



© 2025 CS³ Group – Todos los derechos reservados



Asociación de Seguridad Informática
EuskalHack
Segurtasun Informatika Elkartea

21 de junio de 2025 | VIII EuskalHack 2025 · Donostia (Euskadi)

HACKING CRANES MAMA!

After Sex Toys, TPMS, Avionics... as a Game...

Tipo de documento: Presentación

Autor del documento: CS³ Group (Pedro C. aka s4ur0n)

Código del Documento: EuskalHack25.pdf

Versión: 1.0

Categoría: PÚBLICO

Fecha de elaboración: 03/05/2025

Nº de Páginas: 63



Whoami

```
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.webcorp = 'https://cs3group.com'
        self.role = 'Security Researcher'
        self.work = ['Reversing', 'Malware', 'Offensive Security', '...']
        self.groups = ['mlw.re', 'OWASP', 'NetXploit', '...']
```



CS³ Group (<https://cs3group.com>)

Formación en Seguridad

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

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

Hardware Hacking

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

Forense

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

SIGINT

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

ATM

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

Hacking Ético

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

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

Seguridad en dispositivos móviles

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

DevSecOps

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

T.S.C.M.

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

PoS/TPV

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

Análisis de Malware

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

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

Respuesta ante incidentes

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

Intelligence

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

Telecom

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

LOPD/GPDR/Cumplimiento

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

Contenido

- Introducción a los sistemas inalámbricos para control de maquinaria.
- Características de Seguridad (safety) y “Seguridad”.
- Análisis: ataques a su seguridad y afectación.
- Vulnerabilidades y ataques a estos dispositivos:
 - Repetición (replay)
 - Inyección de comandos
 - Botón de emergencia STOP
 - Re-emparejamiento de sistemas inalámbricos
 - Firmware
- Conclusiones

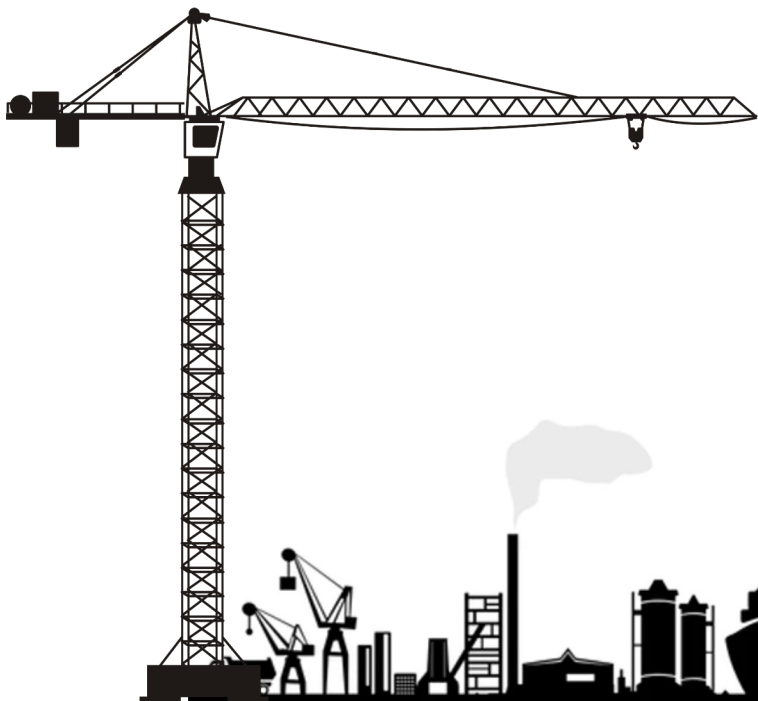


HACKING CRANES MAMA

LEVEL 01: INTRO

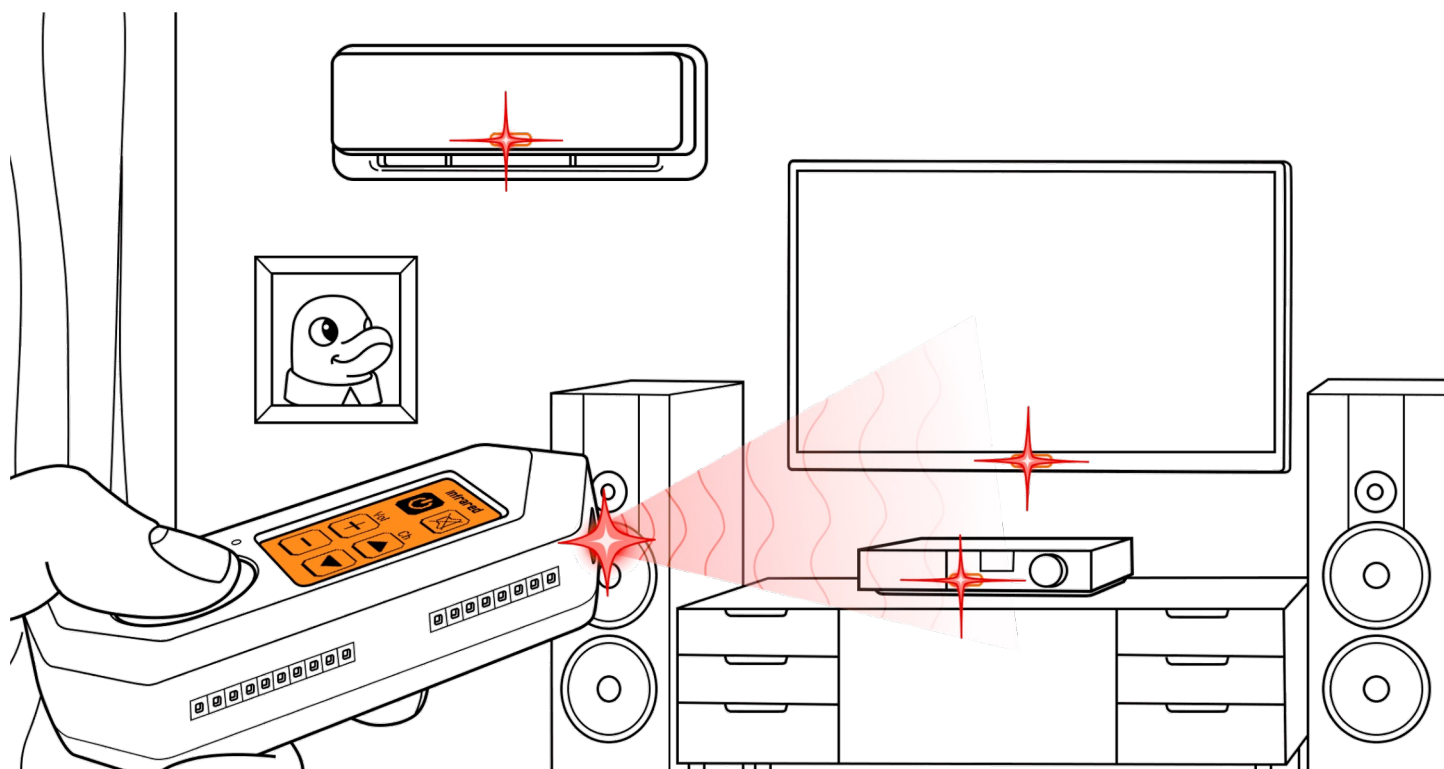
Sistemas inalámbricos de control de maquinaria

Una **grúa** es una **máquina** cuya función es la de ***eleva*r**, ***trasla*dar** y ***descende*r** materiales o cargas. Suelen contar con **poleas**, **cables de acero**, **contrapesos**, **estabilizadores**, **etc...** para crear ventaja mecánica y lograr mover grandes cargas...



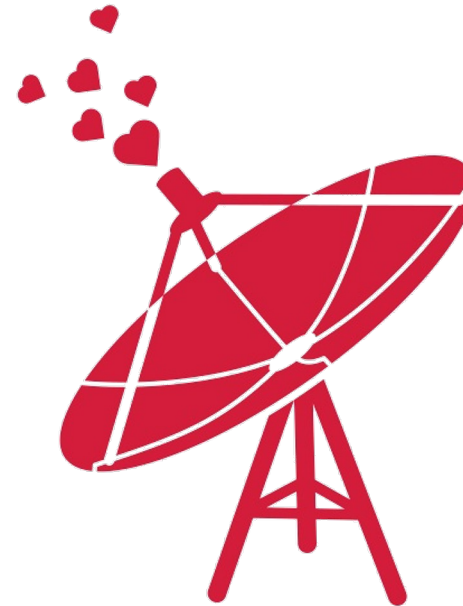
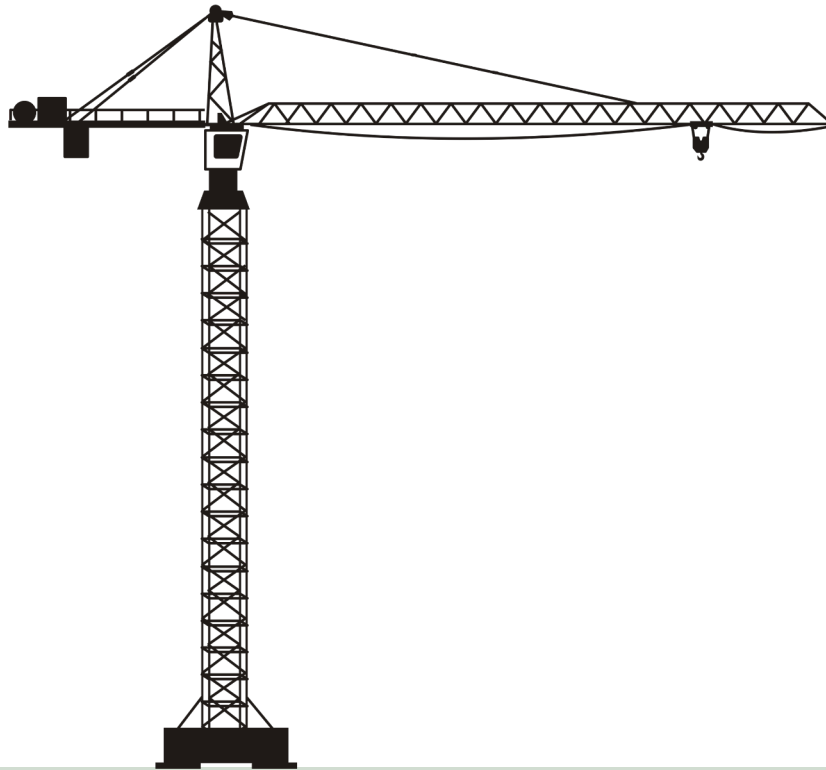
Sistemas inalámbricos de control de maquinaria

