IK4
IKERLAN
Research Alliance

Seguridad de los sistemas embebidos

Factor clave para proteger el negocio

Octubre 2017

IK4
Research Alliance

AZTERLAN | CEIT | CIDETEC | GAIKER | IDEKO | IKERLAN | LORTEK | TEKNIKER | VICOMTECH

IK4 IKERLAN
Research Alliance




- **Datos relevantes** www.ikerlan.es
  - 300
  - 62
  - 20,7 M€
- **Ubicación**

  Arrasate-Mondragón, Gipuzkoa
  Parque Tecnológico de Álava
  Polígono Industrial Galarreta, Gipuzkoa

TECNOLOGÍAS DE ELECTRÓNICA, INFORMACIÓN Y COMUNICACIÓN

ENERGÍA Y ELECTRÓNICA DE POTENCIA

FABRICACIÓN AVANZADA

Áreas de expertise tecnológico

TECNOLOGÍAS DE ELECTRÓNICA, INFORMACIÓN Y COMUNICACIÓN

Sistemas embebidos confiables	· Sistemas tiempo-real · SW Confiable · Security Industrial
TIC	· Cybersecure IoT · Arquitecturas Big Data
Sistemas de comunicación, plataformas HW y microsistemas	· Sistemas de comunicación · Plataformas HW · Microsistemas

ENERGÍA Y ELECTRÓNICA DE POTENCIA

Almacenamiento y Gestión de energía	· Almacenamiento de energía eléctrica · Gestión de energía eléctrica y térmica
Electrónica de potencia	· Electromagnetismo y máquinas eléctricas · Convertidores de potencia

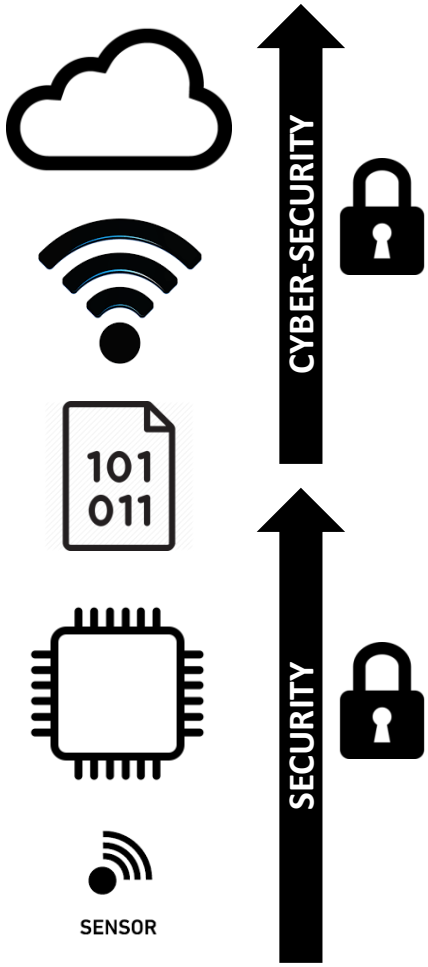
FABRICACIÓN AVANZADA

Mecánica	· Fiabilidad Estructural · Diseño Robusto
Tecnologías de operación y mantenimiento	· Servicios inteligentes de mantenimiento y fabricación
Control y Monitorización	· Monitorización · Control avanzado

