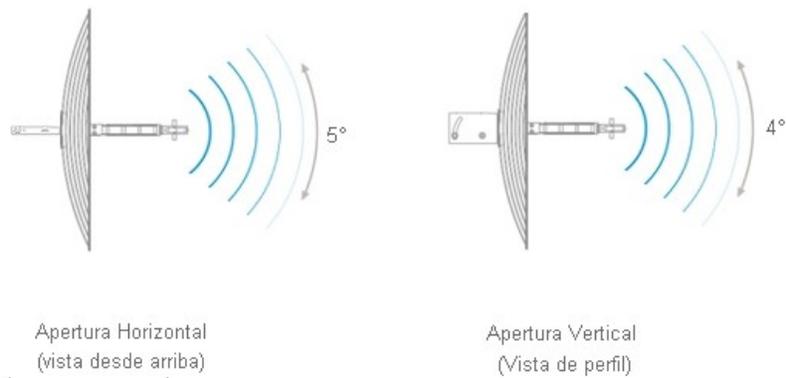


**Figura 2** Principales planos de irradiación de una antena monopolo. En a) se ilustra la propagación de las ondas electromagnéticas de forma omni-direccional, en el plano horizontal, y en b) el comportamiento direccional en el plano vertical.

Fuente:(Alvarez, Garcia, & Ruiz, s.f.)

### 2.2.3.2 Antenas Direccionales

Las antenas las cuales presentan la propiedad de concentrar su energía irradiada en una o más direcciones específicas son denominadas antenas directivas. En la mayoría de los casos este tipo de antenas son usadas para enlaces punto a punto y/o punto multipunto. Ejemplos clásicos de este tipo son la Log Periódicas, Parabólicas, o Yagi-Uda (Chapaca, 2016). En la figura 3 se ilustra la capacidad de concentrar la energía irradiada por una antena parabólica.



**Figura 3** Ilustración que muestra la capacidad de concentración la energía irradiada por la antena parabólica en el plano horizontal ( $\approx 5^\circ$ ) y en el plano vertical ( $\approx 4^\circ$ ).

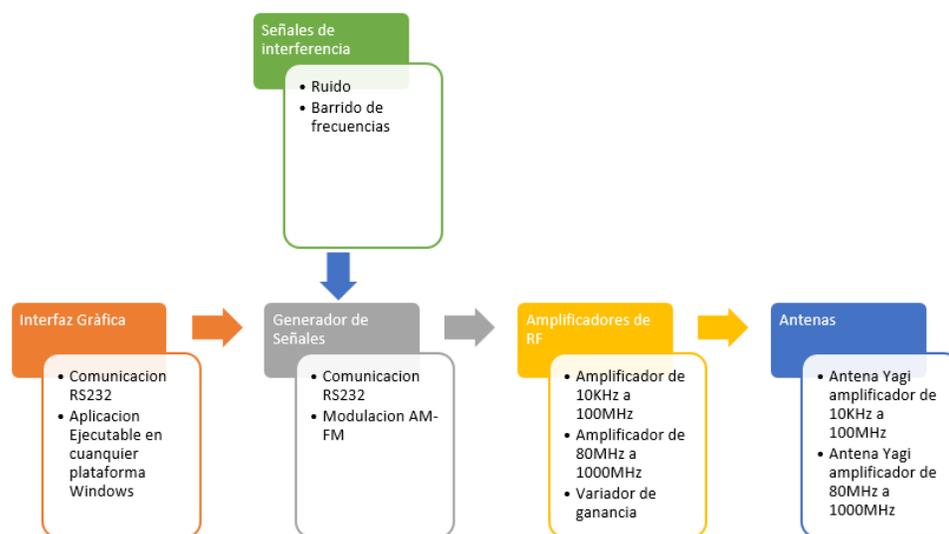
Fuente:(Alvarez, Garcia, & Ruiz, s.f.)

En la figura 3 se puede observar, con una ilustración simple, el motivo por el cual las antenas directivas son principalmente usadas para comunicación punto - multipunto. Al poseer ángulos sólidos muy pequeños (típicamente de  $PH < 10^\circ$  y  $PV < 10^\circ$ ) toda la energía irradiada se concentra dentro de ese ángulo y en una dirección específica, muy poca energía se desperdicia fuera del mismo.

## CAPÍTULO 3

### 3. DISEÑO E IMPLEMENTACIÓN DEL SISTEMA

En el presente capítulo se expondrán los equipos y dispositivos electrónicos utilizados para realizar el proyecto de investigación y como se procedió a verificar el correcto funcionamiento de los mismos.



**Figura 4** Diseño general del sistema.

La figura 4 muestra el diseño teórico, en diagrama de bloques, del sistema implementado para generar Jamming con los equipos disponibles en el AGRUCOMGE. Los bloques de antenas, amplificadores de RF y generadores pertenecen a ese agrupamiento, en cuanto, la interfaz gráfica fue desarrollada enteramente en este trabajo. Adicionalmente, se debe resaltar que para el diseño/recuperación del sistema de Jamming aspectos tales como la banda de frecuencias de

operación, tipos de señales, tipos de modulación de la señal de interferencia niveles de potencia de entrada y/o salida fueron llevados en consideración.

### 3.1 Diseño general del sistema

Tomando en cuenta el diseño general del sistema de la figura 4 se van a indicar, a continuación, los equipos utilizados para el desarrollo de este proyecto de investigación.

En primer lugar, se decidió empezar por el diagnóstico, reparación y análisis de desempeño de los equipos de amplificación de RF del AGRUCOMGE mostrados en la Figura 5 y Figura 6.



**Figura 5** Amplificador de potencia de 500 watts para la banda de 10 kHz a 100 MHz marca *Amplifier Research*.



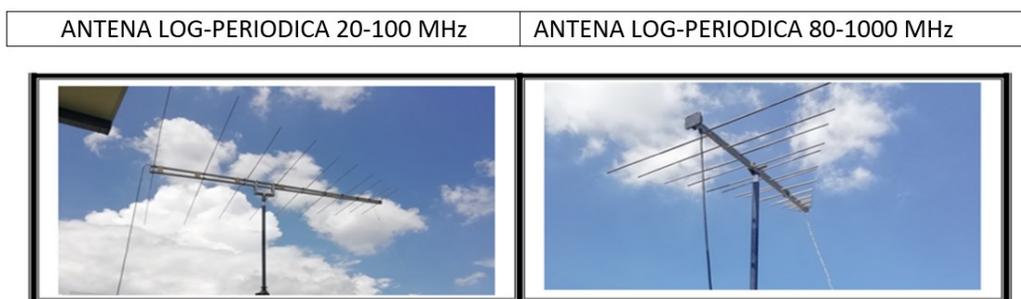
**Figura 6** Amplificador de potencia de 200 watts para la banda de 80 MHz a 1000 MHz  
marca Amplifier Research.

Luego se procedió con la selección de un sistema que nos permita generar una señal de RF la misma que será aplicada a los amplificadores de potencia. Con esta finalidad se optó por utilizar el generador de señales Rohde&Schwarz por sus prestaciones para generar señales, con o sin modulación, de RF.



**Figura 7** Generador de señales.

Una vez que fueron reparados estos dos equipos se procedió a verificar su funcionamiento. Para esto los equipos fueron conectados a sus respectivas antenas y finalmente se probaron los equipos funcionando de forma operacional.



**Figura 8** Antenas direccionales de los amplificadores.

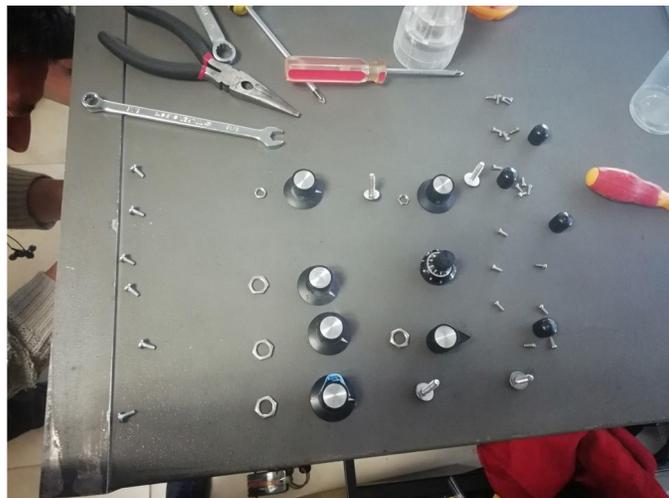
Para que la utilización del sistema sea más sencilla y de respuesta inmediata, se construyó una aplicación automatizada para controlar el generador de señales, la cual es portable y de fácil utilización.

**Figura 9** Aplicación - Interface para el usuario con el generador de señales.

El aplicativo posee regiones para ingresar los datos de frecuencia, potencia, tipo de modulación y activar la señal de salida del generador R&S SML03. Toda la comunicación entre el aplicativo y el generador es vía protocolo de comunicación RS232.

### 3.2 Revisión y puesta en marcha del *Amplifier Research* de 500 watt para la banda de 10 kHz a 100 MHz

Para el diagnóstico del amplificador de potencia de 500 watts inicialmente se procedió a desarmarlo y darle un mantenimiento correctivo, ya que este se encontraba inoperable hace más de 9 años. Previamente se realizó una exhaustiva y completa lectura de los manuales técnicos y de operación, ya que este tiene varios parámetros de funcionamiento, así como varias protecciones. La etapa inicial del mantenimiento se ilustra en la figura 10.



**Figura 10** Desmontaje de la carcasa protectora de ruido o aisladora de interferencias del Amplifier Research de 500 watts en la banda de 10kHz – 100MHz.

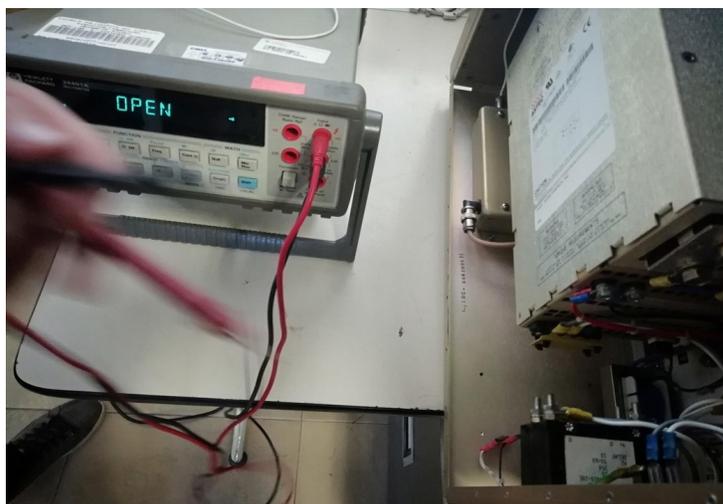
Una vez desmontada la carcasa y corregidas las varias etapas con problemas, se dio una revisión a cada uno de los bloques del equipo para verificar y poder observar si existe algún dispositivo visible quemado o desconectado, seguidamente, se procedió a una limpieza general con aire comprimido, como se observa en la Figura 11.



*Figura 11* Limpieza de los bloques de acondicionamiento, pre amplificación y amplificador de potencia del sistema.

### 3.2.1 Fuentes de Alimentación

Una vez verificados los dispositivos de forma visual, substituido los conectores que estaban dañados y con la información suministrada por el manual se procedió a la revisión de las fuentes de poder del equipo que son mostradas en la Figura 12.



**Figura 12** Revisión de la Fuente de alimentación.

En esta revisión se observó que el equipo usaba dos fuentes diferentes para su funcionamiento, sus características son presentadas en la Tabla 1.

