



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

Departamento:
Ingeniería e Investigaciones Tecnológicas

Programa de acreditación:

CyTMA2

Programa de Investigación¹:

Código del Proyecto:

C2-ING-061

Título del proyecto

Comunicación inalámbrica de baja energía para aplicaciones electromédicas

PIDC:

Elija un elemento.

PII:

Elija un elemento.

Director:

Coulombie, Diego Enrique

Integrantes:

Reyes, Agustín Ignacio

Miguens, Alberto Raúl

Resolución Rectoral de acreditación: N.º 375/19

Fecha de inicio:

01/01/2019

Fecha de finalización:

31/12/2020

¹ Los Programas de Investigación de la UNLaM están acreditados con resolución rectoral, según lo indica la Resolución HCS N° 014/15 sobre **Lineamientos generales para el establecimiento, desarrollo y gestión de Programas de Investigación a desarrollarse en la Universidad Nacional de La Matanza**. Consultar en el departamento académico correspondiente la inscripción del proyecto en un Programa acreditado.



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

A. Desarrollo del proyecto (adjuntar el protocolo)

A.1. Grado de ejecución de los objetivos inicialmente planteados, modificaciones o ampliaciones u obstáculos encontrados para su realización (desarrolle en no más de dos (2) páginas)

Los objetivos planteados originalmente se mantuvieron durante la investigación, tanto el Objetivo general: “Optimizar el método de comunicación para minimizar la interferencia electromagnética, estudiar sus fuentes y modelos teóricos, y dentro de ese contexto desarrollar métodos para tener una tasa de transferencia que resulte útil para las diferentes aplicaciones médicas”, como los Objetivos específicos: “Lograr una velocidad de transmisión con carga útil mayor 768kBit/s o que en todo caso sea posible transmitir datos provenientes de 8 canales de señal, muestreados a 4096Hz y con 24bit de resolución” y “Plantear las metodologías necesarias para minimizar el efecto de la interferencia electromagnética, proponiendo soluciones tanto para la fuente de radiación como para las entradas analógicas de bioseñal que resultan receptoras involuntarias”. Para avanzar con el cumplimiento de cada objetivo se dividió la investigación en tareas con los siguientes resultados:

En la tarea “Situación inicial” se analizó críticamente el problema planteado para este tipo de comunicación inalámbrica y encontrar cuales son las variables adecuadas para medir la relación entre interferencia y velocidad real de transmisión. Esta tarea demoró mucho más de lo planificado. Se investigó sobre la variabilidad de las condiciones ambientales del espectro electromagnético destinado a la comunicación basada en un estándar que usa canales de uso libre, existiendo solapamiento con otros sistemas de comunicación, en particular con las redes WIFI. Dentro del ámbito de la universidad, y exactamente dentro del laboratorio donde se investigó, bajo la influencia de algunas pocas redes activas que nos llevaron a plantear un modelo de problema y una posible solución para la tarea posterior. Este modelo no funcionó en otros ámbitos donde el espectro electromagnético estaba más comprometido, generando una nueva evaluación del problema y nuevas mediciones, que llevaron a la extensión del plazo original asignado a la tarea.

En la tarea “Stack” se analizó el software embebido provisto por el fabricante para el chip de comunicación, se evaluó su funcionamiento, se determinaron su puntos críticos relacionados con la velocidad de transmisión y se plantearon posibles mejoras. Teniendo en cuenta la medición hecha en la tarea “Situación Inicial” se planteó un modelo de funcionamiento de “Búsqueda de canal libre y transmisión siempre en ese canal”. Este modelo funcionó bien en el ámbito de la universidad y en un horario (tarde) en el que había poco tráfico por las redes inalámbricas. Los resultados obtenidos cumplieron con el cometido de velocidad de transferencia originalmente planteado. Pero al probar el método en otro lugar físico o en el mismo laboratorio pero en otro horario (noche) los resultados no fueron repetibles y hubo una gran cantidad de pérdida de datos en la transmisión. A partir de allí se retomó la tarea de evaluar la situación inicial con una mirada más amplia de como está distribuida la asignación de canales del espectro electromagnético para todas las situaciones posibles y según cada una de las necesidades de uso. Se planteó e implementó una segunda estrategia basada en “Búsqueda de canal libre y transmisión en ese canal solo un paquete de datos” que si bien obtuvo una tasa de errores muy inferior, la velocidad de transferencia mermó conside-



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

rablemente llegando a niveles muy por debajo de los 768kBit/s que lo hacía no aplicable a los requisitos. Finalmente se probó una tercera estrategia que tomó en consideración diferentes parámetros de la comunicación como un paquete de datos de mayor longitud, asignación dinámica del canal de transmisión, aumento de potencia al transmitir los canales de advertencia, requisitos sobre distancia máxima entre transceptores, etc. Con esta estrategia se logró tener la velocidad de transmisión deseada y cumplir con uno de los objetivos específicos.

La tarea “Procesamiento” fue planificada para analizar las capacidades disponibles para el procesamiento de la señal, empaquetado y generación de tramas para transmisión óptima y el análisis de la posibilidad de cifrado o protección de datos. Se ejecutó simultáneamente con la tarea “Stack” supliendo las necesidades en su implementación mediante la definición de empaquetado y generación de tramas. Si bien no se implementó un cifrado o protección de datos particular, si se analizó que esa necesaria su aplicación para evitar potenciales vulnerabilidades de ciberseguridad.

La tarea “Compresión” fue planificada para hacer un análisis y descripción de la señal a medir y los efectos de la pérdida de datos en caso que la velocidad de transmisión no fuera suficiente para enviar los datos de forma completa. Dado que se logró una velocidad de transmisión suficiente la tarea resultó innecesaria y no fue ejecutada.

La tarea “Inmunidad” fue planificada para analizar las técnicas de filtrado de radiofrecuencia para entradas analógicas sensibles y para analizar las posibilidades de des-sincronización de la transmisión y la adquisición. Se ejecutó adelantada a su planificación original gracias a que las etapas anteriores brindaron información suficiente para poder avanzar con su desarrollo. Los resultados de su análisis permitieron definir las condiciones necesarias para que la transmisión se hiciera de manera segura sin interferir con la señal biológica.

La tarea “Situación final”, donde se analizaron y evaluaron las soluciones propuestas, nos permitió concluir sobre el resultado favorable de la investigación y el cumplimiento de los objetivos planteados.

B. Principales resultados de la investigación

B.1. Publicaciones en revistas (informar cada producción por separado)

No hubo publicaciones

B.2. Libros

No hubo publicaciones

B.3. Capítulos de libros

No hubo publicaciones



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

B.4. Trabajos presentados a congresos y/o seminarios

Autores	<i>Coulombie, Diego</i> <i>Reyes, Agustín</i>
Título	<i>Compromiso entre RRMC y el rechazo de RF en amplificadores de bioseñales</i>
Año	2019
Evento	<i>X Congreso de Microelectrónica Aplicada</i>
Lugar de realización	<i>San Martín, Buenos Aires</i>
Fecha de presentación de la ponencia	<i>26 de septiembre de 2019</i>
Entidad que organiza	<i>Universidad Nacional de San Martín</i>
URL de descarga del trabajo (especificar solo si es la descarga del trabajo; formatos pdf, e-pub, etc.)	http://www.unsam.edu.ar/uea2019/memorias.asp

Autores	<i>Coulombie, Diego</i> <i>Reyes, Agustín</i> <i>Miguens, Alberto</i>
Título	<i>Merma en la Tasa de Transferencia Efectiva en placa de neuroseñales inalámbrica en entornos desfavorables.</i>
Año	2020
Evento	<i>Congreso Argentino de Sistemas Embebidos, CASE2020</i>
Lugar de realización	<i>Virtual</i>
Fecha de presentación de la ponencia	<i>26 agosto de 2020</i>
Entidad que organiza	<i>Asociación Civil para la Investigación, Promoción y Desarrollo de los Sistemas Electrónicos Embebidos (ACSE)</i>
URL de descarga del trabajo (especificar solo si es la descarga del trabajo; formatos pdf, e-pub, etc.)	ISBN 978-987-46297-7-7 http://www.sase.com.ar/case/ediciones/case2020/

Autores	<i>Coulombie, Diego</i> <i>Reyes, Agustín</i> <i>Miguens, Alberto</i>
Título	<i>Impacto de una debilidad de ciberseguridad en la arquitectura de un sistema electromédico.</i>
Año	2020
Evento	<i>XXVI Congreso Argentino de Ciencias de la Computación CACIC2020</i>
Lugar de realización	<i>Virtual</i>
Fecha de presentación de la ponencia	<i>7 octubre de 2020</i>
Entidad que organiza	<i>Universidad Nacional de La Matanza</i>
URL de descarga del trabajo (especificar solo si es la descarga del trabajo; formatos pdf, e-pub, etc.)	https://cacic2020.unlam.edu.ar/es-ar/congreso.jsp#libroactas



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

B.5. Otras publicaciones

No hubo publicaciones

C. Otros resultados. Indicar aquellos resultados pasibles de ser protegidos a través de instrumentos de propiedad intelectual, como patentes, derechos de autor, derechos de obtentor, etc. y desarrollos que no pueden ser protegidos por instrumentos de propiedad intelectual, como las tecnologías organizacionales y otros. Complete un cuadro por cada uno de estos dos tipos de productos.

