FP7-ICT-2013- 10 (611146) **CONTREX**

Design of embedded mixed-criticality CONTRol systems under consideration of EXtra-functional properties

Project Duration	2013-10-01 – 2016-09-30	Type	IP

	WP no.	Deliverable no.	Lead participant
	WP7	**D7.2.3**	**OFFIS**

Final Publishable Summary Report

Prepared by	**Kim Grüttner (OFFIS)**
Issued by	**OFFIS**
Document Number/Rev.	**CONTREX/OFFIS/D7.2.3/0.9**
Classification	**CONTREX Public**
Submission Date	**2016-11-20**
Due Date	**2016-09-30**

Project co-funded by the European Commission within the Seventh Framework Programme (2007-2013)

©Copyright 2016 OFFIS e.V., STMicroelectronics srl., GMV Aerospace and Defence SA, Vodafone Automotive SpA, Eurotech SPA, Intecs SPA, iXtronics GmbH, EDALab srl, Docea Power, Politecnico di Milano, Politecnico di Torino, Universidad de Cantabria, Kungliga Tekniska Hoegskolan, European Electronic Chips & Systems design Initiative, ST-Polito Societa’ consortile a r.l., Intel Corporation SAS.

This document may be copied freely for use in the public domain. Sections of it may be copied provided that acknowledgement is given of this original work. No responsibility is assumed by CONTREX or its members for any application or design, nor for any infringements of patents or rights of others which may result from the use of this document.

Project duration:	2013-10-01 – 2016-09-30	**Contract no:**	FP7-611146
Title:	Design of embedded mixed-criticality CONTRol systems under consideration of Extra-functional properties		
Acronym:	CONTREX		
Project website:	https://contrex.offis.de		
List of Contractors:	**Name:**	**Short name:**	**Country:**
	OFFIS e.V.	OFFIS	Germany
	STMICROELECTRONICS SRL	ST-I	Italy
	GMV AEROSPACE AND DEFENCE SA UNIPERSONAL	GMV	Spain
	Vodafone Automotive SpA	VOD	Italy
	EUROTECH SPA	EUTH	Italy
	INTECS SPA	INTECS	Italy
	iXtronics GmbH	iX	Germany
	EDALab srl	EDALab	Italy
	DOCEA POWER	DOCEA	France
	POLITECNICO DI MILANO	POLIMI	Italy
	POLITECNICO DI TORINO	POLITO	Italy
	UNIVERSIDAD DE CANTABRIA	UC	Spain
	KUNGLIGA TEKNISKA HOEGSKOLAN	KTH	Sweden
	EUROPEAN ELECTRONIC CHIPS & SYSTEMS DESIGN INITIATIVE	ECSI	France
	ST-POLITO Societa' consortile a r.l.	ST-POLITO	Italy
	Intel Corporation SAS	INTEL	France
Contact:	Kim Grüttner OFFIS - R&D Division Transportation Escherweg 2 - 26121 Oldenburg - Germany Phone/Fax.: +49 441 9722-228/-278 E-Mail: contrex-mgt@offis.de		

Summary description of project context and objectives:

Up to now, mission & safety critical services of SoS (Systems of Systems) have been running on dedicated and often custom designed HW/SW platforms. In the near future, such systems will be accessible, connected with or executed on devices comprising off-the-shelf HW/SW components. Significant improvements have been achieved supporting the design of mixed-critical systems by developing predictable computing platforms and mechanisms for segregation between applications of different criticalities sharing computing resources. Such platforms enable techniques for the compositional certification of applications' correctness, run-time properties and reliability.

CONTREX will complement these important activities with an analysis and segregation along the extra-functional properties real-time, power, temperature and reliability. These properties will be a major cost roadblocks when

1. scaling up the number of applications per platform and the number of cores per chip,
2. in battery powered devices or
3. switching to smaller technology nodes.

