# EuskalHack Security Congress IX

## Sistemas inalámbricos industriales: cerrando la brecha entre aspectos técnicos y regulatorios

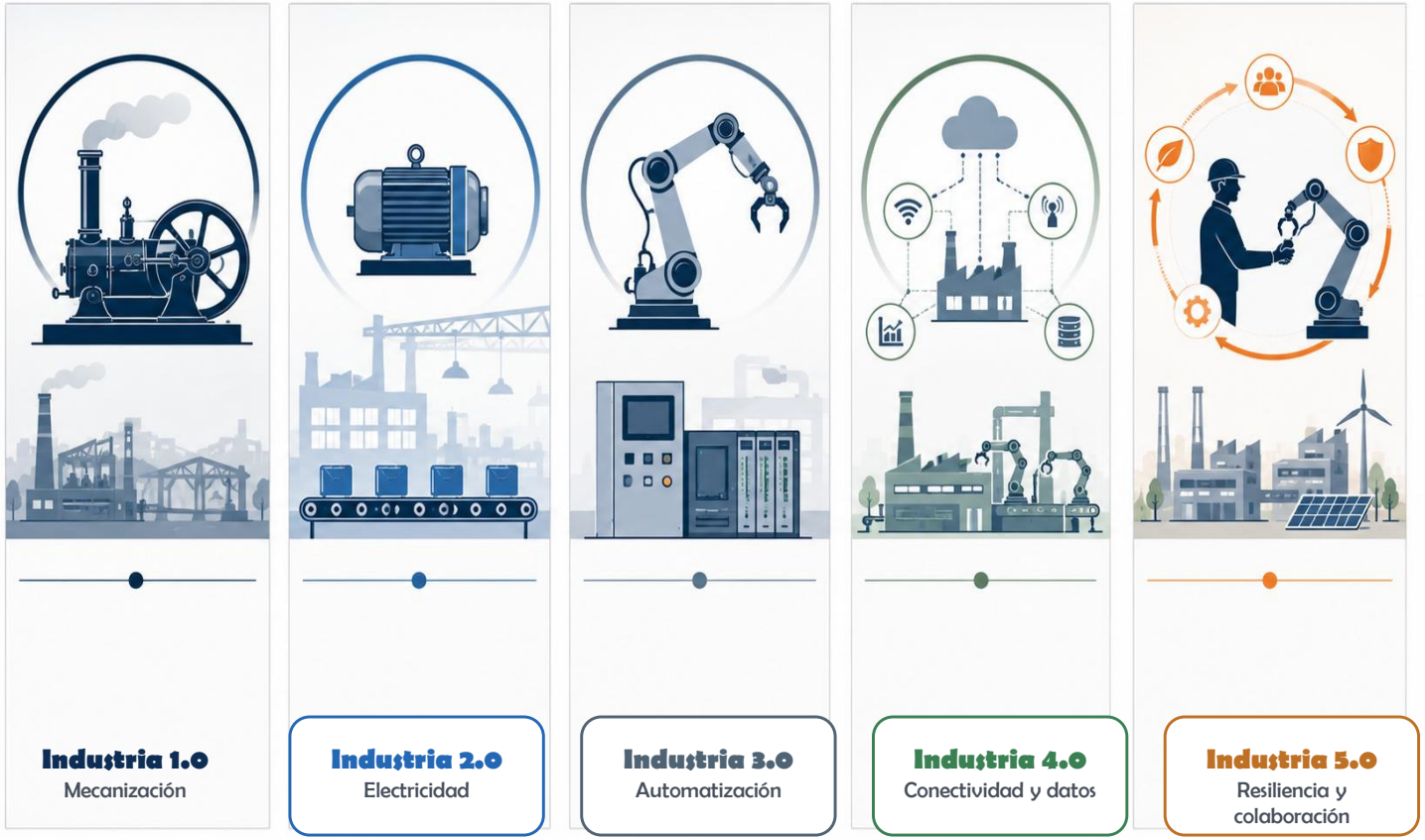

**Lorenzo Fanari, Ph.D**

## Me presento...


Lorenzo Fanari
Academic & Professional Journey
BILBAO
3 UPV/EHU – Bilbao
PhD
Industrial Wireless
Industry 4.0
6 EUNEIZ
Lecturer &
Researcher
Vitoria-Gasteiz
BASQUE COUNTRY
VITORIA-GASTEIZ
5 Alias Robotics
Technical Project
Manager
Vitoria-Gasteiz
SPAIN
4 UMH – Elche
Postdoc
Industry 4.0 Wireless
ELCHE
N
ITALY
2 Cagliari –
University of Cagliari
MSc in
Telecommunication
Engineering
SARDINIA
1 Cagliari –
University of Cagliari
BSc in Electrical &
Electronic Engineering
CAGLIARI
From Cagliari, Italy to Vitoria-Gasteiz, Spain