Áreas de expertise tecnológico

TECNOLOGÍAS DE ELECTRÓNICA, INFORMACIÓN Y COMUNICACIÓN

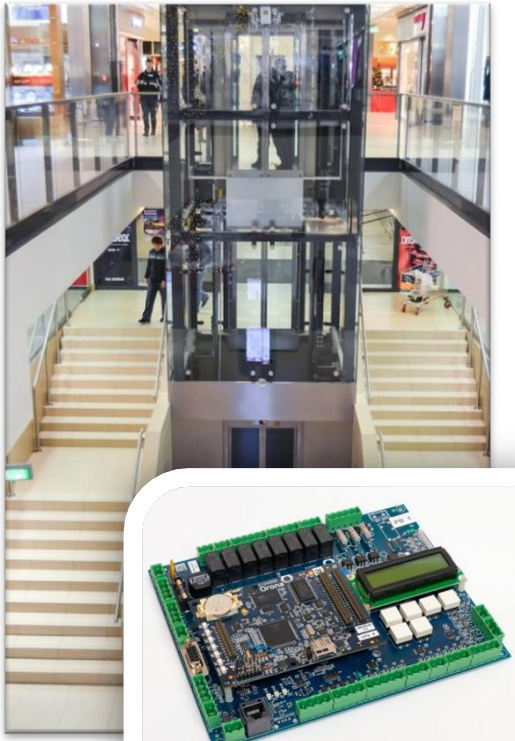
Sistemas embebidos confiables	· Sistemas tiempo-real · SW Confiable · Security Industrial
TIC	· Cybersecure IoT · Arquitecturas Big Data
Sistemas de comunicación, plataformas HW y microsistemas	· Sistemas de comunicación · Plataformas HW · Microsistemas



- 150 investigadores
  - 15 doctorandos
  - 20 estudiantes de Grado/Máster
- 6 M€/año en proyectos de I+D empresa
- 5 M€/año en proyectos de investigación

