Mi casa (digital) es una ruina:

Cuando Alexa te dice “Hazlo tu… ¡si puedes!”

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Advertencia:

- NO es una charla sobre ALEXA
- SI es una charla sobre IoT …
  - en la Industria 4.0 …
  - desde la perspectiva de la Casa Digital

- *Esta charla es divulgativa y se realiza sin interés comercial. Todos los contenidos se encuentran publicados y accesibles en Internet, pero se ha intentado respetar en todo momento el uso o reproducción de material bajo licencias Creative Commons o similares.*

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

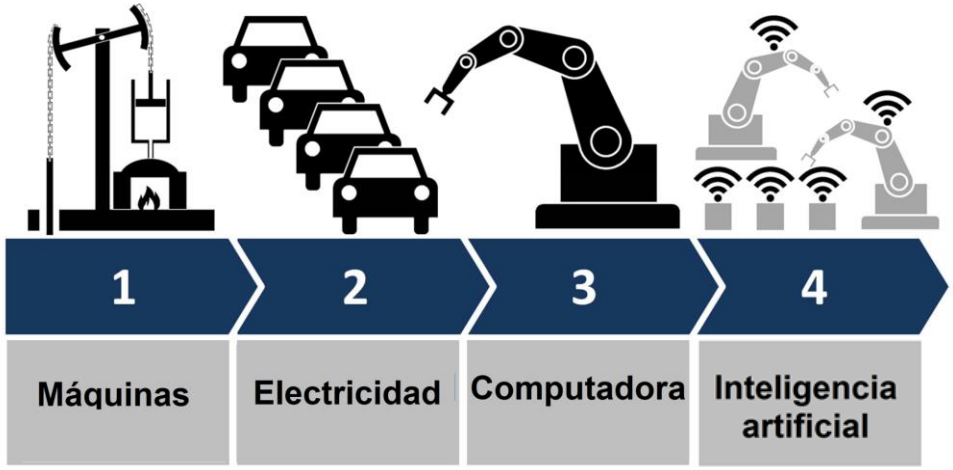
Fuente: YouTube

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Fuente: YouTube

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Industria 4.0



https://commons.wikimedia.org/wiki/File:Industry_4.0_es.png

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Hogar digital

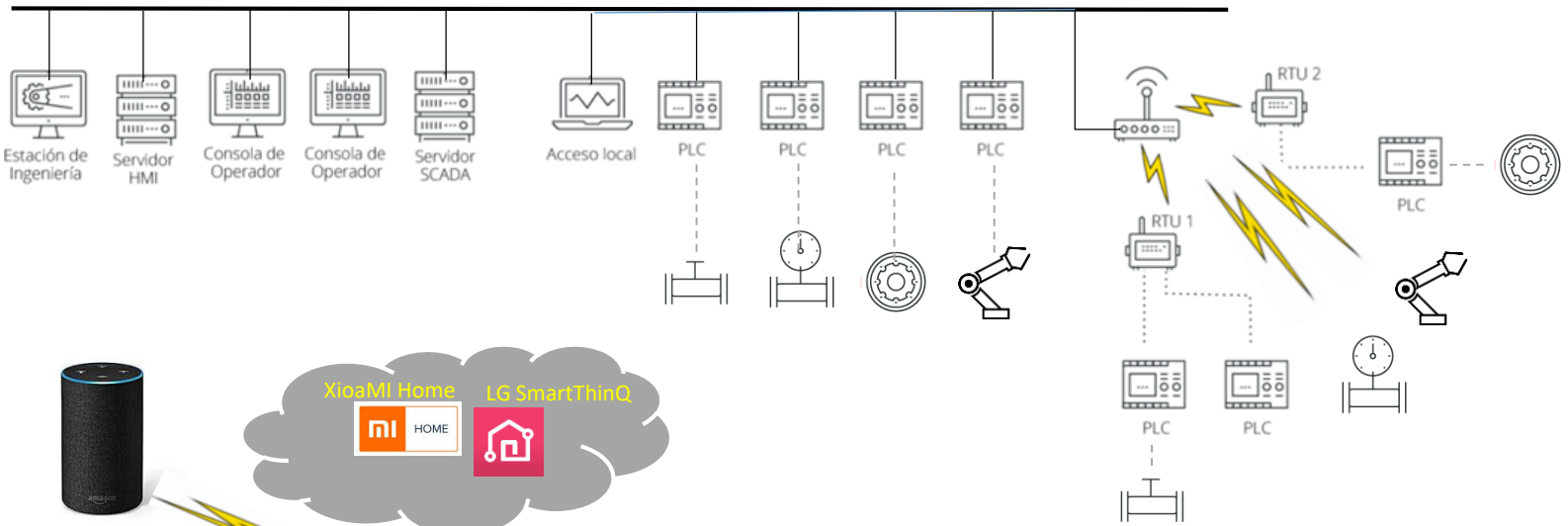
Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Industria 4.0 + IoT