**Tabla 1**

*Fuentes de alimentación*

<b>Fuente de alimentación 1</b>	<b>Fuente de alimentación 2</b>
Voltaje: 36.0 V	Voltaje: 28.0 V
Corriente: 33.2 A	Corriente: 21.4 A

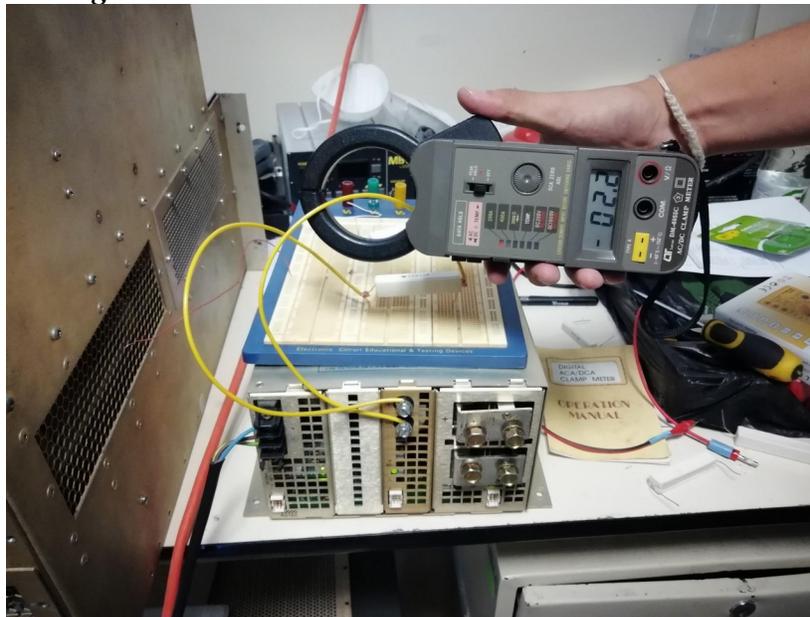
Para poder probar las fuentes de alimentación sin energizar al equipo de amplificación se procedió a retirar la fuente del equipo y probarla fuera de él, sin carga. Para la correcta operación de las fuentes de alimentación se verificó si estaban entregando el voltaje especificado en el manual.

Se evidenció que para que la fuente de 36 voltios y 33.2 amperios opere, se debía conectar una señal de control como se indica en la Figura 13, para de esta forma garantizar su operación.

Para verificar que estén entregando la corriente especificada se hizo una prueba con una carga de 10 ohms con resistencias de potencia (resistencias cerámicas) para la fuente de 36 voltios y una carga de 10 ohms para la fuente de 28 voltios, como se observa en la Figura 14 y 15. En virtud de estas pruebas se determinó el correcto funcionamiento de las dos fuentes.



**Figura 13** Circuito de activación de la fuente de 36 voltios.



**Figura 14** Prueba del funcionamiento de la fuente de 28 voltios con una carga de 10 Ohm

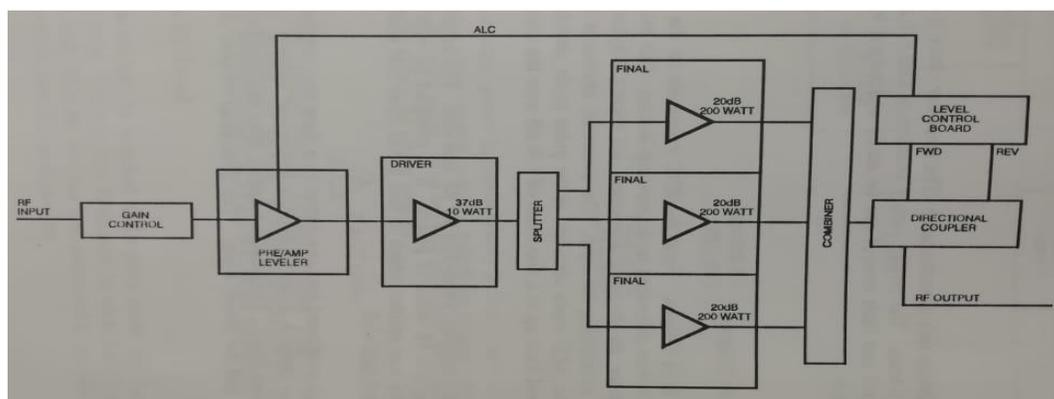
Una vez verificada la energización del amplificador se procedió a verificar todos los subsistemas que forman parte del amplificador. La ilustración, en diagramas de bloques, de las diferentes etapas que constituyen el amplificador se presenta en la Figura 16. Debe resaltarse que

los mencionados bloques fueron verificados de forma aislada, en una primera fase, y en su trabajo en conjunto con las etapas anteriores, en una fase posterior. Esta metodología fue adoptada para evitar daños de sobrecarga o de trabajo en circuito abierto.



**Figura 15** Prueba del funcionamiento de la fuente de 36 voltios con una carga de 10

Ohm



**Figura 16** Etapas de funcionamiento del amplificador.

Fuente:(Operation and service manual, model 500<sup>a</sup>100 Model: 1006900501, 1996)

### 3.2.2. Etapas de pre amplificación y drive del amplificador de 10 kHz a 100 MHz

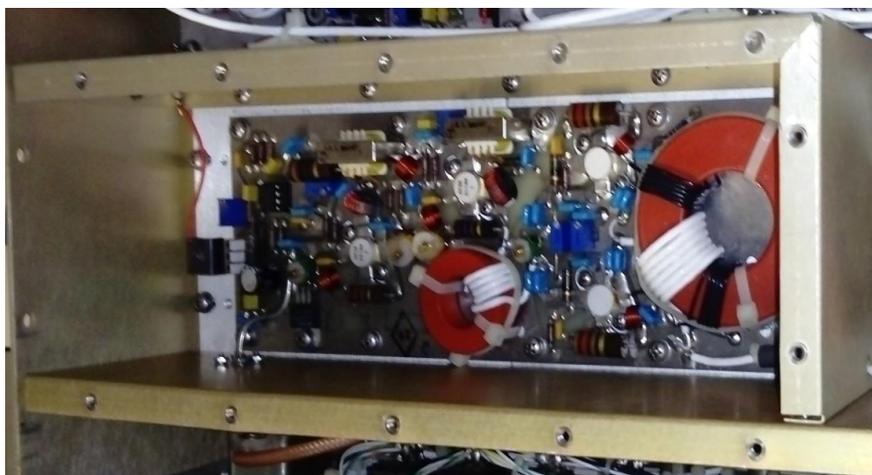
El amplificador para que ingrese en el modo encendido, pero en modo de espera o *standby*, de forma adecuada requiere seguir un protocolo de dos fases que se detalla a seguir:

- Giro de la llave de encendido de la posición 0 a la posición 1.
- Presión del botón POWER para encender la etapa de pre amplificación y del driver.

Esta secuencia garantiza que todos los sub sistemas del amplificador están energizados y que el mismo se encuentra en modo de espera. Luego del proceso de encendido se observó un error en el indicador de la temperatura, que en este punto no se lo tomó en cuenta ya que este error no afectaba en el funcionamiento del preamplificador ni el funcionamiento del driver. Fotografías del pre amplificador y del drive son presentadas en las Figuras 17 y 18.



**Figura 17** Fotografía de la tapa de pre amplificación.



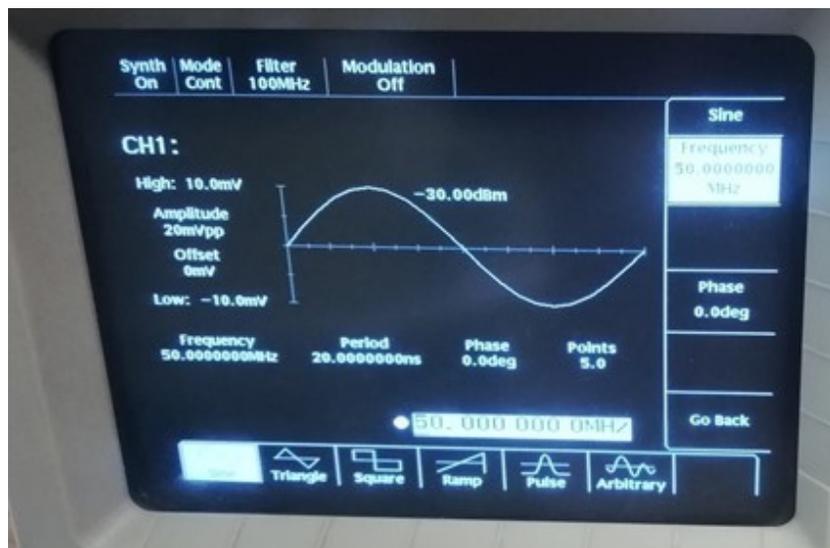
**Figura 18** Fotografía del circuito del Driver.

También se procedió a verificar el funcionamiento de una etapa que estaba localizada antes de la pre amplificación. Se comprobó que la mencionada etapa funcionaba correctamente y que realizada la operación de variar la ganancia de entrada a través de un potenciómetro interconectado a los botones de control del equipo.

Se observó que la unidad constituida por el pre amplificador y el driver mostraba una dependencia con el nivel de potencia aplicado al terminal BNC denominado de *RF – input* en la parte frontal del equipo. A partir de la información que se presenta en los manuales de mantenimiento y uso del amplificador se observó que estos niveles de potencia debían estar en el rango de -10 dBm hasta 0 dBm. Así mismo se verificó que valores inferiores a los - 10 dBm producirá un funcionamiento no adecuado de la etapa denominada Control Automático de Ganancia (CAG). Con base en la misma fuente se concluye que la etapa de pre amplificación funciona correctamente si la de control opera, entonces, para la verificación del funcionamiento de este se

realizaron pruebas conectándolo a la entrada de la siguiente etapa que era la del driver, es decir se verificó el funcionamiento del preamplificador y del driver al mismo tiempo.

En la verificación individual del driver se desconectó la etapa de pre amplificación y se le aplicó una señal de prueba, producida por un generador de señales (ver Figura 19), con nivel de potencia de -30 dBm y una frecuencia 50 MHz. La respuesta que se obtiene a la salida del drive se la monitoreó con un analizador de espectros, como protección se adicionó un atenuador de 40 dB a la entrada del equipo para proteger contra sobre niveles de potencia. La Figura 20 presenta la captura de la pantalla del analizador durante la medida a la salida del drive.



**Figura 19** Gráfica del generador de señales conectado a la entrada del driver.



**Figura 20** Analizador Espectros a la salida del driver, con un atenuador de 40 dB.

Como se observa en la Figura 20 si en la entrada del driver se ingresa -30 dBm a la salida luego del atenuador, se tiene -31,22 dBm, ese nivel de potencia se justifica de la siguiente forma:

Cálculo de ganancia del driver considerando los 40 dB del atenuador colocado como el objetivo de proteger la entrada del analizador de espectros:

$$-30 \text{ dBm} - 40 \text{ dB} + X_{\text{Ganancia del driver}} = -31,22 \text{ dBm}$$

luego

$$X_{\text{Ganancia del driver}} = 38,78 \text{ dB}$$

En forma de resumen las principales características de funcionamiento del drive son presentadas en la Tabla 2.

**Tabla 2**

*Verificación del funcionamiento del driver.*

Señal	de	Ganancia del driver	Atenuación	Potencia de salida
-------	----	---------------------	------------	--------------------

<b>entrada</b>			
<b>-30 dBm</b>	38,78 dB	40 dB	-31,22 dBm

Con esto verificamos que el driver está funcionando correctamente y se procedió a ingresar diferentes potencias de entrada con el generador de señales en el preamplificador conectado al driver, por seguridad, el atenuador de 40 dB fue mantenido. De esta forma se pudo observar en el analizador de espectros el funcionamiento del conjunto pre amplificador - driver, los resultados obtenidos son presentados en la Tabla 3.