C.1. Títulos de propiedad intelectual. Indicar: Tipo (marcas, patentes, modelos y diseños, la transferencia tecnológica) de desarrollo o producto, Titular, Fecha de solicitud, Fecha de otorgamiento

Tipo	Titular	Fecha de Solicitud	Fecha de Emisión
-	-	-	-

C.2. Otros desarrollos no pasibles de ser protegidos por títulos de propiedad intelectual. Indicar: Producto y Descripción.

Producto	Descripción
-	-

D. Formación de recursos humanos. Trabajos finales de graduación, tesis de grado y posgrado. Completar un cuadro por cada uno de los trabajos generados en el marco del proyecto.

D.1. Tesis de grado

Director (apellido y nombre)	Autor (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título de la tesis
-	-	-	-	-	-
-	-	-	-	-	-

D.2 Trabajo Final de Especialización

Director (apellido y nombre)	Autor (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título del Trabajo Final
-	-	-	-	-	-
-	-	-	-	-	-

D.2. Tesis de posgrado: Maestría

Director (apellido y nombre)	Tesista (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título de la tesis
-	-	-	-	-	-
-	-	-	-	-	-

D.3. Tesis de posgrado: Doctorado

Director (apellido y nombre)	Tesista (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título de la tesis
------------------------------	-----------------------------	-------------	--------------	-----------------	--------------------



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

nombre)					
-	-	-	-	-	-
-	-	-	-	-	-
-	-	-	-	-	-

D.4. Trabajos de Posdoctorado

Director (apellido y nombre)	Posdoctorando (apellido y nombre)	Institución	Calificación	Fecha /En curso	Título del trabajo	Publicación
-	-	-	-	-	-	-
-	-	-	-	-	-	-

E. Otros recursos humanos en formación: estudiantes/ investigadores (grado/posgrado/ posdoctorado)

Apellido y nombre del Recurso Humano	Tipo	Institución	Período (desde/hasta)	Actividad asignada ²
Moyano, Matías	Estudiante	UNLaM	06/2020 - 06/2021	Asistencia en las pruebas de velocidad de comunicación

F. Vinculación³: Indicar conformación de redes, intercambio científico, etc. con otros grupos de investigación; con el ámbito productivo o con entidades públicas. Desarrolle en no más de dos (2) páginas.

Hubo vinculación en forma de encuentros donde se discutieron con otros equipos de trabajo los avances de los proyectos UNLAM. Se mantuvieron relaciones académicas permanentes con diversos grupos de investigación de la Red UIE (Red Universitaria de Ingeniería Electrónica) y la Red UNCI (Red de Universidades Nacionales con Carreras en Informática), especialmente luego de las participaciones en los congresos y en relación a la problemática de la interferencia de wifi y la ocupación del espectro electromagnético.

G. Otra información. Incluir toda otra información que se considere pertinente.

El mismo equipo (Coulombie, Reyes, Miguens) preparó el trabajo "Autoinmunidad electromagnética en placa de neuroseñales inalámbrica", para ser presentado en el uEA2020 Congreso de Microelectrónica Aplicada. Lamentablemente, por motivos relacionados con la pandemia, el congreso se transformó en jornadas, es decir sin participación de trabajos científicos. Dada la temática del trabajo muy específica sobre electrónica y no existiendo otro congreso plausible al que presentarse, se reservó para ser presentado en la próxima edición del congreso.

² Descripción de la/s actividad/es a cargo (máximo 30 palabras)

³ Entendemos por acciones de "vinculación" aquellas que tienen por objetivo dar respuesta a problemas, generando la creación de productos o servicios innovadores y confeccionados "a medida" de sus contrapartes.



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

H. Cuerpo de anexos:

- Anexo I: Copia de cada uno de los trabajos mencionados en los puntos B, C y D, y certificaciones cuando corresponda.⁴
- Anexo II:
 - FPI-013: Evaluación de alumnos integrantes. (si corresponde)
 - FPI-014: Comprobante de liquidación y rendición de viáticos. (si corresponde)
 - FPI-015: Rendición de gastos del proyecto de investigación acompañado de las hojas foliadas con los comprobantes de gastos.
 - FPI-035: Formulario de reasignación de fondos en Presupuesto.
- Anexo III: Alta patrimonial de los bienes adquiridos con presupuesto del proyecto (FPI 017)
- Nota justificando baja de integrantes del equipo de investigación.



Diego E. Coulombe

Firma y aclaración del director del proyecto.

Lugar y fecha : Buenos Aires 05/03/2021

⁴ En caso de libros, podrá presentarse una fotocopia de la primera hoja significativa o su equivalente y el índice.



Código	FPI-009
Objeto	Guía de elaboración de Informe final de proyecto
Usuario	Director de proyecto de investigación
Autor	Secretaría de Ciencia y Tecnología de la UNLaM
Versión	5
Vigencia	03/9/2019

- **ANEXO I:**

1 Publicación, Póster y Certificado: X Congreso de Microelectrónica Aplicada: Compromiso entre RRMC y el rechazo de RF en amplificadores de bioseñales

2 Publicación, Póster y Certificado: CASE 2020 Merma en la Tasa de Transferencia Efectiva en placa de neuroseñales inalámbrica en entornos desfavorables.

3 Publicación, Captura de video poster y Certificado: CACIC2020 Impacto de una debilidad de ciberseguridad en la arquitectura de un sistema electromédico.

Compromiso entre RRMC y el rechazo de RF en amplificadores de bioseñales

Diego Enrique Coulombie
Dto de Ingeniería e Investigaciones Tecnológicas
Universidad Nacional de La Matanza
San Justo, Argentina
dcoulombie@unlam.edu.ar

Agustín Ignacio Reyes
Dto de Ingeniería e Investigaciones Tecnológicas
Universidad Nacional de La Matanza
San Justo, Argentina

Resumen — La relación de rechazo de modo común de un amplificador de electroencefalografía según la IEC 60601-2-26 debe medirse con un desbalance en sus entradas mayor a 50kOhm. Esto exige que la etapa de filtrado de radiofrecuencia previa al amplificador tenga características particulares teniéndose que encontrar un compromiso entre el ancho de banda, la impedancia de entrada, la RRMC y el rechazo de la RF interferente.

Keywords—Inmunidad electromagnética, rechazo de modo común

I. INTRODUCCIÓN

Los amplificadores de bioseñales están destinados a manejar señales de muy baja amplitud, del orden de los microvolts hasta algunos milivolts. Estos se conectan a los pacientes mediante electrodos que tienen cables de largo mayor a 1m. Inmersos en un campo electromagnético estos cables actúan como antenas, causando que las señales de radiofrecuencia lleguen a los amplificadores. Las señales entra mayoritariamente por modo común. Los amplificadores tiene una relación de rechazo de modo común (RRMC) que disminuye con la frecuencia, llegando a 0dB de rechazo en el mejor de los casos antes de los 50kHz. Por encima de esa frecuencia la RF que ingresa al amplificador, en lugar de ser atenuada se rectifica por los semiconductores que forman al amplificador, apareciendo un error en su salida. Si el campo electromagnético es constante aparecerá en la salida del amplificador una señal de continua, que es ajena a la señal a medir. Las normas que regulan al equipamiento médico imponen requisitos sobre la inmunidad ante la radiofrecuencia que estos deben tener. En particular, y para el proyecto “Monitor de profundidad de anestesia PICTO 0087” que usa señales de electroencefalografía, las normas que lo regulan [1] exigen que en un campo de 3V/m para la RF radiada y 3Vrms para la RF conducida, este error no se distinga del ruido de base del equipo, es decir 6uVpp. Esta medición se debe hacer con una configuración de cableado de paciente específica, en un banco de inmunidad para RF conducida (hasta 80MHz) y en una cámara semianecóica para la RF radiada (de 80 a 2500MHz). Bajo estas condiciones pudo medirse empíricamente que en un equipo sin protección ante la interferencia de RF, el error ronda los 600uVpp @ 1MHz [2]. Es decir que se necesitan por lo menos 100 veces de atenuación (-40dB) a esa frecuencia para que la interferencia no se distinga del ruido.