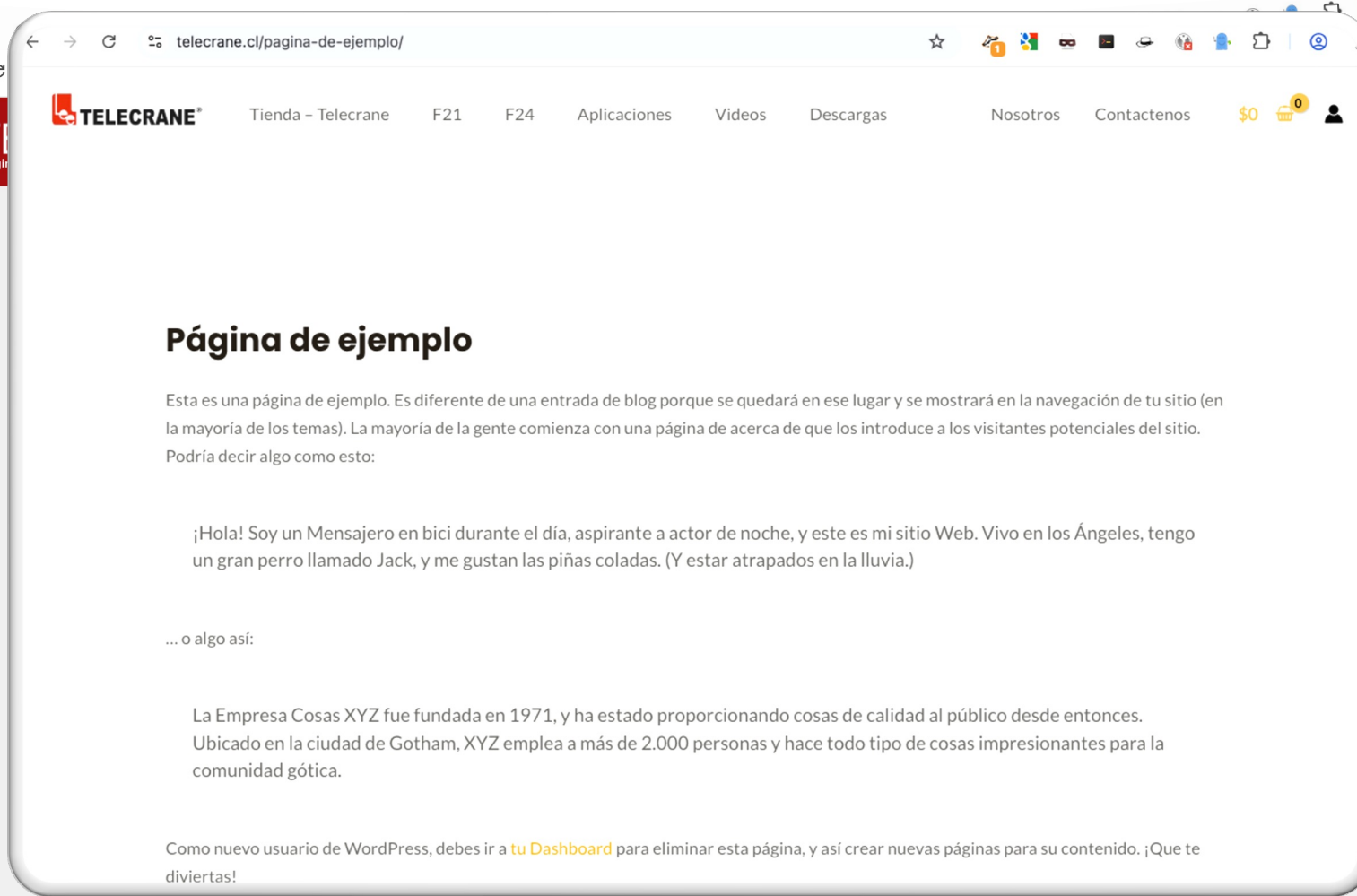
Somos **perezosos** por naturaleza...



Sistemas inalámbricos de control de maquinaria

¿Por qué no controlar máquinas industriales cómodamente?





Sistemas inalámbricos de control de maquinaria

Los controladores remotos de RF se basan en protocolos de *radio por paquetes*, que implican la modulación de un flujo de bytes en unas simples **ondas de radio**.

Tienen una conectividad plena en los **Sistemas Industriales** junto con otros dispositivos (*Anybus, CAN bus, etc...*) lo que les convierte en un objetivo atractivo para un actor de amenazas.

Y los “**abuelos**” todos los días *pasan* el **control de calidad** de las obras...

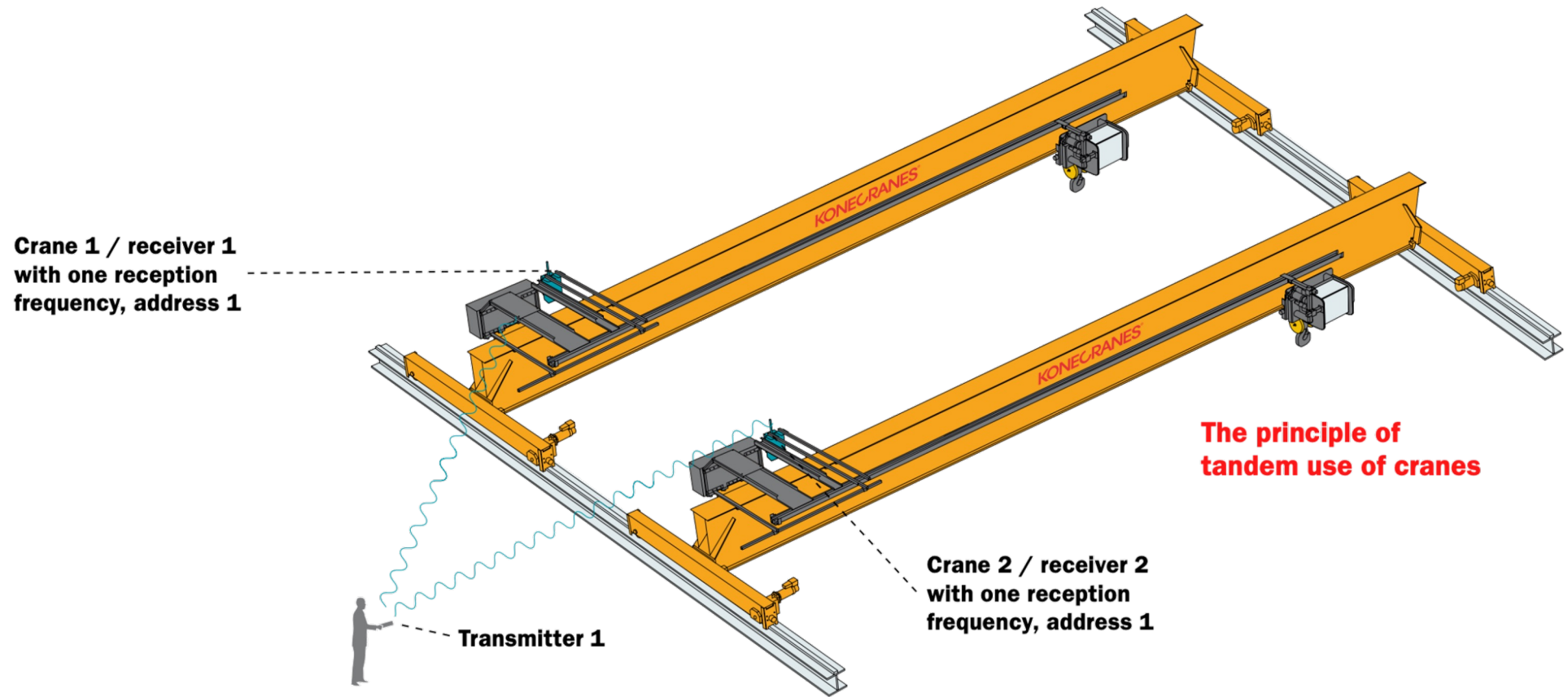
Sistemas inalámbricos de control de maquinaria