Sistemas embebidos confiables

Orona



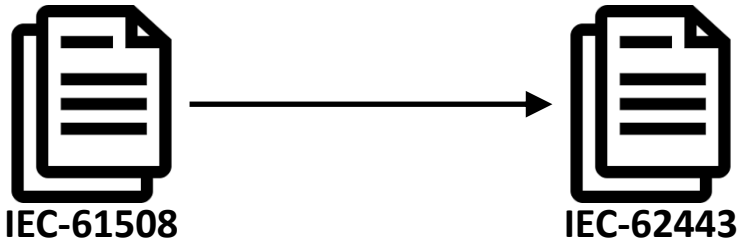
ALSTOM

CAF

Definiciones

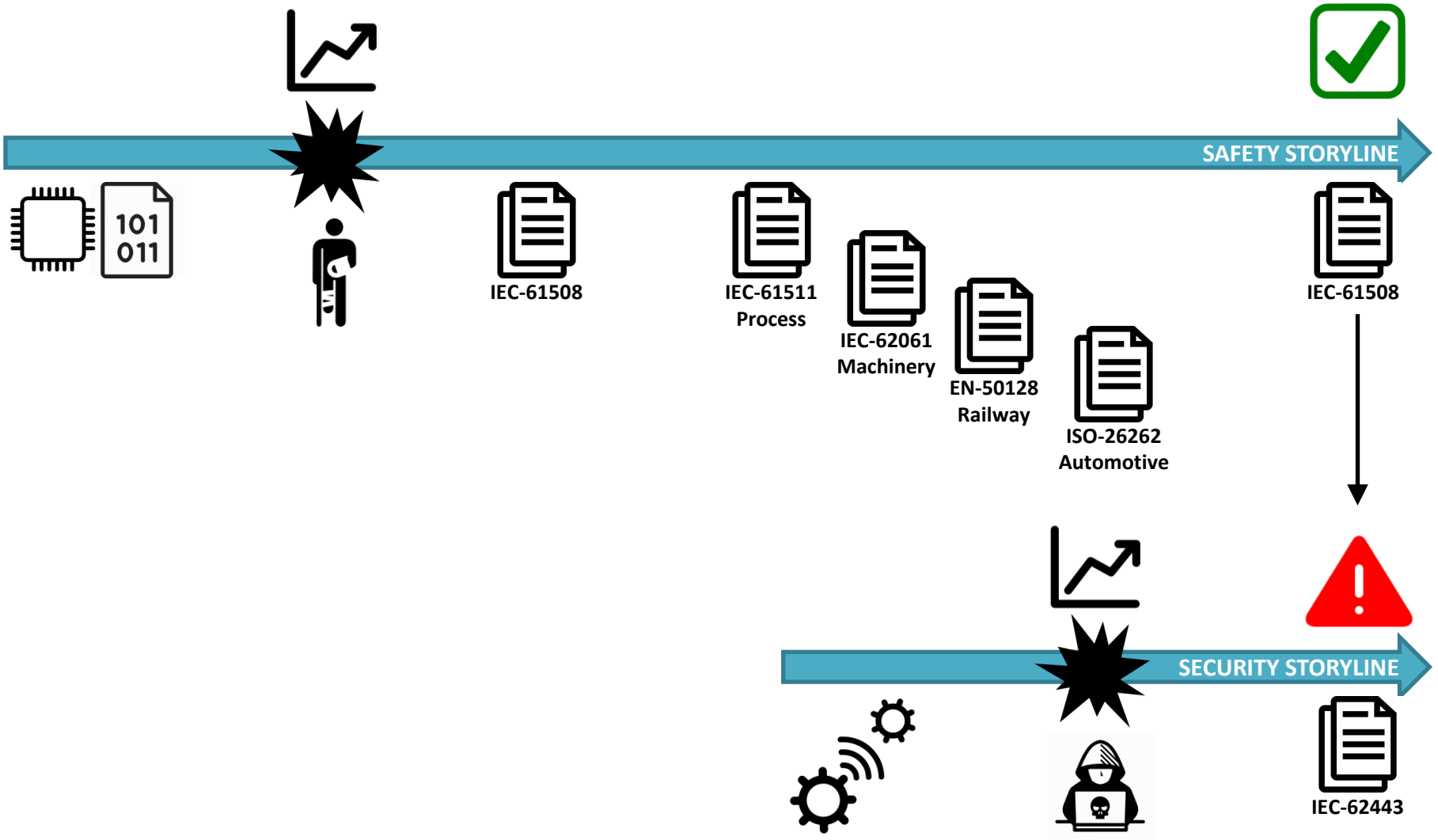
- **Safety**: Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment (IEC-61508-4)

- **Security**: Preventing intentional or unintentional interference with the proper and intended operation, or inappropriate access to confidential information in industrial automation and control systems (IEC-62443-1-2)



No hay SAFETY sin SECURITY!

Surgimiento normativo y situación actual



Safety & Security by Design

- Los estándares de safety y security consideran todo el ciclo de vida de un producto desde la especificación hasta la operación
  - Análisis de riesgos
  - Requisitos
  - Medidas a nivel de organización
  - Medidas técnicas

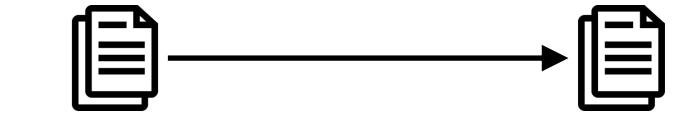
SAFE BY DESIGN

SECURE BY DESIGN

- Seguridad por diseño
  - Primera actividad en desarrollo Safety: safety concept
  - Primera actividad en desarrollo Security: security concept
  - Nadie concibe desarrollar un producto funcional y posteriormente dotarlo de propiedades Safety
  - En security tampoco!

Por qué security en sistemas embebidos?

