WHERE TECHNOLOGY IS AN ATTITUDE

Universidad de Cantabria

ikerlan

MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

ÍNDICE GENERAL

01.
QUIÉNES SOMOS

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

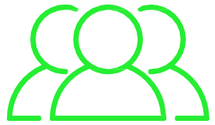
CENTRO TECNOLÓGICO

IKERLAN.
LA TECNOLOGÍA ,
NUESTRA ACTITUD

Comprometidos en desarrollar la tecnología que necesitan las empresas para transformar permanentemente sus productos y servicios.

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

IKERLAN EN CIFRAS (2020)



360
PERSONAS

PREPARADAS PARA RETOS TECNOLÓGICOS PRESENTES Y FUTUROS

23,8 M€
INGRESOS TOTALES EN 2020

- **10,8 M€** EN TRANSFERENCIA TECNOLÓGICA A EMPRESAS (más del 54 % de la facturación)
- **12,3 M€** EN PROYECTOS DE INVESTIGACIÓN EN 2019 (DFG, GV, AGE y H2020)
- **0,7 M€** OTROS INGRESOS

Sectores

- 47 % BIENES DE EQUIPO
- 18 % TRANSPORTE
- 22 % ENERGÍA
- 13 % OTROS

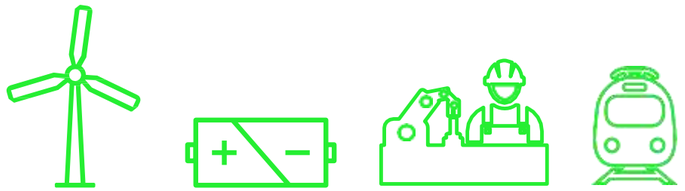
02.
NUESTRA DIFERENCIA EN 4 CLAVES

1.ª
TECNOLOGÍA ÚTIL
CUARENTA Y CINCO AÑOS
TRANSFIRIENDO TECNOLOGÍA
A LA INDUSTRIA

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

1.ª
TECNOLOGÍA ÚTIL.
CUARENTA AÑOS TRANSFIRIENDO
TECNOLOGÍA A LA INDUSTRIA.

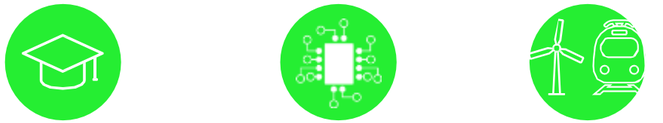
TECNOLOGÍA REAL PARA RETOS REALES



COLABORAMOS CON LAS EMPRESAS EN EL
DESARROLLO DE PRODUCTOS QUE UTILIZAS CADA DÍA.

TECNOLOGÍA Y PERSONAS: LA CLAVE DE NUESTRO ÉXITO.

TECNOLOGÍA



UNIVERSIDAD — IKERLAN — EMPRESAS

PERSONAS

EDUCACIÓN SUPERIOR — ESPECIALIZACIÓN TECNOLÓGICA — INDUSTRIA

2.ª

JUNTOS, ES MEJOR.
MODELO ORGANIZATIVO COOPERATIVO:
COMPROMISO Y EFICIENCIA

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

2.ª
JUNTOS, ES MEJOR.
MODELO ORGANIZATIVO COOPERATIVO:
COMPROMISO Y EFICIENCIA

TRABAJAMOS EN COOPERACIÓN

COOPERAMOS CON NUESTROS CLIENTES

- COLABORAMOS EN LA DEFINICIÓN ESTRATÉGICA.
- EQUIPOS DE TRABAJO CONJUNTOS.
- CAPTACIÓN Y DESARROLLO DE TALENTO.
- OFRECEMOS SOLUCIONES MULTITECNOLÓGICAS.