MCS (Manufacturing Control Systems)

IoT

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)



Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

13°
Min. 13° | Max. 27°

MUNDO | LOSANDES

INGRESAR
REGISTRATE

Inicio | Secciones | Servicios | Todas las Noticias | Nuestra Tapa | Más | Buscar

MUNDO | Viernes, 16 de marzo de 2018

Alarma mundial: un ataque cibernético apuntó a hacer estallar una petroquímica

El ciberataque fue en una planta de Arabia Saudita. Advierten que será la nueva modalidad teorrista en el mundo.

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

01/11/2009
NIGHT DRAGON
- Servidores de acceso públicos comprometidos mediante inyección de SQL
- Spear-phising sobre móviles
- Vulnerabilidades conocidas en Windows

01/06/2010
STUXNET
- USB infectado
- Autoreplicación mediante vulnerabilidad 0-day
- Propagación en LAN/SMB aprovechando 0-days en Windows
- Modificación de código específico Siemens

01/09/2011
DUQU
- Emails dirigidos Spear-phishing
- Documento MS-Word explota vulnerabilidad 0-day
- Propagación a otro sistema por la red o por medios compartidos USB

28/05/2012
FLAME
- Emails dirigidos Spear-phishing Webs de confianza comprometidas (Watering Hole)
- USB infectados
- Propagación a otro sistema por la red o por medios compartidos USB
- Herramientas de Ciber-Espionage: Capturas de pantalla, grabación de pulsaciones de teclado, etc.

15/08/2012
SHAMOON
- Emails dirigidos Spear-phishing (Empleados descontentos)
- Vulnerabilidades 0-day
- Detección de otros sistemas vulnerables en la red
- Borrado sección de arranque MBR en disco duro (wipe)

11/02/2013
DRAGONFLY /ENERGETIC BEAR
- Ataques dirigidos Spear-phishing (Pdf+Havex)
- Webs de confianza comprometidas (Watering Hole). Lightsout exploit (Hello exploit)
- Webs legítimas con aplicaciones comprometidas (Talk2Me, eWon VPN client)