- Relación con safety



- Certificación
  - Requisitos legales
  - Requisito de cliente o mercado, diferenciación

- Riesgos
  - Robo de propiedad intelectual (ingeniería inversa, clonado)
  - Robo de negocio
  - Manipulación, desplazamiento en el mercado
  - Deterioro de marca
  - Impacto en la disponibilidad de los servicios
  - Pérdida de privacidad
  - Pérdida de irrefutabilidad
  - Imposibilidad de desplegar nuevos servicios

Estrategia Basque Industry 4.0

BASQUE INDUSTRY 4.0
LANTEGI ADIMENDUA
LA FÁBRICA INTELIGENTE

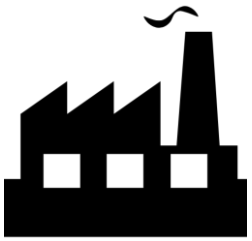
http://www.spri.eus/es/basque-industry/

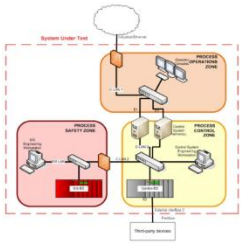
- "**Safety and security are both critical** to the success of smart manufacturing systems. It is important to ensure that production facilities and the products themselves do not pose a danger either to people or to the environment. At the same time, both production facilities and products and in particular the data and information they contain need to be protected against misuse and unauthorized access. This will require, for example, the deployment of integrated safety and security architectures and unique identifiers, together with the relevant enhancements to training and continuing professional development content."

- "The services and applications provided by these platforms will connect people, objects and systems to each other and will possess the following features: **safety, security and reliability for everything from sensors to user interfaces**."

- "**Security by Design as a key design principle**. In the past, security against external attacks was usually provided by physical measures such as access restrictions or other centralized security measures. In CPS-based manufacturing systems, it is not enough simply to add security features on to the system at some later point in time. All aspects relating to safety, and in particular security, need to be designed into the system from the outset."

Estructura IEC-62443





General

62443-1-1	TR62443-1-2	62443-1-3	TR62443-1-4
Concepts and models	Master glossary of terms and abbreviations	System security conformance metrics	IACS security life-cycle and use-cases

Policies & Procedures

62443-2-1	TR62443-2-2	TR62443-2-3	62443-2-4
Requirements for an IACS security management system	Implementation guidance for an IACS security management system	Patch management in the IACS environment	Requirements for IACS solution suppliers

System

TR62443-3-1	62443-3-2	62443-3-3
Security technologies for IACS	Security risk assessment and system design	System security requirements and security levels

Component

62443-4-1	62443-4-2
Product development requirements	Technical security requirements for IACS components

Niveles de seguridad IEC-62443

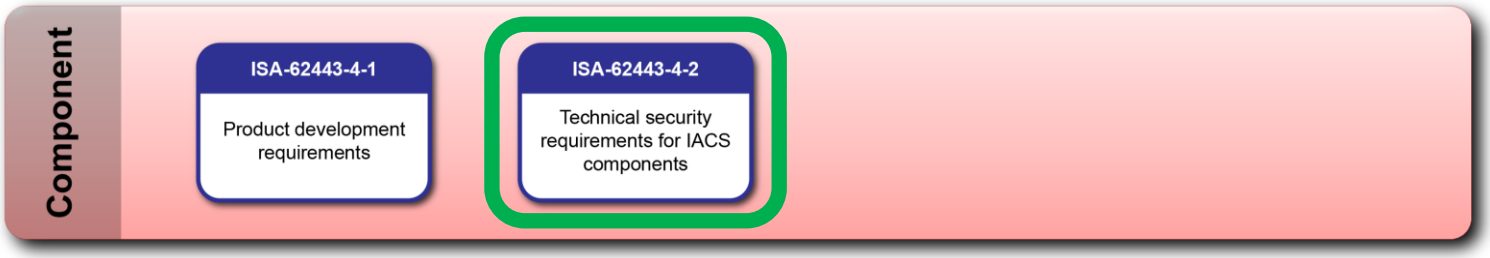
Safety Integrity Level (SIL)	
SIL 1	Probabilidad de un fallo peligroso cada 10 años de operación
SIL 2	Probabilidad de un fallo peligroso cada 100 años de operación
SIL 3	Probabilidad de un fallo peligroso cada 1.000 años de operación
SIL 4	Probabilidad de un fallo peligroso cada 10.000 años de operación