Por otro lado la norma particular para electroencefalógrafos [3] Exige que el equipo deba tener un rechazo de modo común mínimo de 60dB@50Hz medido

con un desbalance en las entradas de 5kOhm, condicionando el diseño del filtro de radiofrecuencia en la entrada del amplificador.

El problema que se plantea es puramente eléctrico ya que la red de filtros solo puede formarse con componentes pasivos y no puede formarse con semiconductores por el riesgo de rectificación de la radiofrecuencia.

II. MÉTODOS

A. Aproximación con filtros de modo común

Una primera aproximación es considerar la hipótesis que como la señal ingresa de modo común a ambas entradas el filtrado de la señal debe ser también de modo común, es decir derivar la radiofrecuencia a tierra mediante un filtro RC. Este enfoque tiene un impacto muy negativo en la RRMC aunque resulta muy eficaz para la eliminación de la RF.

B. Aproximación con filtro diferencial

Otro enfoque de diseño posible es considerando que la señal que ingresa de modo común debe anularse consigo misma antes de ingresar al amplificador. La manera de hacerlo es diseñando un filtro RC entre ambas entradas, sin derivación a tierra. Este enfoque tiene impacto nulo en la RRMC, pero no suele ser efectivo ante la RF por la aparición de ondas reflejadas al no derivarse nada de la energía de RF a tierra.

C. Aproximación con filtro común y diferencial

Por último está el enfoque mixto que considera tanto un filtro de modo común y uno diferencial llegando a un balance entre ambos para afectar lo menos posible la RRMC y optimizar la inmunidad electromagnética. Esta aproximación la metodología es la siguiente [4,5,6]:

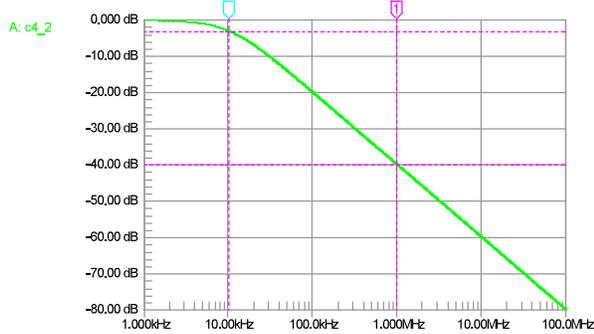
- Fijadas las resistencias de entrada calcular el capacitor diferencial que conserve el ancho de banda de la señal de interés
- Para los capacitores de modo común usar valores 10 veces menor que el de la rama diferencial

Esta relación optimiza la RRMC e inmunidad ante la radiofrecuencia.

III. RESULTADOS

A. Aproximación con filtros de modo común

Para este caso usando un solo polo la respuesta en frecuencia es la del Gráfico 1, con una atenuación a 1MHz de 40dB y un ancho de banda (-3dB) a 10,2kHz.



Measurement Cursors

1 c4_2	X: 997,90k	Y: -39,808
2 c4_2	X: 10,203k	Y: -3,0107

Gráfico 1: Transferencia del filtro modo común

Si fijamos un valor de resistencia de 20kOhm, el capacitor necesario para obtener esta respuesta en frecuencia será de 780pF.

Para medir la RRMC a 50Hz y con un desbalance en las entradas de 51kOhm (R0 y R6) el circuito propuesto es el del Gráfico 2. Donde R1 y R2 son las resistencias de entrada del filtro que van ambas ramas del amplificador junto con C1 y C2 a su vez derivan señal de RF a tierra.

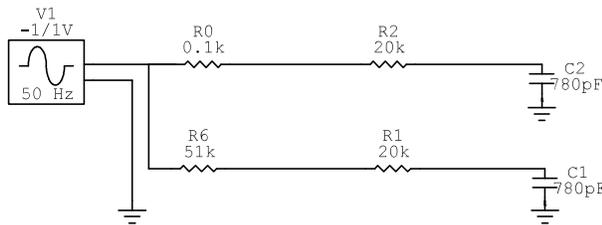


Gráfico 2: Circuito para medir RRMC

El Gráfico 3 muestra que la resta entre las salidas de ambas ramas da una tensión de 12,5mVp, lo que significa que para la entrada de 1Vp la RRMC será de 38dB

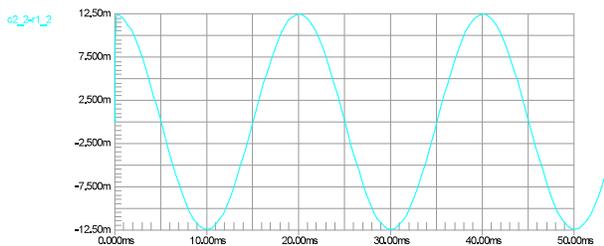


Gráfico 3: Restas de las salidas del filtro de modo común en medición de rechazo de modo común

B. Aproximación con filtro diferencial

Considerando una respuesta en frecuencia idéntica a la del Gráfico 1 pero trabajando de manera diferencial y fijando los valores de las resistencias para cada entrada en 20kOhm el capacitor entre ellas deberá ser de 390pF.

El circuito resultante para la medición del rechazo de modo común es el del Gráfico 4, quedando clara la no influencia de la red para esa medición.

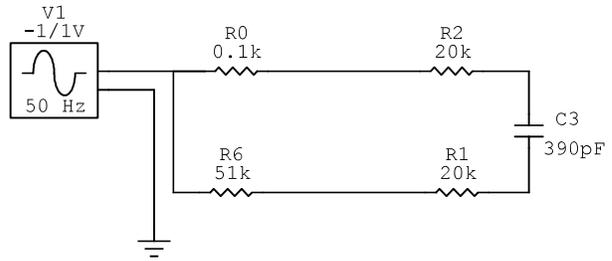


Gráfico 4: Circuito para medición de rechazo de modo común

C. Aproximación con filtro común y diferencial

Para los valores propuestos en el Gráfico 5, la respuesta en frecuencia para el modo común es la del Gráfico 6 y la del modo diferencial coincide con la del Gráfico 1.

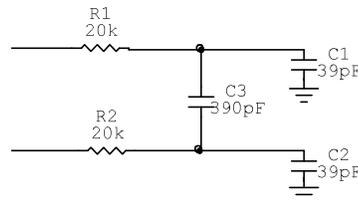
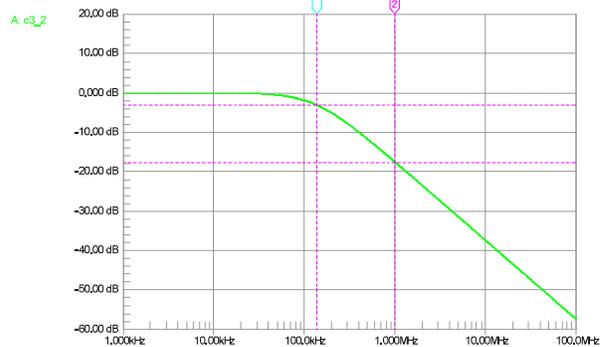


Gráfico 5: Filtro modo común y diferencial



Measurement Cursors

1 c3_2	X: 136,75k	Y: -3,0623
2 c3_2	X: 1,0022M	Y: -17,571

Gráfico 6: Transferencia del filtro parte modo común

Con esta configuración de filtro se obtiene en modo diferencial una atenuación a 1MHz de 40dB y una atenuación para el modo común a esa misma frecuencia de 17dB. La banda de paso para el filtro diferencial continúa alrededor de 10kHz, mientras que la de modo diferencial subió hasta los 136kHz

El circuito para la medición del rechazo de modo común es el del Gráfico 7.

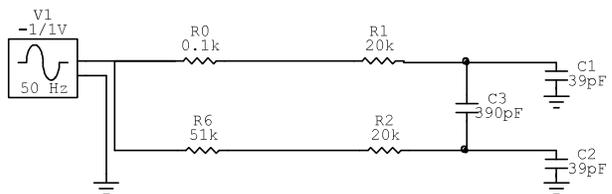


Gráfico 7: Circuito para medición de rechazo de modo común

El Gráfico 8 muestra la resta entre las salidas de ambas ramas da una tensión de 600uVp, lo que significa que para la entrada de 1Vp la RMMC será de 64,5dB

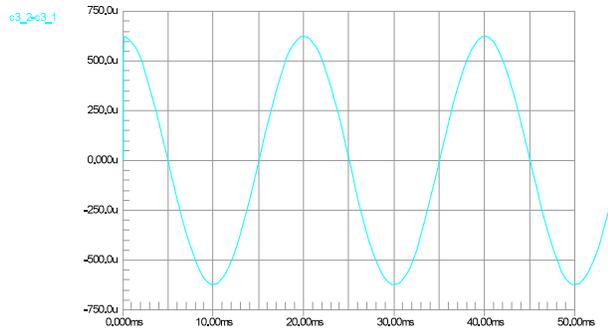


Gráfico 8: Resto de las salidas del filtro en medición de rechazo de modo común

IV. DISCUSIÓN Y CONCLUSIONES

Los resultados obtenidos con el método de filtros de modo común muestran que se puede obtener la atenuación requerida a costa de empeorar el rechazo de modo común. Esta opción se usa habitualmente en sistemas de registro flotantes, es decir con alimentación galvánicamente separada de tierra o alimentados a batería, de manera que el rechazo de los 50Hz a tierra resulta atenuado por la capacidad que tenga el sistema de aislación. También existe el recurso de interponer un filtro notch en etapas posteriores para eliminar el “zumbido” causado por la frecuencia de red. De esta manera se resuelve el problema bajo rechazo de modo común a la frecuencia de línea pero se asegura que la radiofrecuencia tiene una atenuación importante.

