IDENTIFICACIÓN DEL EQUIPO INVESTIGADOR

NOMBRE DEL EQUIPO O GRUPO DE INVESTIGACIÓN	**Cyber-Security and Safety**
UNIDAD/DEPARTAMENTO DE PERTENENCIA	**IT Competitiveness**
CENTRO/INSTITUTO/UNIVERSIDAD/ORGANISMO DE PERTENENCIA	**TECNALIA – División ICT/ESI**

DATOS DE CONTACTO

DATOS DE CONTACTO DEL EQUIPO

PERSONA DE CONTACTO	**Huáscar Espinoza**	TELÉFONO	946440400
ROL EN EL EQUIPO	Investigador principal	MAIL	huascar.espinoza@tecnalia.com
WEB DEL EQUIPO	www.cyberssbytecnalia.com		

DIRECCIÓN POSTAL DEL EQUIPO

EDIFICIO	700	CENTRO	Parque Tecnológico de Bizkaia
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Geldo
NÚMERO	-	CIUDAD	Derio
PROVINCIA	Vizcaya	CÓDIGO POSTAL	48160

DATOS DE CONTACTO DEL ORGANISMO AL QUE PERTENECE

PERSONA DE CONTACTO	**Ana Ayerbe**		
MAIL	ana.ayerbe@tecnalia.com		
TELÉFONO	656791613	WEB	www.tecnalia.com

DIRECCIÓN POSTAL DEL ORGANISMO

EDIFICIO	700	CENTRO	Parque Tecnológico de Bizkaia
TIPO DE VÍA	Calle	NOMBRE DE LA VÍA	Geldo
NÚMERO	-	CIUDAD	Derio
PROVINCIA	Vizcaya	CÓDIGO POSTAL	48160

INVESTIGADOR/ES PRINCIPAL/ES

NOMBRE	TITULACIONES
Huáscar Espinoza Ortiz	Doctor en Ciencias de la Computación Ingeniero en Electrónica

TRAYECTORIA PROFESIONAL

- 18 años de experiencia en investigación, sobre Seguridad de sistemas ciber-físicos (CPS), Aseguramiento y Certificación Incremental
- Ingeniería de Software, Sistemas SCADA, Ingeniería Dirigida por Modelos (MDE), Sistemas Aéreos No Tripulados (UAS), Sistemas de Gestión de energía

WEB Y REDES SOCIALES

MIEMBROS DEL EQUIPO

- Xabier Huascar L.
- Ana Isabel Ayerbe F.
- Maite Álvarez P.
- Idoya Del Río D.
- Alejandra Ruiz L.
- Stefan Schuster
- Eneko Gómez R.
- Iván Gutiérrez A.
- Eider Iturbe Z.
- Ander Juaristi A.
- Garazi Juez U.
- Óscar Lage S.
- Ángel López C.
- Cristina Martínez M.
- Mª Carmen Palacios P.
- Javier Puelles R.
- Nuria Quintano F.
- Erkuden Ríos V.

LÍNEAS Y ÁREAS DE INVESTIGACIÓN

PRINCIPALES LÍNEAS DE INVESTIGACIÓN	ÁREAS DE INVESTIGACIÓN
• Desarrollo, despliegue y monitorización de tecnológicas convergentes (física y lógica, safety y cybersecurity) • Plataformas de ejecución seguras • Seguridad/privacidad mediante el diseño • Diseño de requisitos de seguridad • Ingenieria de seguridad • Ciberriesgos • Internet of things • Desarrollo de metodologías para el incremento de la fiabilidad y actualización de sistemas	• Sistemas fiables y actualizables
• Arquitecturas de sistemas y procesos resilientes • Privacidad de los datos vs personalización • Identificación y autorización segura y ubicua	• Procesado de datos
• Seguridad y privacidad en cloud e iot • Seguridad en servicios digitales y medios de pago • M-commerce • E-commerce	• Otras áreas de interés
• Seguridad de datos operativos y de proceso • Gestión de riesgos • Mecanismos de recolección de datos • Análisis de riesgos estadísticos y predictivos • Evaluación y gestión dinámica de riesgos • Recolección de información sobre amenazas • Métricas de riesgos integrados e indicadores • Detección temprana de ciberriesgos • Métodos para reducir y gestionar sistemas complejos • Auditoria de sistemas de seguridad • Modelado de sistemas y de ataques a sistemas • Interoperabilidad de sistemas	• Evaluación de sistemas y ciberriesgos
• Técnicas y herramientas para asegurar que los productos ciber-físicos y procesos asociados cumplen los requisitos de seguridad, los estándares y las regulaciones • Protección física de datos • Desarrollo de mecanismos de recolección de datos • Creación de barreras de entrada • Detección y eliminación de malware • Gestión de evidencias electrónicas • Filtraciones de información • Contención de ataques • Gestión de periféricos infectados • Desarrollo de herramientas de detección de amenazas	• Ataques y defensa ante amenazas