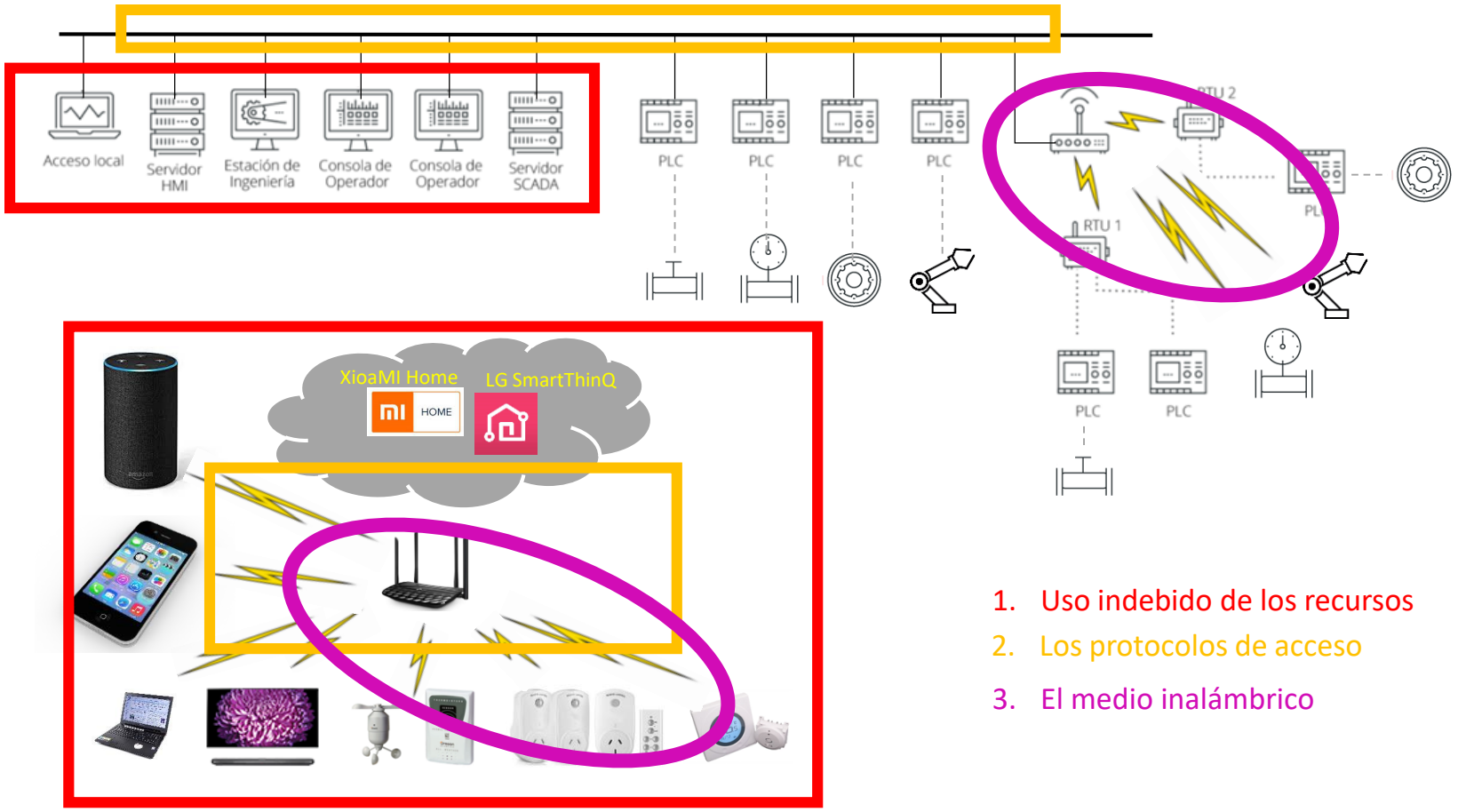
23/12/2015
BLACKENERGY
- Emails dirigidos Spear-phishing (Powerpoint/Diferentes documentos Offfice)
- RAT, Killdisc
- Borrado de ficheros en el disco duro (Wipe)
- Denegación de Servicio DoS, DDoS

17/12/2016
CRASHOVERRIDE
- Emails dirigidos Spear-phishing (Powerpoint/Diferentes documentos Offfice)
- Primer malware con módulos específicos para protocolos industriales (IEC 101, IEC 104, IEC 61850, OPC)
- Módulo adicional que explota una vulnerabilidad en Siemens SIPROTEC (DoS)
- Módulo Wipe

15/11/2017
TRITON / TRISIS
- USB infectado
- Objetivo Schneider Electric´s Triconex SIS (Safety instrumented system)
- Aprovecha una mala configuración, "Program Mode" activado en producción.
- Cambio de la lógica programada

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

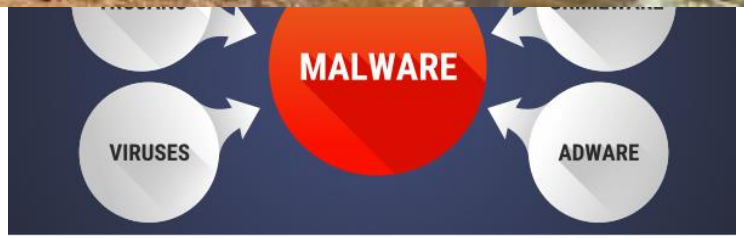
Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)



1. Uso indebido de los recursos
2. Los protocolos de acceso
3. El medio inalámbrico

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Uso indebido de los recurso



Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Uso indebido de los recursos