SOMOS UNA COOPERATIVA, CREADA EN 1974 POR LAS EMPRESAS DE LA ACTUAL CORPORACIÓN MONDRAGON

HUMANITY AT WORK MONDRAGON

MIEMBRO DE BASQUE RESEARCH & TECHNOLOGY ALLIANCE Y DE LA RVCTI

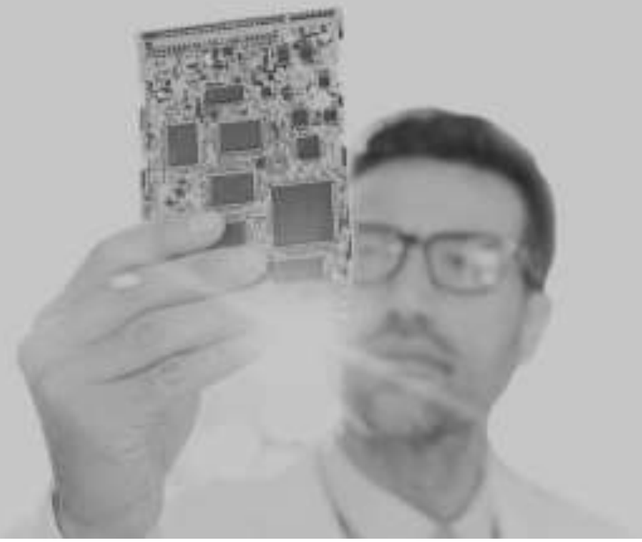
BRTA BASQUE RESEARCH & TECHNOLOGY ALLIANCE

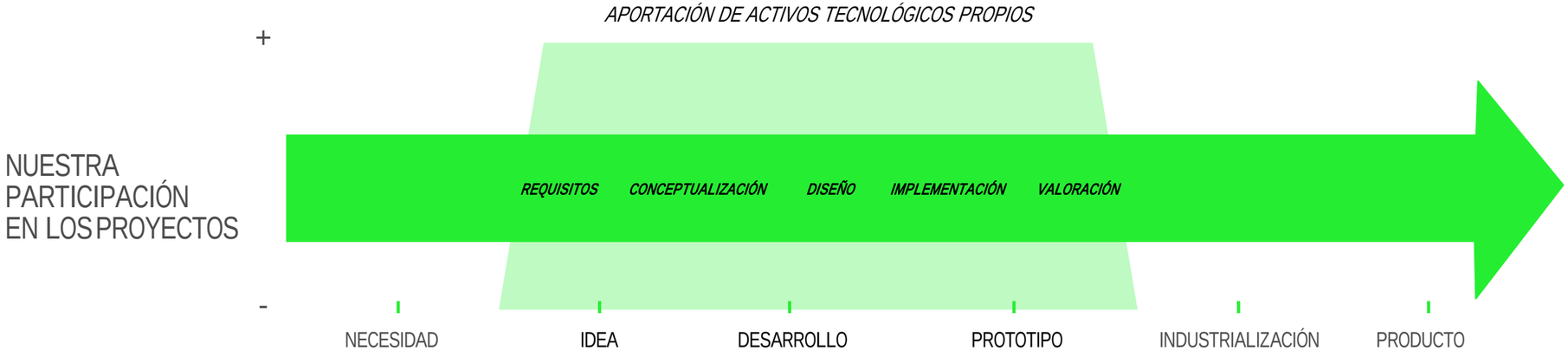
3.ª
SOMOS TECNOLÓGICOS.
DESDE LA IDEA AL PRODUCTO

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

3.ª
SOMOS TECNÓLOGOS.
DESDE LA IDEA AL PRODUCTO.

DESARROLLAMOS PROTOTIPOS INDUSTRIALES MEDIANTE LA APLICACIÓN DE NUESTROS CONOCIMIENTOS TECNOLÓGICOS.





4.ª
EN FORMA.
CENTRO TECNOLÓGICO ÁGIL,
CON LA MIRADA PUESTA EN EL FUTUTO

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

4.ª
EN FORMA.
CENTRO TECNOLÓGICO ÁGIL,
CON LA MIRADA PUESTA
EN EL FUTURO.