Con el método de filtro diferencial se obtuvo una transferencia idéntica a la de modo común y sin deterioro del

rechazo de modo común, pero ineficaz para detener la radiofrecuencia.

Con el método mixto de filtro común y diferencial se obtiene una solución de compromiso entre una buena atenuación con derivación de energía a tierra, pero ajustada de manera tal que esa impedancia de modo común no deteriore la RMMC por demás.

Para el proyecto mencionado en la introducción se utilizó el método mixto, pudiéndose medir la influencia de la red de filtros en el rechazo de modo común con resultados concordantes con el valor teórico. Queda a la espera de hacer las pruebas de inmunidad conducida y radiada para verificar que las hipótesis y consideraciones de diseño resultaron eficaces para lograr la inmunidad electromagnética deseada.

REFERENCIAS

- [1] IEC 60601-1-2:2014 Medical electrical equipment - Part 1-2: General requirements for basic safety and essential performance - Collateral Standard: Electromagnetic disturbances - Requirements and tests
- [2] Comunicación interna proyecto PICTO 0087 “Monitor de Profundidad Anestésica” D. Coulombie, A Reyes. No publicado
- [3] IEC 60601-2-26:2012. Medical electrical equipment - Part 2-26: Particular requirements for the basic safety and essential performance of electroencephalographs
- [4] Improve Instrument Amplifier Performance with X2Y® Optimized Input Filter, Johansson Dielectrics <https://johansondielectrics.com/improve-instrument-amplifier-performance-with-x2y-optimized-input-filter>
- [5] In-Amp Input RFI Protection. MT-070 TUTORIAL, Analog Devices, <https://www.analog.com/media/en/training-seminars/tutorials/MT-070.pdf>
- [6] A Designer’s Guide to Instrumentation Amplifiers 3RD Edition, Analog Devices, <https://www.analog.com/media/en/training-seminars/design-handbooks/designers-guide-instrument-amps-complete.pdf>

Compromiso entre RRMCM y el rechazo de RF en amplificadores de bioseñales

Diego Enrique Coulombie
Agustín Ignacio Reyes



INTRODUCCIÓN	<p>Definición del problema Los amplificadores de bioseñales manejan señales de baja amplitud interferidas por señales de radiofrecuencia de modo común que se rectifica en los semiconductores del amplificador apareciendo un error en su salida.</p>	<p>Requisitos de diseño: El error por la RF rectificada debe ser menor al ruido de base de 6uVpp para un campo de RF de 3V/m radiado desde 80 a 2500MHz y de 3Vrms conducido desde 150kHz a 80MHz. El rechazo de modo común mínimo</p>	<p>debe ser de 60dB@50Hz con un desbalance en las entradas de 51kOhm. La red de filtros debe ser de componentes pasivos sin semiconductores debido al riesgo que ocurra la rectificación de la radiofrecuencia.</p>	<p>Condiciones de diseño En una medición empírica sin protección de RF, el error ronda los 600uVpp @ 1MHz. La necesidad de atenuación es de 100 veces (-40dB) a esa frecuencia para que la interferencia no se distinga del ruido.</p>
--------------	---	---	---	---

FILTRO DE MODO COMÚN

Filtrado óptimo la RRMCM baja -39dB

Respuesta en frecuencia

Salida @ 50Hz

FILTRO DIFERENCIAL

$AB_{com} = \text{infinito}$
 $Ab_{dif} = 10\text{kHz}$
 $RRF_{dif} = -40\text{dB}@1\text{MHz}$
 $RRF_{com} = 0\text{dB}$
 $RRMC = \text{infinito}$

CONCLUSIONES

Con el método de filtro de modo común se logra la atenuación RF a costa de empeorar el rechazo de modo común. Se usa en sistemas de registro flotantes, el rechazo a los 50Hz se mejora con una baja capacidad de aislación. También se interpone un filtro notch para eliminar el “zumbido” causado por la frecuencia de red. De esta manera se resuelve el problema bajo rechazo de modo común a la frecuencia de línea pero se asegura que la radiofrecuencia tenga una atenuación importante.

Con el método de filtro diferencial se obtuvo una transferencia idéntica a la de modo común y sin deterioro del rechazo de modo común, pero ineficaz para detener la radiofrecuencia por ingresar de modo común.

Con el método mixto de filtro común y diferencial se obtiene una solución de compromiso entre una buena atenuación con derivación de energía a tierra, pero ajustada de manera tal que esa impedancia de modo común no deteriore la RRMCM por demás.

FILTRO COMÚN + DIFERENCIAL

Respuesta en frecuencia

Salida @ 50Hz



UNIVERSIDAD
NACIONAL DE
SAN MARTÍN

ESCUELA
**CIENCIA Y
TECNOLOGÍA**



Se deja constancia que

Diego Coulombie

Participó como expositor en el X Congreso de Microelectrónica Aplicada que se llevo a cabo en la Universidad de San Martín del 25 al 26 de septiembre del 2019.

Ing. Jorge Sinderman
Chairman

Merma en la Tasa de Transferencia Efectiva en placa de neuroseñales inalámbrica en entornos desfavorables

Diego Enrique Coulombie
Dto de Ingeniería e Investigaciones
Tecnológicas
Universidad Nacional de La Matanza
San Justo, Argentina
dcoulombie@unlam.edu.ar

Agustín Ignacio Reyes
Dto de Ingeniería e Investigaciones
Tecnológicas
Universidad Nacional de La Matanza
San Justo, Argentina

Alberto Raúl Miguens
Dto de Ingeniería e Investigaciones
Tecnológicas
Universidad Nacional de La Matanza
San Justo, Argentina

Resumen—En un sistema con comunicación Bluetooth 5 de baja energía se encontró que la tasa de transferencia efectiva era mucho menor a la esperada. Se planteó como hipótesis que la merma en la tasa era debida a la congestión causada por el Wifi en la banda de comunicación. Con el objetivo de determinar cual es el nivel de ocupación del espectro en el que podría funcionar el sistema, se midió dicha tasa bajo diferentes condiciones y se encontró que esta disminuyó con pocos canales de uso persistente y que cayó estrepitosamente con muchos canales ocupados. Se concluye que la implementación actual no es apropiada para la aplicación requerida en entornos de mucha ocupación de la banda.

Palabras clave—Bioseñales, Internet de las cosas Médicas, Bluetooth5 BLE, compatibilidad electromagnética

I. INTRODUCCIÓN

Las comunicaciones inalámbricas Bluetooth de baja energía (BLE) y WLAN (o Wifi) comparten la porción del espectro electromagnético entorno a los 2,4GHz denominado Industrial – Comercial – Médico (ICM). El protocolo BLE opera en las frecuencias 2408 a 2483,5MHz. Su banda está dividida en 40 canales de 2MHz. Tres de esos canales (37, 38 y 39) se usan para emitir paquetes de “Advertencia” (en inglés beacons) con el estado del dispositivo, mientras que los restantes se usan para el intercambio de datos durante la conexión. Los 3 canales de advertencia están situados estratégicamente para que no tengan interferencias con los canales Wifi 1, 6 y 11 que no se solapan entre sí (Fig 1) [1]. La especificación de BLE permite usar sus 3 canales de advertencia simultáneamente pero en muchas implementaciones para disminuir energía y costo se usan menos canales [2].

Todos los paquetes (advertencias y datos) tienen el mismo formato: un preámbulo, una dirección de acceso (AA), los datos del paquete (PDU) y un código de redundancia cíclica (CRC). Esto significa que cada vez que se envía (o reenvía) un dato, se debe pagar un costo extra en el ancho de banda para enviar información protocolar.