CONTREX will enable energy efficient and cost aware design through analysis and optimisation of real-time, power, temperature and reliability with regard to application demands at different criticality levels. To reinforce European leadership and industrial competiveness the CONTREX approach will be integrated into existing model-based design methods that can be customized for different application domains and target platforms. CONTREX will focus on the requirements derived from the automotive, aeronautics and telecommunications domain and evaluate its effectiveness and drive integration into existing standards for the design and certification based on three industrial demonstrators. Valuable feedback to the industrial design practice, standards, and certification procedures is pursued.

Our economic goal is to improve energy efficiency by 20 % and to reduce cost per system by 30 % due to a more efficient use of the computing platform.

CONTREX Methodology:

Figure 1shows on overview of the CONTREX methodology for the design of mixed critical systems under consideration of extra-functional properties. Part of the elements shown have been available even before the project started. On one hand, that are inputs for the design flow depicted in the upper part of the figure such as system models from previous model driven design flows and existing legacy hardware or software components. On the other hand, there are various hardware platforms on-hand, e.g., the Xilinx ZYNQ platform or the iNemo platform provided by ST, as well as techniques to measure the timing, power, and temperature behaviour of physically available devices. In between, we have user software, middle-ware components such as the Kura framework, and operating systems with runtime and resource management. The CONTREX project fills this flow in three aspects: Model capturing and timing analysis, functional and extra-functional analysis, and design validation.

For the model-capturing, existing meta-models are extended to support the specification of criticalities as well as extra-functional properties. The integration of these models into the ForSyDe framework allows analytical design space exploration for timing. The functional and extra-functional analysis part is extended to enable simulative design space exploration under consideration of power and temperature properties. To do so, virtual platforms are set up with hardware and communication models and enriched with models for timing, power, batteries, and temperature as well as infrastructure for the runtime-monitoring of these

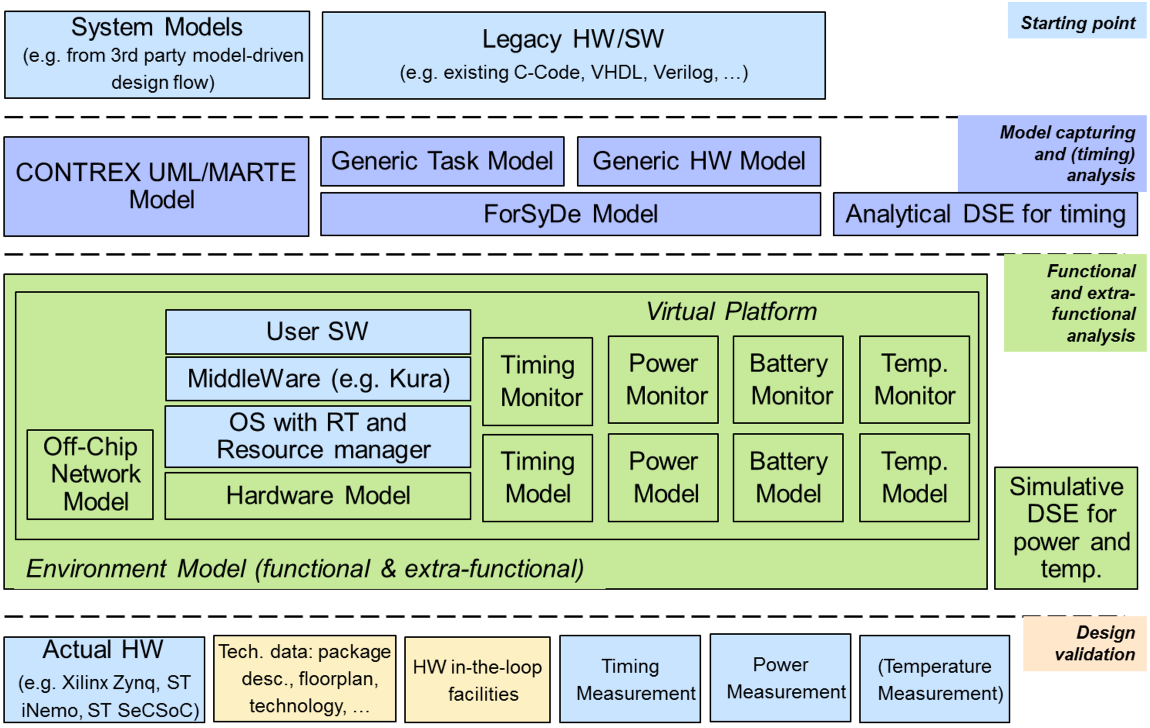
Starting point
System Models
(e.g. from 3rd party model-driven design flow)
Legacy HW/SW
(e.g. existing C-Code, VHDL, Verilog, …)
Model capturing and (timing) analysis
CONTREX UML/MARTE Model
Generic Task Model
Generic HW Model
ForSyDe Model
Analytical DSE for timing
Functional and extra-functional analysis
Virtual Platform
User SW
MiddleWare (e.g. Kura)
OS with RT and Resource manager
Hardware Model
Off-Chip Network Model
Timing Monitor
Power Monitor
Battery Monitor
Temp. Monitor
Timing Model
Power Model
Battery Model
Temp. Model
Simulative DSE for power and temp.
Environment Model (functional & extra-functional)
Design validation
Actual HW
(e.g. Xilinx Zynq, ST iNemo, ST SeCSoC)
Tech. data: package desc., floorplan, technology, …
HW in-the-loop facilities
Timing Measurement
Power Measurement
(Temperature Measurement)