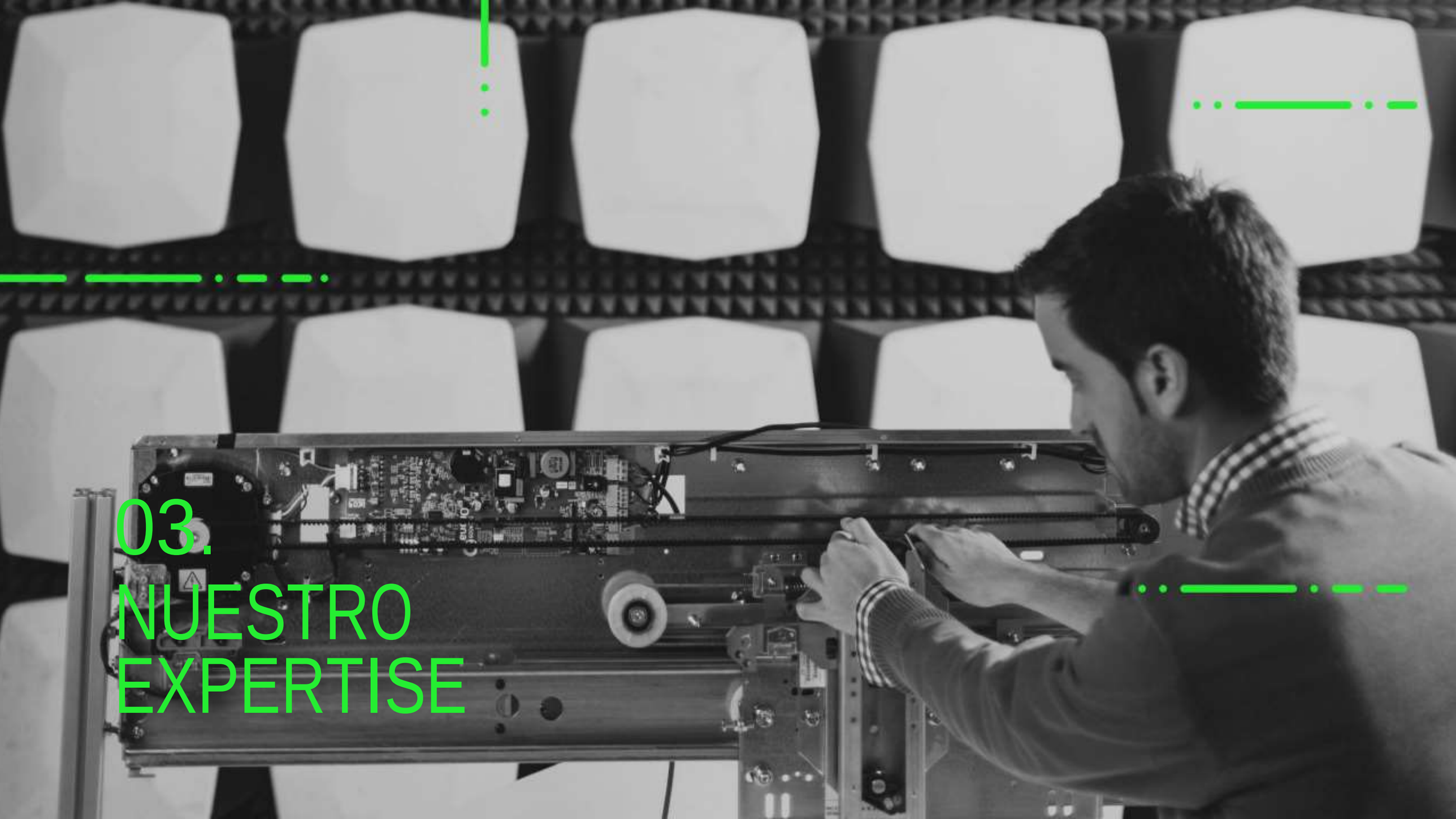
10,8 M€ EN PROYECTOS DE INVESTIGACIÓN EN 2020 (DFG, GV, AGE Y H2020)

MÁS DE **2 M€** EN INVERSIONES TECNOLÓGICAS PARA DISPONER DEL MEJOR EQUIPAMIENTO E INFRAESTRUCTURAS

MÁS DE **1,5 M€** FORMACIÓN DE ESTUDIANTES: INVESTIGADORES DEL FUTURO

- **59** TESIS DOCTORALES EN MARCHA
- **105** PERSONAL EN FORMACIÓN

UN CENTRO VITAL Y PROACTIVO QUE SE MUEVE CON AGILIDAD PARA ESTAR SIEMPRE EN LA VANGUARDIA TECNOLÓGICA



03.
NUESTRO EXPERTISE

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

LABORATORIOS DE REFERENCIA QUE NOS PERMITEN APLICAR LAS TECNOLOGÍAS A CASOS REALES

TECNOLOGÍAS DE ELECTRÓNICA, INFORMACIÓN Y COMUNICACIÓN

Laboratorios de:

· Sistemas embebidos y ciberseguridad.
· Ensayos EMC y RF.
· Microsistemas industriales.
· Laboratorio de montaje PCB

ENERGÍA Y ELECTRÓNICA DE POTENCIA

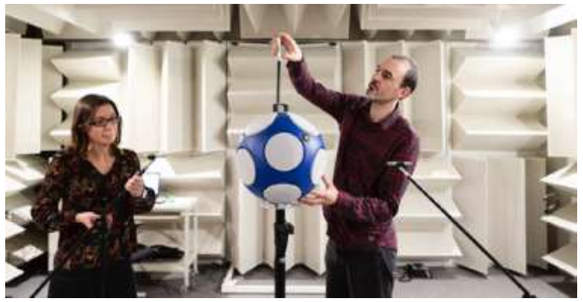
Laboratorios de:

· Smart Mobility
· Smart Storage
· Smart Building

FABRICACIÓN AVANZADA

Laboratorios de:

· Fiabilidad estructural.
· Ensayos acústicos.
· Combustión.



ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

“**COLABORAMOS** CON UNIVERSIDADES Y CENTROS TECNOLÓGICOS REFERENTES EN EL ÁMBITO **MUNDIAL**”

1. PAÍS VASCO
2. SANTANDER
3. OVIEDO
4. GIRONA
5. BARCELONA
6. VALENCIA
7. SEVILLA
8. SANTIAGO DE COMPOSTELA
9. PARÍS
10. BESANÇON
11. GRENOBLE
12. LEUVEN
13. BRUSELAS
14. EDIMBURGO
15. AACHEN
16. SIEGEN
17. ZÚRICH
18. VIENA
19. LULEÅ
20. AALBORG
21. OLDENBURG
22. EE. UU.

04.
TECNOLOGÍA REAL PARA RETOS REALES

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

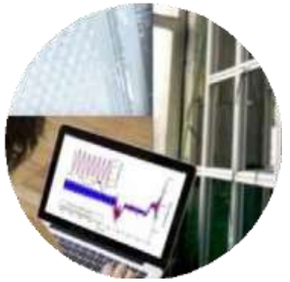
“MÁS DE 20 AÑOS COLABORANDO DE MANERA ESTABLE CON EL 80 % DE NUESTROS CLIENTES”

IKERLAN

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

CASOS DE ÉXITO
I+D CON EMPRESAS

Orona



FABRICACIÓN AVANZADA
Diseño robusto de ascensores.
Diagnosis para el mantenimiento predictivo.

SISTEMAS EMBEBIDOS
Control, conectividad, seguridad e IoT:
sistemas M2M ciberseguros.

ENERGÍA Y ELECTRÓNICA DE POTENCIA
Ascensor con capacidad de regeneración de energía.

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

CASOS DE ÉXITO
I+D CON EMPRESAS

CAF

SISTEMAS EMBEBIDOS
Sistemas de señalización y control ferroviario ERMTS. Proyecto estratégico de TREN DIGITAL.

ENERGÍA Y ELECTRÓNICA DE POTENCIA
Sistemas de electrónica de potencia basados en carburo de silicio.

ALMACENAMIENTO DE ENERGÍA
Sistemas de almacenamiento ultracapacidades-litio para el sector ferroviario.

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

CASOS DE ÉXITO I+D CON EMPRESAS

FAGOR ARRASATE

TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
Desarrollo de plataforma digital FA LINK.
Véase el vídeo

FABRICACIÓN AVANZADA
Eficiencia en la puesta en servicio de bienes de equipo.

FABRICACIÓN AVANZADA
Diseño y control de prensa hidráulica RTM.

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

CASOS DE ÉXITO I+D CON EMPRESAS

·GH·
CRANES & COMPONENTS

FABRICACIÓN AVANZADA
Análisis de fiabilidad de componentes críticos de la grúa. Servicio posventa personalizable.

CYBERSECURE IOT Y BIG DATA
Monitorización y gestión remota de datos de operación de grúas. Arquitectura Cloud con plataforma Big Data.

ENERGÍA Y ELECTRÓNICA DE POTENCIA
Electrificación integral de grúas pórtico automotor.

