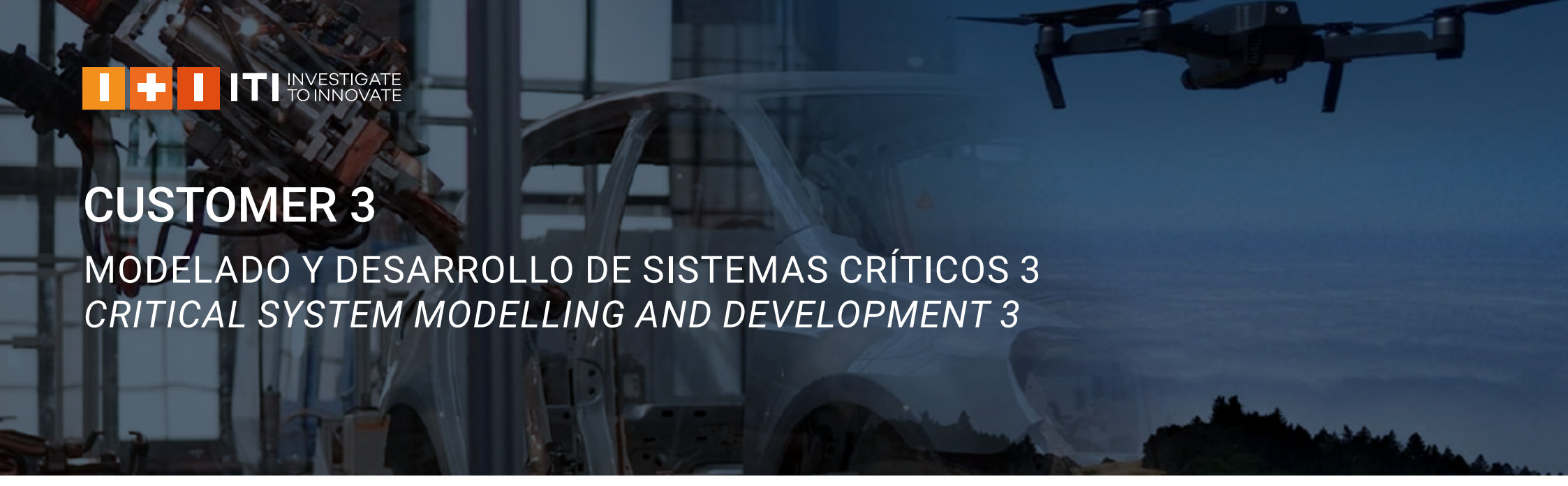

ITI INVESTIGATE TO INNOVATE

CUSTOMER 3

MODELADO Y DESARROLLO DE SISTEMAS CRÍTICOS 3
CRITICAL SYSTEM MODELLING AND DEVELOPMENT 3

EL PROYECTO

Un sistema crítico es aquel en el que un fallo del sistema puede ocasionar daños graves e irreparables tanto económicos, como humanos o medioambientales.

Por ello, **es necesario garantizar el correcto funcionamiento de este tipo de sistemas antes de su puesta en marcha**. Para llevar a cabo dicho proceso, es fundamental hacer una caracterización precisa del mismo, así como realizar un exhaustivo estudio de cuál es su comportamiento en los peores escenarios posibles.

Por tanto, los procesos de caracterización del sistema, en los que se describe los componentes del mismo, sus interacciones y su comportamiento interno, son de vital importancia.

De la misma relevancia son aquellos sistemas de análisis y verificación que son capaces de comprobar que las interacciones entre los componentes continúan cumpliendo con los requisitos definidos para el sistema incluso en las peores condiciones.

Para ayudar en el modelado, análisis y desarrollo de sistemas críticos ITI ha estado desarrollando un entorno denominado art2kitekt©.

En el presente proyecto se pretende extender dicho entorno para dar soporte al proceso completo de desarrollo de los sistemas críticos actuales. En estos sistemas la adaptabilidad, tanto para la incorporación de nuevos comportamientos, como en presencia de fallos transitorios o permanentes, es de vital importancia.

Aunque existen multitud de aproximaciones en esta línea, el hilo conductor principal de este proyecto ha sido el acercar algunas de dichas aproximaciones al sector empresarial. Igualmente se ha intentado dar cobertura a las nuevas necesidades que surgen desde la industria y que no están cubiertas por las soluciones actuales.

OBJETIVOS

Una metodología de Diseño Basado en Componentes (Component-based Engineering/Design) no sólo resulta interesante durante el proceso de diseño y evaluación de sistemas distribuidos, sino que también resulta de especial interés con el diseño de sistemas particionados con criticidad mixta.

Se conoce como sistema particionado o sistema TSP (Time Space Partitioning) a aquel que mantiene de forma separada los distintos componentes software para de esta forma contener y aislar los fallos entre componentes con distintas fiabilidades y restricciones de seguridad. Igualmente, los sistemas particionados permiten reducir el esfuerzo del proceso de integración, verificación y validación del software.

Esta arquitectura se utiliza frecuentemente con los sistemas hipervisores, una capa de software que permite la ejecución de diversos entornos de ejecución independientes sobre una misma máquina. Estas particiones disponen de una planificación de recursos local, pero a su vez estas particiones siguen una planificación a nivel global. Se crea de esta forma una jerarquía de gestión de recursos que no se puede evaluar con algoritmos de análisis convencionales como los que se utilizan habitualmente.

El objetivo general del proyecto es avanzar en la metodología de diseño basado en modelos, aplicando las propuestas y resultados de los procesos de investigación dentro del área de los sistemas ciber-físicos críticos con restricciones temporales.

En ese sentido, se pretende conseguir alcanzar los siguientes objetivos específicos:

- **Continuar la evolución de la herramienta art2kitekt© para su uso en el proceso de diseño de sistemas distribuidos de tiempo real basado en componentes.** Una vez incorporadas capacidades básicas para el modelado de sistemas distribuidos de tiempo real, se quiere ampliar la herramienta con la inclusión de algoritmos de análisis composicional que mejoren la evaluación de viabilidad de los mismos.

- **Incorporar en art2kitekt© soporte para el diseño y evaluación de sistemas particionados con criticidad mixta, arquitectura comúnmente utilizada en tecnologías basadas en hipervisores.** Nos centraremos, en primer lugar, en el modelado de componentes para este tipo de sistemas particionados para, posteriormente, aplicar sobre el modelo, técnicas analíticas que permitan evaluar su comportamiento temporal. Se utilizarán algoritmos de análisis de sistemas de planificación jerárquicos y nos centraremos en las comunicaciones entre las distintas particiones.

Primera anualidad
Este proyecto ha sido financiado por **IVACE**
Nº de expediente: IMDEEA/2019/106
Financiación: 144.720,20€

Segunda anualidad
Este proyecto ha sido financiado por **IVACE**
Nº de expediente: IMDEEA/2020/71
Financiación: 205.910,34€

Tercera anualidad
Este proyecto ha sido financiado por **IVACE**
Nº de expediente: IMDEEA/2021/73
Financiación: 140.966,30€

GENERALITAT VALENCIANA
iVACE INSTITUTO VALENCIANO DE COMPETITIVIDAD EMPRESARIAL
Unión Europea
Fondo Europeo de Desarrollo Regional "Una manera de hacer Europa"