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

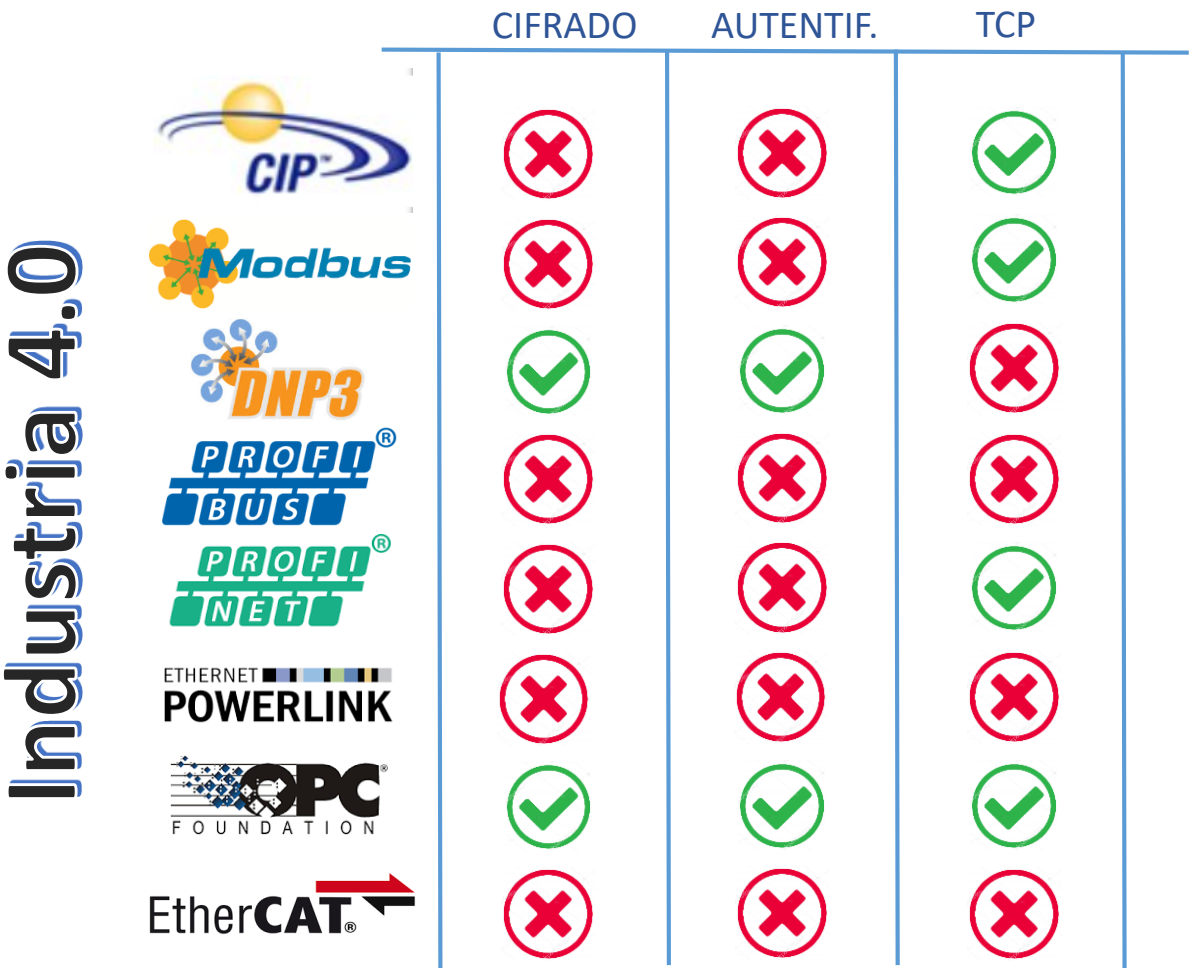
Los protocolos de acceso

V · T · E	**Automation protocols**	[hide]
Process automation	AS-i · BSAP · CC-Link Industrial Networks · CIP · CAN bus (CANopen · DeviceNet) · ControlNet · DF-1 · Powerlink · EtherNet/IP · FF H1 · HSE) · GE SRTP · MECHATROLINK · MelsecNet · SERCOS interface · SERCOS III ·
Industrial control system	
Building automation	strumentation Protocol · KNX ·
Power-system automation	ntation Protocol · IEC 61850 ·
Automatic meter reading	igBee
Automobile / Vehicle	000 · FMS) · · Keyword Protocol 2000 · Unified Diagnostic Services · LIN · MOST · VAN