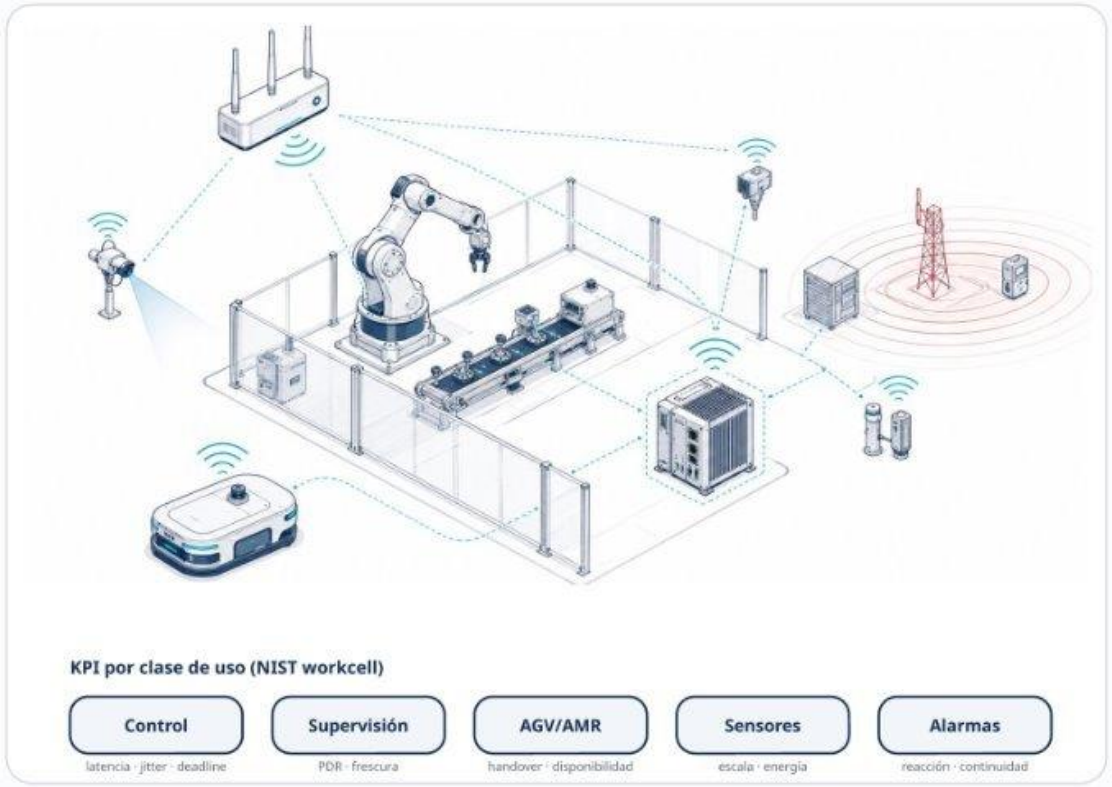
## De la industria 1.0 a la 5.0

- 1.0: mecanización industrial.
- 2.0: electricidad y producción masiva.
- 3.0: automatización y control.
- 4.0: conectividad, datos e IIoT.
- 5.0: resiliencia y colaboración humano-máquina.



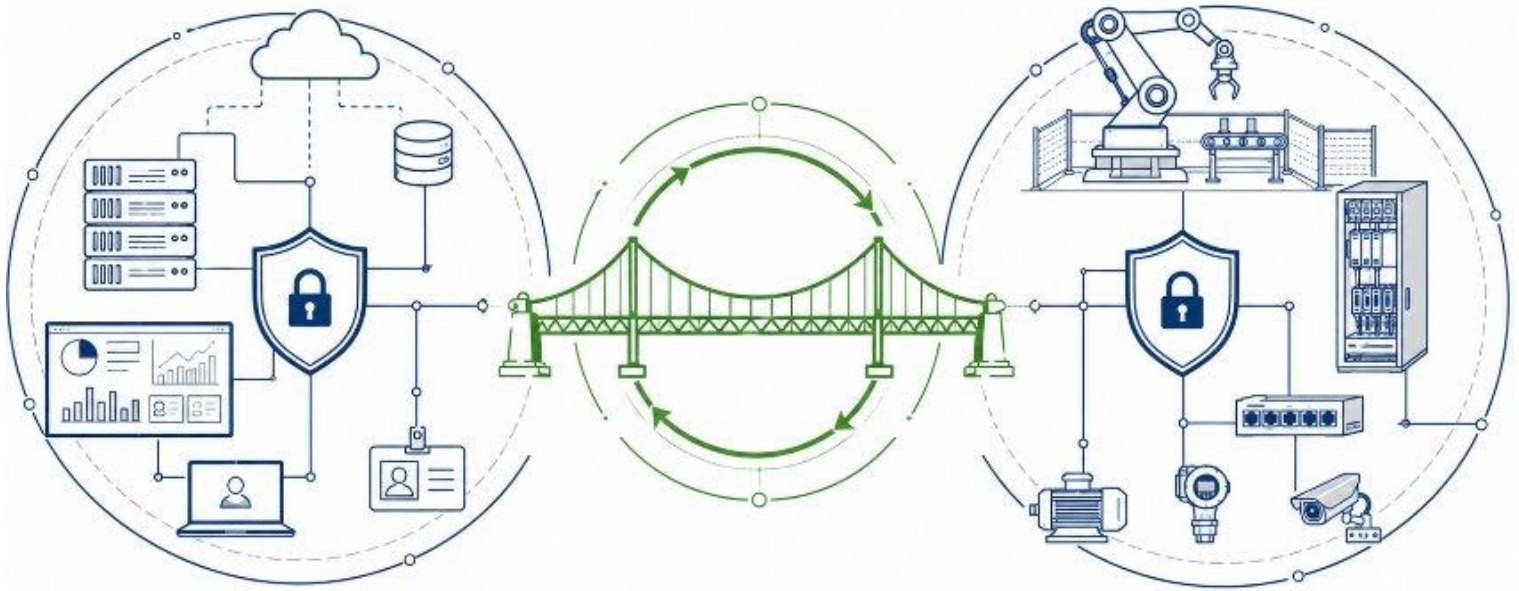
## Novedades tecnológicas 4.0 / 5.0:

- IIoT y sensorización masiva.
- Edge, cloud y gemelos digitales.
- IA y analítica industrial.
- Robots móviles y colaboración.
- Topologías más dinámicas.
- Comunicaciones en Soft y Hard Real-Time:
  - **Dimension de los datos tipicamente en la orden 128 bit-512 bit**
  - Latencias inferiores a los 10ms
  - Tasa de errores hasta 10-9



## De ciberseguridad IT a OT

- IT protege datos y servicios.
- OT protege proceso y continuidad.



En OT, la ciberseguridad afecta directamente a la operación.

# Potencial Amenaza: Dispositivos baratos para operaciones en RF


Flipper Zero — Dispositivo Multiuso Open Source y Personalizable para Geeks, con Lector RFID/NFC, Infrarrojos y exploración de señales inalámbricas, Blanco (Flipper Zero)

Marca: Flipper

4,6 ★★★★½ (1.920)

-4 % 219⁰⁰ €

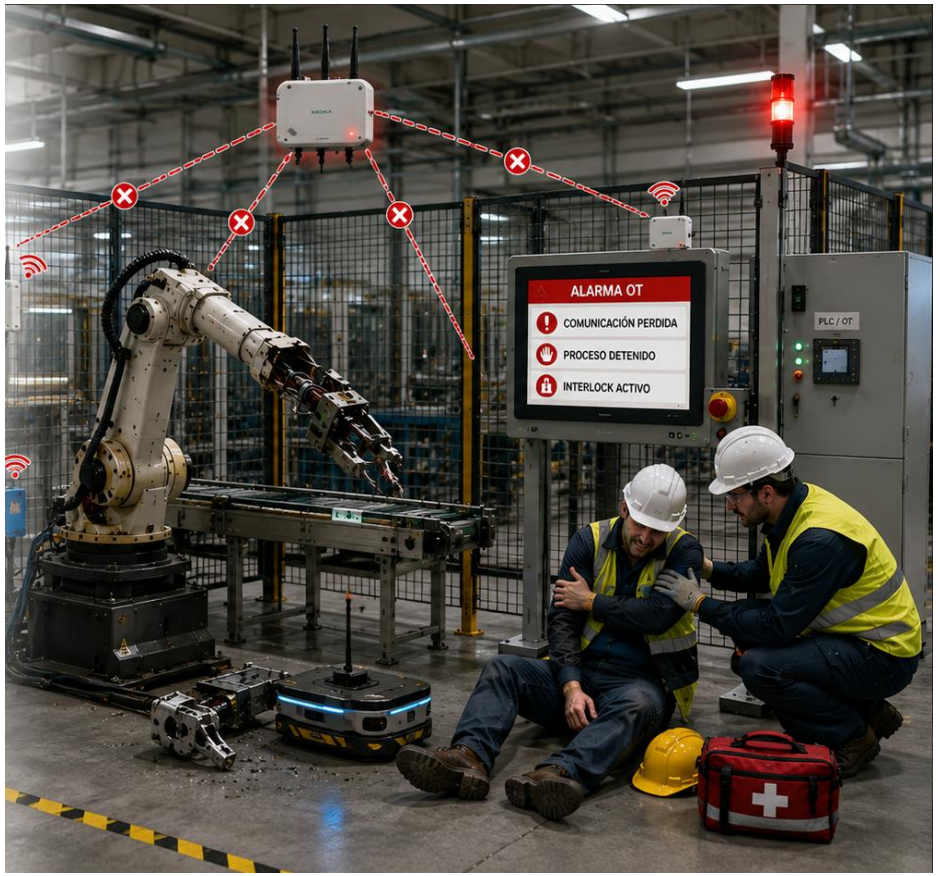
Precio recomendado: ~~229,00€~~

**Financia este producto en 4 cuotas/90 días con Paga en 4 de Cofidis Ver más**

Devoluciones GRATIS

Los precios de los productos vendidos en Amazon incluyen el IVA. Dependiendo de tu dirección de entrega, el IVA puede variar al finalizar la compra. Para obtener más información, haz clic aqui.
Disponible a un precio más bajo en otros vendedores que tal vez no ofrezcan envío de Amazon Prime gratis.