Figure 1: CONTREX Methodology Overview

properties. They can be connected to environment models to stimulate simulation experiments. To complete the flow, technical data of the platforms such as IC package descriptions, floorplans, or technology information, as well as hardware-in-the-loop facilities are added to perform more detailed design validation.

The flow has been evaluated by the use of three demonstrator applications: An unmanned aerial vehicle, an automotive telematics device, and a telecom system (Ethernet-over-Radio).

A description of the main S&T results/foregrounds

The main results of the CONTREX project are:

1) A **meta-model for the design and analysis of mixed-critical systems**, covering the functional, logical, technical, and geometrical perspectives; system, virtual resource, runtime, and platform abstraction levels; and behaviour, time, power, and temperature viewpoints.

   An extension of UML/MARTE with support for

   - extra-functional properties (EFPs) at system inputs/outputs and application, platform and system level;
   - criticalities (represented as a number) that are associated to components, to EFPs and to performance requirements;
   - and a deployment view for distributed systems.

   has been realized.

2) A **deployment and mapping of control applications** to a network of virtualized hardware/software platforms and network infrastructure abiding extra-functional properties.

An Eclipse Plug-in (CONTREP) that supports the CONTREX meta-model (extended UML/MARTE) has been developed. CONTREP can be used for the overall mixed-criticality system development process: specification, modelling, analysis and target code generation. Tools for static model (consistency) analysis, schedulability analysis (MAST), model execution for functionality, timing and power consumption testing (VIPPE), joint analytical and simulative design-space exploration (JSA-DSE), and target platform code generation (software synthesis) have been successfully integrated. The resulting CONTREX modelling and analysis framework is depicted in Figure 2.

