Título: DEPENDABLE SYSTEMS OVER SYNCHRONOUS NETWORKS

Nombre: Gutiérrez Rivas, José Luis

Universidad: Universidad de Granada

Departamento: Arquitectura y tecnología de computadores

Fecha de lectura: 04/12/2018

Mención a doctor europeo: concedido

Programa de doctorado: Programa de Doctorado en Tecnologías de la Información y la Comunicación por la Universidad de Granada

Dirección:

> **Director:** Antonio Javier Díaz Alonso

> **Director:** Eduardo Ros Vidal

Tribunal:

> **presidente:** Mancia Anguita López

> **secretario:** MANUEL RODRÍGUEZ ÁLVAREZ

> **vocal:** ANTONIO MARTÍNEZ ÁLVAREZ

> **vocal:** Héctor Esteban Pinillos

> **vocal:** Elizabeth Laier English

Descriptores:

> SISTEMAS DE CONTROL

> SISTEMAS EN TIEMPO REAL

> FIABILIDAD DE SISTEMAS

El fichero de tesis ya ha sido incorporado al sistema

> https://digibug.ugr.es/bitstream/handle/10481/54624/80925.pdf?sequence=4&isAllowed=y

Resumen: Esta tesis presenta el trabajo realizado sobre aplicaciones distribuidas críticas en infraestructuras de red industriales. Dicho trabajo se centra en proporcionar a todos los elementos de la red capacidades de redundancia para así incrementar la tolerancia a fallos tanto a nivel local como distribuido, poniendo especial énfasis en aspectos de sincronización.

Esta tesis está estructurada en cuatro partes.

En la primera revisaremos el estado del arte, poniendo especial atención en todos aquellos elementos que forman parte de un sistema crítico distribuido. Esta sección comienza con la evolución experimentada por los sistemas críticos (SC) a lo largo de los últimos años y su adaptación desde las arquitecturas mononúcleo a las

multinúcleo. Posteriormente nos centraremos en el crecimiento progresivo experimentado por las redes eléctricas hacia los sistemas inteligentes, conocidos como Smart Grid, junto a su relación con aplicaciones críticas, además de sus necesidades relacionadas con la sincronización de los diferentes eventos que tiene lugar a lo largo de la red. Mostraremos diferentes tipos de tecnologías de sincronización, con especial atención sobre la principalmente utilizada en esta tesis, la tecnología White Rabbit (WR). Esta tecnología es capaz de proporcionar una precisión por debajo del nanosegundo en redes Ethernet. Para finalizar este apartado, hemos incluido un breve estudio de mercado para comparar nuestra contribución con otras tecnologías existentes en el mercado.

En la segunda parte revisaremos los métodos utilizados para incrementar la fiabilidad en sistemas finales (nodos hoja) de criticidad mixta utilizando arquitecturas multinúcleo. Pondremos especial atención en el desarrollo de métodos para aislar las partes críticas de las no críticas tanto en software como en hardware, sin incrementar los costes del proceso de certificación del sistema final. Este desarrollo está basado en un caso de uso industrial utilizado como prueba de concepto, en el que se define la parada de emergencia de un controlador de un motor industrial. Finalizaremos esta parte con un análisis de las características de tolerancia a fallos añadidas al sistema gracias a la duplicidad de los recursos hardware, la definición de arquitecturas software redundantes y de la integración de canales de comunicación confiables entre diferentes procesadores.

En la tercera parte, pasaremos de la problemática de las comunicaciones entre núcleos de un mismo dispositivo, a las comunicaciones entre diferentes procesos distribuidos a lo largo de la red. Revisaremos diferentes métodos para incrementar la fiabilidad, escalabilidad y compatibilidad en redes industriales, poniendo especial interés en la distribución de tiempo y datos. En primer lugar, introduciremos el desarrollo de diferentes tipos de relojes para la tecnología WR con el fin de incrementar su escalabilidad y su compatibilidad industrial. A continuación, describiremos los métodos desarrollados para proporcionar a las redes de sincronización WR mecanismos para incrementar la tolerancia a fallos y así evitar puntos únicos de error en topologías de red en anillo. Esto requiere la implementación de mecanismos de conmutación para cambiar de una fuente primaria de sincronización a una de respaldo (backup), los cuales son también descritos en esta parte del documento. Del mismo modo, describiremos los mecanismos de redundancia desarrollados para garantizar la distribución y recepción de datos, incrementando así la disponibilidad de los servicios proporcionados en la red y reduciendo la latencia de transmisión. Finalmente, analizaremos el ancho de banda y la fiabilidad con la que se transmiten dichos datos.