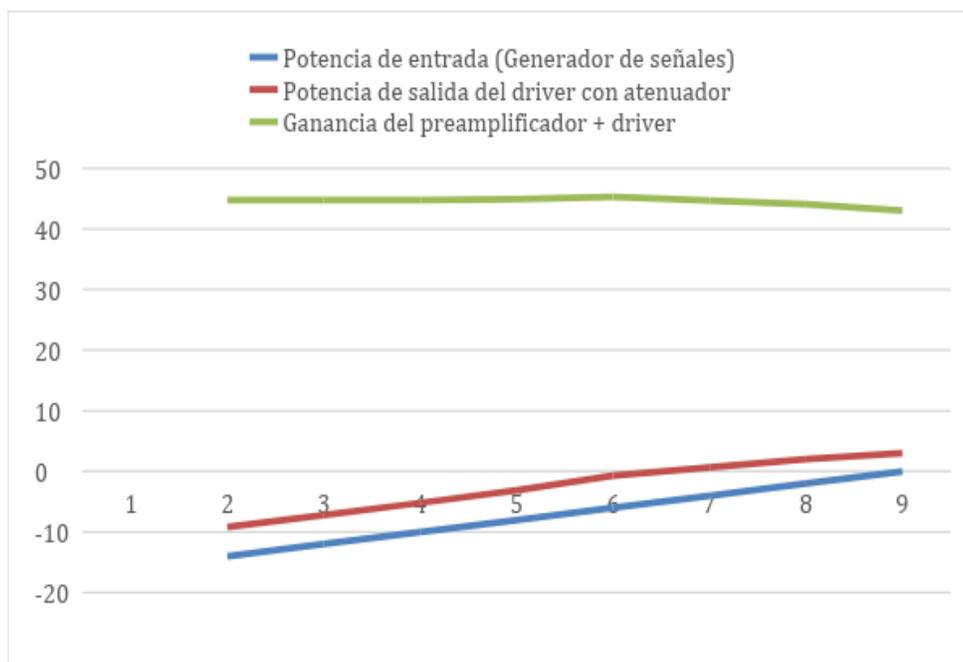
**Tabla 3**

*Comprobación de ganancia del driver y el preamplificador.*

<b>Potencia de entrada</b> <b>(generador de</b>	<b>Frecuencia</b>	<b>Potencia de salida del</b>	<b>50 MHz</b>
<b>señales) [dBm]</b>		<b>driver con atenuador</b>	<b>Ganancia del pre</b>
		<b>driver con atenuador</b>	<b>amplificador + driver</b>
		<b>[dBm]</b>	<b>[dB]</b>
<b>-14,01</b>		-9,20	44,81
<b>-11,99</b>		-7,20	44,79
<b>-10,00</b>		-5,20	44,80
<b>-8,03</b>		-3,10	44,93
<b>-6,00</b>		-0,70	45,30
<b>-4,00</b>		0,70	44,70
<b>-2,01</b>		2,06	44,07
<b>-0,01</b>		3	43,01
		<b>Ganancia Promedio</b>	<b>44,55</b>

**CONTINÚA** →

Las pequeñas fluctuaciones que se observan en la Tabla 3, cuando se compara la ganancia promedio y las ganancias para cada nivel de potencia de la señal de entrada, es plenamente justificable por variaciones en el instante de hacer la lectura en el analizador de espectros. Con el objetivo de visualizar el comportamiento plano de la ganancia del conjunto pre amplificador – driver se ilustra en la Figura 21 los datos de la Tabla 3.



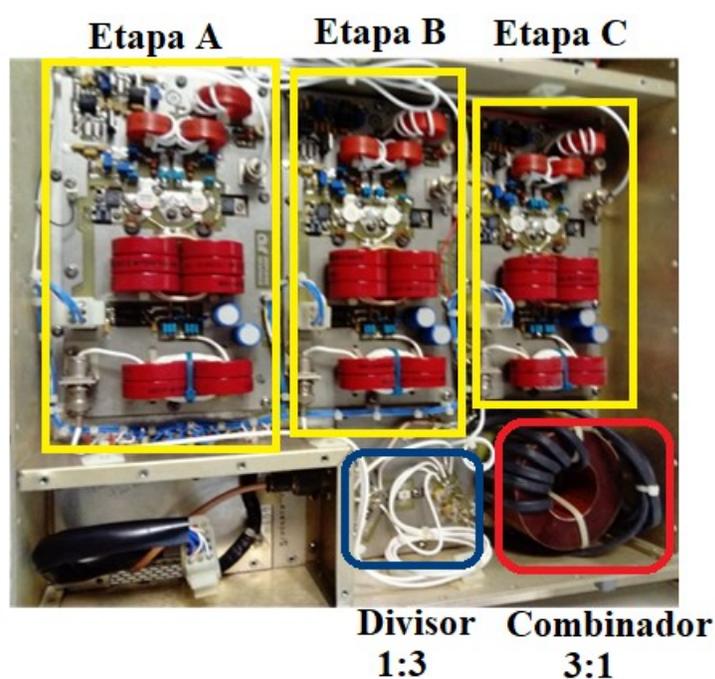
**Figura 21** Ganancia y potencia de entrada y salida del preamplificador con el driver con atenuador de 40 dB.

La Figura 21 muestra claramente la característica lineal del bloque pre amplificador – drive. Adicionalmente, con los datos de la tabla 3, la Figura 21 y las informaciones que se incluyen en el manual de servicio del amplificador se puede inferir que el bloque driver y pre amplificador están funcionando correctamente.

### 3.2.3 Etapa de amplificación de potencia

La etapa de amplificación de potencia está constituida de un divisor de potencia 1:3 en fase, de tres etapas idénticas de amplificadores de potencia configurados para trabajar en paralelo y un combinador de potencia 3:1 en fase. Una fotografía de todo el bloque de potencia se muestra en la Figura 22.

El procedimiento seguido para verificar el funcionamiento de este bloque fue el siguiente. Primero se aplicó una señal de entrada, producida por el generador de señales de RF, en la entrada del divisor de potencia 1:3. Seguidamente, una de sus salidas, manteniendo las otras dos con cargas casadas, fue aplicada a la entrada del analizador de espectros y se verificó que la potencia medida por este sea  $1/3$  de la potencia de entrada. Ese procedimiento fue repetido con las otras dos salidas. Después de esta primera prueba se concluyó que el divisor de potencia estaba trabajando adecuadamente. Se debe resaltar que para el encendido del amplificador de RF se siguió el protocolo de encendido que ya fue presentado anteriormente, caso contrario puede producirse alguna avería en uno de los bloques del amplificador.

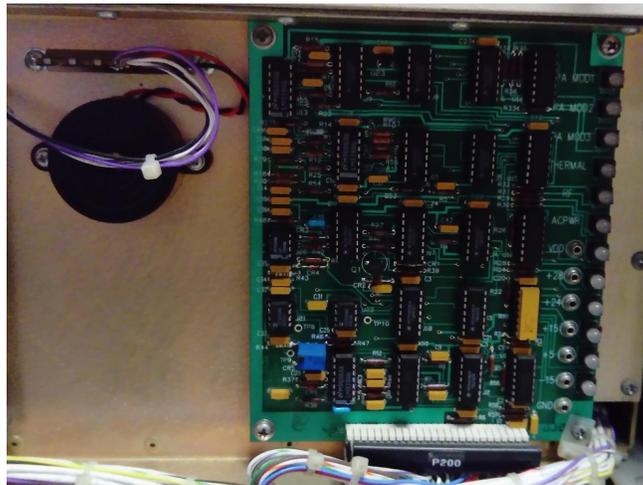


*Figura 22* Etapa de amplificación de potencia.

En esta fase encontramos el primer problema, el botón de operación no encendía las fuentes de alimentación para los amplificadores de potencia, inclusive al querer activarlo la placa

de control (ver Figura 23) nos informaba de un mal funcionamiento de temperatura y este, según el manual decía que las fuentes no están funcionando correctamente o que el sistema se encuentra en circuito abierto.

Para esto se desarmó la etapa de control del amplificador como se observa en la Figura 24 y de esta manera poder observar qué pasa con la señal de control del amplificador al querer encender la etapa de potencia. Luego de desarmar el panel de control y verificar el funcionamiento de los botones nos encontramos con que el botón de operación no funcionaba correctamente, se desarmo completamente el botón y se lo armo nuevamente limpiándolo con un limpia contactos y colocándolo de forma correcta ya que por el uso se había salido uno de los contactos del botón. Al volver a ponerlo en el panel de control se verificó su funcionamiento y en este caso ya encendió la etapa de potencia eliminando el error que se tenía anteriormente de la temperatura.



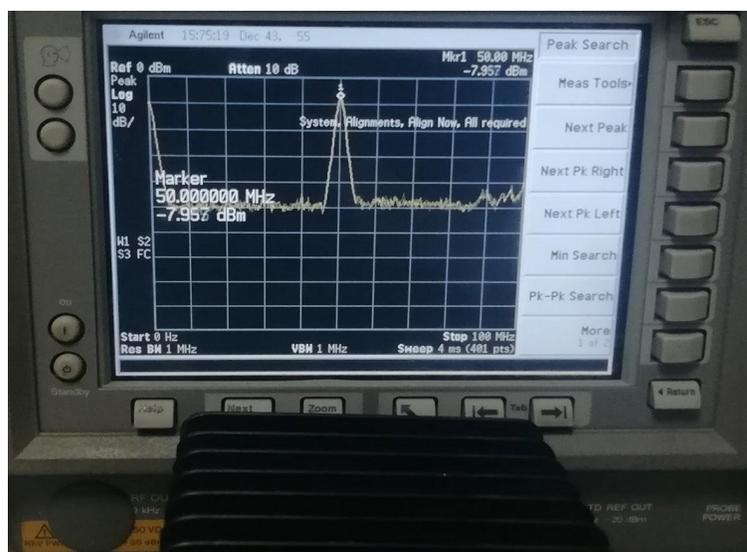
**Figura 23** Etapa de control.



**Figura 24** Desmontaje del panel de control.

A grandes rasgos el procedimiento seguido para verificar el estado de las etapas de potencia fue el siguiente: Primeramente, se verificó cada una de las etapas de potencia, a saber etapas A, B y C (ver Figura 22). Para esto se desconectó el divisor 1:3 y se aplicó una señal de RF en la entrada de la etapa de potencia, manteniendo conectado el analizador de espectro a la salida de la etapa. Ese procedimiento fue repetido en las otras dos etapas de potencia restantes. Después de esa verificación se concluyó que cada una de las etapas funciona adecuadamente. El combinador 3:1, por su propia topología, se juzgó, a priori, que debería estar funcionando correctamente. Finalmente, se volvió a interconectar el divisor a las etapas de potencia y cada una de sus salidas al combinador 3:1. Se aplicó una señal de RF en la entrada del divisor y se conectó a la salida del combinador un acoplador bidireccional y una carga casada de potencia. Para concluir con la verificación del bloque de potencia el nivel de potencia medido, a la salida del acoplador bidireccional usado para determinar la potencia entregado a la carga, comprobaron que toda la etapa de potencia estaba funcionando adecuadamente.

Para cada una de las etapas de potencia del amplificador se aplicó una señal de entrada con el generador de señales en  $-30\text{dBm}$  y verificando su comportamiento con el analizador de espectros y con un atenuador de potencia en su entrada y se obtuvo medida de la potencia como se ilustra en la Figura 25:



**Figura 25** Potencia de salida de una etapa de potencia.

Verificando el dato obtenido por el analizador de espectros y la información del manual y la Figura 16 de la ganancia de cada una de las etapas de potencia que va de 18 a 20 dB, podemos observar en la Figura 25 que esta etapa de potencia funciona correctamente por las razones que se muestran en la Tabla 4 y los cálculos de la ganancia de la etapa de potencia.

**Tabla 4**

*Verificación del funcionamiento de las etapas de potencia.*

Nivel de la señal de entrada	Ganancia driver + preamplifica dor	Ganancia por etapa de potencia	Atenuad or	Potencia de salida
<b>-30 dBm</b>	37 dBm	de 18 a 20 dB	-40 dB	-31,22 dBm

Para el cálculo de ganancia del driver se tiene que:

$$- 30 \text{ dBm} - 40 \text{ dB} + 44 \text{ dB} + X_{\text{Ganancia\_etapa\_potencia}} = - 7,96 \text{ dBm}$$

luego

$$X_{\text{Ganancia\_etapa\_potencia}} = 18,43 \text{ dBm}$$

Con esta información se verificó que la etapa de potencia funciona de acuerdo a lo esperado y, seguidamente, fueron probadas las otras dos etapas de potencia obteniendo se igual comportamiento. Finalmente se conectan todas las etapas para medir la señal de salida del equipo ya directamente desde su conector de salida.

Al realizar la medida en el conector de salida, con el analizador de espectros, se observó que el nivel de potencia era nulo, esto fue producido por el desperfecto del conector tipo N macho de la salida, como puede ser visto en la Figura 26.



**Figura 26** Fotografías que ilustran la avería del conector de salida tipo N.

Como se observa en la Figura 26 la razón por la cual el analizador de espectros no media ninguna potencia a salida del amplificador era porque el conector estaba averiado, para lo cual se procedió a cambiarlo por uno nuevo como se muestra en la Figura 27.



