ANTEPROYECTO DE TRABAJO FIN DE GRADO

(Modelo TFG-5)

Convocatoria ordinaria ☑	Convocatoria extraordinaria ☐

A CUMPLIMENTAR POR EL ESTUDIANTE			
Nombre y apellidos:	Mario Rubio Asensio	**DNI:**	
Dirección:		**CP:**	
Ciudad:		**Provincia:**	
E-mail:	Mario.rubio2@alu.uclm.es	**Teléfono:**	

Título del TFG: Analizador USB			
Modalidad		**Orientación**	
General ☐	Especifico ☑	Tareas de desarrollo ☐	Ejercicio de la profesión libre ☑

DATOS DEL DIRECTOR
Nombre y apellidos: Francisco Moya Fernández

Palabras clave: USB, bus, captura, FPGA, analizador, Verilog, WireShark.

BREVE DESCRIPCIÓN DEL TFG

Antecedentes:

Desde el momento de su lanzamiento en la última década del siglo pasado, el bus de comunicación USB *(Universal Serial Bus)* se ha proclamando paulatinamente, tanto en el ámbito industrial como en el comercial, como el bus más conocido y usado.

Una de las gran ventajas que trae consigo la implementación de este bus, a parte de la sencillez general en su uso y la amplia disponibilidad de sistemas capaces a los que conectarse, es la gran versatilidad que puede proporcionar, por eso, no es de extrañar que haya surgido un extenso catálogo de aplicaciones, tales como:

- Dispositivos de interfaz humana, también llamados HID de las siglas inglesas de *Human Interface Device*. Ejemplos de este tipo son ratones o teclados.
- Dispositivos de almacenamiento masivo *"USB-MSC"*. Ejemplos de este tipo son *pendrives* o adaptadores USB a SATA.
- Herramientas de adquisición de datos y comunicación. Ejemplos de este tipos son adaptadores de USB a Serie o USB a WiFi.

Debido a todo lo anterior, y a la escasez de equipos económicos, sería de gran interés y utilidad disponer un sistema de captación USB, que de forma pasiva y poca invasiva, pueda captar la trama de comunicación que se transmite por el bus, transferirla a un equipo, y posteriormente, analizarla para su uso en depuración, ingeniería inversa o análisis de seguridad.

Objetivos:

Los objetivos de este trabajo se pueden dividir en dos grupos totalmente diferenciados, en el primero se tratarán elementos a nivel hardware y comunicación entre dispositivos, mientras que en el segundo se contempla el tratamiento y análisis de los resultados del primer grupo.
Cabe destacar que durante la totalidad de este trabajo prevalecerá el uso de software libre.

1. En el primer grupo, se espera poder capturar y transmitir a un equipo tramas provenientes de un bus USB, para ello:
   - Utilizando un FPGA, concretamente el modelo ICE40HX1K [1] de la empresa Lattice, se generará un sintetizado a partir del lenguaje de descripción de Hardware Verilog [2][3][4] que contenga toda la lógica para la captación (con ayuda de circuito integrado USB3300 [14]) y transmisión de tramas, independientemente del tipo (*Low-Speed, Full-Speed, etc…)* [5][9][12].
   - Se implantará una librería escrita en lenguaje C/C++ que permita comunicar la plataforma de captación anterior con un equipo (como puede ser una Raspberry Pi [7]) . El método de comunicación es a través del propio puerto serie creado por el circuito integrado FTDI situado en la placa de la FPGA.

2. A partir de una trama USB obtenida de cualquier método, tanto por el método anteriormente descrito, como a partir de medios externos, se pretende poder trabajar sobre ella pudiendo integrar los siguientes aspectos.
   - Capacidad de almacenar la trama en archivos de capturas, tal como *pcap* [8], de gran utilidad para análisis en WireShark [6].
   - Plataforma de análisis de dispositivos de interfaz humana (HID), tales como Keylogger o seguidor de puntero de ratón [11].

Resultados esperados:

Los resultados esperados incluyen en primer lugar un prototipo *hardware* totalmente funcional para la captura y transmisión de tramas USB (principalmente 1.1 y 2.0 con velocidades *Low Speed* y *Full Speed*), y posteriormente, *software* especifico que obtenga y almacene dicha trama.
Es además de gran interés que la captura sea fácilmente analizable, pudiendo comprobar su funcionamiento con dispositivos HID.

Temporización:

Tal como se ha comentado en los *"Objetivos"*, este proyecto se puede separar en dos grupos, cada uno subdividido en varios apartados. Se incluye además un apartado adicional en el que se realiza un estudio previo.