## … Potenciales Riesgos



Europa / ENISA · DDoS / ENISA · España / INCIBE · Euskadi

# De ciberseguridad IT a OT: Tendencias de ciberataques industriales

- Europa: DDoS domina incidentes reportados.
- España: más de 97.000 incidentes gestionados.
- Euskadi: ataques crecen un 48%.
- La disponibilidad se vuelve crítica.

**4.875**
incidentes analizados
(jul. 2024–jun. 2025)

**76,7%**
de incidentes reportados
son DDoS

**97.348**
incidentes gestionados
(+16,6% vs 2023)

**+48%**
ciberataques en dos años
(contexto regional)

## Impacto en disponibilidad industrial

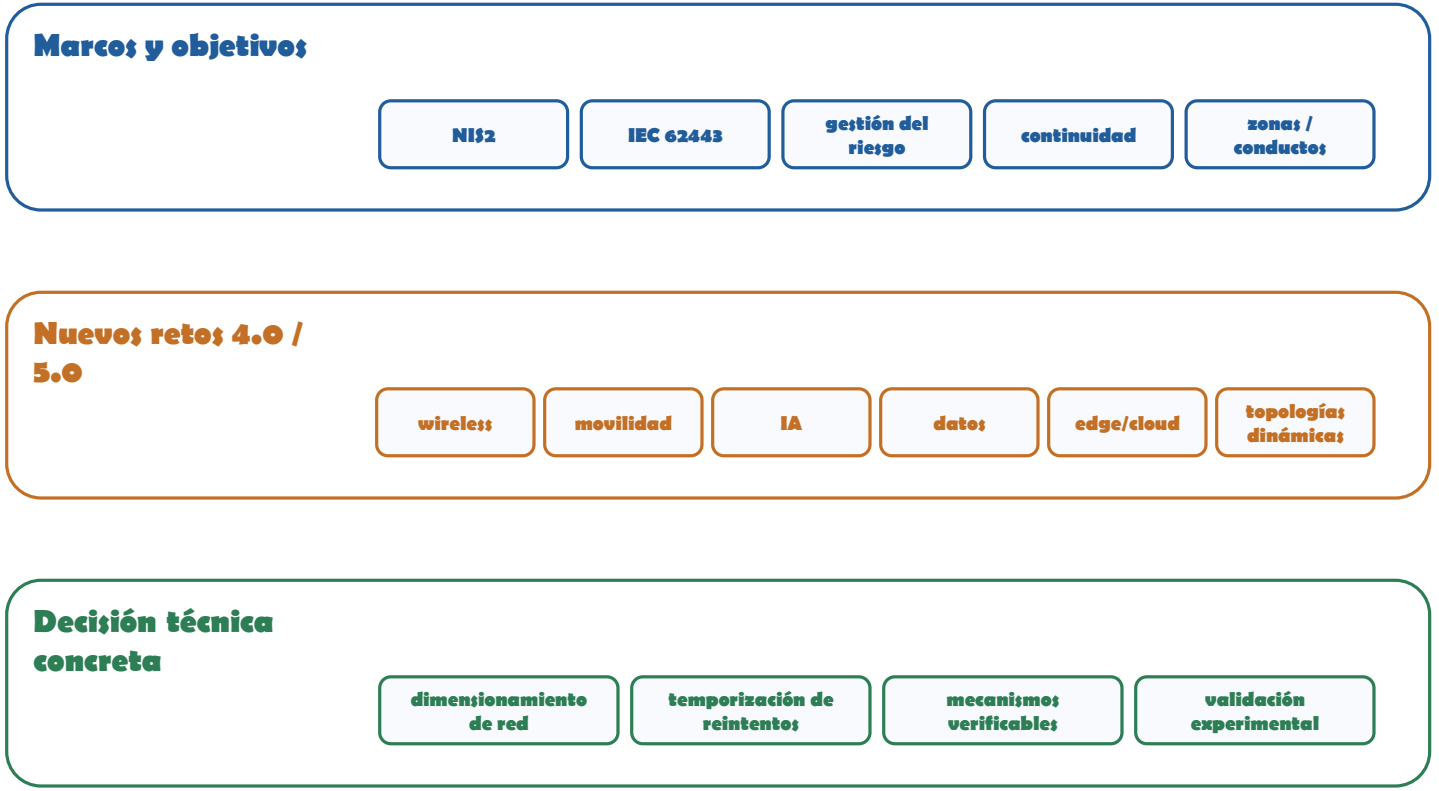
disponibilidad · continuidad · acceso remoto · convergencia IT/OT · datos e IA

**DDoS = disponibilidad en red • jamming = disponibilidad en radio**
**No son lo mismo, pero apuntan al mismo objetivo: continuidad.**

Las cifras orientan riesgo, no comparan territorios.