**Figura 27** Conector tipo N nuevo y conectado.

Después de la sustitución del conector tipo N(M) se pudo comprobar que la etapa de potencia está funcionando correctamente y que el amplificador *Amplifier Research* 500 watt, que trabaja en la banda de 10 kHz a 100 MHz, está operacional nuevamente.

### **3.3 Revisión y reparación del amplificador de 200 (W) de 80 – 1000MHz**

Como ya fue mencionado anteriormente la etapa de amplificación de potencia del sistema de *Jamming* de la AGRUCONGE está formado por dos amplificadores de la marca *Amplifier Research*. El primero, que fue presentado en la sección 3.2, ya está completamente recuperado y el segundo es un amplificador de 200 W destinado para cubrir la banda de 80 a 1000 MHz. Ese amplificador está constituido por dos etapas principales, una de pre-amplificación y la segunda constituida por la etapa de potencia propiamente dicha. A continuación, se detallará el procedimiento realizado en cada etapa:

### 3.3.1 Etapa de pre amplificación.

El subconjunto de pre-amplificación se encuentra constituida por cuatro partes principales, i.e.: la fuente de alimentación, el circuito de control, el driver de amplificación y de una primera etapa de amplificación y acoplamiento de la señal.

#### 3.3.1.1 Fuente de alimentación:

El correcto funcionamiento de la fuente principal de alimentación, para esta etapa, depende de una fuente DC de 20 V y 18,5 A. Para su control se requiere de una señal de activación que procede de una segunda fuente rectificadora de 24 V.

Para verificar el funcionamiento de las fuentes, estas fueron aisladas del resto de los subsistemas para mantener los demás componentes a salvo en caso de ocurrir un mal funcionamiento de estas. Inicialmente se comprobó el funcionamiento de la fuente reguladora de 24 V (figura 28), la cual activará la fuente principal.



**Figura 28** Fuente reguladora 24(V).

A partir de esto se verificó que la mencionada fuente está trabajando correctamente. Posteriormente, se procedió a realizar la conexión con la fuente principal para comprobar su operación. Para esta fase se requiere que la entrada de 110 V AC esté aplicada a la fuente regulada de 24 V y,

adicionalmente, que la señal de power sea activada mediante el switch del panel frontal del amplificador. Al realizar las conexiones pertinentes se pudo comprobar que la fuente se encuentra funcionando correctamente, ver Figura 29.



*Figura 29* Fuente principal 20 V.

### 3.3.1.2. Circuito de Control

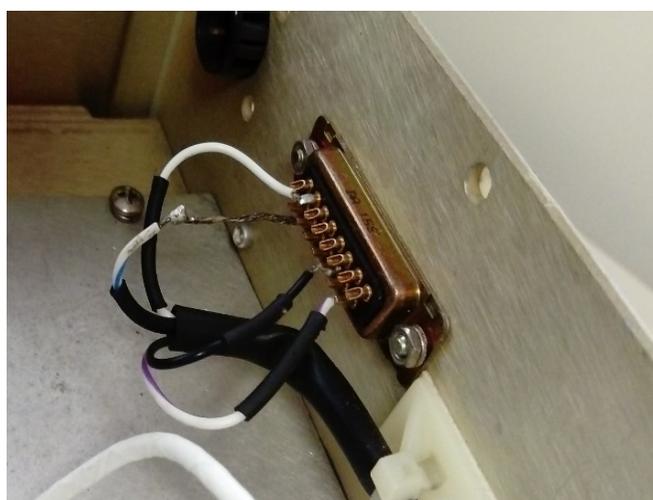
Una vez comprobado el buen funcionamiento de las fuentes de poder se conectó el circuito de control que se encuentra junto a la fuente principal. Al encender el equipo, en caso de que exista una condición de error, el señalizador de mal funcionamiento se iluminará indicando el tipo de error presente. Al encender el equipo no se iluminó ningún indicador, por lo cual se conjeturó que el circuito de control trabajaba de forma adecuada.

En lo referente a la etapa de preamplificación, sin embargo, al realizar la conexión de la etapa final de amplificación se observó que la señal de falla en el amplificador final se encontraba encendida. Esto se debía a dos errores dentro del equipo. El primer error, ubicado en la etapa de preamplificación, correspondía a una desconexión del pin número 10 del conector que se encuentra en la parte posterior del preamplificador. Este pino recibe señales de control y las

fotografías del defecto encontrado, así como de su reparación son presentadas en la Figuras 30 y 31.



*Figura 30* Ruptura pin 10.

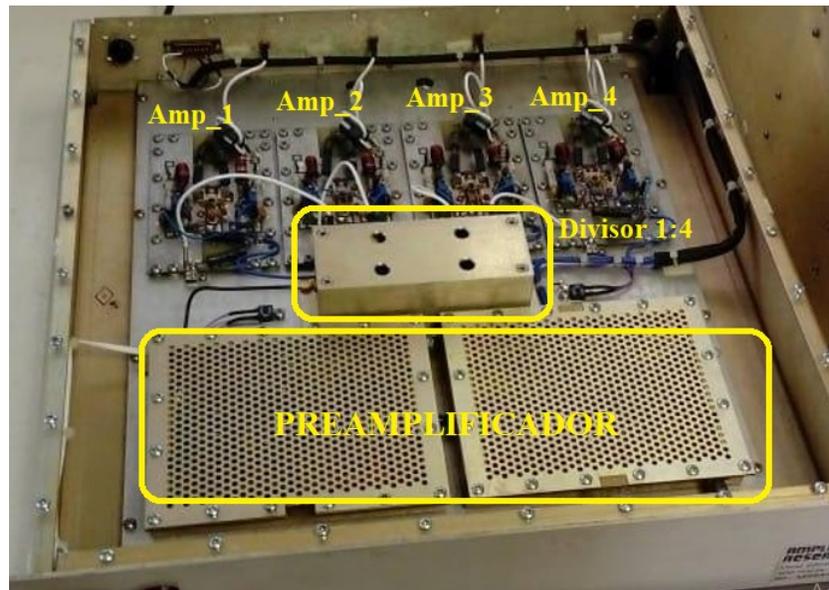


*Figura 31* Reparación del pin 10.

### 3.3.1.3. Driver y amplificador:

En cuanto a la etapa de driver esta se encuentra constituida por un preamplificador y un driver que se encargan de dar una ganancia de 30 dB a la señal de entrada. Para comprobar el funcionamiento de esta etapa se aplicó una señal de RF con un nivel de -30 dBm a la entrada del conjunto preamplificador más driver. El nivel de la señal obtenida en su salida fue de 0 dBm, con lo cual se comprobó el correcto funcionamiento del conjunto. Adicionalmente, se realizó un barrido dentro del espectro de frecuencias que corresponde al equipo comprobando a su vez la linealidad de esta etapa. La señal de la salida de este conjunto es aplicada a la entrada de un divisor o *splitter*, el mismo que divide la señal en una relación 1:4. Cada una de estas salidas se ingresa a la entrada de cuatro etapas de amplificación que trabajan en paralelo y de forma independiente. Se resalta que la ganancia de cada una de estas etapas puede variar en un rango de 0 a 10 dB y es controlada por un selector de ganancia ubicado en el panel frontal del equipo. De la misma forma se debe mencionar que la fase de todas las entradas de las cuatro etapas de amplificación están en fase lo que permite que sus salidas puedan ser correctamente acopladas en la etapa final de potencia.

Con el objetivo de comparar el desempeño de las cuatro etapas de potencia con los datos disponibles en el manual de mantenimiento, se realizó la medición de la potencia de entrada y salida para realizar el cálculo de su VSWR del sistema. La correcta operación de la etapa de preamplificación fue la conclusión al obtener valores de VSWR a uno, el VSWR obtenido fue 1,01725. Una fotografía del divisor y de la etapa de preamplificación es presentada en la figura 32.



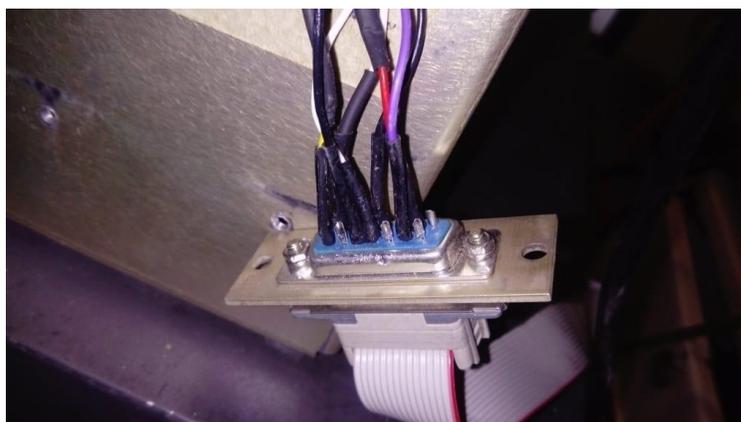
*Figura 32* Etapa final de pre-amplificación.

#### 3.3.1.4. Etapa final de potencia:

Esta etapa se encuentra formada por una etapa de alimentación, por 16 sub-bloques de amplificación y un sumador de RF de dieciséis entradas a una salida. Al iniciar con el diagnóstico se trató de poner en operación esta etapa, la misma que reflejó en los leds mencionados anteriormente un fallo en la temperatura y en el voltaje de la etapa. Al abrir el equipo para continuar con el diagnóstico se observó que el pin número 2 (figura 33) en el conector que envía las señales de control a la etapa de pre-amplificación se encontraba averiado. Después de la sustitución del conector se solucionó el problema de la señal de fallo en el voltaje de la etapa final pero no el problema de temperatura.

Posteriormente, se determinó que esta señal provenía de la medición de varios sensores de temperatura posicionados en la etapa de amplificación y de acoplamiento. Al realizar una inspección de la conexión de estos sensores se pudo determinar que el fallo se debía a que uno de los sensores ubicados en la etapa de acoplamiento se encontraba averiada. Reparado este sensor

la etapa final del equipo pudo volver a operar y se continuó con el diagnóstico, como se detalla a continuación.



*Figura 33* Conector D-sub reemplazado.

### **3.3.2. Fuentes de alimentación:**

El subsistema de alimentación consiste de una etapa de reducción de voltaje, mediante un transformador que lleva el voltaje de entrada de 110 V AC a 23 V AC. La función de esa etapa es alimentar la etapa posterior de rectificación. Inicialmente fueron verificados estos valores, una vez corroborado los niveles de alimentación las fuentes que convierten el voltaje de 23 V AC a un voltaje DC de 20 V fueron comprobados. Dichas fuentes cumplen la función de alimentar las 16 sub-etapas de amplificación, las cuales requieren una fuente por cada sub-etapa. Se observó que una de estas fuentes se encontraba deshabilitada (Figura 34). Por tanto, se decidió realizar la medición de cada una de las fuentes para determinar cualquier avería en las mismas incluyendo la que se encontraba deshabilitada. Al realizar las mediciones se determinó que la tensión de la fuente deshabilitada era de 14 V, claramente distinta a los 20 V que entregaban las fuentes restantes.

Tras una inspección de la mencionada fuente se determinó que la variación del valor de tensión que está entregaba se debía a cambios en los valores nominales de los elementos de la fuente. Finalmente, varios valores de componentes que permitían ser alterados fueron reajustados

y la fuente pasó a operar correctamente. Sin embargo al conectarla a su respectiva sub-etapa de amplificación la fuente indicó un valor de falla en el voltaje de alimentación. Adicionalmente, se observó que cuando la corriente que cada sub-etapa de amplificación consumía era de 3 A la correspondía a la fuente deshabilitada era del doble, es decir 6 A. Este comportamiento nos permitió inferir que la sub-etapa de amplificación se encontraba averiada, ya que su elemento de amplificación se encontraba quemado por lo que consumía demasiada corriente y eso había ausado que su respectiva fuente de alimentación se encontraría deshabilitada.