IEC-61508

Security Level (SL)	
SL 1	Protección contra violación casual o no intencionada
SL 2	Protección contra violación intencionada usando medios sencillos con pocos recursos, habilidades genéricas y motivación baja
SL 3	Protección contra violación intencionada usando medios sofisticados con recursos moderados, habilidades específicas IACS y motivación moderada
SL 4	Protección contra violación intencionada usando medios sofisticados con recursos extendidos, habilidades específicas IACS y motivación alta

IEC-62443

IEC-62443-4-2 Requisitos de security (Qué)



- **FSA-1. Access Control**
- **FSA-2. Use Control**
- **FSA-3. System Integrity**
- **FSA-4. Data Confidentiality**
- **FSA-5. Restricted Data Flow**
- **FSA-6. Timely Response to Events**
- **FSA-7. Resource Availability**

- Factores que impiden el uso de tecnología IT en sistemas embebidos

IT

Industria

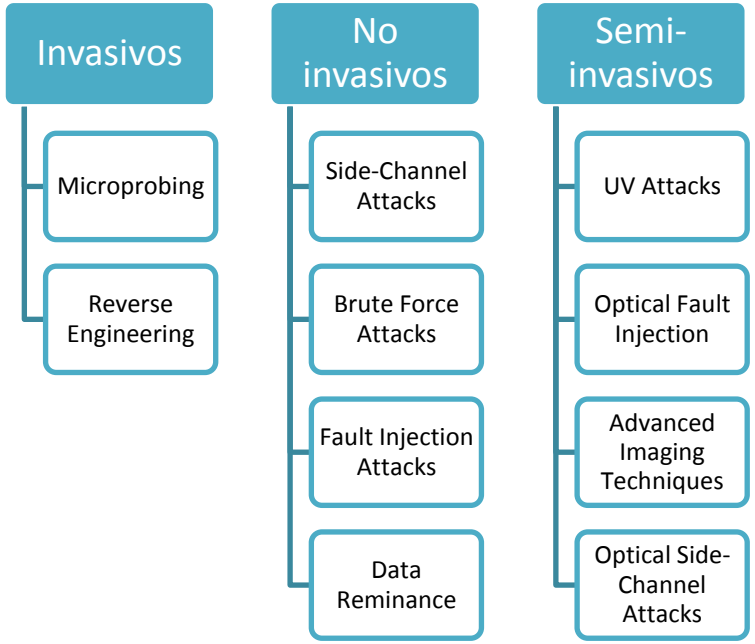
Sistemas embebidos
Hay requisitos safety
La disponibilidad es crítica
Hay requisitos tiempo-real
Existe gran dispersión de tecnologías
Dispersión de fabricantes
Recursos limitados
Diversidad de protocolos
Regulaciones sectoriales

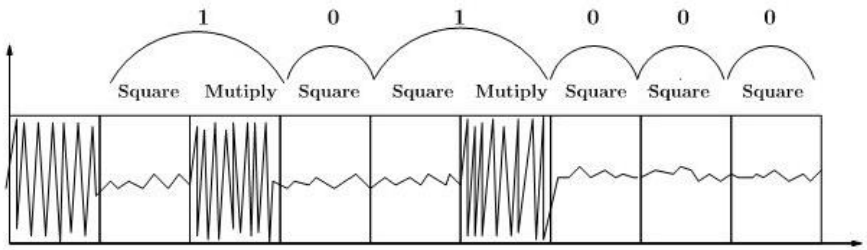
Hardware seguro

- Razones para incluir hardware seguro:
  - Implementación segura de los requisitos IEC-62443-4-2
  - Protección contra ataques físicos
  - Aceleración criptográfica
  - Garantía de implementación correcta

Necesario incorporar en el diseño!

La seguridad absoluta no existe!