LÍNEAS Y ÁREAS DE INVESTIGACIÓN

PRINCIPALES LÍNEAS DE INVESTIGACIÓN	ÁREAS DE INVESTIGACIÓN
• Métodos y herramientas de protección • Detección de amenazas • Monitorizado y seguridad de redes • Vigilancia del entorno • Arquitectura de protección y resilientes • Análisis y gestión de riesgos • Cumplimiento normativo de seguridad • Sistema de control industrial en redes (agua, electricidad, alimentación, transporte, finanzas, salud, etc) • Modelado de sistemas y de ataques a sistemas • Efecto en cascada	• Infraestructuras críticas
• Políticas de privacidad • Sistemas de anonimidad • Protocolos criptográficos de preservación de la privacidad • PET para organizaciones e infraestructuras • Privacidad en Cloud • Privacidad en IoT • Tecnologías de potenciadores de la privacidad (PET) • Private Information Retrieval (PIR) • Usabilidad de las PET	• Privacidad

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES 2016

TIER competency-based training course for the first receivers of CBRN casualties: a European perspective
A. Djalali, F. Della Corte, F. Segond, M.H. Metzger, L. Gabilly, F. Grieger, X. Larrucea, C. Violi, C. López, P. Arnod-Prin, P.L. Ingrassia, 2016

Standards-based metamodel for the management of goals, risks and evidences in critical systems development
Xabier Larrucea, César González-Pérez, Tom McBridec, Brian Henderson-Sellers, 2016

Hospital preparedness and response in CBRN emergencies: TIER assessment tool.
C. Olivieri, P.L. Ingrassia, F. Della Corte, L. Carenzo, J.M. Sapori, L. Gabilly, F. Segond, F. Grieger, P. Arnod-Prin, X. Larrucea, C. Violi, C. López, A. Djalali, 2016

Model-based specification of safety compliance needs for critical systems: A holistic generic metamodel.
Jose Luis de la Vara, Alejandra Ruiz, Katrina Attwood, Huáscar Espinoza, Rajwinder Kaur Panesar-Walawege, Ángel López, Idoya del Río, Tim Kelly, 2016

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES 2015

Towards Self-Protective Multi-Cloud applications
Erkuden Rios, Eider Iturbe, Leire Orue-Echevarria, Massimiliano Rak, Valentina Casola, 2015

Un système expert fondé sur une analyse sémantique pour l'identification de menaces d'ordre biologique
Cédric Lopez, Aleksandra Ponomareva, Aleksandra, Cécile Robin, André Bittar, Xabier Larrucea, Frédérique Segond, Marie-Hélène Metzger, 2015

A GSN Approach for risk management in structured assurance cases
Xabier Larrucea, Izaskun Santamaría, 2015

A review of travel time estimation and forecasting for Advanced Traveller Information Systems
Usue Mori, Alexander Mendiburu, Maite Álvarez, Jose A. Lozano, 2015

Design considerations of an unmanned aerial vehicle for aerial filming
D. Casazola, F. Arnez, H. Espinoza, 2015

Systematic application of ISO 26262 on a SEooC: support by applying a systematic reuse approach
Alejandra Ruiz, Alberto Melzi, Tim Kelly, 2015

A tool suite for Assurance Cases and Evidences: Avionics experiences
Alejandra Ruiz López, Xabier Larrucea, Huascar Espinoza, 2015

An industrial experience in cross-domain assurance project
Alejandra Ruiz López, Xabier Larrucea, Huascar Espinoza, 2015

A safe generic adaptation mechanism for smart cars
Alejandra Ruiz, Garazi Juez, Philipp Schleiss, Gereon Weiss, 2015

Safety Case Driven Development for Medical Devices
Alejandra Ruiz, Paulo Barbosa,Yang Medeiros, Huascar Espinoza, 2015

Multidirectional modular conditional safety certificates
Tiago Amorim, Alejandra Ruiz, Christoph Dropmann, Daniel Schneider, 2015

MUSA : Multi-cloud secure applications –Objectives and challenges
Erkuden Ríos, 2015