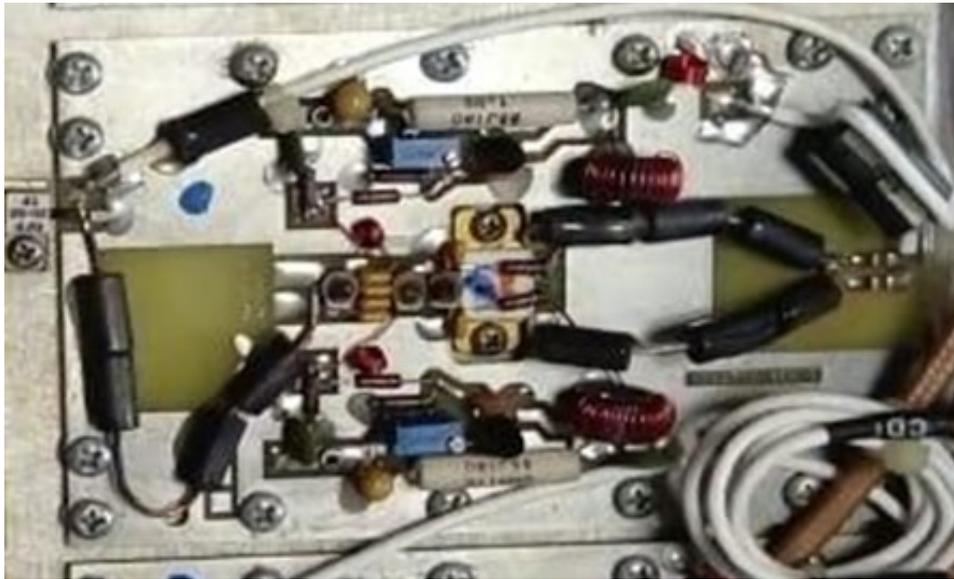


*Figura 34* Fuente regulada deshabilitada.

### **3.3.3. Amplificador de potencia:**

En la etapa de entrada del amplificador de potencia se tiene cuatro señales que son originadas desde la etapa de pre-amplificación. Cada una de estas señales es dividida en cuatro mediante un divisor 4:1. En total, estas dieciséis salidas son aplicadas a 16 sub-etapas de amplificación (ver figura 35). Cada una trabaja en paralelo y en fase de manera que las 16 señales de salida puedan combinarse de manera adecuada. De esta forma, este conjunto se encargan de entregar la potencia final de 200 W. Al realizar la inspección se encontró que una de las 16 sub-etapas se encontraba con una falla en la conexión del cable coaxial. Tras una inspección como se detalló anteriormente se pudo determinar que esta sub-etapa

se encontraba averiada, por lo cual se mantuvo deshabilitada (no fue posible conseguir el repuesto necesario para dejarlo operacional).



*Figura 35* Sub-etapa de amplificación averiada.

#### **3.3.4. Combinador de señales de 16 entradas y 1 salida:**

La función del combinador de 16:1 es realizar la suma de la potencia de salida de los 16 amplificadores de potencia y presentarla en una única salida de RF. Al realizar un diagnóstico de este componente se encontró que una de las 16 entradas se encontraba desconectada (ver figura 36). Posteriormente, se determinó que esta señal correspondía a la etapa del amplificador de potencia que se encontraba con avería. Por lo que en su lugar se colocó una carga de 50 ohmios para mantener el balance del combinador.

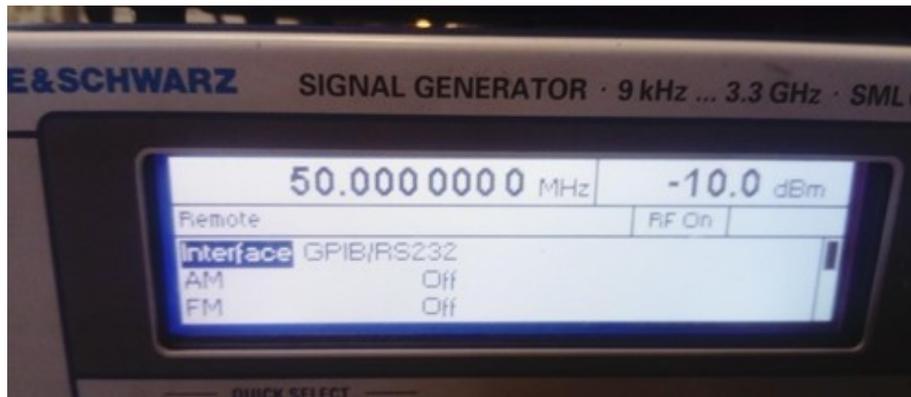


**Figura 36** Señal desconectada en acoplador.

### **3.4. Utilización del Generador de señales Rohde&Schwarz**

En todas las pruebas realizadas para comprobar el funcionamiento de los amplificadores se utilizó el generador *Rohde&Schwarz SML01* (figuras 37 - 40). Este equipo fue seleccionado para las pruebas por tener las opciones necesarias para generar una señal de RF para simular el Jamming, conforme se detallada a continuación.

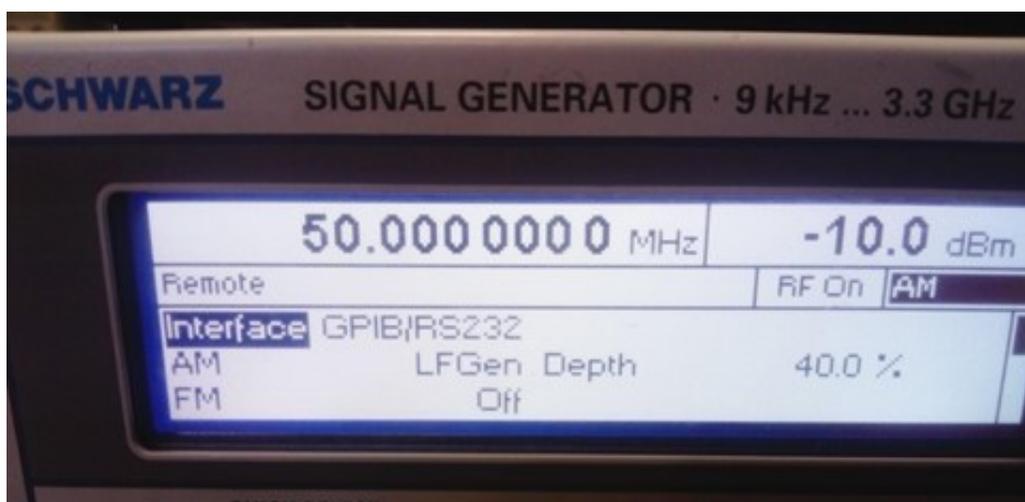
- Posee una conexión serial la cual será utilizada para facilitar la configurar del equipo y tornar la más amigable con el usuario.
- Tiene la capacidad de generar señales moduladas de forma interna y obtener una señal combinada en su salida.
- Su operación es muy amigable con el usuario y toda su información está en su manual.



*Figura 37* Generador conectado con comunicación serial.



*Figura 38* Generador activado la modulación FM mediante comunicación serial.



*Figura 39* Generador activado la modulación AM mediante comunicación serial.



**Figura 40** Conectores para salida e ingreso de señales a ser moduladas.

### 3.5. Utilización de una interfaz gráfica

Se implementó una interfaz gráfica para que los usuarios no manipulen el equipo directamente y también para reducir el riesgo de daños por mala utilización del equipo. La interfaz se diseñó en *Visual Studio* en lenguaje C# por su facilidad de implementación y por sus herramientas. Para la comunicación con el generador de señales se escogieron parámetros de sincronía correspondientes al protocolo de comunicación RS232. Generando el código mostrado en la Figura 41.

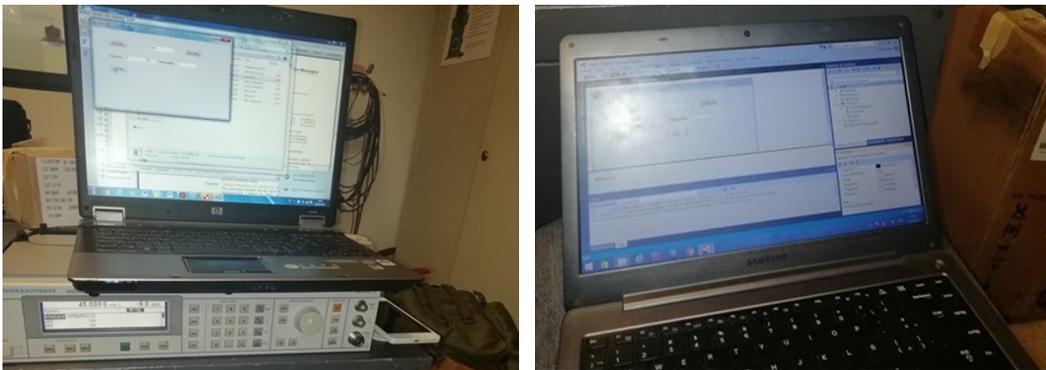
```

1 referencia
private void BtnBuscarPuertos_Click(object sender, EventArgs e)
{
    string[] PuertosDisponibles = SerialPort.GetPortNames();
    CboPuertos.Items.Clear();
    foreach (String puerto_simple in PuertosDisponibles) {
        CboPuertos.Items.Add(puerto_simple);
    }
    if (CboPuertos.Items.Count > 0) {
        CboPuertos.SelectedIndex= 0;
        MessageBox.Show("Seleccionar el puerto");
        BtnConectar.Enabled = true;
    }
    else {
        MessageBox.Show("Ningun puerto detectado");
        CboPuertos.Items.Clear();
        CboPuertos.Text = " ";
        strBufferOut = "";
        BtnConectar.Enabled = false;
        BtnEnviarDatos.Enabled = false;
    }
}
}

```

**Figura 41** Código de comunicación serial y conexión con el puerto.

Se realizaron pruebas con el generador y un computador mediante el Software PUTTY utilizado para la comunicación serial y así poder observar la comunicación entre estos y variar los parámetros del generador para verificar todos los comandos posibles a ser accedidos mediante la interfaz creada.



**Figura 42** Esquema de comunicación entre el generador SML01 y el computador.

Para poder realizar pruebas de funcionamiento de la interfaz implementada se realizó un ejecutable portátil para no depender de herramientas de compilación. De esta manera, se creó la aplicación final mostrada en la Figura 43 con todos los parámetros necesarios para la generación de señales de Jamming.



**Figura 43** Interfaz de usuario desarrollada para controlar el generador SML01.

### 3.5. Verificación de las antenas de 20 – 100 MHz y de 80 – 1000MHz

Para verificar fallas en la estructura mecánica o en los conectores de RF de las antenas se procedió con el ensamblaje de las mismas. Fueron encontrados problemas con los tornillos destinados para fijar los dipolos en la antena de 80 – 1000 MHz y en los fijadores de los dipolos a la antena de 20 – 100 MHz, como se muestran en las Figuras 44 y 45.

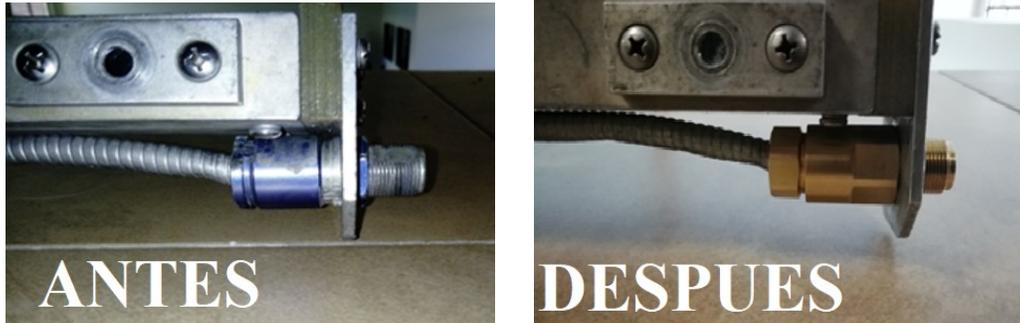


**Figura 44** Dipolos de la antena de VHF.



**Figura 45** Tornillos de fijación de los dipolos de la antena de HF.

Inmediatamente, fueron substituidos los tornillos fijadores dañificados y se ensambló las antenas para que estén listas para su verificación funcional. Al conectar las antenas se observó que la antena de 20 – 100 MHz no estaba funcionando y al revisar su conector tipo N se verificó que estaba roto por lo que se procedió a remplazarlo como se muestra en la figura 46.