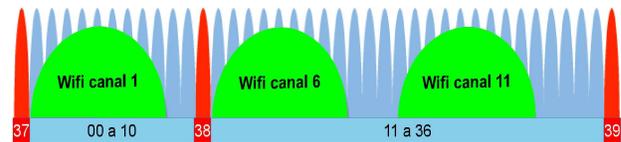


Fig 1 Distribución de canales: verde: Wifi solo se muestran 1, 6, 11, rojo: BLE advertencia, celeste: BLE datos

Teniendo protocolos, características y aplicaciones diferentes los dispositivos que usan ambos sistemas de comunicación compiten por usar del espectro electromagnético. Los canales Wifi invaden a los canales BLE interfiriéndose y necesitando una retransmisión de datos, con la consecuente pérdida en la Tasa de Transferencia Efectiva (TTE) [3].

Esto se hizo evidente en el proyecto “Monitor de profundidad anestésica”, donde un sistema de adquisición de neuroseñales inalámbrico mostró una tasa muy inferior a la esperada. El sistema utiliza el microcontrolador Texas CC2640R2 para manejar la comunicación de bajo el protocolo Bluetooth 5 BLE. El sistema embebido (SE) desarrollado para la placa usa para la capa de comunicación el stack provisto por el fabricante del microcontrolador [4]. Las necesidades definidas para esta capa en el diseño del sistema son: comunicación bidireccional punto a punto de latencia máxima 300ms con envío de datos de forma constante a una tasa de transferencia efectiva de 700kb/s. Por el tipo de uso debe ser encriptada y por motivos de implementación no se definió ningún tipo de compresión. En el análisis hecho durante el diseño se llegó a la conclusión que el protocolo de comunicación elegido cumplía con las condiciones requeridas. Pero en la prueba inicial se verificó que la TTE no era constante y estaba muy por debajo de la teórica esperada.

Para investigar cual era el problema se planteó la hipótesis que la disminución en la tasa de transferencia de datos de la comunicación BLE se debe al alto nivel de ocupación y congestión de esa banda del espectro. El objetivo del ensayo fue evaluar el desempeño de la comunicación en diferentes locaciones, con diferentes ocupaciones de la banda para evaluar bajo que condiciones podría funcionar la implementación actual del sistema.

II. MATERIALES Y MÉTODOS

A. Materiales

Para hacer el ensayo se usaron 2 placas de desarrollo Launchpad LAUNCHXL-CC2640R2, con los programas MASTER y SLAVE del stack de comunicación Bluetooth 5.0 provisto por el fabricante. La transmisión de datos se hizo a una potencia de 0dB. En el receptor se calculó la tasa de datos recibidos sin errores. Se usó la aplicación Wifi Analyzer para identificar los canales de Wifi ocupados y el analizador de espectro AARONIA SPECTRAN 6065 con antena para la banda de 2,4GHz para visualizar los canales de Bluetooth BLE IEEE 802.15.1 y de Wifi IEEE 802.11.

B. Métodos

Se colocaron ambas placas de desarrollo separadas a 2m de distancia, corriendo en una de ellas el programa transmisor MASTER y en la otra el programa receptor SLAVE. Se ubicó la antena del analizador de espectro a 200mm co-lineal a la antena de recepción. Se hicieron mediciones en los turnos mañana, tarde y noche en el laboratorio de la universidad y una medición en un edificio de departamentos de una zona densamente poblada. Se midió la tasa de transferencia efectiva, la cantidad y uso de canales de WiFi detectados, y la presencia de las señales de Bluetooth para cada una de las locaciones

III. RESULTADOS

Las tasas de transferencia efectiva en las distintas locaciones se muestran en la Tabla I.

TABLA I TASA DE TRANSFERENCIA EFECTIVA

Locación	TTE [kb/s]
Laboratorio Turno Mañana	100
Laboratorio Turno Tarde	360
Laboratorio Turno Noche	70
Edificio muy poblado	12

La Tabla II muestra la cantidad de canales Wifi identificados en cada una de las mediciones y el uso del ancho de banda de los canales. En caso de mucho uso la ocupación de los canales fue “persistente” y para poco uso su aparición fue “esporádica”.

TABLA II OCUPACIÓN DEL ESPECTRO POR WIFI

Locación	Uso de los canales Wifi	Canales Wifi ocupados
Laboratorio Turno Mañana	persistente	4*
Laboratorio Turno Tarde	esporádico	4*
Laboratorio Turno Noche	persistente	4*
Edificio muy poblado	persistente	13

* canales IEEE 802.11: 4, 6, 9 y 11

En la locación con mayor población, la ocupación del espectro fue completa, ver “Fig 1”. Inclusive hubo cambios en los SSID lo que sugiere que varias redes compartían el mismo canal.

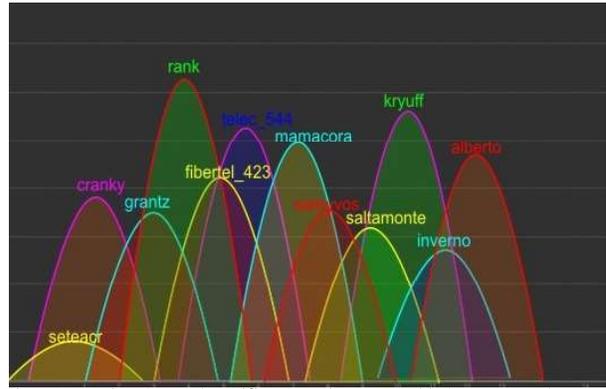


Fig 2 Ocupación de canales wifi en locación muy poblada. Extracto de captura de pantalla de la aplicación Wifi Analyzer.

La Tabla III muestra los canales que pudieron identificarse alternativamente con la señal de transmisión Bluetooth.

TABLA III CANALES DE BLUETOOTH

Locación	Señal Bluetooth identificada en canales IEEE 802.15.1:
Laboratorio Turno Mañana	37, 0 a 6,
Laboratorio Turno Tarde	37, 0 a 6, 10, 38, 34 a 36 y 39
Laboratorio Turno Noche	37, 0 a 6,
Edificio muy poblado	No identificada

IV. CONCLUSIONES

Se pudo confirmar la hipótesis que las diferencias en la tasa de transferencia efectiva están relacionadas con el nivel de congestión del espectro Wifi. Se infiere por el grado de persistencia de las señales observadas que en las locaciones con mayor cantidad de usuarios hay mayor flujo de datos. Eso nos lleva a la conclusión que aún en locaciones donde hay unas pocas redes instaladas cuando hay una gran transmisión de datos, hay un uso considerable en el espectro y una merma en la TTE. El solapamiento de los canales Wifi le dejan poco margen al BLE para hacer una comunicación eficiente. Al usar la técnica de espectro ensanchado por salto de frecuencia (del inglés Frequency Hopping Spread Spectrum o FHSS) [5], termina cayendo indefectiblemente en un canal interferido. Esta técnica dispone de un nuevo salto cada intervalos definidos o ante la llegada de paquetes con error. La solución robustece a la comunicación pero a costa una alta tasa de retransmisión [6] bajando la TTE. En el caso de varias redes Wifi que cubren todo el espectro, la congestión es aún peor perdiendo ya no solo datos sino también los canales de advertencia y como consecuencia la tasa del BLE cae estrepitosamente [7].

Para el caso en particular del proyecto que dio origen a esta investigación se concluyó que la implementación no es adecuada para entornos desfavorables. Ante la necesidad de mejorar o paliar esa situación se propone aumentar la potencia de transmisión para disminuir la pérdida de datos y evaluar la posibilidad de implementar algún tipo de compresión. Otra alternativa aunque con modificaciones de hardware drásticas es cambiar la banda de comunicación por otra sin licencia, que esté menos concurrida, como 915 a 928MHz

REFERENCIAS

- [1] Bluetooth SIG, Bluetooth Core Specification <https://www.bluetooth.com/specifications/bluetoothcorespecification/>
- [2] Abdelmoumen, R. A Review of Link Layer Protocols for Internet of Things. *International Journal of Computer Applications*. 182. 22-28. 10.5120/ijca2019918618.
- [3] Bosch, P. De Schepper, T. Zeljković, E. Famaey, J. Latré, S. Orchestration of heterogeneous wireless networks: State of the art and remaining challenges. *Computer Communications*. 149. 10.1016/j.comcom.2019.10.008.
- [4] Texas Instruments Inc, Stack User's Guide, http://software-dl.ti.com/lprf/simplelink_cc2640r2_sdk/1.35.00.33/exports/docs/ble5stack/ble_user_guide/html/cc2640/index.html .
- [5] A. Jedda, G. Jourdan and N. Zaguia, Some side effects of FHSS on Bluetooth networks distributed algorithms, *ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010*, Hammamet, 2010, pp. 1-8, doi: 10.1109/AICCSA.2010.5587029.
- [6] Oliveira, L., Rodrigues, J.J.P.C., Kozlov, S.A., Rabêlo, R., Albuquerque, V.H.C., MAC Layer Protocols for Internet of Things: A Survey. *Future Internet* 2019, 11, 16.
- [7] Al Kalaa, M. Balid, W. Bitar, N. Refai, H. Evaluating Bluetooth Low Energy in Realistic Wireless Environments. *IEEE Wireless Communications and Networking Conference 2016 - Services, Applications, and Business*, At Doha, Qatar