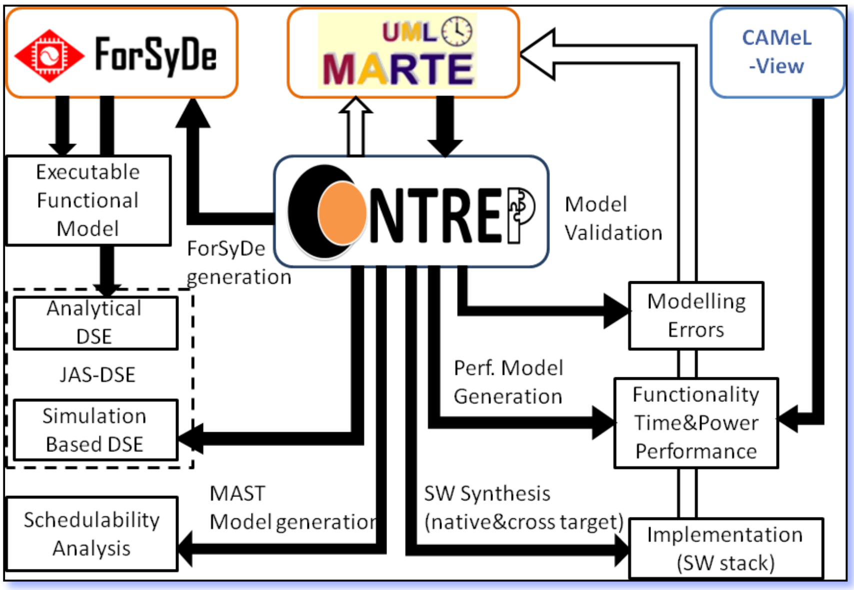

Figure 2: The CONTREX modelling and analysis framework

3) An (service-based) **executable and analysable power and temperature model for multi-core execution platforms**.

A virtual platform has been equipped with a power and a temperature model. Figure 3 depicts the overall CONTREX power and temperature simulation and analysis framework. Activity traces from a virtual platform that executed the target platform software are collected as a timed trace and processed by a platform specific power model. The spatial distribution of the power consumption is reconstructed in a power map, where the power consumption is annotated at its hardware component location in the chip's floorplan. For the temperature simulation, a thermal model of the chip's package (considering the different material layers), is generated using the Thermal Profiler from Docea. The spatial power distribution over time that is represented in the power map and the thermal profile of the chip package is used to run a temperature simulation by using the Aceplorer tool from Docea. The results is a temperature map of the chip and a temperature over time trace.

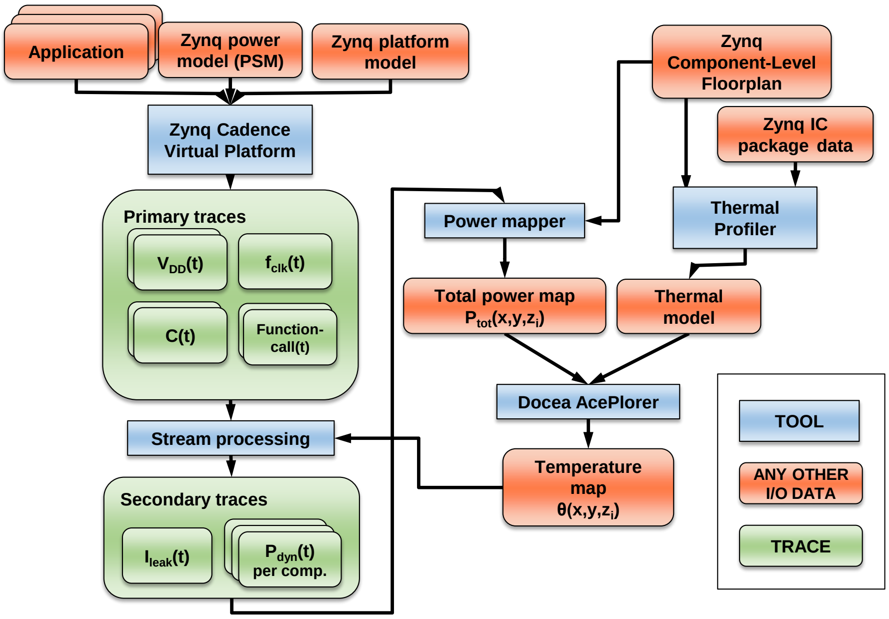

Figure 3: The CONTREX power and temperature simulation and analysis framework

The CONTREX power and temperature analysis framework is independent from the used simulation and analysis tools. The following different simulation and analysis tools have been successfully used within the same framework:

- Virtual Platform: Cadence Virtual Platform, Open Virtual Platform, SystemC
- Power Model: Power State Machines, Performance Counter based power calculation
- Thermal Profiling: Docea Thermal Profiler, SystemC-AMS
- Temperature Simulation: Docea Aceplorer, C++

The CONTREX power and temperature simulation framework can be used in two different modes:

- Offline analysis: Activity traces are recorded. Power state machines can be generated from collected traces. Power and temperature analysis is performed after the simulation
- Online analysis: Activity traces are collected and analysed when enough data has been collected. This mode supports a temperature- dependent static power analysis and the verification of adaptive polices based on software access to power and temperature virtual sensors.

4) A **run-time resource management** taking into account local and distributed power and temperature monitoring and control techniques.

For the management of resources at run-time a new lightweight (low complexity, no operating system required and low memory footprint) resource has been developed. This BBQLite run-time resource manager is depicted in Figure 4.

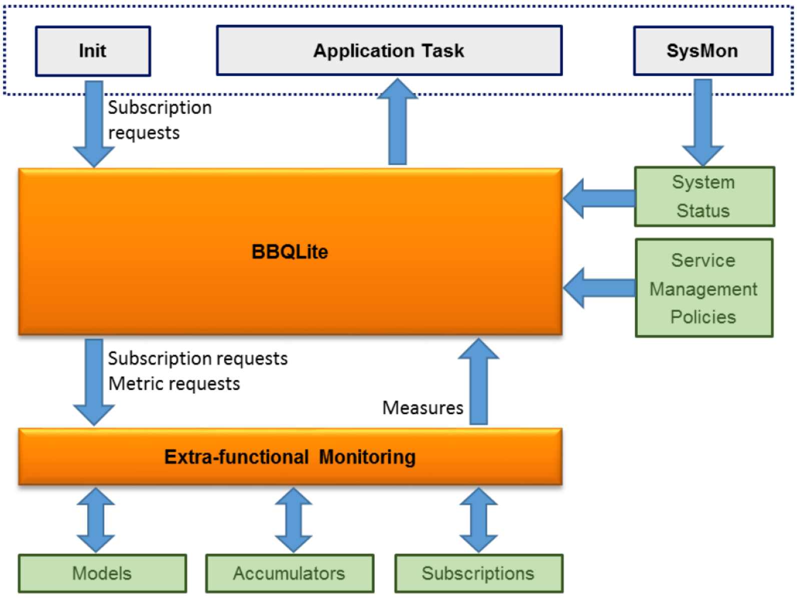

Figure 4: The CONTREX run-time resource management framework

The operation condition profiles for BBQlite are derived at design time (e.g. by the application of the CONTREX power and temperature simulation framework). The offline pre-computed resource management decisions are taken based on 1) the functional status (e.g. operation mode of the device), 2) extra-functional status (metrics exposed by extra-functional monitoring and information obtained from power sensors, temperature sensors and the battery status), 3) design-time configurations (derived from expert knowledge of simulation results).

5) The successful **demonstration of a seamless integration of mixed criticalities under consideration of extra-functional power and temperature properties** (combining 1, 2 and 3) **in three different domains**: avionics, automotive telematics, and telecommunications.

Avionics: The avionics demonstrator concerns a subset of the Flight Control Computer (FCC) software developed for a medium sized Remotely Piloted Aircraft (RPA) applicable for surveillance missions such as damage assessment and intelligence. A further avionics application, a multi-rotor system, is developed. It implements the safety-, mission- and non-critical functions of a civilian UAV in a single Multi-Processor on Chip. Gained benefits are improvements of the current techniques for extra-functional budget analysis resulting in improved weight, power, size, and waste heat dissipation.