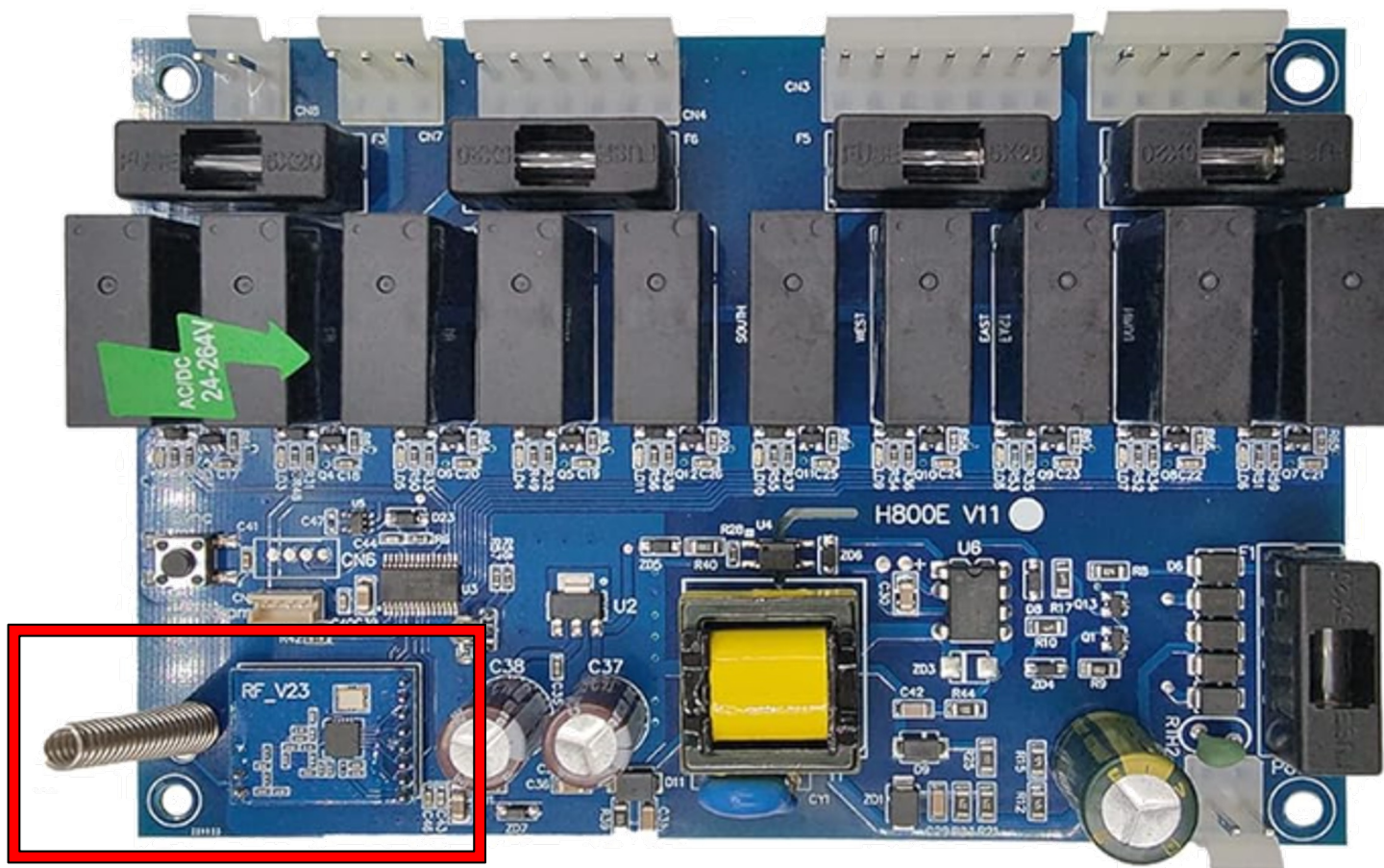
Sistemas inalámbricos de control de maquinaria



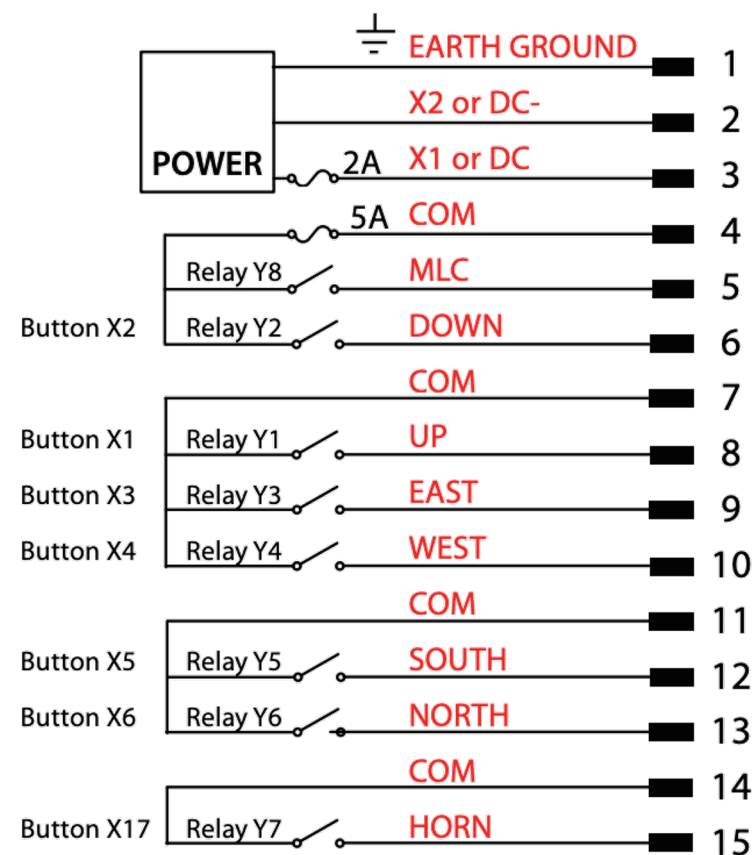
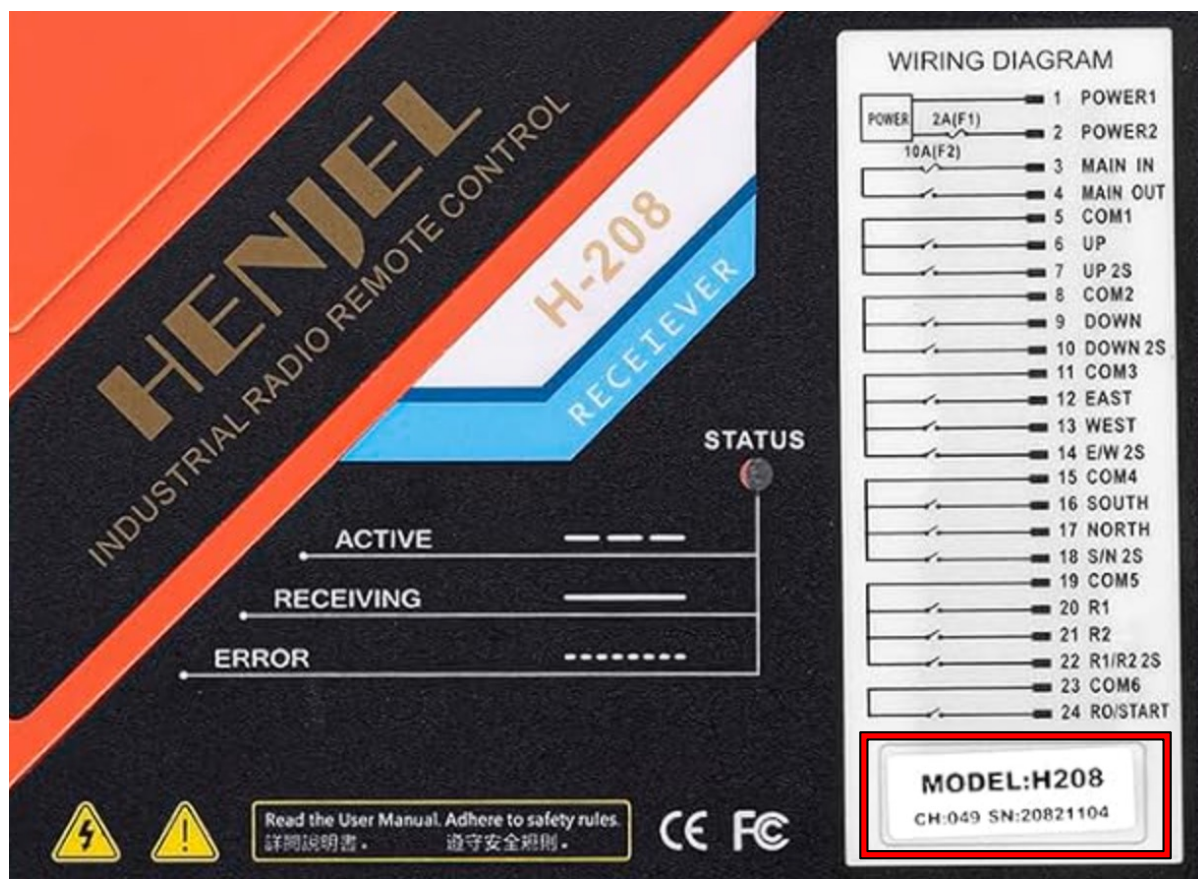
Sistemas inalámbricos de control de maquinaria



Sistemas inalámbricos de control de maquinaria



Sistemas inalámbricos de control de maquinaria



Sistemas inalámbricos de control de maquinaria



Sistemas inalámbricos de control de maquinaria

Technical data

TRANSMITTER

Frequency range	434.040Mhz~434.790Mhz
Modulation method	4 FSK
Typical operating range	100M
Control system	PLL
Antenna impedance	50Ω
Typical response time for Stop command and commands	50mS~100mS
Power supply	LR6(AA)1.5V x2
Antenna	Internal
Average power consumption	16mA@DC3V (default setting)
Radio-frequency power	<10dBm (default setting)
Operating and storage temperature	(-20°C)~(+55°C) / (-40°C)~(+65°C)
Protection degree	IP65
Dimensions	193x57x51mm
Weight (including battery)	approx.325g
Housing material	PA6(30% GF)