0. Análisis y estudio previo.
   - ***Estudio de sistemas actuales***.
     Se realizará un pequeño estudio comparando los diversos productos ya existentes que se asemejen al resultado esperado en el proyecto.
   - ***Selección de componente Hardware sobre los que trabajar.***
   - ***Creación de la metodología a utilizar.***

1. Captura y transmisión.
    - ***Diseño de método de transmisión de la trama a un equipo.***
      Para poder llevar un control adecuado, se necesita en primer lugar poder implementar una transmisión serie básica de información entre la *FPGA* y el equipo de análisis. Este método de comunicación se prevé que se implemente en **dos semanas**, pudiendo añadir pequeñas funcionalidades en el transcurso del siguiente apartado según se necesite.

    - ***Desarrollo en la FPGA de un módulo capaz de comunicarse a través del protocolo ULPI.***
      Utilizando una FPGA, concretamente una de la familia ICE40[1] del fabricante Lattice, y junto al circuito integrado USB3300[14] del fabricante Microchip, se pretende desarrollar un sistema capaz de comunicarse (lectura y escritura de registros, y recepción de datos USB) con el integrado USB3300. Este apartado se puede considerar como el de mayor carga en este grupo, por eso, se plantea un periodo de realización de **dos meses.**

    - ***Implementación básica del método de captura del bus USB.***
      A partir del resultado obtenido en el punto anterior, se finaliza el desarrollo en la FPGA con los módulos capaces de leer y almacenar temporalmente la trama obtenida a través del bus ULPI. Se prevé una duración de **un mes y medio**.

    - ***Pruebas de funcionamiento.***
      En todas las etapas de desarrollado, se realizarán pruebas que aseguren un buen funcionamiento del sistema final.

    En total se pretende trabajar en este grupo un total de **cuatro meses.**

2. Procesado de la trama.
    - ***Librería que permita obtener y utilizar la trama transmitida según el grupo anterior.***
      Al depender este apartado del grupo anterior, se dispone de una gran cantidad de recursos comunes ya realizados, por lo que se prevé una duración de **una semana** en la que depurar, mejorar y limpiar el código anterior.

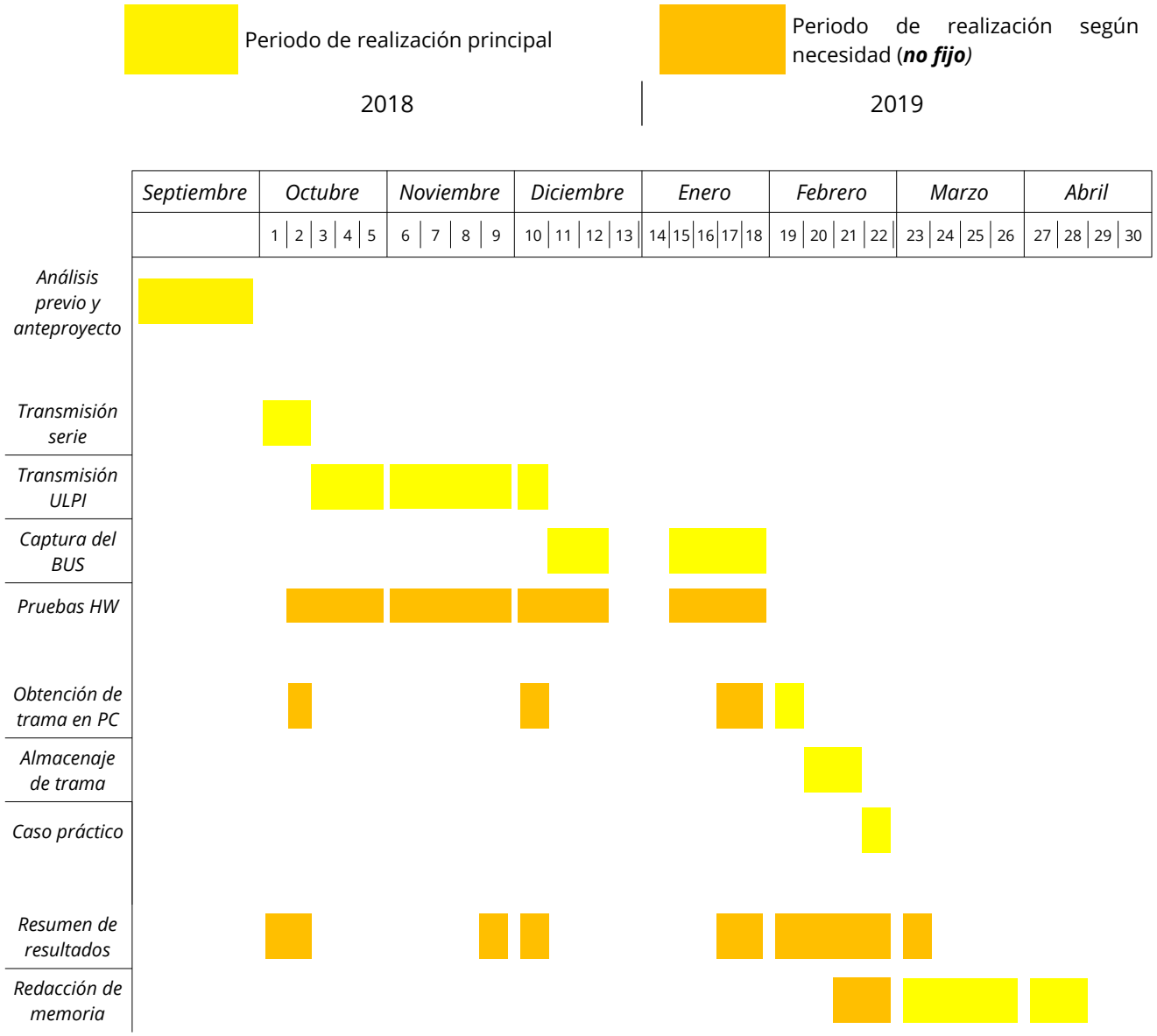
    - ***Utilizando la librería del apartado anterior, ampliarla para poder guardar la trama en un archivo de fácil utilización, como puede ser PCAP.***
      Existe multitud de recursos y librería útiles[13][15] desde los que partir, por tanto, no se plantea un extenso periodo para el desarrollo de este apartado, pudiendo ser este de **dos semanas**.