05. Propuestas TFM y Tesis Doctoral

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

TFM, TESIS y una carrera profesional por desarrollar…

Algunos ejemplos de TFM

Nuevas técnicas de Test de Penetración en Sistemas Embebidos

Descripción:

Los sistemas embebidos de control industrial están cada vez más conectados. Esto los hace susceptibles de recibir ciberataques que pueden tener consecuencias muy graves debido a la criticidad de los procesos que controlan. Por ello es importante garantizar su ciberseguridad mediante la implementación y despliegue de las contramedidas necesarias. Una vez implementadas, estas medidas deben ser evaluadas mediante un test de penetración. Un test de penetración es un ciber-ataque simulado y autorizado contra un sistema, realizado con el fin de evaluar el nivel de seguridad del mismo. Se realiza tanto a nivel lógico (a través de sus interfaces de comunicación) como físico (a través de la manipulación del hardware). Este proyecto cubre el desarrollo y puesta en marcha de las herramientas necesarias y un framework que automatice la ejecución de las distintas fases del test de penetración.

Objetivos:

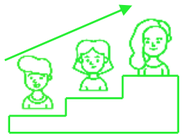
- Conocer las herramientas existentes de test de penetración de sistemas industriales.
- Disponer de herramientas de test de penetración para múltiples protocolos industriales.
- Disponer de un framework de automatización de tests de penetración.

Fases:

- Identificar y probar las herramientas existentes para hacer un test de penetración en un sistema de control industrial.
- Diseñar, implementar y probar las herramientas que no existan para hacer un test de penetración en un sistema de control industrial.
- Diseñar, implementar y probar un framework de ejecución automática

Flexibilidad horaria

Formación



Formar parte de la cantera

Ticket comedor

840€ al mes

Entorno joven

Análisis de Canal Lateral (Side-Channel Analysis) de algoritmos criptográficos en laboratorio

Descripción:

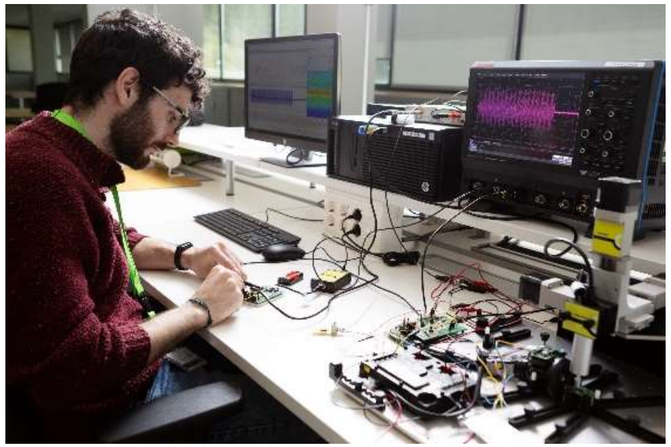
El alumno colaborará en la actividad del laboratorio de ciberseguridad de IKERLAN, utilizando equipamiento altamente especializado para evaluar la seguridad de distintos productos electrónicos. Se centrará en el manejo del equipamiento de Side-Channel Analysis (SCA), utilizado para romper la seguridad de implementaciones criptográficas y obtener la clave secreta, mediante el análisis de variables físicas como el consumo de potencia o las emisiones electromagnéticas. Las mediciones obtenidas deberán ser procesadas, utilizando para ello distintas técnicas estadísticas y de procesamiento de señal, hasta encontrar la información buscada.
Se requieren conocimientos de electrónica y procesamiento de señal, así como una gran iniciativa e ingenio para buscar nuevas vías de ataque a través de estas técnicas.

Objetivos:

- Adquirir conocimiento teórico y experiencia práctica en la técnicas y herramientas existentes de análisis de canal lateral.
- Evaluar el nivel de protección de distintas implementaciones criptográficas.
- Proponer nuevas técnicas y métodos de evaluación.

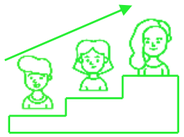
Fases:

- Estudio de los métodos más comunes para la realización de ataques SCA.
- Prueba y manejo de las herramientas.
- Elección de circuitos a atacar (claramente vulnerables, probablemente vulnerables, protegidos...).
- Realización de ataques sobre diseños escogidos.
- Análisis y comparación de resultados.