Technical Data Sheet

Technical Data Sheet

TRANSMITTER		RECEIVER			
Certification	 10821A-898961620	 Reference No. T121109W02	 ID No. RN489896162JK01		
Frequency	433.0525 > 434.7775 MHz	433.0525 > 434.7775 MHz			
Modulation Type	4GFSK	4GFSK			
Maximum operating distance	100 meters	Sensitivity	-112dBm a 1,2Kbps		
Control system frequency	PLL multifreq. 140 ch.	PLL multifrequency 140 channels			
Antenna impedance	50 ohm	50 ohm			
Typical response time command	50 > 100mS	50 > 100mS			
Power Supply	2 x (AA) alkaline battery	H - 24-240 Vac / HV - 12/24 Vdc / HS - 24/264 Vac/dc / HM - 90-160 Vac/dc			
Antenna	Internal	External			
Average consumption	16mA a 3Vcc	Power consumption in standby	16mA at 220Vca		
Transmission power	< 10dBm	+ 10dBm			
Operating temperature	-30°C > +75°C	-30°C > +75°C			
Degree of protection	IP65	Relay Output 1NO 5 A 250 Vac	H - 2 stop + 2 start + 2 command HS - 2 stop + 2 start + 13 command HM - 2 stop + 2 start + 19 command	MOSFET output 7,5 Amps	HV - 14 programm. output
Overall Size and weight	K200/808 H193xL57xD51 mm - 290 g K1000/1212 H245xL57xD51 mm - 350 g	H - H142 x L141,2 x D58,5 (mm) - weight 800 g HV - H142 x L141,2 x D58,5 (mm) - weight 800 g HS - H190 x L184 x D64 (mm) - weight 1750 g HM - H272 x L260 x D96 (mm) - weight 2950 g			
Case Material	Nylon and fiberglass	Nylon and fiberglass IP65			

Sistemas inalámbricos de control de maquinaria



Compliance Certification Services Inc.

FCC ID: RN489896162JK01

Report No.: T121109W02-RP1

FCC 47 CFR PART 15 SUBPART C

TEST REPORT

For

K series Remote Control Device

**Model: K808 Series, K1200, K1202, K1204, K1206, K1208, K1210, K1212,
K1000, K1002, K1004, K1006, K1008, K1010, K800, K802, K804, K806, K808,
K600, K602, K604, K606, K400, K402, K404, K200, K202**



Asociación de Seguridad Informática
EuskalHack
Segurtasun Informatika Elkartea

© 2025 CS³ Group – Todos los derechos reservados

Sistemas inalámbricos de control de maquinaria

2. EUT DESCRIPTION

Product	K series Remote Control Device		
Trade Name	JUUKO		
Model Number	K808 Series, K1200, K1202, K1204, K1206, K1208, K1210, K1212, K1000, K1002, K1004, K1006, K1008, K1010, K800, K802, K804, K806, K808, K600, K602, K604, K606, K400, K402, K404, K200, K202		
Model Difference	Model Number	Frequency Range	433.0525 - 434.780MHz
	K1200, K1202, K1204, K1206, K1208, K1210, K1212, K1000, K1002, K1004, K1006, K1008, K1010, K800, K802, K804, K806, K808, K600, K602, K604, K606, K400, K402, K404, K200, K202	Number of Channels	139 Channels
	K800, K802, K804, K806, K808, K600, K602, K604, K606, K400, K402, K404, K200, K202	Frequency Spacing	12.5KHz
	K800, K802, K804, K806, K808, K600, K602, K604, K606, K400, K402, K404, K200, K202	Modulation Technique	GFSK
	K800, K802, K804, K806, K808, K600, K602, K604, K606, K400, K402, K404, K200, K202	Antenna Specification	Brand: JUUKO / Model: ANT-K800 Monopole Antenna / Gain: 3 dBi
Received Date	November		
Power Supply	Power from Vdc1.5*2 (		
Frequency Range	433.0525 -		
Number of Channels	139 Channels		
Frequency Spacing	12.5KHz		
Modulation Technique	GFSK		
Antenna Specification	Brand: JUUKO / Model: ANT-K800 Monopole Antenna / Gain: 3 dBi		



HACKING CRANES MAMA

LEVEL 02: SAFETY OR SECURITY?

CS³ SERVICES
<https://cs3group.com>



Asociación de Seguridad Informática
EuskalHack
Segurtasun Informatika Elkarteak

© 2025 CS³ Group – Todos los derechos reservados

Características de Seguridad (safety) y “Seguridad”

Riesgos indirectos

Durante la utilización

Circunstancias peligrosas	Medidas preventivas
Desplome de la grúa.	No debe utilizarse la grúa con velocidad del viento igual o superior a 60 Km/h. o al límite fijado por el constructor. Cuando la velocidad del viento supere este límite hay que llevar la grúa móvil sobre el tramo de seguridad del rail y anclarla con las tenazas. La pluma debe orientarse en el sentido de los vientos dominantes y ser puesta en veleta (giro libre), desfrenando el motor de orientación. No deben arrancarse con la grúa objetos adheridos al suelo. No deben elevarse cargas con tiros inclinados.
Caída de la carga o parte de ella.	Las cargas de forma alargada se sujetarán con eslingas dobles para evitar que puedan caer por deslizamiento. Cuando sea preciso se guiarán con cuerdas, estando la persona que guía la carga fuera del alcance de caída de la misma. Las plataformas de transporte de materiales estarán apantalladas; de no ser posible el apantallamiento, las cargas se atarán a las plataformas.
Caída de personas al recoger la carga junto a aberturas exteriores (se hace mención de este riesgo, no siendo imponible a la grúa ni a las maniobras con esta máquina realizadas, por considerarlo muy grave y origen de accidentes).	Se instalarán en las plantas de los edificios plataformas en voladizo, dotadas de barandillas y rodapié para la descarga de los materiales.
Caída del gruísta.	En caso necesario, el gruísta se colocará sobre una plataforma volada del borde del forjado, dotada de barandillas y rodapiés.

NTP 125: Grúa torre
Grue à tour
Tower crane

Las NTP son guías de buenas prácticas. Sus indicaciones no son obligatorias salvo que estén recogidas en una disposición normativa viciada. A efectos de valorar la pertinencia de las recomendaciones contenidas en una NTP concreta es conveniente tener en cuenta su fecha de edición.

Actualizada parcialmente por la NTP 701.

Características de Seguridad (safety) y “Seguridad”

Fuertes vientos

- Realizar siempre correctamente la puesta fuera de servicio de la grúa, especialmente la puesta en veleta de la grúa, desplazarla al lugar de seguridad y amarrarla a la vía si dispone de ella. (Fig. 6 a y b)
- Comprobar que el anemómetro funciona correctamente (sonido intermitente con vientos de 50 Km/h y continuo a los 70 Km/h) y suspender el trabajo con la grúa en cuanto el anemómetro emita la señal de aviso de manera continua. (Fig. 7)
- Comprobar que no se coloquen en la estructura de la grúa elementos ajenos a la misma, no autorizados por el fabricante, como carteles en la torre, en la pluma o banderas en la cúspide. (Fig. 8)

Figura 6
Actuaciones en caso de fuertes vientos



Figura 7
Anemómetro

Características de Seguridad (safety) y “Seguridad”

Figura 7
Anemómetro

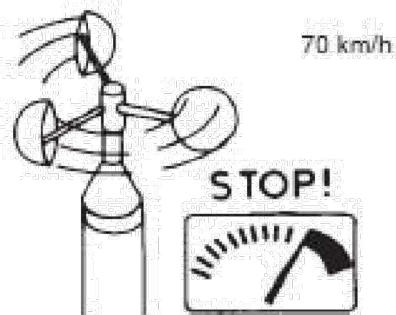
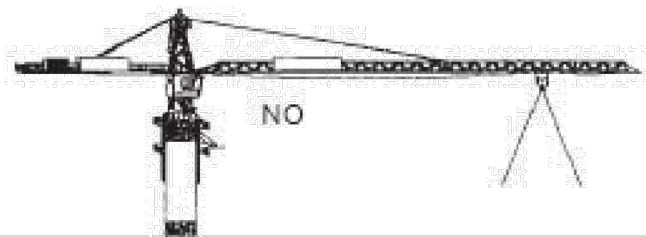


Figura 8
Grúa con elementos ajenos



Características de Seguridad (safety) y “Seguridad”

articuweb.wordpress.com/2010/02/06/frases-de-albaniles-sus-piropos/

4. iiiTanta carne y yo en cuaresma!!!
5. iiiHay qué curvas!!! iiiY yo sin frenos!!!
6. iiiDime quién es tu ginecólogo para chuparle el dedo!!!
7. iiiMozaa!!! iiiTienes dos ojos como dos sartenes que cuando te los miro se me fríen los huevos!!!
8. iiiNiña!!! iiiEstás más apretada que los tornillos de un submarino!!!
9. iiiQuién fuese bizco para verte dos veces!!!
10. iiiMaría!!! iiiTienes unos ojos que..., que..., que te comería todo el coño!!!
11. iiiSi fueras barco pirata te comería el tesoro que tienes entre las patas!!!
12. iiiSeñora!!! iiiLe cambio la hija por un piano y así tocamos los dos!!!
13. iiiSería capaz de follarme a tu perro para entrar en tu familia!!!
14. iiiEstás tan buena que te haría un traje de saliva!!!
15. iiiCon ese culo te invito a cagar en mi casa!!!
16. iiiSi me caigo ya se donde agarrarme!!!
17. iiiPreciosa!!! iiiCon esa mirada tan dulce me dan ganas de chuparte un ojo!!!
18. iiiMozaa!!! iiiSi tu culo fuera un banco te la metería a plazo fijo!!!