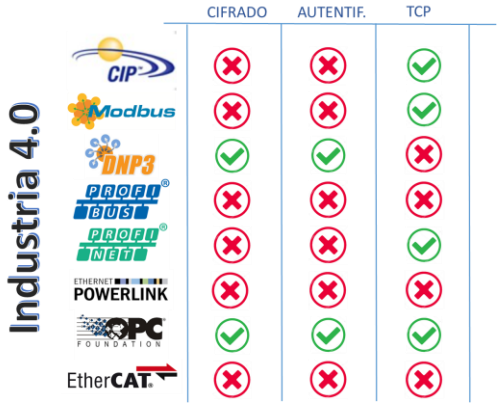
https://en.wikipedia.org/wiki/List_of_automation_protocols

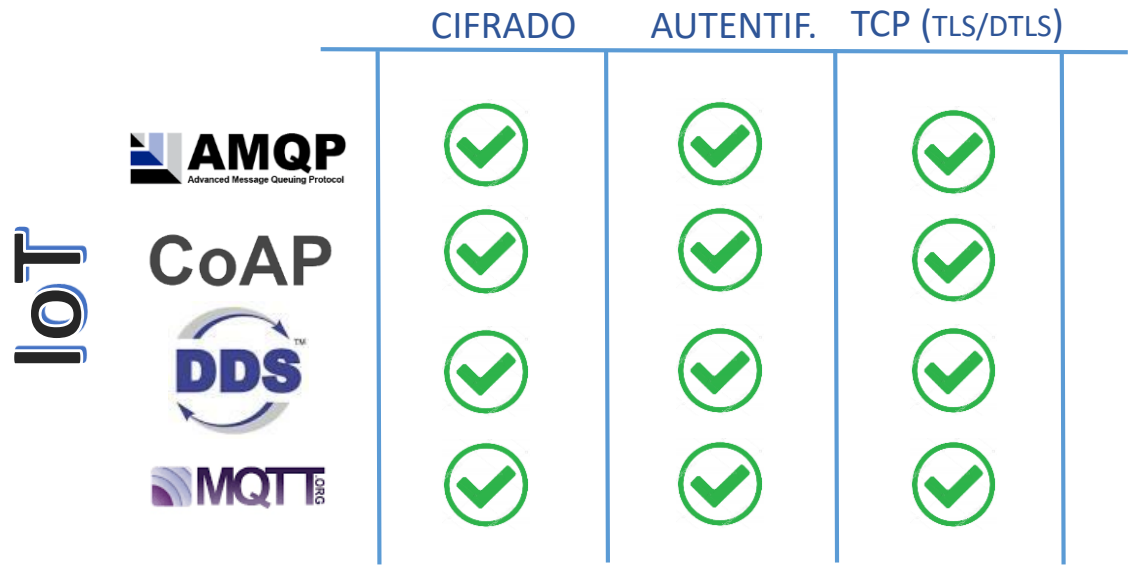
Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Industria 4.0