# NIS2, IEC 62443 y brecha técnica

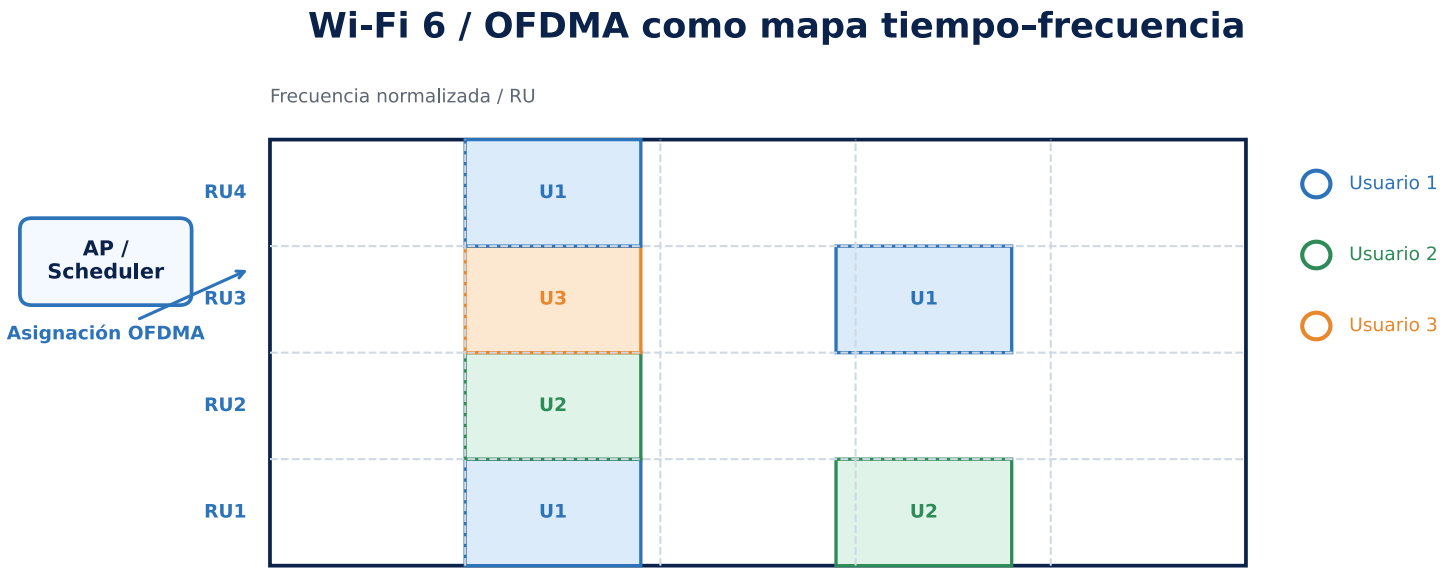
- NIS2 fija gobernanza y gestión del riesgo.
- IEC 62443 estructura seguridad OT/IACS.
- 4.0/5.0 añade wireless, IA y movilidad.
- Falta traducir objetivos en diseño verificable.




La brecha no es ausencia de normas: es traducir objetivos en decisiones técnicas verificables.

# Tecnología de análisis: Wi-Fi 6 / OFDMA

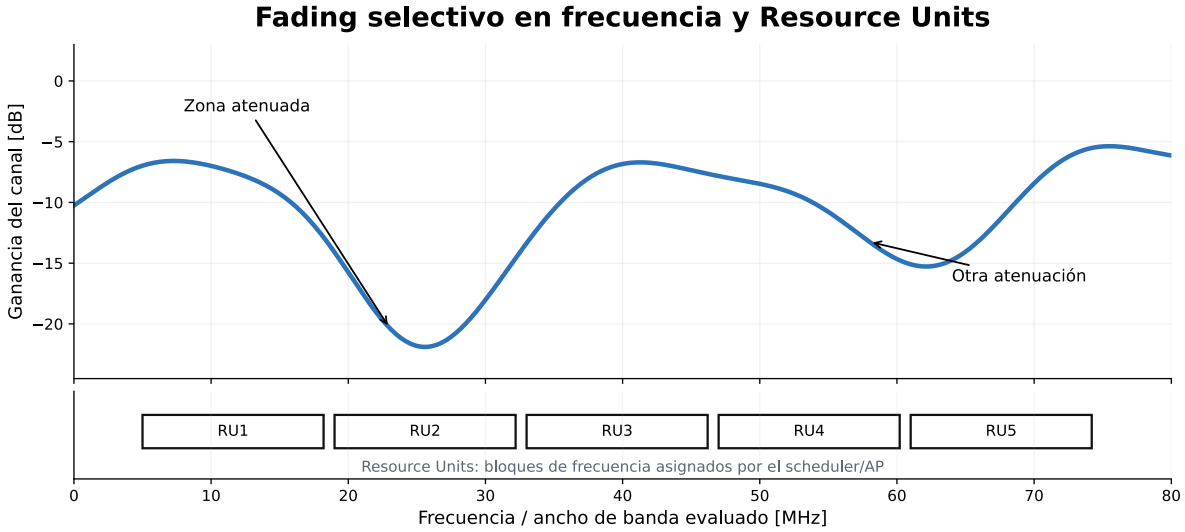
- El AP coordina usuarios.
- OFDMA reparte Resource Units.
  - Eficiente para real-time
- Cada usuario ocupa RUs asignados.
- El scheduler decide el reintento.