Si,

Comienzo:

Atención

Ilustración



Características de Seguridad (safety) y “Seguridad”

Tabla 2
Ficha de control de las condiciones de seguridad

Operador de grúa torre		
Nº de Carné		
Lugar de trabajo		Fecha
Datos de la grúa:		
Marca	Modelo	Nº
CUESTIONARIO		
	SI	NO
1. El acceso al puesto de conducción se realiza de manera segura		
2. La visibilidad desde el puesto de conducción permite maniobrar de manera segura		
3. Existe «encargado de las señales» y código de comunicación para cuando éste sea necesario		
4. La cabina en caso de disponerla es confortable y dispone de limpiaparabrisas		
5. Las zonas de trabajo, por donde deben discurrir las cargas está señalizada		
6. Existen dispositivos de alarma sonora, para avisar de la presencia de cargas		
7. Existen plataformas de descarga para impedir el tiro en oblicuo		

Características de Seguridad (safety) y “Seguridad”



UNE-EN 13557:2024

Grúas. Dispositivos

Prólogo europeo

5	Verificación de los requisitos y/o medidas de seguridad.....	15
6	Información para la utilización	16
Anexo A (Informativo)	Lista de peligros significativos.....	17
Anexo B (Informativo)	Selección del conjunto adecuado de normas de grúa para una aplicación determinada.....	19
Anexo ZA (Informativo)	Relación entre esta norma europea y los requisitos esenciales de la Directiva 2006/42/CE.....	21
Bibliografía		23

4.4.3	Dispositivos conectados por cable	11
	Centros de mando inalámbrico	11

Características de Seguridad (safety) y “Seguridad”



UNE-EN 62745:2017 (Ratified)

5	Verification	19
5.1	General.....	19
5.2	Labelling and markings	19
5.3	Documentation.....	19
5.4	Functional verifications	19
6	Information for use	22
6.1	General.....	22
6.2	Information to be provided	22
7	Labelling and markings.....	24
	Annex A (informative) Logic of stop functions	25
	Bibliography.....	27

4.14	Suspension of the CCS	14
4.15	Configurability protection	13
	Indication of transmission and communication	14

Características de Seguridad (safety) y “Seguridad”

4	Functional requirements	19
4.1	General	19
5	Verification	19
5.1	General	19
5.2	Labelling and markings	19
5.3	Documentation	22
5.4	Functional verifications	22
6	Information for use	22
6.1	General	24
6.2	Information to be provided	25
7	Labelling and markings	27
Annex A (informative) Logic of stop functions		27
Bibliography		25
Figure 1 – Block diagram example of a cableless control system and its interaction with the machine control		12
Figure A.1 – Logic for stop functions		18
4.15 Configurability protection		19



HACKING CRANES MAMA

LEVEL 03: AMENAZAS,
RIESGOS Y ATAQUES

Análisis: amenazas

Amenaza	Descripción	Previene	Problemas
Asociación	RX y TX se asocian con un código fijo (¿ Todos igual?) que si se desconoce, no lo permite.	Interferencias cercanas con otros dispositivos, pues aunque tenga TX, el RX sólo atenderá al que “conozca”.	Conocer la clave o dónde se transmite para alterar las tramas de las señales.
Protección del código de “inicio”	Hay que introducir un código para arrancar el sistema.	Que sólo quien lo conozca podrá operar la maquinaria.	Suelen ser comunes y con pocas opciones.
Autorización	Dependiendo del operador, se habilitan más o menos funciones , en función de su código de acceso.	Es necesario conocer la maquinaria manejada, ya que puede causar daños materiales.	Reutilización de credenciales “por si acaso”...

Análisis: amenazas

Amenaza	Descripción	Previene	Problemas
Rango de alcance	Posible canal secundario para que si no se recibe señal, usen otros canales (IR) o no se acepten comandos.	Radio cercano de acción.	Repetidores que pasen nuestras señales, al igual que TOR u otras (y que no se sepa el origen)...

Análisis: ataques a su seguridad y afectación

Ataque	Descripción	Afectados
Ataque de repetición	Se puede grabar la señal al ser abierta.	Todos
Inyección de comandos	Si se conoce el protocolo, se puede hacer sin mayor problema, fácil, sencillo y para toda la familia, que no se aburra el “abuelo”...	Todos
Parada de emergencia	Es uno de los comandos, no es problema, pero puede provocar un DoS (Denegación de Servicio).	Todos
Recodificación de los códigos	En “CHAINA, CHAIWAN, etc...” se pueden comprar, sin identificación alguna, mandos de “repuesto” aparejados.	Todos
Modificación del firmware	Lo que funciona “no lo toques”...	Todos

Análisis: vulnerabilidades de seguridad y remediación

Vulnerabilidad	Descripción	Solución
Sin Códigos Rolling	Cada paquete contiene todo y no hay ningún secreto dinámico, por lo que son válidos	iLOG Key
Ausencia de criptografía o muy débil	Los datos viajan sin cifrar o simplemente están ofuscados o son predecibles	HMAC o similares
Ausencia de protección en el software	El SW para actualizar y el propio firmware carecen de protecciones	Tampers y firmas criptográficas

Análisis: CVEs

CVE-2018-17921 Detail

MODIFIED	MODIFIED	MODIFIED
This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.	This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.	This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

All versions of Hetronic SAGA1-L8B with any firmware versions prior to A0.10 are vulnerable to an attack that may allow an attacker to force-pair the device without human interaction.

Metrics	Metrics	Metrics
NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.	NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.	NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.
CVSS 3.x Severity and Vector Strings:	CVSS 3.x Severity and Vector Strings:	CVSS 3.x Severity and Vector Strings:
NIST: NVD	Base Score: 8.8 HIGH	Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

QUICK INFO

CVE Dictionary Entry:

[CVE-2018-17921](#)

NVD Published Date:

10/24/2018

NVD Last Modified:

11/20/2024

Source:

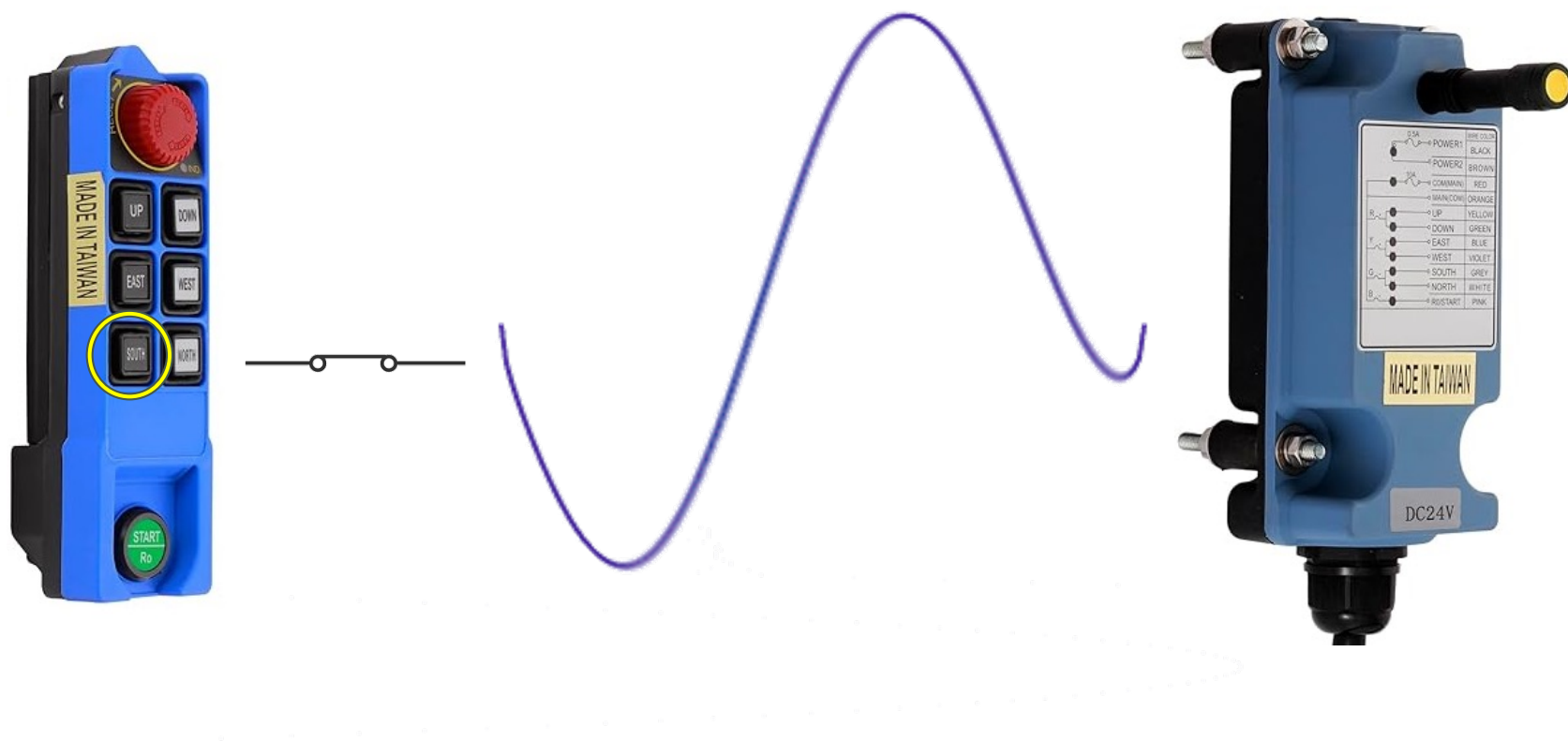
ICS-CERT



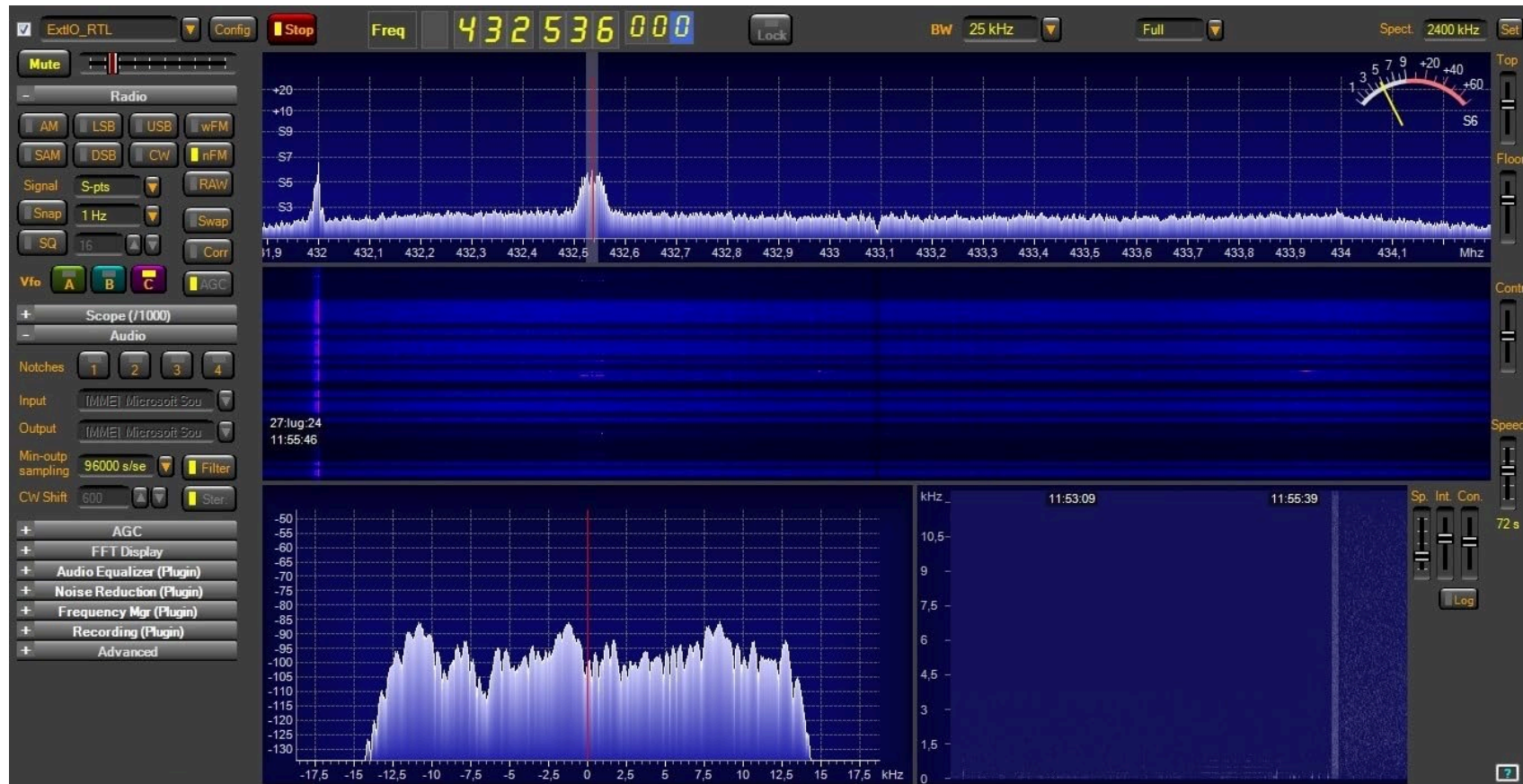
HACKING CRANES MAMA

LEVEL 04: ATACANDO LA INFRA

Análisis de la señal (RF reversing)



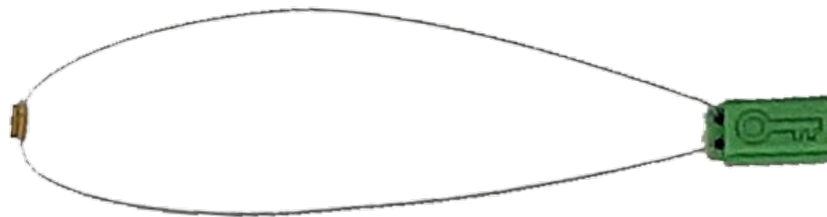
Recepción de la señal con un SDR



Ataque de repetición (replay)

- **Grabar la señal inicial** (de arranque), para su análisis. Si se graba mal, tocará **esperar al día siguiente**, ya que se abre la obra, se señaliza y se transmite...

Nota: consultad a los abuelos *cuál es la mejor hora* para hacerlo...



<https://telecraneshop.com/product/set-of-n-3-magnetic-start-keys-for-telecrane-f21-2s-transmitter-unit/>

- **Grabar otras señales** (los “Rolling Codes” son los padres) y **reinyectarlas** como si no hubiera un mañana...

Análisis de la señal (RF reversing)

Documentación técnica:

- FCC: <https://fcc.report/FCC-ID/NCTSAGA1-L8/273419>
- Banda frecuencias: 433.050 - 434.7875 MHz
- Separación de canales: 25 kHz
- Modulación: FSK
- Longitud del código ID: 2^{20}
- Empleo de seguridad: Hamming code

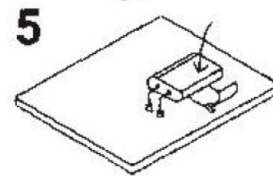
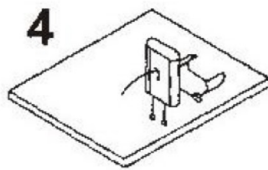
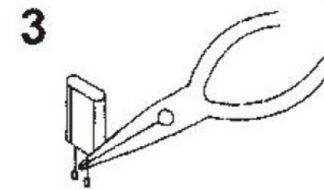
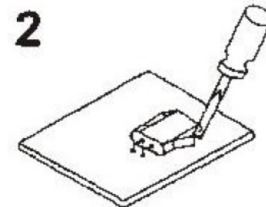
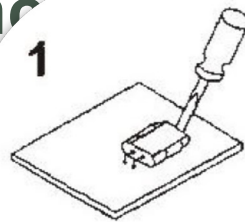
Realidad:

- Longitud del código ID: 2^{24}
- Empleo de seguridad: ***Hamming code***

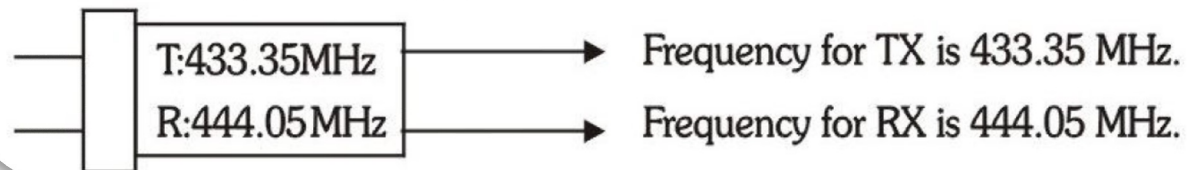
Análisis de la señal (RF reversing)

Frecuencia

- No
- ma
- Se
- Se
- cri



Note: The frequency will be different when plugging the same quartz unit into TX or RX, for example,



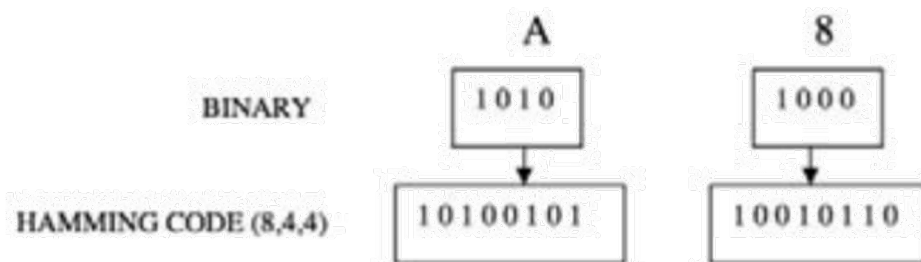
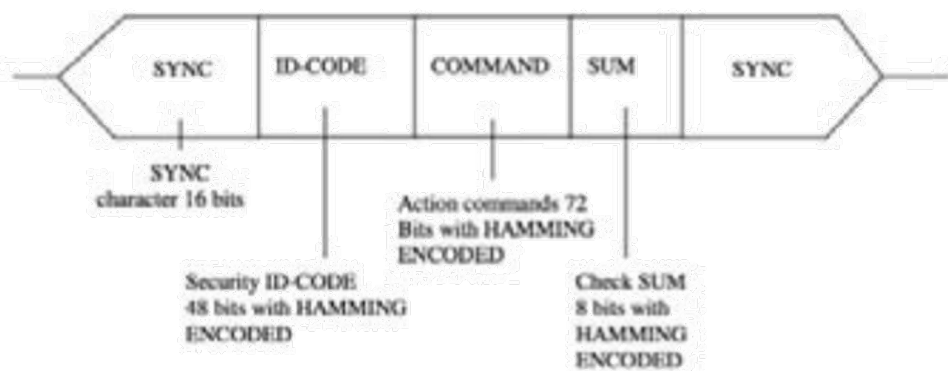
ero tiene

lador de

Análisis de la señal (RF reversing)