    - ***Caso practico de análisis de dispositivo USB HID [10][11].***
      Utilizando todos los resultados anteriores, se realizará un caso practico de funcionamiento, capturando y analizando un dispositivo HID. Se prevé una duración de **una semana**.

    En total se pretende trabajar en este grupo un total de **un mes.**

A parte del tiempo anteriormente utilizado, también se prevé utilizar **un mes y medio** para la redacción del documento final, así como todos los recursos y ayudas necesarios para ello.

En la siguiente tabla se muestra una distribución temporal más detallada



Bibliografía:

1. ICE40 LP/HX Family Data Sheet - Lattice Semiconductor – Marzo 2017 (Versión 3.3) - http://www.latticesemi.com/view_document?document_id=49312

2. Lattice ICE Technology Library - Lattice Semiconductor - Marzo 2015 (Versión 2.9) - http://www.latticesemi.com/~/media/LatticeSemi/Documents/TechnicalBriefs/SBTICETechnologyLibrary201504.pdf

3. Tutorial de FPGA utilizando lenguaje descriptivo Verilog - Juan Gonzalez-Gomez (Obijuan) – Noviembre 2015 - https://github.com/Obijuan/open-fpga-verilog-tutorial/wiki

4. Verilog HDL Quick Reference Guide - Stuart Sutherland – 2001 - http://sutherland-hdl.com/pdfs/verilog_2001_ref_guide.pdf

5. USB made simple - MQP Electronics Ltd – 2008 - http://www.usbmadesimple.co.uk/

6. Adding a basic dissector - Ulf Lamping, Luis E. Garcia Ontanon, Graham Bloice – diciembre 2014 (revisión 1.1) - https://www.wireshark.org/docs/wsdg_html_chunked/ChDissectAdd.html

7. Introducción a Raspberry Pi - Francisco Moya Fernández – Enero 2017 - https://franciscomoya.gitbooks.io/taller-de-raspberry-pi/content/es/index.html

8. PCAP next generation file format specification - M. Tuexen, Ed., Muenster Univ. of Appl. Sciences, F. Risso, Politecnico di Torino, J. Bongertz, Airbus DS CyberSecurity, G. Combs, Wireshark, G. Harris – 2017 - https://github.com/pcapng/pcapng

9. USB Complete (2nd Edition) – Jan Axelson – 2004

10. Device Class Definition for Human Interface Devices (HID) V1.11- USB Implementers Forum, Inc. - Junio 2001 - http://www.usb.org/developers/hidpage/HID1_11.pdf

11. USB-based attacks - Nir Nissim,Ran Yahalom,Yuval Elovici - 2017 - https://doi.org/10.1016/j.cose.2017.08.002

12. USB in a nutshell - Craig Peacock – 2010 - http://www.beyondlogic.org/usbnutshell/usb1.shtml

13. Awesome pcaptools - caesar0301 - 2015 - https://github.com/caesar0301/awesome-pcaptools

14. USB3300 USB PHY IC Data Sheet – Microchip Technology Inc. - Enero 2013 (Rev. 1.1) - http://ww1.microchip.com/downloads/en/DeviceDoc/00001783C.pdf

15. PCAP reference manual - The Tcpdump Group – Julio 2018 - https://www.tcpdump.org/manpages/pcap.3pcap.html

Vº Bº y firma del DIRECTOR *Firma del ESTUDIANTE*

Toledo, a 27 de febrero de 2019