Flexibilidad horaria

Formación



Formar parte de la cantera

Ticket comedor

840€ al mes

Entorno joven

Desarrollo de mecanismo de arranque seguro (Secure boot) con y sin apoyo hardware

Descripción:

Uno de los puntos más vulnerables en un sistema embebido o dispositivo IoT es el arranque. Si un atacante consigue violar la secuencia de arranque, podrá ejecutar un binario alternativo, o alterar el comportamiento del sistema de forma interesada. Para evitar estas situaciones, es necesario integrar un mecanismo de arranque seguro (Secure Boot), que permita garantizar que la secuencia no ha sido alterada, y todos los elementos hardware y software son originales.

El alumno implementará dos mecanismos de arranque seguro. En uno de ellos se apoyará en hardware especializado (raíz de confianza), mientras que en el otro propondrá una implementación exclusivamente software. Deberá medir el nivel de robustez y seguridad alcanzado en cada uno de ellos.

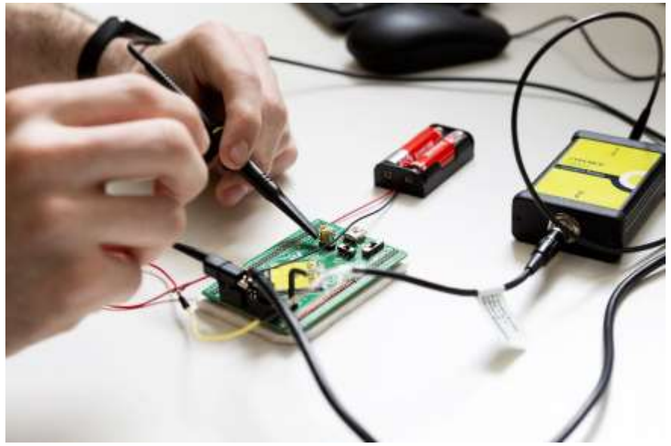
Se requieren conocimientos de electrónica, así como iniciativa e ingenio para conseguir el máximo nivel de protección con los medios disponibles.

Objetivos:

- Adquirir conocimiento teórico y experiencia práctica en las técnicas de arranque seguro.
- Implementar dos mecanismos de arranque seguro, con y sin apoyo hardware.
- Entender las ventajas y las debilidades de cada uno de ellos.

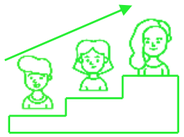
Fases:

- Análisis del estado del arte: estudio de los métodos para la implementación de mecanismos de arranque seguro.
- Selección de hardware y raíz de confianza.
- Implementación de arranque seguro, con y sin soporte hardware.
- Evaluación del nivel de protección alcanzado en ambas implementaciones.
- Análisis y comparación de resultados.



Flexibilidad horaria

Formación



Formar parte de la cantera

Ticket comedor

840€ al mes

Entorno joven

Detección de atacantes mediante técnicas de IA para la protección de infraestructuras críticas

Descripción:

El ataque a empresas y grandes organizaciones que gestionan infraestructuras críticas se está viendo incrementado en los últimos años debido a los grandes beneficios que los atacantes obtienen de estos. De cara a poder defender sus redes es muy importante conocer qué tipos de ataques se realizan a esas infraestructuras. Con este objetivo en mente, es cada vez más común el uso de herramientas que permiten crear una red ficticia (o honeypot) para engañar a los atacantes, haciéndoles creer que han accedido a la red real y de esta manera poder observar su comportamiento y poder crear o reforzar las medidas necesarias para proteger la red de estos ataques.

Objetivos:

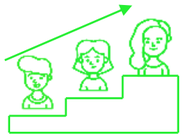
La categorización de los atacantes se hace generalmente mediante reglas predefinidas. En este proyecto se pretende explorar el uso de técnicas de Inteligencia Artificial avanzadas para reconocer e identificar aquellos usuarios con intención de atacar el sistema, de manera que se les pueda derivar al honeypot, alejandolos de la red auténtica, y observar así su comportamiento de manera segura.

Fases:

- Estudio de técnicas de defensa y ataque.
- Estudio de técnicas basadas en Honeypots.
- Diseño de una solución basada en IA para el reconocimiento de patrones de un atacante.
- Implementación de una prueba de concepto de la solución diseñada.