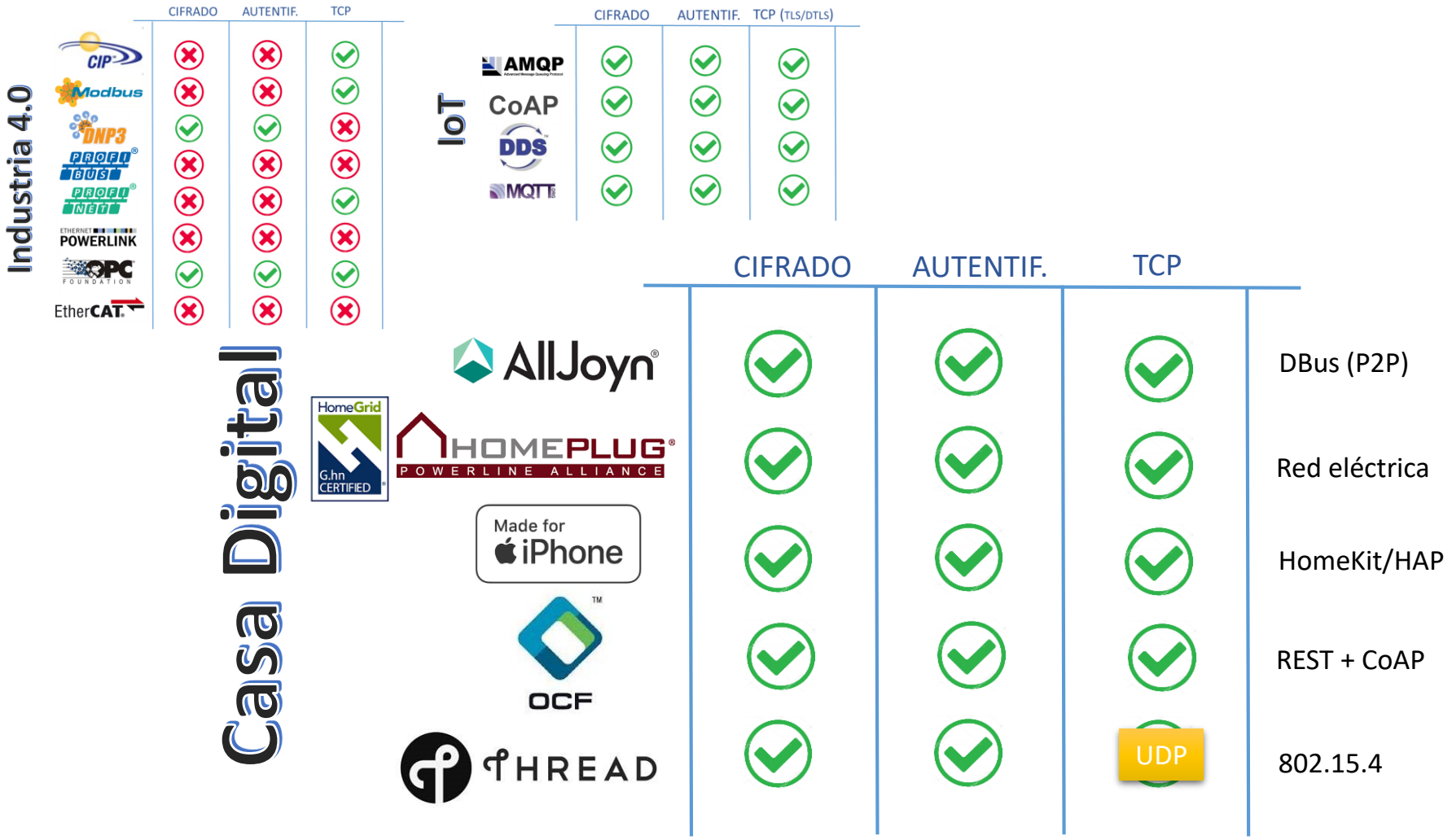


Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)





Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)



Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

El medio inalámbrico

CompartirWIFI

TIENDA Wifi | Ofertas

Guía sobre cómo descifrar claves wifi facilmente en 2019, para seguridad WEP, WPA, WPA2 y WPA2-PSK

9 enero, 2018 tartigues

¿Es legal esta guía para descifrar claves wifi 2019 WEP, WPA y WPA2?

Sí, esta guía y todas las herramientas y métodos que se indican son totalmente legales, estas herramientas para descifrar claves wifi se usan para hacer auditoría de redes, el objetivo es determina si una red es o no segura.

La única finalidad de seguir esta guía debe ser para descifrar la clave de tu propia wifi, o bien de una wifi en la que tengas permiso, para poder averiguar si esta wifi es o no segura.

Mucho cuidado porque piratear una wifi es delito, si descifras la clave wifi de tu vecino y luego la usas sin permiso puedes tener problemas, es algo que está penado por la ley, tal y como puedes ver en este artículo sobre penas por piratear una red wifi.

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Manual de usuario:

1 - Enchufar

2 - Descargar la App y registrar en Servidor del Fabricante/Proveedor

4 - La App pide usuario/pass del AP de nuestra WIFI
La App envía usuario/pass al dispositivo.
El dispositivo inteligente se conecta a nuestra WIFI
El dispositivo se registra en el servidor del fabricante

3 - En la App, seleccionar instalar dispositivo
La App detecta y conecta al AP del dispositivo

- Periódicamente manda UDP con modelo, nombre, MAC y estado al servidor
- El servidor devuelve los datos a la APP, más versión de firmware, puerto y dirección IP local

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

¿Problemas?