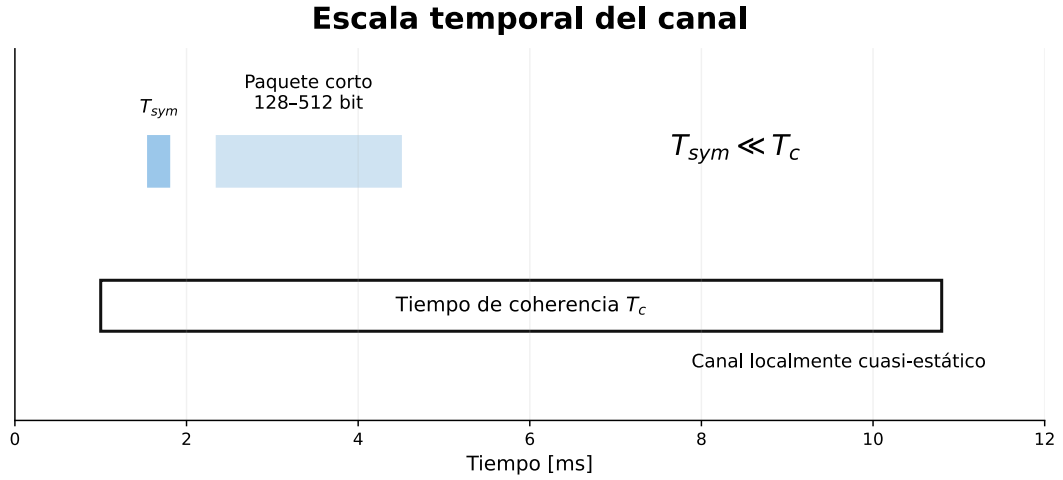



El AP decide qué RU asignar y cuándo reintentar.

# Fenómeno físico de interés

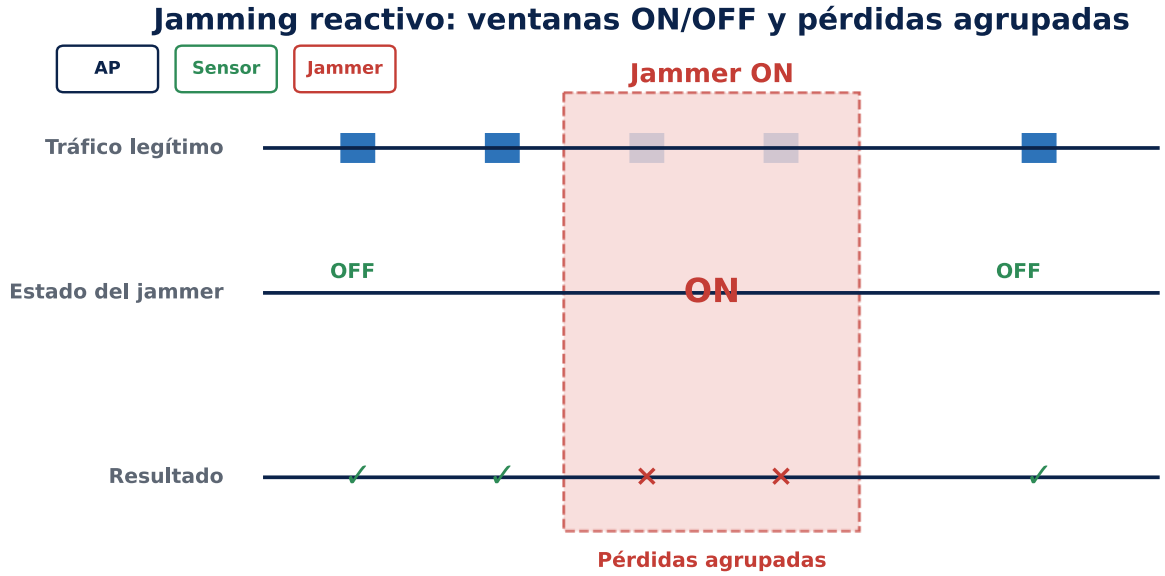
- Paquetes cortos: 128–512 bit.
- T_sym mucho menor que T_c.
- Canal localmente cuasi-estático.
- Fading selectivo en frecuencia.
- Jammer fija la ventana crítica.