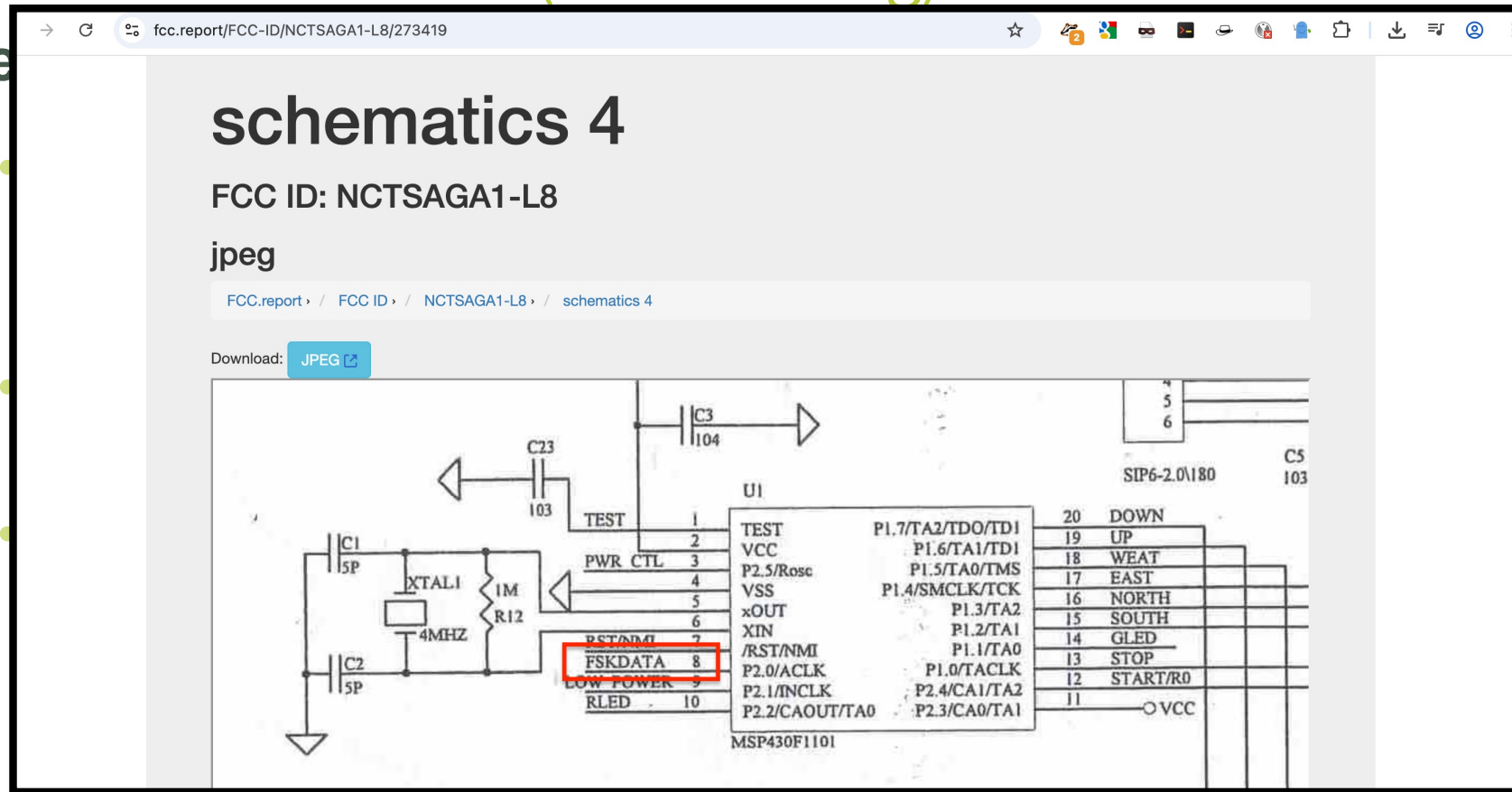
Modulación:

- **2-FSK** con la documentación FCC de 315 (pero tiene marcado CE)
- Estructura de paquete y codificación (Doc. Técnica SAGA)



Análisis de la señal (RF reversing)

Ele



no
que

8

Análisis de la señal (RF reversing)

Análisis de muestras:

- **Sonda lógica** y como no usa el hamming, en la documentación de FCC se observa “***codificación Manchester***”, vuelve una clásica recurrente.
- **Ratio de muestreo:** 2 Mbps
- **Longitud de bit:** 240 muestras.

Resultados:

- **Velocidad de transferencia:** 8,333 bps (bits por segundo)

Análisis de la señal (RF reversing)

- **Patrón recurrente:** 224 bits.
- **Decodificación Manchester** de cada paquete: 72 bits de secuencia:

```
000 1111 0000 0101 0101 0101 0101 0000 0010 0111 0100 0001 0110 0011 0100 0100 0011 0110 0
```

- Con otros mandos, se prueba y se “identifica” el posible paquete, ya que ***coinciden en muchos bytes excepto en 3.***

Análisis de la señal (RF reversing)

- **Diferencias entre mandos:**

0F 55 55 50 27 41 | xx xx xx | COMANDO | Checksum

0F 55 55 50 27 41 | yy yy yy | COMANDO | Checksum

- **Cambian** también los **COMANDOS**. Es decir, si se pulsa un botón sale AAAAAA y otro botónBBBBBB, pero en **varios mandos son los mismos**.
- Se procede botón a botón para ***analizar qué transmiten***.

Análisis de la señal (RF reversing)

Botón	Envía Mando #1	Checksum M1	Envía Mando #2	Checksum M2
Reset (EMO)	55 50 50	11	55 50 50	11
START	55 55 41	14	55 55 41	14
Arriba	66 55 50	36	66 55 50	36
Abajo	27 55 50	77	27 55 50	77
Este	50 55 50	11	50 55 50	11
Oeste	44 55 50	14	44 55 50	14
Sur	55 66 50	36	55 66 50	36
Norte	55 27 50	77	55 27 50	77
End of Packet (EOP)	55 55 50	05	55 55 50	05

Análisis de la señal (RF reversing)

Además, siempre se obtiene el mismo checksum

- El comando son 3 bytes. **El checksum es fijo (*no cambia en ambos mandos*)**.
- **No hace falta reversing.** Conocido el preámbulo y el ID de un paquete, se puede construir con el ID de emparejamiento.

Ataque de emparejamiento

SYNC from an original Transmitter to a NEW transmitter

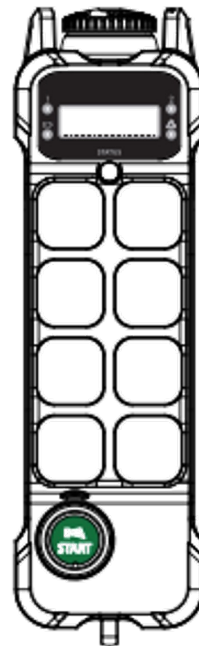
Step1

1. Turn both transmitters "OFF" by pushing the EMO button.

Step2

1. Press **A** once then press **B** once vice versa for 4 times. The Status LED blinks green and red.
Press **1** until (> 5 secs) the "1" and "2" LED blinks faster, release the button.

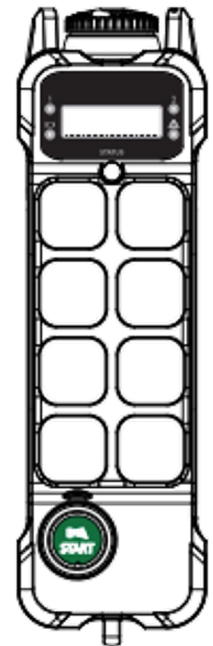
Ps. Keep distance more than 50cm while doing the "copy"



Original

Step3

1. Press **A** once then press **B** once vice versa 4 times. The Status LED blinks green and red.
Press **2** until (> 5 secs) the "1" and "2" LED stay ON, then release the button. DONE!



NEW copy

Ataque de emparejamiento

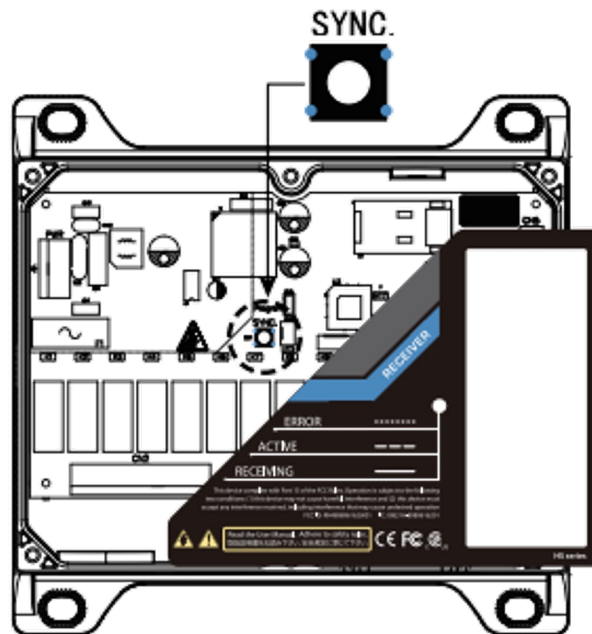
SYNC from a Receiver to a NEW Transmitter

Step1

Power the receiver.
Press the SYNC.
button >3 secs.
The STATUS blinks .

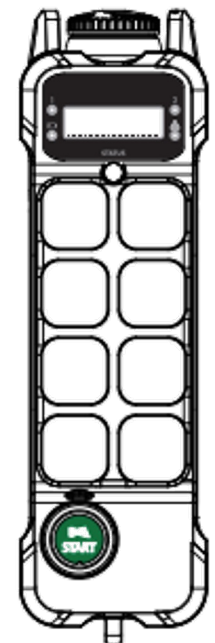


Warning against
electrical voltage



Step2

1. push the EMO button.
2. Press **A** once then press
B once vice versa for 4
times. The Status LED blinks
green and red.
Press **2**
until (> 5 secs) the "1" and
"2" LED stay ON, then release
the button. DONE!