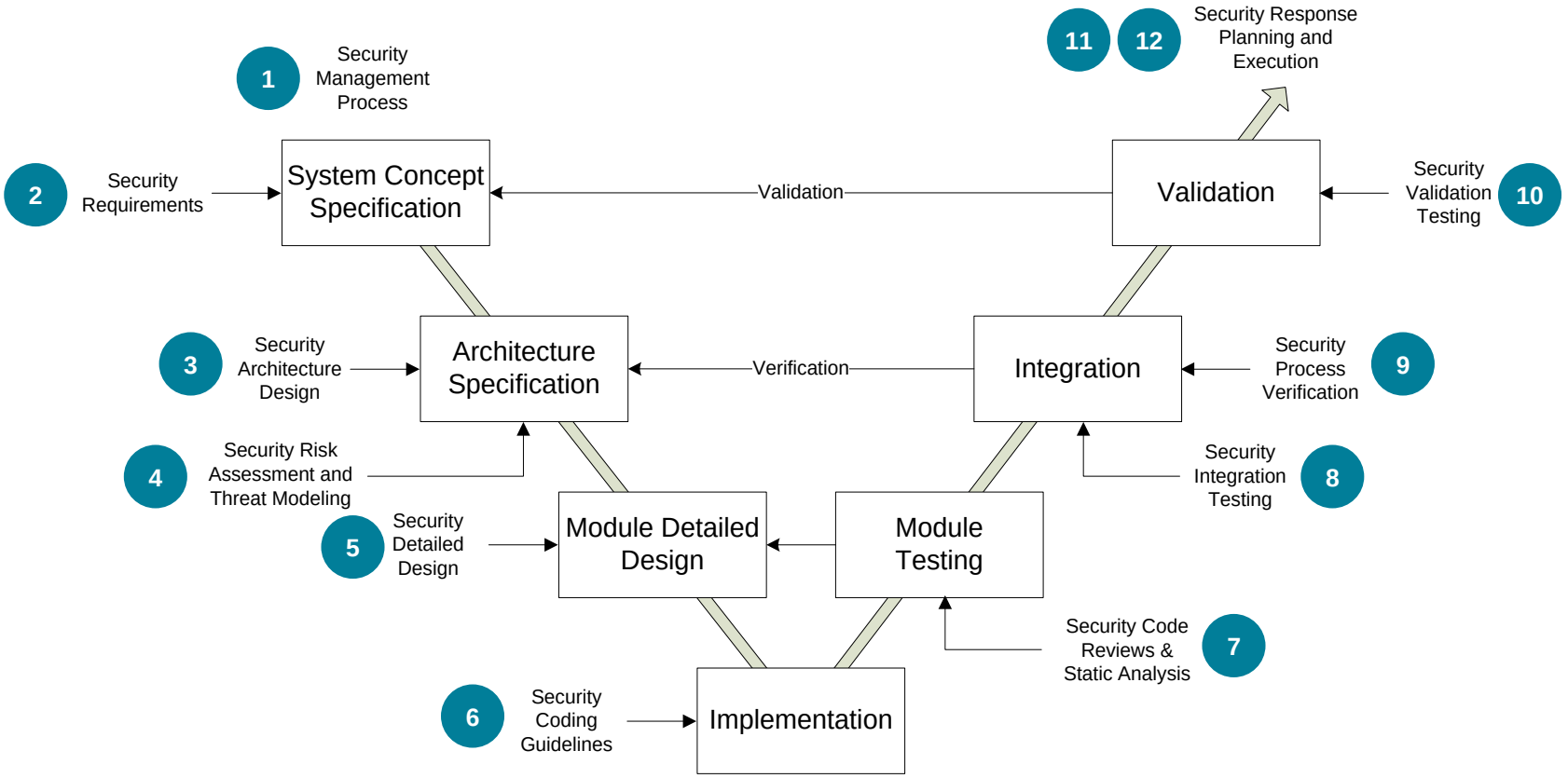


Simple Power Analysis (SPA) for RSA

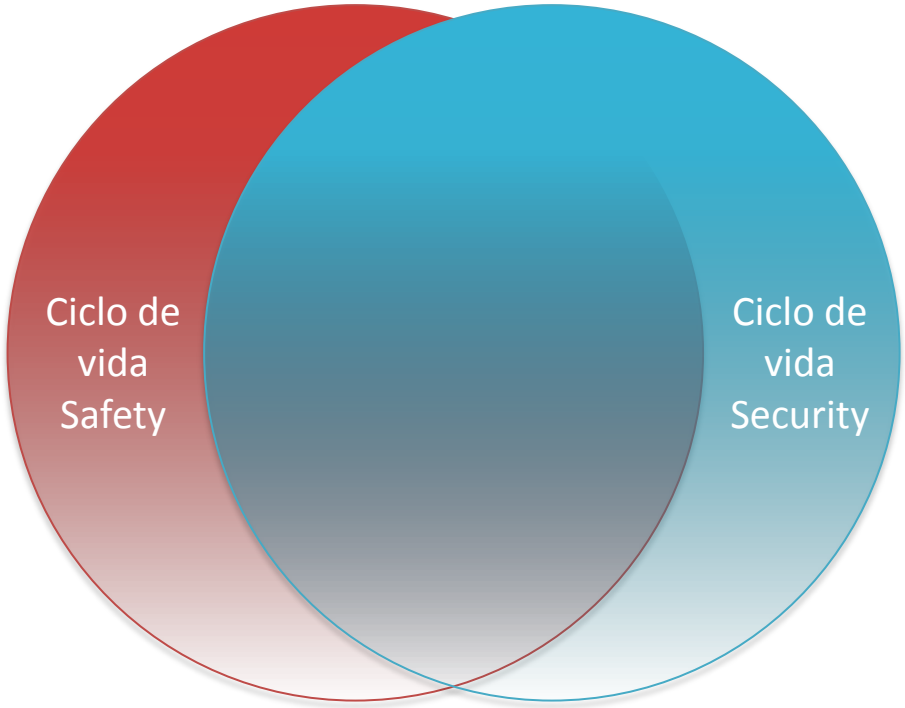
IEC-62443-4-2 Requisitos de ciclo de vida (Cómo)

- **SDSA-1. Security Management**
- **SDSA-2. Security Requirements**
- **SDSA-3. Software Architecture**
- **SDSA-4. Security Risk Assessment**
- **SDSA-5. Detailed Software Design**
- **…**
- **SDSA-12. Security Response Execution**

Ciclo de vida de desarrollo seguro



Ciclo de vida de desarrollo seguro



Security testing

Test de penetración

Test de robustez de comunicaciones

Test funcional

Test de seguridad física

Certificación

Certificación de robustez de comunicaciones

CRT
Communication Robustness Testing

achilles CERTIFIED

SDLA
Security Development Lifecycle Assurance

Desarrollo con ciclo de vida certificado

CERTIFIED

Certificación de producto

VIT
Vulnerability Identification Testing

FSA
Functional Security Assessment

IECEE

ISA Security Compliance Institute

CERTIFIED

Certificación

Security Level 1

- Secure Development Lifecycle Assessment
- Functional Security Assessment
- Vulnerability Identifaction Testing

Security Level 2

- Secure Development Lifecycle Assessment
- Functional Security Assessment
- Vulnerability Identifaction Testing

Security Level 3

- Secure Development Lifecycle Assessment
- Functional Security Assessment
- Vulnerability Identifaction Testing

Security Level 4

- Secure Development Lifecycle Assessment
- Functional Security Assessment
- Vulnerability Identifaction Testing

- Communication Robustness Testing

IKERLAN

David González
dgonzalez@ikerlan.es

IK4 Research Alliance

AZTERLAN | CEIT | CIDETEC | GAIKER | IDEKO | IKERLAN | LORTEK | TEKNIKER | VICOMTECH