Coulombie D., Reyes A., Miguens A.
 Dto de Ingeniería e Investigaciones Tecnológicas
 Universidad Nacional de La Matanza
 San Justo, Argentina
 dcoulombie@unlam.edu.ar

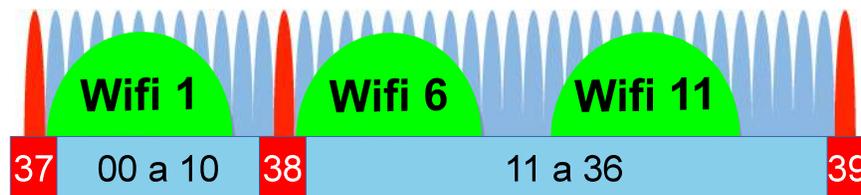
Merma en la Tasa de Transferencia Efectiva en placa de neuroseñales inalámbrica en entornos desfavorables

Resumen—En un sistema con comunicación Bluetooth 5 de baja energía se encontró que la tasa de transferencia efectiva era mucho menor a la esperada. Se planteó como hipótesis que la merma era debida a la congestión causada por el Wifi en la banda de comunicación. Con el objetivo de determinar cual es el nivel de ocupación del espectro en el que podría funcionar el sistema, se midió dicha tasa bajo diferentes condiciones y se encontró que esta disminuyó con pocos canales de uso persistente y que cayó estrepitosamente con muchos canales ocupados. Se concluye que la implementación actual no es apropiada para la aplicación requerida en entornos de mucha ocupación de la banda.

INTRODUCCIÓN

¿Cuanto impacta la ocupación del Wifi en el Bluetooth de baja energía (BLE)?

2408MHz - Canales en banda de uso libre - 2483,5MHz

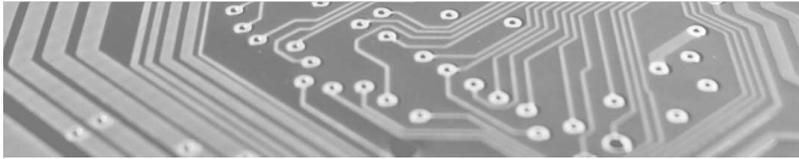


Canales
Advertencia
BLE

Canales
Datos
BLE

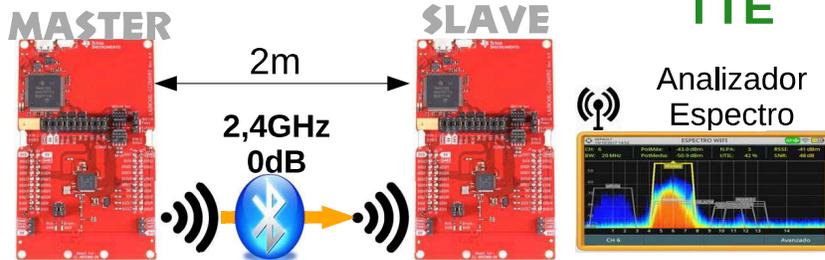
Canales
No solapados
Wifi

No están dibujados los otros 11 Canales Wifi que cubren toda la banda ICM de 2,4GHz



MAT & MET

Comunicación entre 2 placas de desarrollo
Medición de la banda de interés
y de la Tasa de Transferencia Efectiva



4
Escenarios



Mañana

Tarde

Noche



3
Variables
medidas

- TTE tasa de transferencia efectiva
- Persistencia y uso de canales de WiFi
- Discriminación de señales de Bluetooth

RESULTADOS

Locación	TTE [kb/s]
Laboratorio Mañana	100
Laboratorio Tarde	360
Laboratorio Noche	70
Edificio muy poblado	12

RESULTADOS

Locación	Cantidad de canales Uso del Wifi	Señal BT identificada
Laboratorio Mañana	4 persistente	37, 0 a 6
Laboratorio Tarde	4 esporádico	37, 0 a 6, 10, 38, 34 a 36 y 39
Laboratorio Noche	4 persistente	37, 0 a 6
Edificio muy poblado	13 persistente	No identificada

Canales BLE de advertencia

CONCLUSIONES

La TTE disminuye con la congestión de la banda

Incluso con pocos canales Wifi y mucho flujo de datos

Con muchos canales ocupados pierde advertencias

Mejoras:

- aumentar la potencia
- comprimir datos
- banda menos concurrida 915-928MHz

Agradecimiento

Agradecemos la participación de
**Diego Enrique Coulombie, Agustín Ignacio Reyes y
Alberto Raúl Miguens**

por presentar el siguiente trabajo en la modalidad *Reporte*:
**“Merma en la Tasa de Transferencia Efectiva en placa de
neuroseñales inalámbrica en entornos desfavorables”**
en el **Congreso Argentino de Sistemas Embebidos**
realizado del 24 al 26 de Agosto de 2020.



Dr. Maximiliano Antonelli
Comité CASE 2020

Dra. Luciana De Micco
Comité CASE 2020

Mg. Ing. Diego J. Brengi
Comité CASE 2020

Impacto de una debilidad de ciberseguridad en la arquitectura de un sistema electromédico

Diego Coulombie¹, Agustín Reyes¹, Alberto Miguens¹

¹ Dto de Ingeniería e Investigaciones Tecnológicas, Universidad Nacional de La Matanza
San Justo, Buenos Aires, Argentina
{dcoulombie, aireyes, amiguens}@unlam.edu.ar

Resumen. El diseño de un equipamiento médico dedicado al monitoreo de profundidad de anestesia, que utiliza conectividad en su arquitectura con el fin de hacer el monitoreo de forma remota, se ve perjudicado cuando se enfrenta a las amenazas de ciberseguridad en la etapa de análisis de riesgos. La imposibilidad de validar de manera objetiva las medidas de control por parte de la organización que lo diseña, obligó a mitigar el elevado riesgo ante ciberataques con la drástica solución de hacer un cambio de arquitectura y de modelo de negocio abandonando la posibilidad de conectividad remota.

Palabras clave: Aplicaciones de uso médico, Internet de las Cosas, Telemedicina, Análisis de riesgo, Requisitos regulatorios de seguridad y protección.

1 Introducción

A veces las cosas se complican. Aquello que en un boceto parece una idea maravillosa y revolucionaria se desarma cuando se enfrenta con la realidad. Incluso cuando se tomaron precauciones previas puede ocurrir que algo inesperado, que no se imaginó al momento del diseño, se revele ante nosotros como un problema. La envergadura del problema puede tener gran importancia según el campo de aplicación de esa idea. En áreas que se saben sensibles, los contextos en los que se practican los diseños están ordenados por regulaciones y por autoridades de control que se encargan de verificar su cumplimiento.

En el área de la tecnología médica las regulaciones no solo plantean requisitos sobre el producto final, sino que también exigen, controlan y evalúan las estructuras y metodologías destinadas al diseño. La mejor forma de satisfacer esas regulaciones es logrando el cumplimiento de normas específicas, definidas por la industria y aceptadas por los organismos de control.

El conjunto de normas aplicables depende de las características del producto. En particular nos enfocamos en el marco regulatorio que cubre al producto electromédico para monitorizar la profundidad de anestesia. El desarrollo hecho en el ámbito de la universidad en los proyectos “PICTO 0087 Monitor de profundidad de anestesia” y “C2-ING-061 Comunicación inalámbrica de baja energía para aplicaciones electromédicas” consta de un sistema de adquisición de neuroseñales inalámbrico (Fig.1, Cabezal) con una pantalla de monitorización (Fig.1, Monitor) dentro del área

de uso y otra interfaz remota (Fig.1, Aplicación). Se trata de un dispositivo médico de aplicación en quirófano y terapia intensiva [1].

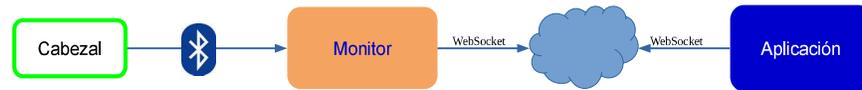


Fig. 1. Arquitectura del Monitor de profundidad de anestesia

El modelo de negocio al que responde esta arquitectura es el de telemedicina aplicada a un subsector de la salud en el que hay una dependencia absoluta del profesional de manera presencial. La anestesia en las intervenciones quirúrgicas y la sedación en terapia intensiva se hicieron durante muchas décadas mediante un profesional médico especializado en anestesiología. Este ajustaba la dosis para obtener el estado anestésico del paciente deseado, midiendo variables hemodinámicas como el ritmo cardíaco y la presión arterial; y parámetros clínicos como la sudoración, la piloerección, la dilatación de las pupilas, la sialorrea, y los movimientos espontáneos [2]. Hace unos cuantos años vienen usándose monitores de profundidad anestésica basados en parámetros objetivos que complementan la observación del profesional. Existen pocos fabricantes en el mundo. La mayoría usa señales electrofisiológicas que procesadas por un algoritmo propietario, dan un indicador dentro de una escala y registran los valores durante toda la maniobra anestésica con fines legales y de historia clínica [3].