(a)

(b)

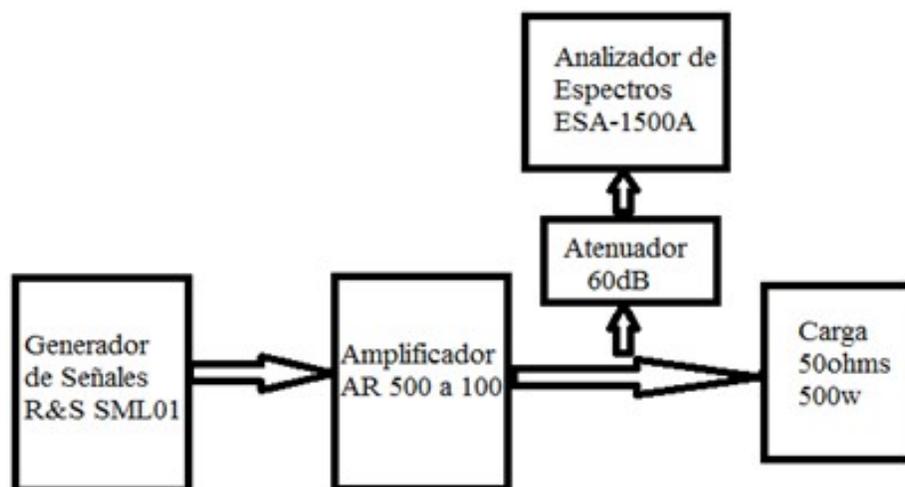
**Figura 46** Fotografías del conector tipo N de la antena de 20 – 100 MHz. En (a) conector dañado y en (b) conector sustituido.

## CAPÍTULO 4

### 4. PRUEBAS DE FUNCIONAMIENTO

#### 4.1. Pruebas de funcionamiento del amplificador de 10 kHz – 100 MHz

Una vez realizado el diagnóstico del equipo y habiendo reparado el mismo, el siguiente paso corresponde en cerciorarse del correcto funcionamiento del mismo, para dicha prueba el escenario planteado fue el ilustrado en la figura 47.



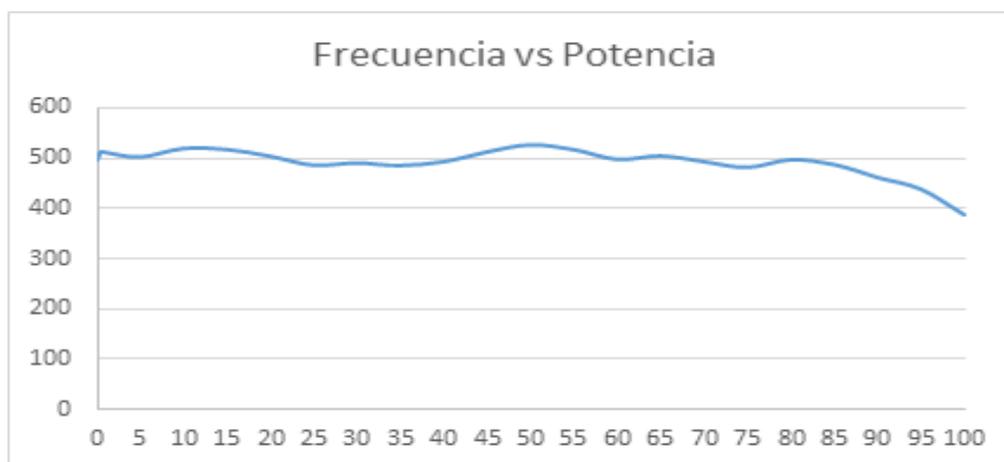
**Figura 47** Escenario prueba de funcionamiento amplificador de 10 kHz – 100 MHz.

En el escenario planteado se introdujeron en el generador de señales R&S SML01 los parámetros especificados para que el amplificador opere en máxima potencia, el mismo que corresponde a una potencia de entrada máxima igual a 0 dBm, con este valor de potencia se realizaron mediciones en el rango de frecuencias de operación del equipo, es decir entre (10 kHz – 100 MHz) obteniendo los resultados presentados en la Tabla 5 y en la Figura 48.

**Tabla 5**

*Potencia de salida versus frecuencia de operación (0 dBm entrada).*

Frecuencia	Potencia	Frecuencia	Potencia	Frecuencia	Potencia
[MHz]	[W]	[MHz]	[W]	[MHz]	[W]
0,1	497,452	30	491,198	70	493,79
0,5	513,214	35	485,982	75	482,261
1	512,465	40	493,745	80	497,537
5	502,963	45	513,244	85	488,085
10	520,132	50	527,608	90	462,036
15	518,324	55	518,062	95	438,304
20	504,574	60	498,315	100	386,893
25	486,853	65	505,422		

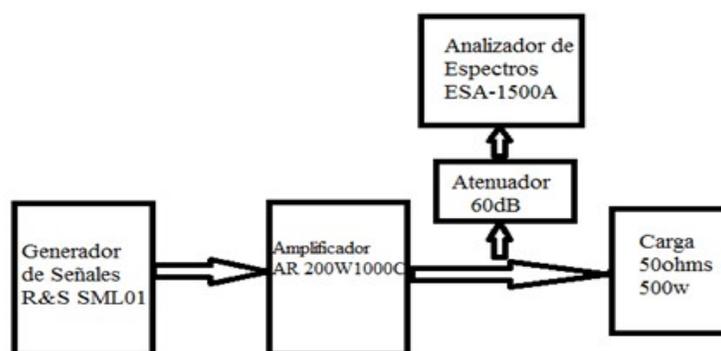


**Figura 48** Potencia de Salida amplificador 10 kHz - 100 MHz.

Con base a los resultados presentados anteriormente se puede observar que la potencia de salida entregada por el amplificador se encuentra dentro del rango adecuado especificado en el manual, el cual es de 500 watts de potencia de salida, comprobando así el correcto funcionamiento del equipo trabajando a máxima potencia.

#### 4.2. Pruebas de funcionamiento del amplificador 80 MHz – 1000 MHz.

De manera similar a la prueba anterior e ilustrado en la figura 47 se ilustra, a seguir, el diagrama para evaluar el amplificador de 80 MHz – 1000 MHz.



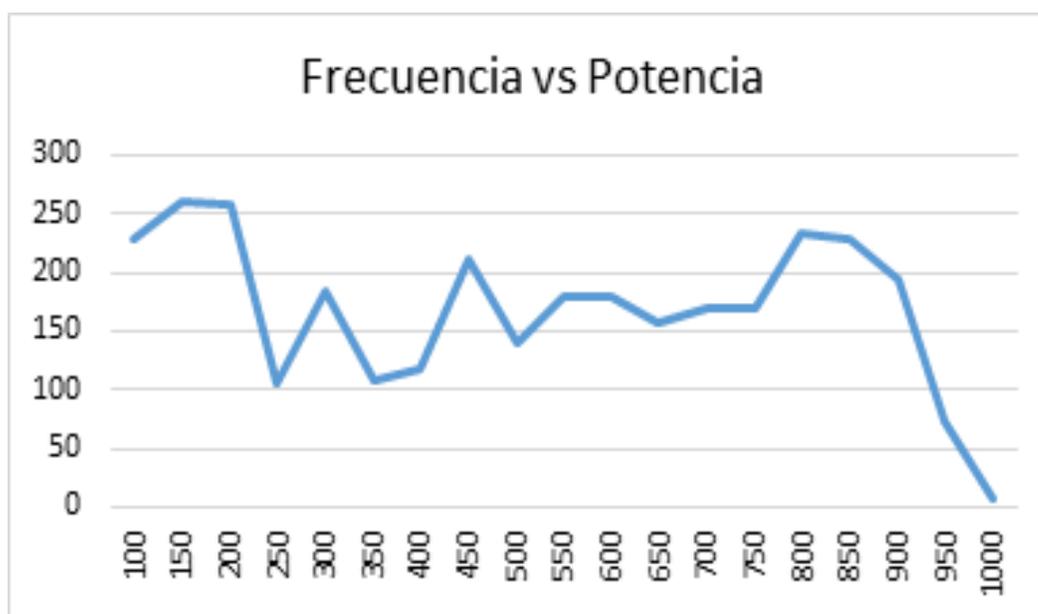
**Figura 49** Escenario prueba de funcionamiento amplificador de 80 MHz – 1000 MHz.

En el escenario planteado se introdujeron en el generador de señales R&S SML01 los parámetros especificados para que el amplificador trabaje en máxima potencia, esto es nivel de potencia de entrada igual a 0 (dBm). Con este valor de potencia de entrada se realizaron mediciones en el rango de frecuencias de interés del equipo, es decir entre 100 MHz a 1000 MHz obteniendo los siguientes que son presentados en la Tabla 6 y en la Figura 50.

**Tabla 6**

*Potencia de Salida versus Frecuencia de Operación.*

Frecuencia	Potencia	Frecuencia	Potencia	Frecuencia	Potencia
[MHz]	[W]	[MHz]	[W]	[MHz]	[W]
100	228,5599	450	212,3244	800	234,4229
150	261,2161	500	139,3157	850	228,0342
200	257,0396	550	179,0606	900	193,6422
250	105,9254	600	179,8871	950	73,79042
300	184,9269	650	157,3983	1000	8,279422
350	108,893	700	168,6553		
400	118,3042	750	170,6082		



*Figura 50* Potencia de Salida amplificador AR 200W1000C.

Con los resultados obtenidos es posible observar que la potencia de salida entregada por el amplificador se encuentra fluctuando dentro del rango especificado en el manual para este equipo es decir 200 watts de potencia a la salida del amplificador, comprobando así el funcionamiento del mismo, pese a que una de las 16 etapas de salida se encontraba deshabilitada.

Una vez que se han recuperado ambos amplificadores y se ha verificado el correcto funcionamiento de los mismos, es posible pasar a la etapa de pruebas del sistema de Jamming para el AGRUCOMGE. Para esto se empleará un Spot Jamming, así como un Jamming Reactivo en las pruebas que se detallan a continuación.

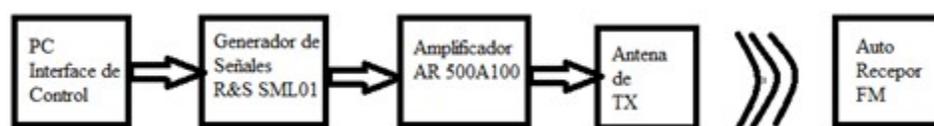
#### **4.3. Pruebas de funcionamiento del sistema de Jamming**

Para la comprobación del sistema se plantearon varias pruebas entre las cuales inicialmente se realizó un ataque a los receptores de prueba dentro del campus de la Universidad de Las Fuerzas

Armadas, modificando la posición del Jammer, para posteriormente realizar pruebas junto con el accionar del sistema de monitoreo de señales COMINT mediante el cual se obtuvieron las características de varias señales que actuarían como objetivo a ser interferido.

#### 4.3.1. Prueba de Jamming a receptor de prueba con la antena a 2 m de altura sobre el móvil.

Para el accionar de esta prueba se seleccionaron inicialmente dos receptores de prueba que se encontraban dentro del rango de operación de cada amplificador. El objetivo de la prueba es determinar el funcionamiento del sistema de Jamming y a su vez establecer el nivel de cobertura subjetiva que se obtiene al realizar el ataque, para lo cual se colocó ambas antenas a una altura de 2 m del suelo, adicionalmente la señal que sería inyectada a través del Jammer es una señal centrada en la frecuencia mencionada anteriormente correspondiente a cada equipo, esta señal se encuentra modulada en frecuencia con una desviación de 230 kHz para asegurar la anulación total del objetivo. Adicionalmente se moduló la señal con un tono de 1 kHz para que la interferencia fuera apreciable de manera que se note claramente el funcionamiento del sistema, el escenario planteado para la prueba fue el descrito a continuación.



*Figura 51* Escenario Jamming a receptor de prueba a 2m de altura.

Al accionar el generador de señales con las características señaladas anteriormente y colocar la potencia de salida del amplificador en 200 W, se dispuso un auto con el receptor de prueba y

adicionalmente se indicó que el auto recorriera una trayectoria por el campus de la universidad para determinar el área de cobertura del Jammer. Obteniendo una cobertura del 30% del terreno, esto debido a la baja altura de la antena transmisora, así como de varios obstáculos que se encuentran dentro del campo como edificios y árboles de gran tamaño. Además, es necesario tomar en cuenta que el campus de la Universidad de Las Fuerzas Armadas se encuentra en un terreno inclinado y la transmisión se realizó desde uno de los puntos más bajos del terreno. Sin embargo, al sintonizar la frecuencia mencionada en el receptor de prueba se comprobó claramente el accionar del sistema de Jamming dentro del área de cobertura el mismo que resultó claramente audible debido al tono de 1kHz con el cual se realizó el ataque.