Automotive Telematics: This demonstrator provides private and/or fleet vehicle drivers with a support service in case of accident. The architecture is based on three main components: a sensing unit for acceleration measurements, a localization unit for GPS reading and a data processing and communication system for identification of accidents and communication of position data to either public authorities (hospital, police) or private support providers. CONTREX results help to improve performance, energy efficiency, and cost of the system.

Telecommunications: The Telecom demonstrator is based on the Ethernet Over Radio System. It is specifically designed and engineered for such situations where E1 signal transportation is required. It allows a smooth transition with the past generation of transport (PDH) networks, encapsulating the E1 signal into an Ethernet frame. Furthermore, it is particularly suited to cover mobile broadband infrastructure data growth from GSM to WDCMA to LTE and many other needs of high data transport. It is composed of two units: Indoor Unit and Outdoor Unit, connected by a POE GE cable (100-300 m). It is a naturally mixed critical scenario. Guarantee of timing requirements under optimization of power consumption and temperature maps of the hosting equipment, as well as installation weight and space footprint, is essential. The new CONTREX techniques for global optimization over the entire installation greatly enhance cost/performance characteristics.

6) **Proposals and feedback to standard and certification bodie**s in the area of model-based mixed-critical system design, MPSoC power and temperature simulation & analysis, and power and temperature management architectures.

   In particular the following standardization efforts have been successfully conducted:
   - The UML/MARTE criticality extension has been raised to the Object Management Group (OMG) the UML standardization body.
   - Tracing of arbitrary and explicit physical quantities through timed value stream has been presented to the Accellera Initiative's SystemC Core Language group. The technical infrastructure for an efficient implementation of this extra-functional tracing has been implemented in the latest version of the Accellera SystemC proof-of-concept simulator.

The following software tool have been improved and extended within the project to support extra-functional properties and mixed criticalities:

- Commercial tools:
  - SCNSL (https://sourceforge.net/p/scnsl/wiki/Home/) and HIFSuite (http://www.hifsuite.com/) [EDALab]
  - Kura Middleware (http://www.eclipse.org/kura/) [Eurotech]
  - Cloud Platform (https://www.eurotech.com/en/products/software+services/everyware+device+cloud) [EUROTECH]
  - Aceplorer and Thermal Profiler (http://www.doceapower.com/) (Intel, Docea Power)
  - CamelView (http://www.ixtronics.de/3/index.html) [iXtronics]
  - iNemo (http://www.st.com/en/mems-and-sensors/inemo-inertial-modules.html?querycriteria=productId=SC1448) and SeCSoC platforms (ST)
- Academic tools:
  - UML/Marte framework (http://contrep.teisa.unican.es/) and VIPPE simulator (http://vippe.teisa.unican.es/) [UC]
  - ForSyDe framework (https://forsyde.ict.kth.se/trac/wiki/WikiStart) [KTH]
  - Battery models and monitors [PoliTo]
  - SystemC tracing framework [OFFIS]
  - BBQLite Runtime & Resource Manager (http://bosp.dei.polimi.it/) [PoliMi]

Exploitation and success stories

NAME

UML-MARTE based modelling, analysis and simulation of a mixed-criticality avionics platform

DESCRIPTION

CONTREX provides an integrated design flow for system modelling, model-based analysis, simulation and Design Space Exploration (DSE), as well as an integrated toolset that automates many of the aforementioned activities. This way, it provides the necessary means for early assessment of system performance and efficient exploration of wide design spaces, thus enabling to find optimal configurations that minimize cost, size, weight and power consumption, without compromising safety and overall performance.