# Riesgo potencial: jamming Reactivo

- Detecta tráfico legítimo.
- Activa interferencia ON/OFF.
- Agrupa pérdidas de paquetes.
- Afecta reintentos y deadlines.

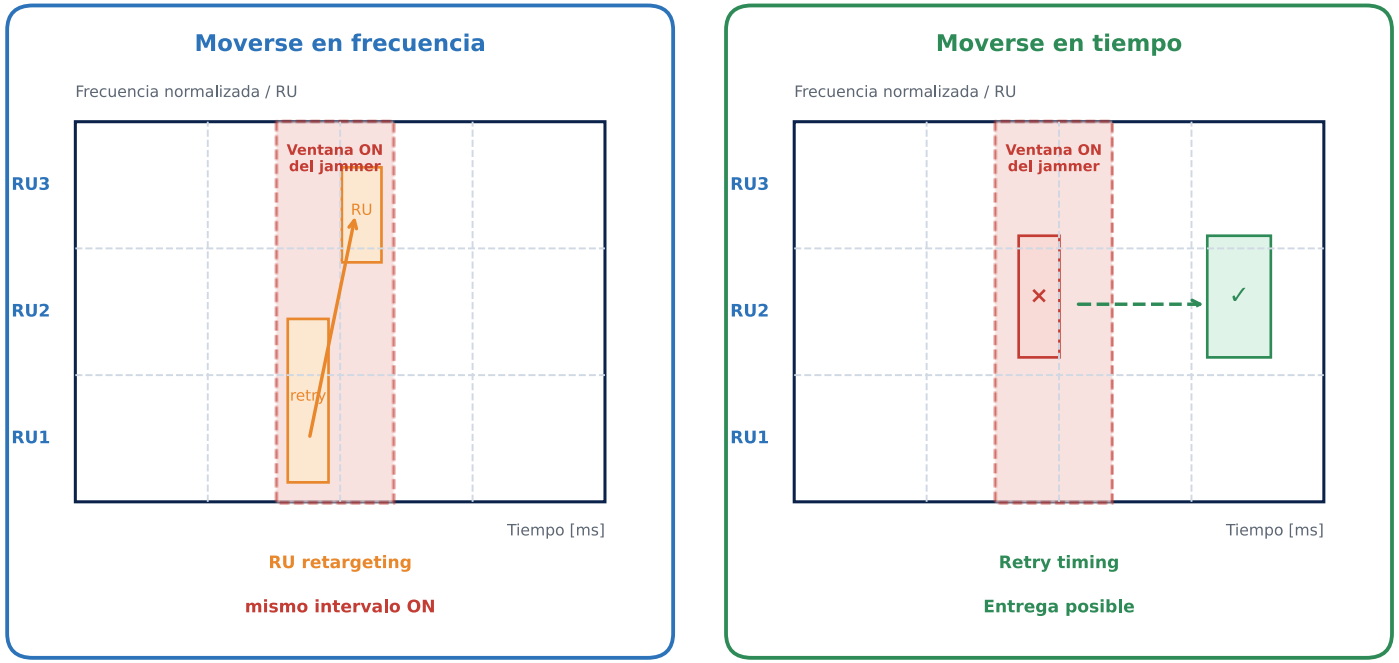



El jamming reactivo crea ventanas temporales de pérdida.

# Tiempo frente a frecuencia

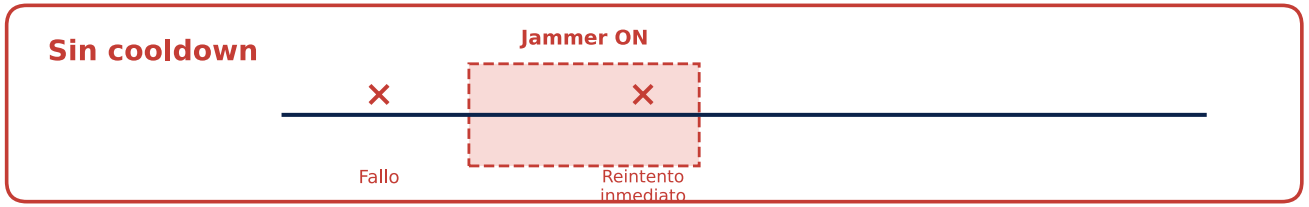
- OFDMA ofrece recursos múltiples.
- Cambiar RU puede ayudar.
- El patrón ON/OFF domina aquí.
- El retry debe evitar ráfagas.
- La interpretación sólida es temporal.