**Figura 52** Escenario Jamming a receptor de prueba a 2m de altura.

Para el caso en que se utilizó el amplificador de 100 - 1000 MHz inyectando una señal de características similares al caso anterior, es decir, con una modulación en frecuencia con una desviación de 230 kHz y un tono de 1 kHz, obteniendo resultados similares a los producidos por el amplificador anterior.



**Figura 53** Cobertura del campus prueba a 2m de altura.

#### 4.3.2. Prueba de Jamming con altura a 5,5m de altura.

El objetivo de la prueba es determinar nivel de cobertura que se obtiene al realizar el ataque, para lo cual se colocó ambas antenas a una altura de 5,5m del suelo, adicionalmente las señales que serían inyectadas a través del Jammer son las mismas del ítem anterior, y el escenario planteado para la prueba fue el descrito a continuación.



**Figura 54** Escenario Jamming a receptor FM a 5,5m de altura.

Al accionar el generador de señales con las características señaladas anteriormente y colocar la potencia de salida del amplificador en 200 W (máxima potencia para este equipo), se dispuso un auto con el receptor de prueba, adicionalmente se indicó que el auto realizase un recorrido por el campus de la universidad para determinar el área de cobertura del Jammer, obteniendo una cobertura del 45% del terreno.



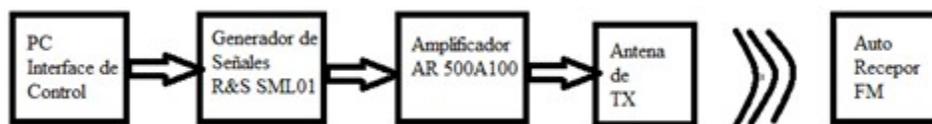
**Figura 55** Antena de transmisión a 5,5m de altura, amplificador de 10 kHz –  
100 MHz.



**Figura 56** Cobertura del campus prueba a 5,5m de altura, banda de  
10 – 1000MHz.

#### **4.3.3. Prueba de Jamming a receptor de prueba a una altura de 15 metros.**

En esta prueba se hará uso de las frecuencias seleccionadas previamente. El objetivo de la prueba es determinar nivel de cobertura que se obtiene al realizar el ataque desde una altura de 15 m, para lo cual se colocó ambas antenas a una altura de 15 m del suelo, el escenario planteado para la prueba fue el descrito en la primera prueba.



**Figura 57** Escenario Jamming a receptor de prueba a 15 m de altura.

Al comparar los resultados presentados en las pruebas realizadas, fue posible comprobar el correcto funcionamiento del sistema de Jamming de la AGRUCOMGE, ya que las señales que se tomaron como objetivos eran inhibidas con éxito al accionar los amplificadores corroborando que el ataque a determinada señal puede realizarse con éxito. Adicionalmente, los resultados del área de cobertura revelaron que al momento de realizar un ataque en un contexto de guerra electrónica se requiere tener en cuenta factores como la topografía del terreno y los obstáculos que pueden estar presentes. De estos factores depende el éxito del ataque. Así mismo otro factor que debe ser llevado en consideración es la altura para maximizar los efectos del Jamming. Para finalizar se concluyó que para realizar un ataque efectivo de Jamming es necesario el trabajo conjunto entre este y el sistema de monitoreo de señales COMINT, para lo cual se realizaron pruebas adicionales.



**Figura 58** Cobertura del campus prueba a 15m de altura.

#### 4.4. Pruebas del sistema de Jamming en conjunto con el sistema COMINT

Para la ejecución de estas pruebas se organizó un grupo de trabajo dentro del sistema de monitoreo de señales COMINT (ver figura 59), el cual se encargó de realizar un barrido del espectro de frecuencias presentes en el campus de la Universidad de las Fuerzas Armadas, para posteriormente seleccionar una de estas señales y obtener sus parámetros característicos, tales como:

- Frecuencia central.
- Ancho de banda.
- Coordenadas del posible receptor.

De manera que estas características fueran entregadas al sistema de Jamming del AGRUCOMGE para ser colocadas dentro de los equipos y proceder a realizar el ataque a las señales seleccionadas como objetivo, una vez que el ataque era realizado el sistema COMINT se encargó de monitorear la señal objetivo para corroborar que el ataque había sido exitoso, con este procedimiento se realizaron varias pruebas en diferentes frecuencias obtenidas por el COMINT, a continuación, se presentan los resultados obtenidos para las frecuencias de prueba. Para las cuales se realizó el proceso detallado con anterioridad.



**Figura 59** Sistema de monitoreo de señales COMINT.

### **Prueba 1**

Se realizaron dos pruebas conjuntas ente el JAMMING y el COMINT. En la primera se observó que el ataque en la frecuencia blanco no se realizó con el éxito deseado. La señal planificada como objetivo debido a que no se compartieron de manera adecuada las características de la señal, en este caso el dato erróneo fue el de la frecuencia central por lo cual se puede apreciar que la señal no se logra inhibir por completo.

Como se puede apreciar en las figuras 60 y 61, en la primera se muestra el objetivo captado por el COMINT la cual corresponde a la frecuencia de prueba y en la segunda figura es posible apreciar la señal que se encuentra interferida por el ataque emitido desde el sistema de jamming de la AGRUCOMGE en donde se aprecia claramente que esta se encuentra interferida, más no totalmente ya que la frecuencia central no es la adecuada para conseguir suprimir por completo la señal que se ha tomado como objetivo previamente, el error se produjo por un fallo entre la comunicación desde el sistema COMINT con el sistema de Jamming del AGRUCOMGE, razón por la cual resulta propicio un entrenamiento previo a la ejecución práctica de ambos sistemas, el mismo que se llevó a cabo en una capacitación y pruebas que se realizaron por el personal militar que manipulará los equipos la cual será detallada más adelante.



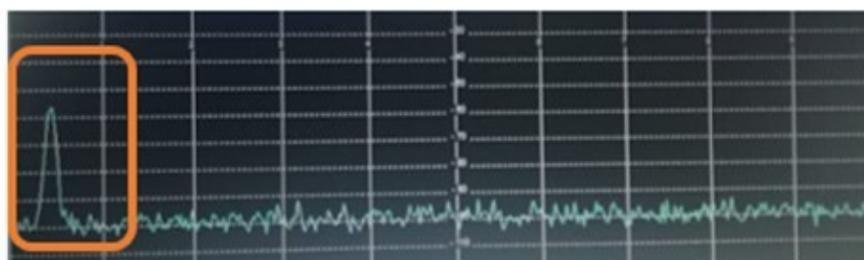
**Figura 60** Señal objetivo COMINT prueba 01.



**Figura 61** Señal objetivo Jamming COMINT prueba 01.

## Prueba 2

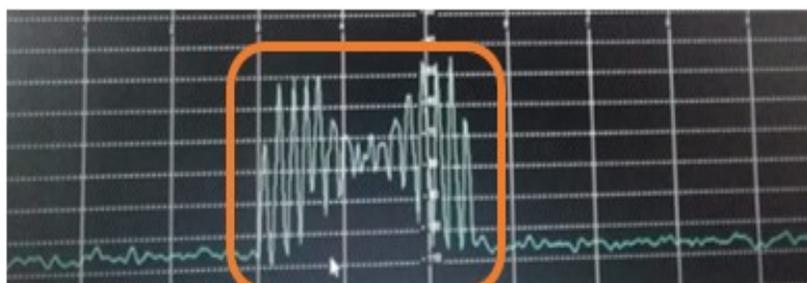
En este caso se detalla una prueba realizando un ataque exitoso a la señal de prueba 02, de manera similar al caso anterior, la frecuencia fue encontrada gracias a un barrido del espectro realizado por el sistema de monitoreo de señales COMINT, el cual entregó las características de la misma al sistema de Jamming, en donde se planteó un escenario igual al de las primeras pruebas detalladas anteriormente de manera que se realizará un ataque a la frecuencia seleccionada como objetivo, posteriormente se puso en operación los equipos correspondientes para realizar el ataque, con lo cual el sistema COMINT se encargó de monitorear nuevamente el objetivo para corroborar que el ataque que se estaba llevando a cabo fuera completamente exitoso, lo cual se puede apreciar en las figuras presentadas a continuación.



**Figura 62** Señal objetivo COMINT prueba 02.

Como se puede apreciar en la figura 62, se encuentra la señal objetivo a la cual se realizará el ataque, el procedimiento posterior a su localización es la obtención de su frecuencia

central, así como su ancho de banda, de manera que estos valores puedan ser usados para generar la señal de Jamming, la misma que se observa en la figura 63.



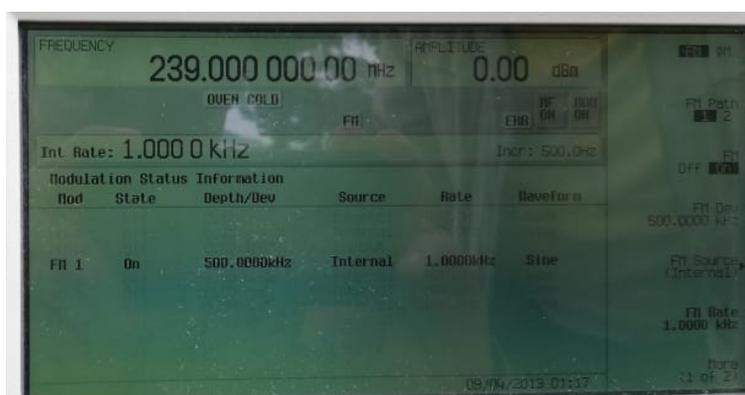
*Figura 63 Señal objetivo Jamming COMINT prueba 02.*

En la figura 63, se encuentra el resultado del ataque generado a la señal correspondiente a la frecuencia de prueba 02 tomada como objetivo, es posible apreciar que la señal se encuentra completamente interrumpida por la señal generada en el sistema de Jamming de la AGRUCOMGE, como se señaló con anterioridad al realizar un ataque es necesario tener en cuenta si resulta más beneficioso atacar al emisor o al receptor de la señal, para este cometido el sistema de monitoreo de señales COMINT puede obtener las coordenadas del emisor de la señal de manera que se oriente la antena del Jammer para poder inhibir al emisor, sin embargo para las pruebas planteadas se decidió atacar únicamente a los receptores por lo cual la ubicación de los emisores de ambas señales atacadas fue obviado ya que el objetivo de las pruebas era coordinar el trabajo entre el sistema COMINT y el sistema de Jamming de la AGRUCOMGE.

#### **4.5. Jamming al sistema israelí ELBIT**

Adicionalmente se realizó una prueba de interferencia al sistema de comunicaciones israelí ELBIT, el mismo que trabaja a una frecuencia de 239 MHz, con un ancho de banda de 1 MHz, estos parámetros fueron introducidos en el generador de señales adicionando una

modulación FM cuya frecuencia interna correspondió a 1kHz, usando una potencia de 0 dBm a la salida del generador, estos parámetros se pueden apreciar en la figura 64.



**Figura 64** Parámetros de la señal de jamming.

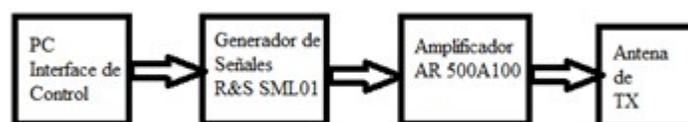
Con los parámetros especificados anteriormente es posible obtener una señal de 42,1 dBm de potencia a la salida del amplificador, con lo cual fue posible realizar un bloqueo total en la operación del sistema ELBIT como se ilustra en la figura 65, en donde se aprecia que la señal se encuentra completamente intervenida por la señal generada por el sistema de Jamming, corroborando de esta manera su correcto funcionamiento.



**Figura 65** Sistema ELBIT interferido.

#### 4.6. Capacitación Práctica al personal Militar

Para la capacitación práctica al personal militar como se mencionó anteriormente se realizó una interfaz que permite el manejo del generador de señales para facilitar y agilizar la operación del sistema, por lo cual se presentó el escenario de la figura 66 a los asistentes de la capacitación.