TP-LINK

Comunicación con el servidor (“Nube”):

- Protocolo JSON casi **legible** ("encriptado" con un cifrado XOR fácilmente reversible)

Actualizaciones del firmware:

- Automática desde la App (confirmada por el usuario)

Comunicación con la App:

- Protocolo de depuración y configuración encriptado DES

  DES (TDDP - TP-Link Device Debug Protocol)

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

TP-LINK

IFTTT

Amazon

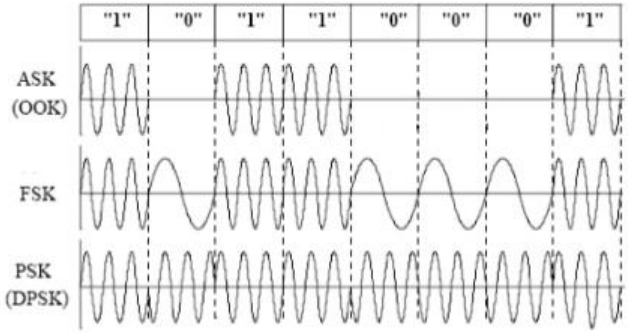
Volviendo al medio inalámbrico…

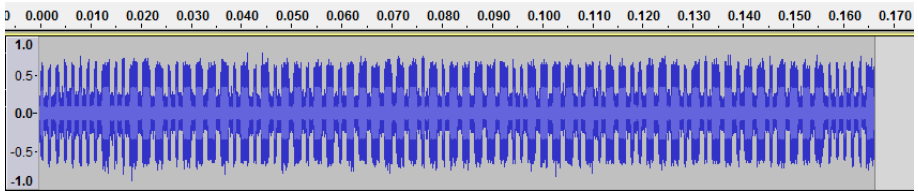
	WPAN (< 75 m)			LPWAN (< 15 Km)			
	ZigBee	Bluetooth	Wi Fi	sigfox	LoRa	Lte	5G
Frecuencia	868 MHz	2,4 GHz	2,4 - 5 GHz	868 MHz	868 MHz	7-900 MHz	7-900 MHz
Licencia	IMS	IMS	IMS	IMS	IMS	Operador	Operador