La cuarta y última parte corresponde a la integración de los conceptos anteriormente descritos, tales como pueden ser las implementaciones redundantes y los métodos para incrementar la compatibilidad entre los diferentes elementos que forman un sistema de control distribuido para aplicaciones de misión-crítica sobre redes sincronizadas real. Dicho sistema estará formado por dispositivos de red que integran capacidades redundantes, módulos de adquisición de datos y terminales remotos (RTUs), todos ellos interconectados en una red anillada. Este despliegue incluye la diseminación de una referencia de tiempo duplicada, en la cual se utiliza WR para el núcleo de sincronización de la red, proporcionando la mejor precisión posible (por debajo de 1 ns). Por otro lado, se han utilizado otras soluciones industriales para sincronizar los módulos de adquisición y RTUs, como son el Protocolo de Precisión de Tiempo (PTP) e IRIG-B. Además, los datos se envían a través de la red de forma segura gracias a los canales de comunicación confiables. Finalmente, se ha utilizado una herramienta de seguridad capaz de evaluar los elementos que forman el sistema según su grado de criticidad para así definir

sus niveles de integridad.

This thesis dissertation presents our work with critical distributed applications in industrial network infrastructures. This work focuses on providing all elements on the grid with redundancy features to increase fault tolerance at both local and distributed levels with particular emphasis on timing features.

This dissertation is structured in four parts.

In the first part, we review the state-of-the-art, paying special attention to all the elements that conform a critical distributed system. This section starts with the evolution that safety-critical (SC) systems have experienced during the last years and their adaptation from single to multi-core architectures. Then, the progressive growth of power grid technologies into Smart Grid systems and their relationship with critical applications and their event synchronization needs. Different timing technologies are detailed with particular emphasis in the main one used in this thesis, the White Rabbit technology (WR), which is capable of providing sub-nanosecond accuracies over Ethernet-based networks. Finally, it has been included a brief market survey to compare our contribution to other existing technologies in the market.

In the second part, we review the methods to increase reliability in mixed-critical end-systems using multi-core architectures. We focus on the developed methods to isolate non-critical and critical parts in terms of hardware and software without increasing the certification costs of the system. This deployment is based on an industrial use case that describes an emergency stop of an industrial motor controller, used as proof of concept. This part ends with an analysis of the fault tolerance features of the system due to the implementation of redundant hardware components, safe communication channels and redundant software architectures.

In the third part, we move from inter-core communication problems to inter-processor communication networks. We review the methods to increase reliability, scalability and compatibility in industrial networks, focusing on data and time distribution. We firstly introduce the development of different clocks for the WR technology to increase scalability and industrial compatibility. Later, we describe the methods developed to provide WR timing networks with fault tolerance and single point of failure avoidance in ring topologies. This requires of switchover mechanisms to change from a primary to a backup time reference, which is also described in this part of the text. The same way and for the sake of data transmission, we describe the redundancy mechanisms developed to guarantee data distribution and reception, thus increasing services availability and reducing network latency. Finally, we analyze the bandwidth and reliability of data distribution.

The fourth part corresponds to the integration of all previous concepts, redundant implementations and compatibility methods into a real mission-critical distributed control system over a synchronous network scenario. This system is composed of network devices with redundancy capabilities, acquisition modules and Remote Terminal Units (RTUs) interconnected in a ring network topology. This deployment includes the dissemination of redundant timing references using WR for the core of the network with the best accuracy possible (below 1 ns). Moreover, other industrial timing solutions like the Precision Time Protocol (PTP) and IRIG-B are used for the acquisition modules and RTUs. Data is also exchanged through reliable communication channels. Finally, a safety tool has been used to evaluate all the elements that form the system in terms of their criticality and integrity levels.