**Figura 66** Capacitación: Escenario de equipos.

Para iniciar la capacitación se tomó como punto de inicio la conexión que debe llevarse a cabo entre los equipos, especificando los cables y conectores que se requieren, tanto para la conexión serial entre el PC y el Generador de señales R&S SML01 para la cual se utiliza un cable RS232, así como los que se encargan de conectar el generador de señales con los amplificadores y a cada amplificador con su respectiva antena para esto se usan cables coaxiales de bajas pérdidas con conectores tipo N. Una vez se culminó este paso el siguiente procedimiento consistió en instruir a los futuros operarios las secuencias de encendido de los amplificadores ya que cada uno maneja una secuencia distinta, para el caso del amplificador 10 kHz – 100 MHz, su secuencia de arranque es:

- Girar la llave en el panel frontal hasta la posición de encendido.
- Pulsar el botón de *Power* (Botón blanco) situado en el panel frontal.
- Cerciorarse de que la ganancia del equipo se encuentre en el nivel más bajo (este nivel se modificará de acuerdo a lo necesario), para evitar la emisión de una potencia excesiva de arranque.

- Cerciorarse que el botón *Reset* (Botón Rojo) situado en el panel frontal se encuentre apagado.
- Presionar el botón *Operate* (Botón Verde) situado en el panel frontal.

Para apagar el equipo el procedimiento a seguir es el contrario al encendido con un ligero cambio, es decir:

- Presionar el botón *Standby* (Botón Amarillo) Situado en el panel frontal.
- Presionar el botón *Power* (Botón Blanco)
- Girar la llave hasta la posición de apagado.



**Figura 67** Capacitación: Secuencia de encendido de equipos.

Una vez realizados estos pasos el equipo se encontrará completamente apagado, Para el amplificador de 100 MHz – 1000 MHz, el procedimiento de encendido es mucho más sencillo, consiste en:

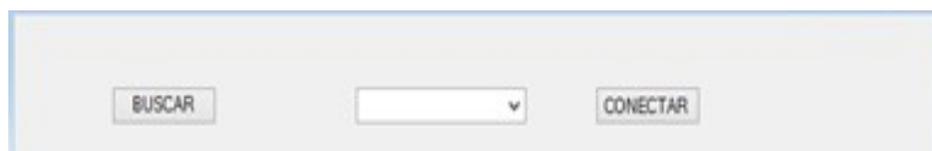
- Cerciorarse que la ganancia del equipo situada en el panel frontal se encuentre en el nivel más bajo.
- Presionar el Swtich de *Power* negro colocado en la parte superior del panel frontal del equipo.
- Presionar el Swtich de *Power* blanco colocado en la parte Media del panel frontal del equipo.

Para el procedimiento de apagado de debe realizar el procedimiento contrario:

- Presionar el Swtich de *Power* blanco colocado en la parte Media del panel frontal del equipo.
- Presionar el Swtich de *Power* negro colocado en la parte superior del panel frontal del equipo.

El siguiente paso fue enseñar el manejo del software para la manipulación de la señal que se usará para el sistema de Jamming, dicho software puede dividirse en varios pasos siendo el primero la conexión entre la PC y el generador de señales R&S SML01.

En la figura 68 se ilustran los botones correspondientes a la conexión entre el PC y el generador de señales, el procedimiento a realizar es pulsar el botón BUSCAR el cual nos informará en qué puerto se encuentra conectado el generador de señales y permitirán seleccionarlo, para continuar se debe pulsar el botón CONECTAR una vez realizado este paso se habilita el siguiente nivel del software el cual se ilustra a continuación.



**Figura 68** Capacitación: Etapa de conexión entre PC y generador de señales.

En este nivel inicia la entrada de valores para la señal que se usó como Jammer, en donde es posible ingresar el valor de la frecuencia de la señal y seleccionar su respectiva medida (Hz, kHz, MHz o GHz), adicionalmente se ingresa el nivel de potencia en dBm que se requiere inyectar al amplificador teniendo en cuenta que para obtener un desempeño máximo en ambos equipos este nivel de señal debe ser de 0 dBm y por último es posible seleccionar si la señal se encuentra encendida o apagada, para poder colocar estos datos en el equipo se debe presionar el botón ENVIAR.



**Figura 69** Capacitación: Etapa de selección de parámetros de la señal.

De igual manera si se requiere se puede resetear el equipo pulsando el botón RESET el que se encarga de apagar la señal de salida del equipo, así como apagar cualquier modulación que se encontrase activa en el equipo, finalmente en este nivel es posible escoger si se requiere adicionar a la señal una modulación ya sea AM o FM, una vez seleccionada el tipo de modulación requerida se activará el siguiente nivel dentro del software.

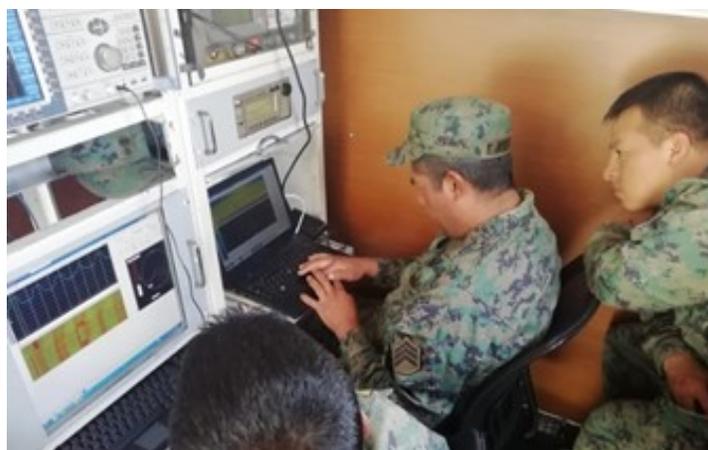
En el nivel mostrado en la figura 70 es posible escoger los parámetros principales de las modulaciones disponibles en el equipo, en donde los parámetros de Fuente y Acople

generalmente son constantes ya que son los que maneja el equipo internamente. Mientras que, para los parámetros de Profundidad, Frecuencia INT y Desviación, Frecuencia INT, dependiendo de la modulación usada siendo los primeros correspondientes a la modulación AM y los segundos a la modulación FM, los valores de aceptación cuentan con un sistema de mensajes que notificarán cada vez que se introduzca un valor erróneo o fuera del rango, una vez que todos estos parámetros se han colocado de manera correcta se presiona el botón ON el cual se encarga de enviar los datos al equipo y de esta manera generar la señal de jamming requerida.

The image shows a software interface with two rows of controls. The first row is for 'Profundidad (%)' and 'Frecuencia INT', and the second row is for 'Desviación (khz)' and 'Frecuencia INT'. Each row contains a text input field, a 'Fuente' dropdown menu, an 'Acople' dropdown menu, another text input field, and an 'ON' button.

**Figura 70** Capacitación: Etapa de selección de parámetros de modulación.

Con estos procedimientos debidamente puestos en práctica por cada uno de los asistentes a la capacitación se organizaron dos grupos para realizar pruebas similares a las detalladas en los incisos 4.2 y 4.4 de manera que los grupos se familiarizan con el trabajo conjunto entre el sistema COMINT y el sistema de Jamming.



**Figura 71** Capacitación: Pruebas sistema COMINT.



**Figura 72** Capacitación: Pruebas sistema Jamming.

Luego de realizadas estas pruebas varias veces y habiendo comprobado que los futuros operarios dominaban el manejo de ambos sistemas tanto de monitoreo de señales como de ataque a las mismas se dio con concluida la capacitación, así como la etapa de pruebas.

## CAPÍTULO 5

### 5. CONCLUSIONES Y RECOMENDACIONES

#### 5.1. Conclusiones

Se recuperó un valor estimado de \$ 118.600,00 tras realizar el diagnóstico del estado de los equipos del sistema de Jamming del AGRUCOMGE y luego del trabajo detallado en el capítulo 3 se consiguió volver a poner en operación ambos amplificadores y antenas dando paso a la rehabilitación del sistema de Jamming de la AGRUCOMGE.

Al desarrollar la metodología para la generación de las características de las señales usadas para el sistema de jamming, en base a las pruebas se determinó que resulta imperativo un análisis, así como un trabajo de inteligencia una vez localizado el objetivo para determinar la posición correcta del Jammer, así como tomar la decisión de interferir al receptor con el objetivo de que el ataque sea totalmente efectivo.

En el escenario de una guerra electrónica se concluyó que el trabajo conjunto del sistema de monitoreo de señales COMINT con el sistema de Jamming del AGRUCOMGE debe enfocarse en mantener una comunicación clara en cuanto a las características de los objetivos de manera que se asegure la mayor efectividad posible en el ataque, de igual manera se concluye que dentro del estudio a realizarse previo al ataque es necesario escoger el mejor método de jamming para el caso que se trabaje.

## 5.2. Recomendaciones

Para la manipulación de los equipos y en cuanto a la conexión de los mismos se recomienda tener en cuenta siempre las secuencias de encendido y apagado de cada uno de ellos, así como el uso de cables conectores adecuados para cada equipo y sus respectivas antenas de modo que se prolongue la vida útil de los mismos.

Al realizar un ataque se recomienda tener en cuenta las características del terreno, sus obstáculos, así como determinar la posición correcta del jammer con el objetivo de que la señal no presente grandes pérdidas en su potencia, las cuales podrán ser mayormente causadas por la presencia de obstáculos como bosques o edificaciones.

Al escoger el ataque que se realizará es recomendable usar un Spot Jamming Reactivo ya que este se encargará de abarcar todo el ancho de banda de la señal objetivo y a su vez reduce la posibilidad de detectabilidad en el ataque.

## 6. BIBLIOGRAFÍA

- CHAPACA, C. N. (2016). *Diseño E Implementación de un Inhibidor (Jammer) de señales de redes Wi-Fi para la red de CISCO*. Quito: Universidad Politécnica Salesiana.
- Zhang Yu, L. F. (s.f.). *RMR Method for Jamming Air-ground and Mobile*. Chongqing, China: School of Computer and Information Science, Southwest University.
- Alvarez, A., Garcia, Z., & Ruiz, M. (s.f.). *Antenas y Propagación*. Obtenido de <http://antenasypropagacionuft.blogspot.com/2013/05/antenas.html>
- CONATEL. (17 de diciembre de 2014). *Agencia de Regulación y Control de las Telecomunicaciones*. Obtenido de ARCOTEL: <http://www.arcotel.gob.ec/wp-content/uploads/downloads/2015/06/Norma-Tecnica-Actualizada-de-FM-RTV-973-29-CONATEL-2014.pdf>
- Nave, C. R. (2014). *HyperPhysics*. Obtenido de <http://hyperphysics.phy-astr.gsu.edu/hbasees/Electronic/amtran.html>
- División, R. &. (s.f.). *Operating Manual R&S SML01*. Alemania: Rohde & Swarz GmbH & Co. KG. Recuperado el Noviembre de 2018
- Pantaleone Nespoli, D. P. (2017). *Optimal Countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks*. IEEE.
- Robert J. McEliece, E. R. (1983). *A study of optimal abstract jamming strategies vs. Noncoherent MFSK*. IEEE.
- Yan, Q., Zeng, H., Jiang, T., Li, M., Lou, W., & Hou, Y. T. (2014). MIMO-based jamming resilient communication in wireless networks. IEEE INFOCOM 2014 - IEEE Conference on Computer Communications. doi:10.1109/infocom.2014.6848218
- Tippenhauer, N. O., Malisa, L., Ranganathan, A., & Capkun, S. (2013). On Limitations of Friendly

Jamming for Confidentiality. 2013 IEEE Symposium on Security and Privacy. doi:10.1109/sp.2013.21

Wenbo Shen, Peng Ning, Xiaofan He, & Huaiyu Dai. (2013). Ally Friendly Jamming: How to Jam Your Enemy and Maintain Your Own Wireless Connectivity at the Same Time. 2013 IEEE Symposium on Security and Privacy. doi:10.1109/sp.2013.22

Gezici, S., Gholami, M. R., Bayram, S., & Jansson, M. (2015). Optimal jamming of wireless localization systems. 2015 IEEE International Conference on Communication Workshop (ICCW). doi:10.1109/iccw.2015.7247286

Amuru, S., Tekin, C., van der Schaar, M., & Buehrer, R. M. (2015). A systematic learning method for optimal jamming. 2015 IEEE International Conference on Communications (ICC). doi:10.1109/icc.2015.7248754