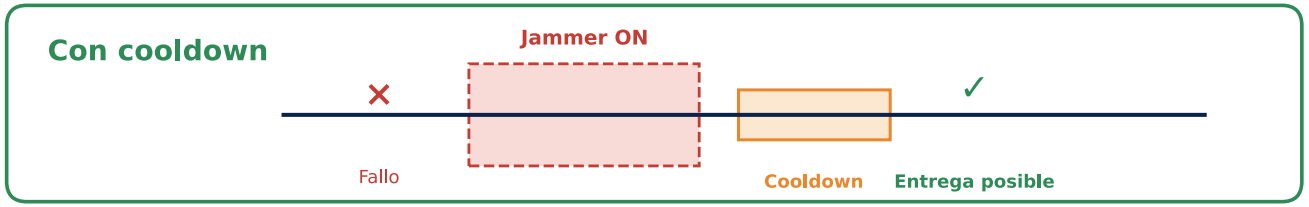
## Mecanismo en el plano tiempo-frecuencia




No se descarta la frecuencia: aquí domina la temporización del reintento.

# Potencial solución: Cooldown




### Formulación simple

$$t_{retry} = t_{fallo} + T_{cd}$$

$$T_{cd} \geq T_{ON,residuo} + \varepsilon$$

pero $T_{cd} \leq D - t_{elapsed} - T_{tx}$

Elegir $T_{cd}$ = salir del jammer sin romper el deadline.

No garantiza entrega; reduce exposición repetida a la misma ventana activa.

### Regla de diseño

$T_{cd}$ demasiado corto → el retry cae en ON

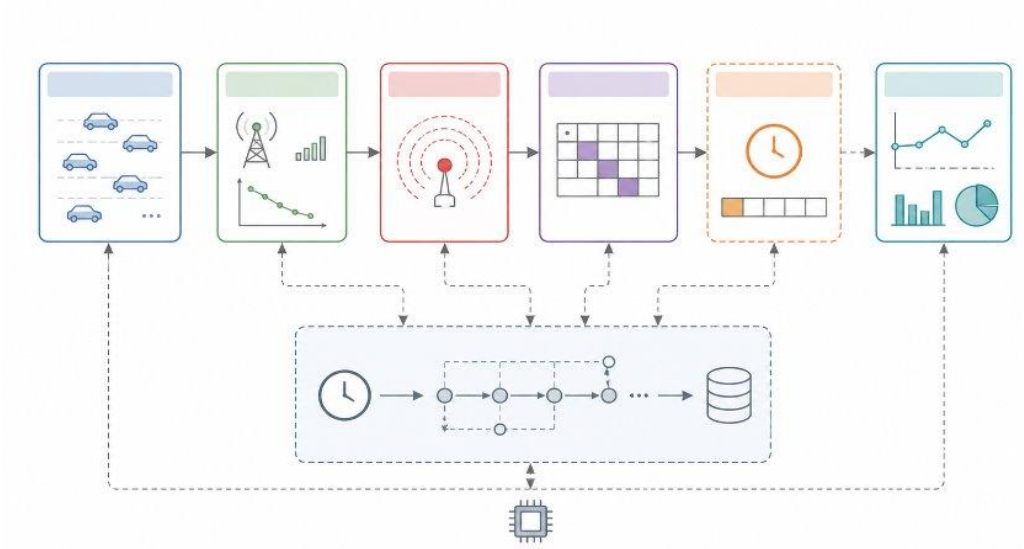
$T_{cd}$ demasiado largo → aumenta la latencia

$T_{cd}$ adecuado → reintento en ventana más favorable

El cooldown cambia el cuándo del reintento, no elimina el ataque.

## Cómo se simuló: arquitectura

- ns-3 core harness, link: https://github.com/Lorenzofanari/scheduler-ieee-802.11.
- Tráfico, canal y jammer.
- Comparacion entre cooldown y sin cooldown
- Escenarios simulados: 18
  - MCS
  - Dimension Datos
  - Users



# Resultados del Estudio

- Benchmark: Baseline-PF.
- Comparación: cooldown-only.
- Pérdidas casi eliminadas.
- Coste temporal visible.
- Evidencia scheduler-level.
- El cooldown reduce pérdidas bajo jamming controlado, con coste temporal **aceptable**

**Broadband reactive — por 10.000 intentos equivalentes**

**Benchmark Sin Cooldown**

Baseline-PF

**2,467**

pérdidas estimadas

PLR = 24.672 %

p95 = 0.090 ms

**paquetes salvados ≈ 2,467**

**Cooldown-only**

reintento diferido

**0.22**

pérdidas estimadas

PLR = 0.00222 %

p95 = 5.014 ms

**reducción relativa de pérdidas = ((x - y) / x) × 100 ≈ 99.991 %**

La mejora de pérdidas tiene un coste temporal: p95 pasa de 0.090 ms a 5.014 ms.

# Conclusiones

- Industria 4.0/5.0 aumenta la dependencia digital y la complejidad del diseño de soluciones capaces de garantizar una automatización completa.
- Los ciberataques en la industria están creciendo.
- NIS2 e IEC 62443 orientan, pero falta una traducción técnica medible.
    - Cooldown es un ejemplo concreto.


# ¡MUCHAS GRACIAS!

# ESKERRIK ASKO!

**Lorenzo Fanari, Ph.D**
Lorenzo.fanari@euneiz.com