Flexibilidad horaria

Formación



Formar parte de la cantera

Ticket comedor

840€ al mes

Entorno joven

Identificación y control de accesos mediante infraestructuras pki para eNtornos iiot

Descripción:

Los sistemas de gestión de identidad y acceso permiten gestionar el acceso a los sistemas de información de una plataforma digital. Estos sistemas de gestión de identidad ofrecen las funcionalidades de autenticación (verificar que uno es quien dice ser), autorización (verificar que puede realizar la operación que se pretende realizar), delegación (temporalmente se permite realizar una operación con mayores privilegios) e intercambio (permite integrarse con otros sistemas de gestión de dispositivos). El uso de estos sistemas de gestión cobra más relevancia en el mundo IoT industrial, donde el número de dispositivos a integrar es grande (automatización), gestionar su ciclo de vida es laborioso (puesta en marcha, actualización, retirada), y el acceso físico para el mantenimiento de estos dispositivos es limitado (telegestión).

Objetivos:

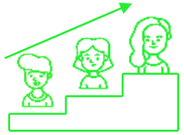
El objetivo es conocer e implantar un sistema de gestión de identidades que contemple mecanismos de autenticación y autorización en un entorno orientado al Internet de las Cosas (IoT) en el contexto de la Industria 4.0. La propuesta tiene que permitir la gestión y monitorización de la identidad de dispositivos remotos y su integración en las plataformas digitales.

Fases:

- Análisis de la funcionalidad de un sistema de autenticación y autorización basado en PKI para IIoT.
- Análisis, diseño y configuración de un mecanismo adaptado a entornos IIoT.
- Integración con otros sistemas dentro de una plataforma digital.
- Despliegue de solución en entorno de pruebas IKERLAN KONNEKT.

Flexibilidad horaria

Formación



Formar parte de la cantera

Ticket comedor

840€ al mes

Entorno joven

SISTEMAS ENRIQUECIDOS DE MONITORIZACIÓN DE DISPOSITIVOS EN ENTORNOS INDUSTRIALES

Descripción:

Los SIEM (Security Information and Event Management) son sistema de centralización de información que recopilan la información de seguridad en los entornos en los que se implantan. En entornos industriales y debido a la diversidad y limitaciones de los dispositivos que la componen, la monitorización y recolección de datos de seguridad se ve limitada. Para superar esas limitaciones se han de adaptar las soluciones de forma especifica, para aquellos entornos en los que se pretende integrar.

Tras la creación de un SIEM a partir de herramientas de software libre, el objetivo de este proyecto es centrarse en la mejora y adaptabilidad de esa solución en entornos industriales e IoT de diversa índole. Se deberá trabajar en los despliegues de la plataforma de gestión y análisis de datos para la detección de posibles amenazas y ataques.

Objetivos:

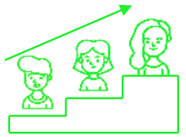
El principal objetivo del presente proyecto será el del desarrollo o extensión del SIEM seleccionado para la detección temprana de ataques y vulnerabilidades en sistemas IoT.

Fases:

- Familiarización con el SIEM empleado en IKERLAN.
- Análisis de requisitos asociados a la detección temprana de ataques y vulnerabilidades.
- Diseño de la solución basándose en técnicas de Inteligencia Artificial.
- Implementación de la solución.

Flexibilidad horaria

Formación



Formar parte de la cantera

Ticket comedor

840€ al mes

Entorno joven

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

TFM, TESIS y una carrera profesional por desarrollar…

cONDICIONES

grado	MÁSTER	DOCTORANDO	contratado
Prácticas 567 €/mes	Prácticas 676 €/mes	1.620 € brutos/mes	36. 960 € brutos /año
Proyecto 567 €/mes	Proyecto 840 €/mes		38. 965 € brutos/año (DOC)

ikerlan MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

IKERLAN

per@ikerlan.es

“ GRACIAS POR COMPARTIR NUESTRA ACTITUD POR LA TECNOLOGÍA”

P.º J. M.ª Arizmendiarrieta, 2 - 20500 Arrasate-Mondragón
Tel. +34 943 712 400 F. +34 943 796 944

ikerlan

MEMBER OF
BASQUE RESEARCH
& TECHNOLOGY ALLIANCE