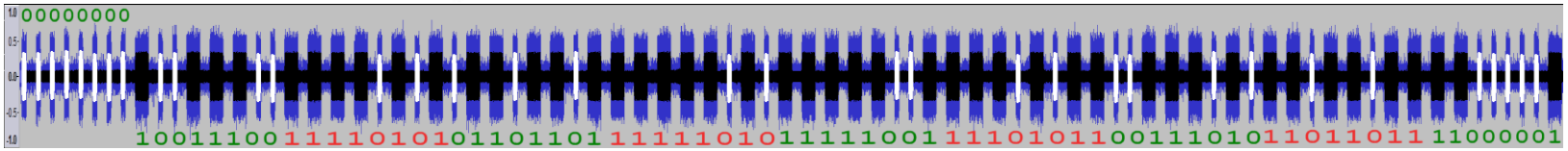
868 MHz

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

868 MHz

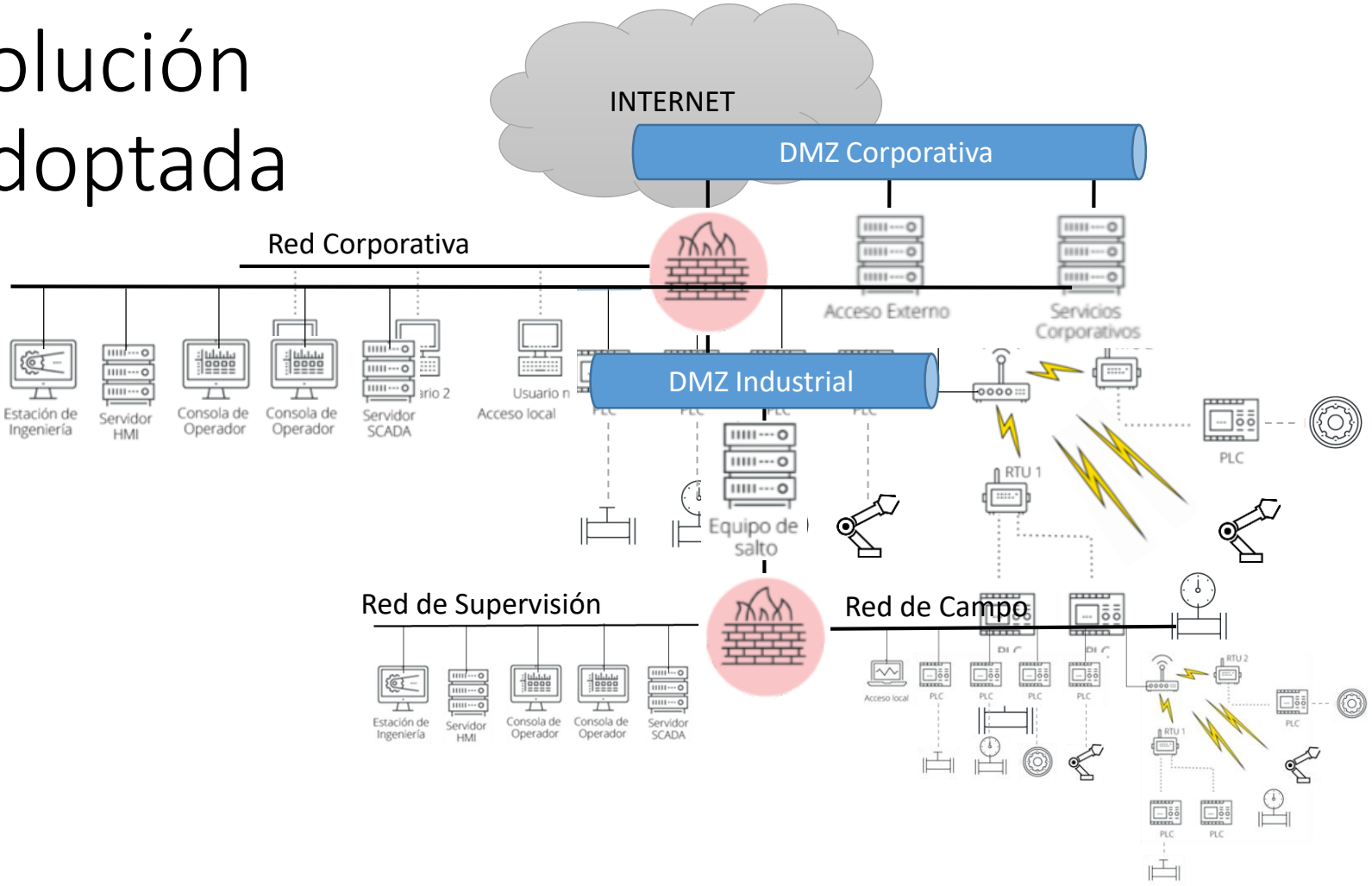






Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Solución adoptada



Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Y en casa???

Actualiza SIEMPRE tus dispositivos A LA ÚLTIMA VERSIÓN (OFICIAL!!!)…

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Los peligros de un medidor inteligente

Un medidor inteligente puede comunicarse con dispositivos de red conectados en nuestra red doméstica, como por ejemplo los sistemas de aire acondicionado, neveras y otros aparatos *IoT*. Un atacante que pudiera infiltrarse en un medidor conectado a internet podría controlar estos dispositivos. Podrían incluso abrir puertas si están controladas con estos sistemas.

- NO dejes nunca las contraseñas por defecto
- Utiliza contraseñas diferentes siempre que puedas
- Cambia las contraseñas periódicamente…

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

eSMARTCITY.es
Todo sobre Ciudades Inteligentes

SÍGUENOS:

INICIO CIUDADES INTELIGENTES GOBIERNO / ECONOMÍA MOVILIDAD ENERGÍA MEDIO AMBIENTE >SERVICIOS >CONGRESOS

Inicio » Ciudades Inteligentes » La telegestión del agua alerta sobre la ausencia de consumo entre personas solas con movilidad reducida en una localidad aragonesa

La telegestión del agua alerta sobre la ausencia de consumo entre personas solas con movilidad reducida en una localidad aragonesa

Publicado: 13/02/2019

…Ten siempre presente los pros y contras de tener tu hogar conectado…

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

…y recuerda que SIEMPRE HAY ALGUIEN MAS INTELIGENTE !!!

Alberto Eloy García Gutiérrez
UC (alberto.garcia@unican.es)

Gracias!!!

- Principal referencia de esta charla:

  https://www.incibe-cert.es

Para cualquier pregunta/consulta/duda:

Alberto Eloy García Gutiérrez
Universidad de Cantabria
(alberto.garcia@unican.es)