PUBLICACIONES RELACIONADAS DESTACADAS

PUBLICACIONES 2015

Self-protecting Multi-Cloud applications
Antonio M. Ortiz, Erkuden Rios, Wissam Mallouli, Eider Iturbe, Edgardo Montes de Oca , 2015

From consumer requirements to policies in secure services
Erkuden Rios, Francesco Malmignati, Eider Iturbe, Michela D'Errico, Mattia Salnitri, 2015

PUBLICACIONES 2014

A meta-heuristically Optimized Fuzzy Approach towards Multi-metric Security Risk. Assessment in heterogeneous systems of systems
Iñaki Eguia, Javier Del Ser, 2014

An industrial assessment for a multimodel framework
Xabier Larrucea, Izaskun Santamaria, 2014

PUBLICACIONES 2013

Open platform for evolutionary certification of safety-critical systems introduction
Xabier Larrucea Uriarte, Annie Combelles, John Favaro, 2013

Making software safety assessable and transparent
Risto Nevalainen, Alejandra Ruiz, Timo Varkoi, 2013

Design considerations of an unmanned aerial vehicle for aerial filming
D. Casazola, F. Arnez, H. Espinoza, 2013

PROYECTOS RELEVANTES

OPENCOSS
Objetivos: Definición de un marco común de certificación y establecimiento de una infraestructura de certificación de seguridad de código abierto

AMASS
Objetivos: AMASS creará y consolidará una plataforma-herramienta de código abierto, que conforme un mecanismo de certificación y aseguramiento de facto a nivel Europeo, elaborando un ecosistema y comunidad auto-sostenible, que abarque los mayores mercados verticales CPS

SAFEADAPT
Objetivos: Mejorar significativamente los vehículos totalmente eléctricos haciéndolos más eficientes y seguros, llevándolos al mercado en una escala de tiempo apropiada

RECOMP
Objetivos: Diseños y arquitecturas de referencia junto con los métodos de diseño necesarios y herramientas para lograr obtener una certificación re-certificación rentable de sistemas multi-core con criticidad mixta

ANIKETOS
Objetivos: Creación y mantenimiento de servicios seguros y confiables. La plataforma provee de metódos, soporte con herramientas y servicios de comunidad para ayudar a la implementación, descubrimiento, composición, adaptación y gestión de los servicios web a través del ciclo de vida completo de la ingeniería de seguridad

COSSIM
Objetivos: Desarrollar herramientas que mejoren el rendimiento y aceleren (optimicen) el procesamiento de las CPSs teniendo en cuenta las peturbaciones de seguridad. Para ello, es necesario desarrollar optimizaciones a través de FPGAs para desarrollar simulaciones eventuales

NSHIELD
Objetivos: Directrices de monitorización y control de seguridad, privacidad y dependabilidad (SPD) en los sistemas embebidos y en un entorno para Sistemas Críticos y Sistemas de Sistemas

SWEPT
Objetivos: Ofrecer una protección eficaz y definitiva frente al casi 100% de los ataques maliciosos conocidos en sitios web, a través de la detección de malware, phising y otros tipos de ciberamenazas crecientes

INTERNA
Objetivos: Asignación de fondos propios para la especialización y el desarrollo de activos

ELKARTEK
Objetivos: GENESI - Investigación para la GEstión y monitorizacióN Eficiente y Segura de procesos en entornos inteligentes de producción Industrial

PROYECTOS RELEVANTES

Retos Colaboración
Objetivos: DRONE-FS - FileSystem autoprotegido para drones y equipos con información confidencial

TACIT
Objetivos: Threat Assessment framework for Critical Infrastructures protection

TRIAL
Objetivos: ThReat Identification and Assessment against criticaL infrastructures

TIER
Objetivos: Estrategia Integrada para CBRN Threat Identification and Emergency Response

FM-BIASED
Objetivos: Formal Methods: Business Impact of Application to Security relevant Devices

RISC
Objetivos: Desarrollo de un modelo para la convergencia de la seguridad física y cibernética de las infraestructuras críticas desde un punto de vista integral

MUSA
Objetivos: Apoyar la gestión inteligente en seguridad del ciclo de vida de las aplicaciones distribuidas sobre recursos cloud heterogéneos, a través de un marco de seguridad

OPERANDO
Objetivos: Especificación, ejecución, pruebas de campo, validación y explotación de una plataforma de aplicación de la privacidad innovadora que permita generar Privacidad como un Servicio (PAS), paradigma de negocio y del mercado de servicios de privacidad en línea

CIPHER
Objetivos: Desarrollar un marco metodológico que contiene recomendaciones destinadas a prevenir los delitos cibernéticos y para reaccionar en caso de ciberataques