La arquitectura propuesta con un “Cabezal” que registra y adecúa la señal junto a un “Monitor” con conectividad (que podría ser un Smartphone u otra plataforma con software embebido) permitirían sacar del área de quirófano al profesional de anestesia, para que actúe, verifique, avale, revise y registre de manera remota el efecto de la dosis suministrada al paciente. En un caso superador de telemedicina podría también ajustar la dosis de manera remota, si es que la mesa de anestesia lo permite

Considerando el producto electromédico descrito, el conjunto de normas aplicables para gestionar su seguridad y eficacia, abarca desde el sistema de gestión de calidad (ISO13485) [4], la gestión de riesgos (ISO 14971) [5], la de usabilidad (IEC 62366) [6], la del proceso del ciclo de vida del software (IEC 62304) [7], la de seguridad básica y funcionamiento esencial (IEC 60601-1, cuyo punto 14 se encarga del software del producto electro medico o PEMS) [8] y la de seguridad del software que puede funcionar autónomamente (IEC 82304-1) [9]. La relación entre estas normas y el producto se puede ver en la Fig. 2.

La gestión de riesgos es un estudio sistemático y predefinido hecho por el fabricante que busca conocer de antemano la mayor cantidad posible de los peligros que puedan afectar al usuario o paciente al entrar en contacto con el dispositivo médico. Atraviesa todo el ciclo de vida del producto, desde la concepción de la idea, las diferentes etapas del diseño, la producción, la posproducción, el uso, el mantenimiento y finaliza con la retirada del producto del mercado. Busca también que se valoren los peligros ponderándolos como riesgos para así poder justificar cual será la acción que se tomará con cada uno de ellos, con el fin de eliminarlos, mitigarlos o aceptarlos. La ISO 14971 brinda un marco de referencia y propone metodologías para abordar ese estudio sistemático para encontrar peligros, evaluar su gravedad y su probabilidad de ocurrencia, encontrando así riesgos. Requiere que el fabricante defina

critérios de aceptación o rechazo de esos riesgos, para definir cuales de ellos serán mitigados con soluciones técnicas que este proponga. La norma también establece requisitos de trazabilidad entre los peligros y entradas al diseño. La IEC 62304-1 establece el marco de responsabilidades, registro y verificación para cada una de las etapas del proceso del ciclo de vida del software, incluyendo obviamente las entradas de diseño que surgen de la gestión de riesgo y especialmente sobre como se trata la realimentación que brinda el proceso de resolución de problemas (bugs). Así como la norma de gestión de riesgos alimenta las entradas del proceso de diseño regido por la de ciclo de vida de software, la ISO 14971 se alimenta también de requisitos de seguridad y eficacia planteados por la IEC 60601-1 y la IEC 82604-1 que actúan como disparadores para el análisis de los riesgos. Estas normas son específicas de producto y proponen requisitos destinados a controlar peligros que están reconocidos por la industria.

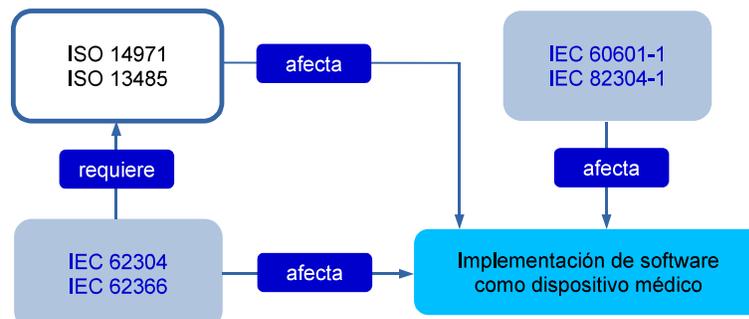


Fig. 2. Relaciones entre normas aplicables al producto, extraído y adaptado de IEC 62304-1 AMD:2015

Uno de esos peligros conocidos es la vulnerabilidad ante ataques a la ciberseguridad (Fig.3). Si bien es un elemento no definido en la norma de equipamiento médico [8] que se encarga estrictamente de los peligros relacionados con la seguridad (safety: prevención de accidentes sin intencionalidad), si se hace mención específica en la norma de software autónomo [9] considerando también como fuente de peligros a la amenaza proveniente de la falta de protección del dispositivo (security: prevención de actividades maliciosas intencionadas).



Fig. 3. Impacto de las medidas de protección en la seguridad, adaptado de TIR57 [10]

Esta diferencia que no era considerada hace unos años, hoy con el avance de la conectividad de los productos médicos hace que el problema de la ciberseguridad esté tomando cada vez más relevancia [11]. Esto significa un cambio de paradigma en el enfoque de la gestión de riesgos, en donde transversalmente al diseño se debe considerar la protección del sistema como una entrada más al diseño.

El objetivo de este trabajo es mostrar cual fue el impacto que causó en la arquitectura de un sistema electromédico cuando en la gestión de riesgos se incorporaron herramientas de análisis de la ciberseguridad.

2 Métodos

Para hacer la gestión de riesgos de todo el producto médico se usó la herramienta Análisis Modal de Fallos y Efectos (AMFE) enunciándose aquí únicamente aquellos ítems relacionados con la ciberseguridad.

Las siguientes tablas establecen criterios para la aceptabilidad del riesgo. Las Tablas 1 y 2 dan una guía la valoración de la gravedad y la ocurrencia. La Tabla 3 establece los límites que definen cuando un riesgo es aceptable o cuando es inaceptable

Tabla 1. Guía para valoración de la Gravedad:

Gravedad	Consecuencias asociadas	Valor
Catastrófico	Origina la muerte del paciente	5
Crítico	Origina un deterioro permanente o una lesión que pone en peligro la vida	4
Serio	Origina una lesión o un deterioro que requiere intervención médica profesional	3
Pequeño	Origina una lesión temporal o un deterioro que no requiere intervención médica profesional	2
Insignificante	Inconveniente o molestia transitoria	1

Tabla 2. Guía para valoración de la Ocurrencia:

Probabilidad	Frecuencia del fallo	Valor
Frecuente	Fallo casi inevitable. Es seguro que el fallo se producirá frecuentemente.	5
Probable	El fallo se ha presentado con cierta frecuencia en el pasado en procesos similares o previos procesos que han fallado.	4
Ocasional	Defecto aparecido ocasionalmente en procesos similares o previos al actual. Probablemente aparecerá algunas veces en la vida del componente/sistema.	3
Remoto	Fallos aislados en procesos similares o casi idénticos. Es	2

	razonablemente esperable en la vida del sistema, aunque es poco probable que suceda.	
Improbable	Ningún fallo se asocia a procesos casi idénticos, ni se ha dado nunca en el pasado, pero es concebible.	1

Tabla 3. Guía para aceptar el Riesgo A = ADMISIBLE; I = INADMISIBLE:

Ocurrencia	Gravedad	Improbable	Remoto	Ocasional	Probable	Frecuente
		1	2	3	4	5
Catastrófico	5	A	I	I	I	I
Crítico	4	A	A	I	I	I
Serio	3	A	A	I	I	I
Pequeño	2	A	A	A	I	I
Insignificante	1	A	A	A	A	I

Para la detección de los peligros se usó la técnica de análisis de situaciones relacionando los aspectos de uso de cada uno de los componentes del sistema y las amenazas de ciberseguridad a las que están expuestos. Estas amenazas pueden ser:

- Interrupción de la atención / servicio
- Engaño del personal con correo electrónico falso o sitios web falsos para obtener credenciales de inicio de sesión o instalar malware
- Amenaza interna, involuntaria o intencional, que puede representar una amenaza significativa debido a la posición de confianza dentro de la organización
- Pérdida de información del paciente
- Violación de datos, filtración de información y pérdida de privacidad
- Chantaje, extorsión y coacción a través de la explotación de datos filtrados.

El análisis permitió descubrir los peligros, y estos se registraron y sistematizaron como ítems en el AMFE de la sección resultados. De esta manera se identificó cual

es la secuencia de sucesos que desencadena una situación peligrosa causando un daño específico (columnas: Secuencia de sucesos, Situación peligrosa, Daño). También se ponderó el riesgo mediante las tablas 1, 2 y 3 antes mencionadas (columnas: O, G, R) y se propuso la medida de control que busca que el riesgo baje a niveles aceptables (columna: Mitigación). Como cada situación peligrosa debe ser trazable se la identificó alfa numericamente (columna: ID).