Ps. Keep distance more than 50cm
while doing the "copy"

NEW copy

Ataque de emparejamiento

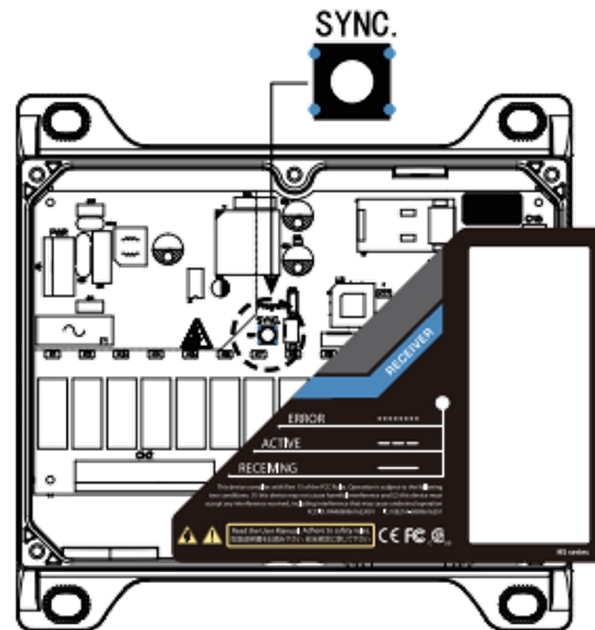
SYNC from a Transmitter to a NEW Receiver

Step1

Power the receiver.
Press the SYNC.
button >3 secs.
The STATUS blinks.



Warning against
electrical voltage

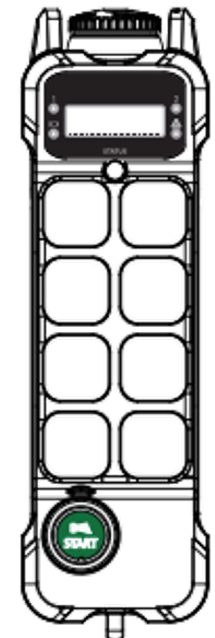


NEW copy

Step2

1. push the EMO button.
2. Press **A** once then press **B** once vice versa for 4 times. The Status LED blinks green and red.
Press **1**

until (> 5 secs) the "1" and
"2" LED stay ON, then release
the button. DONE!



Ps. Keep distance more than 50cm
while doing the "copy"

Ataque de emparejamiento

1-34. "Model": Display model number after reading the data.

Model : F21-4D

1-35. "ID Code": Display ID Code after reading the data which is an unique code for each Remote Control, both transmitter and receiver won't work if they have different ID codes.

ID-Code: CA040663



Ataque de **emparejamiento**

¿Abrir el receptor y pulsar un botón? Qué **pereza...** somos **juanquers...**

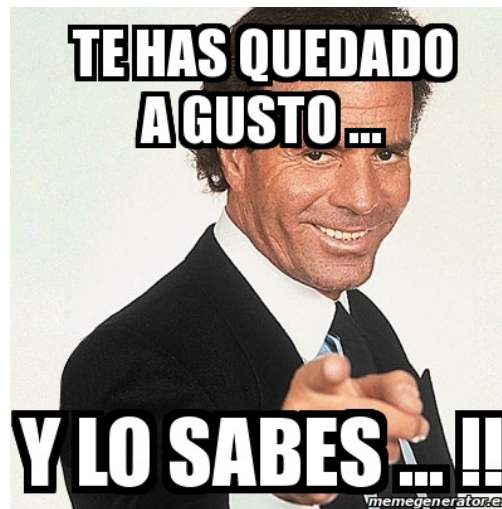
SAGAMATIC Co., Ltd (SAGA)

- El mando **original** “*se borra*” y queda el “ilegítimo” (**DoS**).
- No es necesario abrirlo, se trata de un **comando de “emparejamiento”**.
- Basta con capturar una trama y **cambiar el Fixed Code** (único “*secreto compartido*”) entre ambos.

Ataque de emparejamiento

Transmitir una trama con “el nuevo mando”:

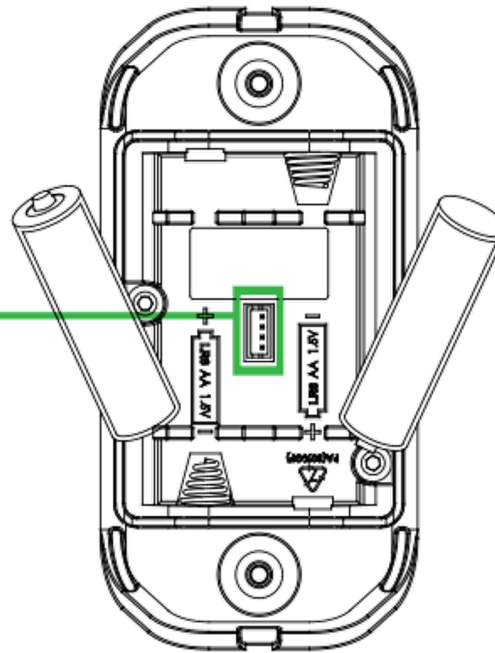
Preámbulo	Sync	ID Dispositivo	Comando (Emparejar)	CRC	Sync
0xF0	0x055550	0xAB1337DEAD	0x555050	0x11	0x0F



Interface de programación

Program the transmitters

1. Remove the battery cover
 2. Remove both batteries.
- The programming connector is placed behind the battery



Telecrane y SAGA emplean el mismo dongle

Interface de programación

F24 SETUP PROGRAM V4.00M(09/01/2005) 01-12-2009 11:36:51

File Tools About

Settaggio delle funzioni User-Information

R/C INFORMATION

Numero di seri: 24025713

Model: F24 Tx-Date: 2008/5/19

ID-Code: 24025713 Rx-Date: 2008/5/19

R/C FUNCTION

ID-Code Remote Setting: Disable

Power On Mode: Start-Pushbutton / Key

RECEIVER FUNCTION

Passive Act: Power-Off

Auto Off (RX): 1 hour

START KEY FUNCTION

Normal

TRANSMITTER FUNCTION

Transmit Mode: Continuous

Powersaving: Disable

Save-Power: 5 min

Auto Off (TX): Enable

Led-On/Off: On

Led-Off-Time: 1.0 sec

COM PORT: COM7

Up Down Normal Acc. ritardo 0.0 sec

Mode 1 Interlock InterlockDelay 0.0 sec

East West Normal Acc. ritardo 0.0 sec

Mode 1 Interlock InterlockDelay 0.0 sec

South North Normal Acc. ritardo 0.0 sec

Mode 1 Interlock InterlockDelay 0.0 sec

R1 R2 Normal Acc. ritardo 0.0 sec

Mode 1 Interlock InterlockDelay 0.0 sec

R3 R4 Normal Acc. ritardo 0.0 sec

Mode 1 Interlock InterlockDelay 0.0 sec

0% READ R/C WRITE R/C





HACKING CRANES MAMA

LEVEL 05: MODE ON

demo





HACKING CRANES MAMA

LEVEL 06: CONCLUSIONES

Recomendaciones

- Implementación de **Rolling-Codes**.
- **Actualización del firmware** para los “*abuelos*” existentes.
- Incluir de **actualizaciones OTA** (Over-the-Air)
- Considerar **cifrado por hardware** (CC1110Fx/CC1111Fx).
- Emplear **claves distribuidas**.
- Usar mecanismos de **tampering** para evitar ingeniería inversa y borrado masivo si es abierto el dispositivo.
- Emplear **canales separados** para proteger el firmware (RS-232) u otros circuitos dedicados.

Conclusiones

- Algunos juguetes de radiocontrol **son más seguros...**
- Pero no manejan cargas pesadas ni ponen en juego la **seguridad de las personas...**



¿Preguntas?



ESKERRIK ASKO



© 2025 CS³ GROUP. Todos los derechos reservados.

Todas las demás marcas comerciales, productos, servicios, logotipos, imágenes, etc. referenciados aquí son propiedad de sus respectivos dueños. La información presentada es exclusivamente con propósitos informativos y únicamente expresa la opinión del autor en el momento de su publicación. CS³ GROUP no puede garantizar la veracidad y licitud del contenido o información aquí presentada. CS³ GROUP ofrece TODO EL MATERIAL Y EL CONTENIDO DE ESTA PRESENTACION "COMO ESTÁ", SIN NINGUNA GARANTÍA EXPRESA O TÁCITA DE NINGÚN TIPO, INCLUYÉNDOSE SIN LIMITACIÓN LAS GARANTÍAS DE QUE EL PRODUCTO O SERVICIO SEA COMERCIALIZABLE, NO INFRACTORA DE LA PROPIEDAD INTELECTUAL DE NADIE, O IDÓNEA PARA UN DETERMINADO PROPÓSITO. CS³ GROUP NO TIENE NINGUNA OBLIGACIÓN DE PAGAR INDEMNIZACIÓN POR DAÑOS Y PERJUICIOS DE NINGÚN TIPO (INCLUYENDO, ENTRE OTRAS, LA PÉRDIDA DE GANANCIAS, PÉRDIDA DE EXPLOTACIÓN, PÉRDIDA DE INFORMACIONES) PRODUCIDOS POR EL USO O POR LA INCAPACIDAD DE USAR EL MATERIAL Y/O INFORMACION AQUÍ PRESENTADA.