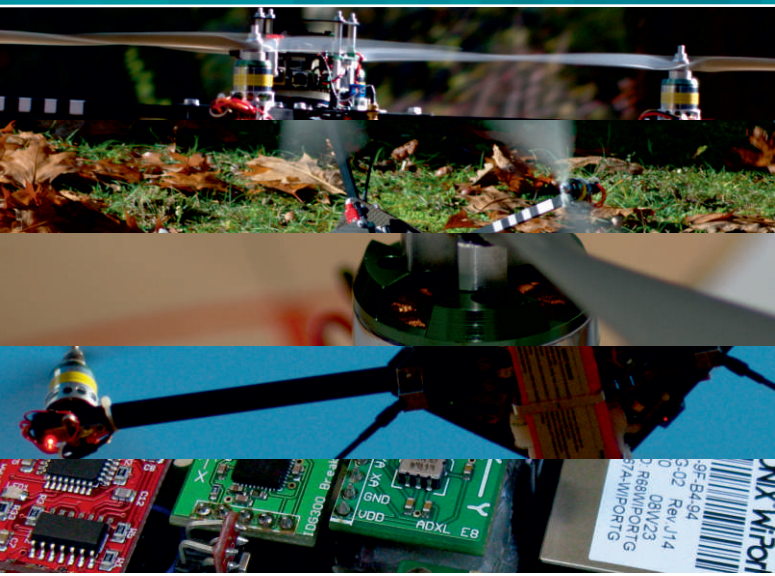
ESI Embedded Systems Institute

The *CoSa* Research Project

The *I4Copter* Real-Time Research Platform



A Research Cooperation:

SIEMENS

CHAIR IN DISTRIBUTED SYSTEMS
AND OPERATING SYSTEMS

ANWENDUNGSZENTRUM esi

Friedrich-Alexander-Universität Erlangen-Nürnberg

The I4*Copter* Demonstrator for Safety-Critical Embedded Systems

SPECIFICATION

The I4*Copter* is a mid-sized model quadrotor helicopter, equipped with fixed pitch propellers and a gearless drive. Its attitude is solely controlled by varying the rotation speed of the engines. Due to its inherently unstable flight characteristics, flight control has to be realised using inertial measurement and digital flight control. Therefore, a quadrotor helicopter is an ideal example of a safety-critical embedded real-time system.

MOTIVATION

The I4*Copter* has been designed and developed to resemble embedded real-time systems as employed in real-world industrial scenarios. Therefore, it uses an Infineon TriCore® TC1796 microcontroller commonly used in automotive ECUs and a custom-made sensor periphery board featuring a wide range of sensors (12 in total) with a variety of interfaces (analog, digital, SPI and RS232).

SYSTEM ARCHITECTURE

The system itself has been developed within the *CoSa* research project. Continually evolving since 2007 the I4*Copter* is available in its 4th generation. In total, the application comprises over 26.000 LOC, is written in C++ and features a component-style architecture with high coherency and minimal coupling among the components.

REAL-TIME PROPERTIES

There are periodical (e.g., flight control) and sporadic (e.g., wireless remote control) real-time tasks with firm as well as hard deadlines. The tasks are executed by HighTec's PXROS-HR or alternatively by our CiAO research real-time operating system.

COMPONENT ISOLATION

The components are isolated using the hardware memory protection offered by the TriCore® mircocontroller; an important feature in embedded real-time systems.

HIGH TEC

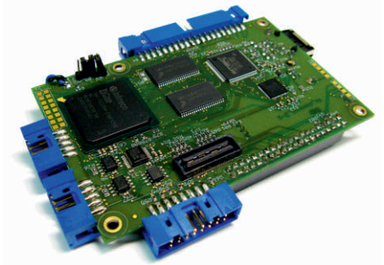
CHAIR IN DISTRIBUTED SYSTEMS AND OPERATING SYSTEMS

SIEMENS

TriCore® power for the I4*Copter*

The *CoSa* Project

Component Architecture for Safety-Critical Embedded Systems



HighTec EasyRun TC1796 Evaluation Board

EASYRUN BOARD

Ready to fly - HighTec's EasyRun board perfectly fits the I4*Copter*'s needs:

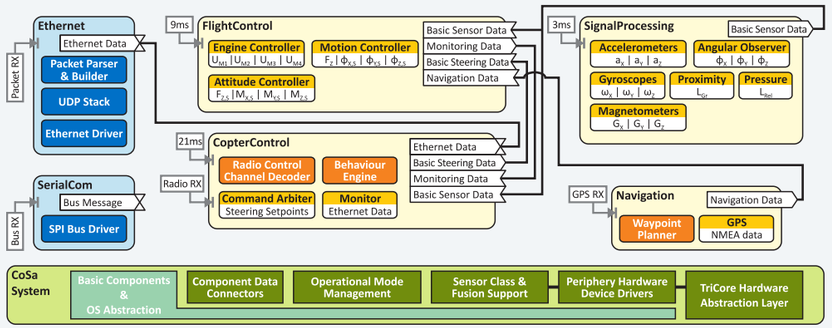
- Infineon TriCore® TC1796 with 150MHz
- Ethernet 100 MBit Full Duplex
- 1 MB MRAM (35ns access time)
- Small form factor and weight

PXROS-HR RTOS

The real-time operating system PXROS-HR enabled fast and efficient development and deployment of the I4*Copter*'s control and application tasks due to its isolation features and the built-in support for the EasyRun board. :

- PXROS-HR manages the MPU for encapsulating data, stack and messages of each task and thus supports component-based design
- Ethernet communication integration (PXtcp)
- Easy-to-use task tracing using PXview and PXmon

PXROS-HR
embedded safety



Component-Based Real-Time System Architecture
(using the example of the I4Copter application)

OVERVIEW

The *CoSa* project addresses various aspects of safety-critical embedded systems development. The primary focus is on component-based architectures and the dependable operation of embedded real-time applications. Here, the I4*Copter* is used as a platform for evaluation and demonstration of the research concepts.

COMPONENT ARCHITECTURE

The *CoSa* component architecture targets safety-critical embedded systems with respect to real-time and dependability properties as well as resource restrictions common in this domain.

The actual implementation is based on a light-weight C++ template programming framework combined with high-level real-time modelling using the MARTE UML profile.

REAL-TIME ANALYSIS

Model-driven real-time analysis in existing systems: We propose an approach for modelling existing real-time systems using the MARTE UML profile. This way they can benefit from model-based analysis techniques without the need to switch to a fully-fledged MDD approach.

- Reverse engineering of an existing code base
- Extraction of explicit real-time properties using existing analysis tools (e.g., WCET analyser)
- Modelling of implicit real-time properties
- Real-time analysis using MARTE-enabled tools

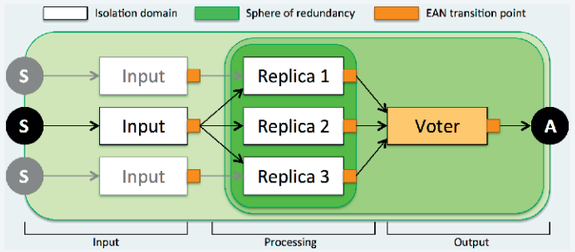
SOFT ERROR RESILIENCE

Due to the continuing miniaturization of hardware, soft errors caused by temporal hardware faults (i.e., bit flips in memory, data caches or processor registers) are increasingly becoming a major threat for safety-critical embedded systems.

The ***CoRed*** (Combined Redundancy) approach is tuned to provide a holistic, dependable and easy to use approach to provide resilience against soft errors at the application level. It features an input to output protection by using a combination of redundant execution and encoded processing. ***CoRed*** does not require specific knowledge about the application and is hardware independent.

Combined Redundancy Approach:

- Hardware redundancy and sensor fusion on input
- Temporal and spatial component isolation
- Triple execution of processing components
- Algorithmic output protection
- Easy-to-use modelling and implementation



Redundant Execution of the I4Copter Flight-Control

WEB

http://www4.informatik.uni-erlangen.de/Research/**I4Copter**
http://www4.informatik.uni-erlangen.de/Research/**CoSa**

CONTACT

Dipl.-Inf. Peter Ulbrich
Chair in Distributed Systems and Operating Systems
Friedrich-Alexander University Erlangen-Nuremberg
Tel. +49 (0) 9131 / 85-27906
E-mail Peter.Ulbrich@informatik.uni-erlangen.de

Dr. Reiner Schmid
Systems Architecture and Platforms
Siemens Corporate Technology, Munich
Tel. +49 (0) 89 / 636-53504
E-mail Reiner.Schmid@siemens.com

Dipl.-Ing. Mario Cupelli
HighTec EDV-Systeme GmbH, Saarbrücken
Tel. +49 (0) 681 / 926-1337
E-mail Mario.Cupelli@hightec-rt.com

Dr.-Ing. Torsten Klie
Embedded Systems Institute
Friedrich-Alexander University Erlangen-Nuremberg
Tel. +49 (0) 9131 / 85-25151
E-mail klie@esi.uni-erlangen.de

Picture credits: Peter Ulbrich, Florian Franzmann (FAU Erlangen); HighTec; Siemens
Layout: Peter Ulbrich, FAU Erlangen, 2011

HIGH TEC

SIEMENS