3 Resultados

Los resultados del análisis de riesgos y soluciones propuestas para mitigar los riesgos se enuncian en la Tabla 4 en el formato tradicional de un AMFE, aceptado por la industria y por los organismos regulatorios.

Se analizaron las secuencias de sucesos para ataques que logran modificar parámetros de funcionamiento, suplantan dispositivos y usuarios, detienen la acción del sistema, corrompen su funcionamiento y/o generan nuevas vulnerabilidades.

Los daños que responden a cada uno de los peligros detectados se circunscriben a la falta de monitorización tanto presencial como remota, a una posible dosificación incorrecta del agente anestésico y a la pérdida de privacidad de los pacientes.

Se proponen las medidas de mitigación que buscan disminuir el riesgo mediante un blindaje del sistema minimizando las vías de conectividad lo que implica suprimir la aplicación remota. Las propuestas incluyen mejorar la protección de partes vitales del software impidiendo el acceso remoto, permitiendo solo el resguardo de datos de manera física y la ejecución de actualizaciones solo por personal autorizado. Las medidas de control también impactan en la selección del hardware donde ya no se permite la selección de una plataforma de uso general y se exige una plataforma de uso exclusivo para cumplir con la función de monitor.

Tabla 4. Extracto del AMFE con los ítems relacionados a la ciberseguridad con riesgo Inadmisibles (I). MPA = Monitoreo de Profundidad Anestésica

ID	Secuencia de sucesos	Situación peligrosa	Daño	O	G	R	Mitigación
CS01	El monitor sufre un ataque que modifica parámetros de funcionamiento del cabezal	El cabezal interrumpe su transmisión	MPA no disponible	3	3	I	Desactivar conectividad monitor red externa. Protección contra escrituras y CRC de partes vitales. Resguardo de datos presencial (USB). Monitor en
CS02		El cabezal envía datos erróneos	Dosificación incorrecta de anestesia	2	5	I	

CS03	El monitor sufre un ataque que modifica sus propios parámetros de funcionamiento	El monitor genera e informa valores espurios al usuario local y/o al usuario remoto de la aplicación	Dosificación incorrecta de anestesia	2	5	I	plataforma exclusiva.
CS04	Suplantación de dispositivo cabezal por comunicación Bluetooth	El monitor recibe datos espurios interrumpiendo su funcionamiento	MPA no disponible	3	3	I	Identificación de cabezal encriptada periódica
CS05		El monitor recibe datos espurios y continúa funcionando	Dosificación incorrecta de anestesia	2	5	I	
CS06	Suplantación de dispositivo monitor	La aplicación recibe valores espurios	Dosificación incorrecta de anestesia	2	5	I	
CS07	Suplantación de usuario en aplicación remota	Un tercero toma control de la maniobra de dosificación	Dosificación incorrecta de anestesia	2	5	I	
CS08		Un tercero se apodera de la base de datos de pacientes.	Perdida de privacidad de pacientes	4	3	I	Suprimir la aplicación remota
CS09	La aplicación sufre un ataque	La aplicación no inicia, se desinstaló o muestra error.	MPA remoto disponible	4	3	I	
CS10		La aplicación muestra valores espurios	Dosificación incorrecta de anestesia	2	5	I	
CS11	Una actualización de alguna parte del sistema no controlada corrompe el funcionamiento o genera vulnerabilidades	El sistema queda fuera de funcionamiento	MPA no disponible	3	3	I	Permitir actualizaciones validadas del sistema solo de forma presencial en fábrica o por personal autorizado
CS12		El sistema queda vulnerable a ataques	MPA no disponible Dosificación incorrecta de anestesia	2	5	I	

4 Conclusiones

Las medidas para mitigar los peligros que surgen de los ciber-ataques, pueden parecer extremas a primera vista (Fig. 4). Todas las medidas de control no solo deben implementarse sino que también deben validarse. La validación de una solución muchas veces implica un esfuerzo mayor al de la implementación misma. Este motivo justifica lo radical de las soluciones planteadas que obligaron a abandonar el modelo de negocio de la telemedicina y blindaron al dispositivo de monitoreo de toda conexión externa.

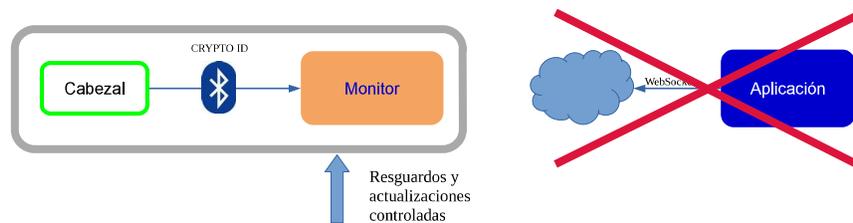


Fig. 4. Cambios en la Arquitectura del Monitor de profundidad de anestesia

Es importante destacar que no es imposible implementar y validar soluciones mejores. En este caso y en particular para la organización encargada de hacer el diseño, resultó estar muy por encima de sus posibilidades y recursos el hecho de proporcionar de manera objetiva evidencias que permitieran llevar adelante estrategias superadoras. Esta situación puede extenderse a muchos de los fabricantes de equipamiento médico tecnológico local que son PyMES [12]. Sus limitados recursos destinados al I+D+i están más inclinados a satisfacer los requisitos de funcionamiento y a mejorar las soluciones clínicas que a la protección de los sistemas. La incorporación de la ciberseguridad implica un cambio de paradigma donde más temprano que tarde los expertos en equipamiento médico deberán volverse también expertos en protección de sistemas médicos para hacer productos sostenibles en un mercado con cada vez más avidez de dispositivos conectados.

Referencias

1. D. Coulombie, F. Orthusteguy, A. Reyes, F. Ortalda. Monitor de Profundidad Anestésica , proyecto. Argentina. Buenos Aires. 2017. Libro. Artículo Breve. Workshop. WICC 2017 XIX Workshop de Investigadores en Ciencias de la Computación. Instituto Tecnológico de Buenos Aires.
2. Luis Miguel Torres Morera, "Tratado de anestesia y reanimación", Madrid Arán cop. (2001)
3. J. Bruhn et al; "Depth of anaesthesia monitoring: what's available, what's validated and what's next?" British Journal of Anaesthesia,(2006), 97(1):85-94
4. ISO 13485:2016 Medical devices Quality management systems Requirements for regulatory purposes (2016)
5. ISO 14971:2019 Medical devices Application of risk management to medical devices

6. IEC 62366-1:2015 Medical devices Part 1: Application of usability engineering to medical devices.
7. IEC 62304:2006 Medical device software Software life cycle processes
8. IEC 60601-1:2005+AMD1:2012 CSV Consolidated version Medical electrical equipment Part 1: General requirements for basic safety and essential performance
9. IEC 82304-1:2016 Health software Part 1: General requirements for product safety
10. AAMI TIR57: 2016 Principles For Medical Device Security - Risk Management
11. Williams, Patricia & Woodward, Andrew. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Medical devices (Auckland, N.Z.). 8. 305-16. 10.2147/MDER.S50048.
12. F. Porta, G. Baruj, Nucleo Socio Productivo Estratégico Equipamiento Médico- Documento de Referencia, Argentina Innovadora 2020, 2012 Ministerio de Ciencia Tecnología e innovación productiva,



Impacto de una debilidad de ciberseguridad en la arquitectura de un sistema electromédico



Diego Coulombie, Agustín Reyes, Alberto Miguens

Dto de Ingeniería e Investigaciones Tecnológicas,
Universidad Nacional de La Matanza San Justo, Buenos Aires, Argentina

{dcoulombie, aireyes, amiguens}@unlam.edu.ar



Proyectos:
PICTO 0087 Monitor de profundidad de anestesia
CYTMA C2-ING-061 Comunicación inalámbrica de baja energía para aplicaciones
electromédicas



San Justo, Octubre de 2020

Se certifica que

Diego Coulombie, Agustín Reyes y Alberto Miguens

han participado como Autores del artículo 13353 *“Impacto de una debilidad de ciberseguridad en la arquitectura de un sistema electromédico”*, aceptado en el XXVI Congreso Argentino de Ciencias de la Computación, organizado por la Universidad Nacional de La Matanza, del 5 al 9 de octubre de 2020.

A handwritten signature in black ink, appearing to read 'Patricia Pesado', is written over a horizontal line.

Lic. Patricia Pesado
Coordinadora Titular de RedUNCI

A handwritten signature in black ink, appearing to read 'Jorge Eterovic', is written over a horizontal line.

Mg. Jorge Eterovic
Decano DIIT UNLaM



Universidad Nacional
de La Matanza