IMPACT

The CONTREX integrated flow has been assessed in its applicability to the tailoring of existing Flight Control Computer systems to future avionics solutions for light remotely piloted aircraft platforms, based on all-purpose commercial MPSoC platforms. A significant advance in knowledge about current techniques on analysis, modelling and design space exploration as well as a set of relevant evaluation figures have resulted from the work performed during CONTREX. Additionally, an avionics demonstrator platform has been developed to serve as prototype for future commercial avionics platforms.

Contact information: mclomba@gmv.com, villar@teisa.unican.es

NAME

An experimentation platform for mixed-criticality avionics architectures for multi-rotor system

DESCRIPTION

The experimental platform consist of a commercial multi-rotor chassis with a custom designed mixed-criticality avionics hardware platform based on the Xilinx Zynq SoC. On the system, the safety-critical flight control and stabilizing algorithm and a non-critical video capturing and object-tracking algorithm are implemented. The system comes with an OVP-based virtual platform for functional and power validation of the integrated system based on a co-simulation with a flight simulator based on the CAMeLView tool.

IMPACT

The experimentation platform is fully extensible and can be used as a research vehicle or industrial pre-study for the assessment of future mixed-critical avionics platform. The CONTREX multi-rotor platform is used as demonstrator for different studies of mixed criticality systems in the EMC2 and SAFEPOWER project. The platform will be made fully available to the public within the SAFEPOWER project.

Contact information: soeren.schreiner@offis.de, kim.gruettner@offis.de

NAME

Insurance telematics for reduced cost of ownership

DESCRIPTION

Telematics boxes for vehicles mainly monitor the driver journey and his driving style. They typically include a sensing unit installed on the car for acceleration/orientation measurements, a GPS unit and a data processing and communication module. The main benefit up to now is to obtain a discount on the car insurance fee. At present, companies provide private and/or fleet vehicle drivers with a support service in case of accident. Vodafone Automotive in cooperation with the CONTREX automotive use case team extended such scenario to cover the following topics: 1) Enhanced and semi-automated accident classification and reporting, with a reconstruction of the crash dynamics. 2) Real-time analysis of driver behaviour and crash severity. 3) Extraction of features on the driving style. 4) Extreme low energy requirements. 5) Recognition of low energy crashes. 6) Filtering of false positives. 7) Self-calibration of the device orientation.

IMPACT

It is now possible to analyse low energy crashes even when the engine is switched off for months. This is a totally new feature that is added to the Vodafone automotive product portfolio. This feature will be activated both on new products and 200k devices already on the fieldby the end of 2016. A complete new 1-2 years roadmap has been opened starting from CONTREX, to introduce the low energy events detection also at key-on. Improved crash management and advances in terms of power consumption, enable conceiving a black box for the motorbike. The Vodafone goal is to be the first player with a real product, with the possibility to multiply the number of customers by a factor of 2. Some members of the POLIMI team have created a start-up in July 2017, to work with Vodafone Automotive on the development of a new product for the motorbike market. The algorithms for crash detection have been reused to develop a pilot product for the rally cross racing market in order to collect telemetry and crash information to be shown during a television live broadcast.

Contact information: luca.ceva@vodafonetelematics.com, william.fornaciari@polimi.it

NAME

A multiservice gateway as IoT enabling technology & Eclipse Kura IoT Platform

DESCRIPTION

The EUTH Minigateway is the prototype of a compact size multiservice gateway oriented to IoT and M2M application in the industrial and automotive domains. It is an industrial grade smart device targeting low cost and low power applications. It provides full support to the Kura framework for M2M platform integration and services applications. Kura IoT is a Java/OSGi-based framework for IoT gateways. It is an open-source Eclipse project and, currently the most downloaded project of the Eclipse IoT initiative. The prototype has been adopted in the CONTREX automotive use-case as a vehicle control unit in charge of controlling and monitoring the sensing devices in the vehicle, collecting/elaborating the data of vehicle crashes and storing data on the cloud.

IMPACT

The EUTH Minigateway prototype inspired a new family of low cost industrial grade gateways, called ReliaGate. It will be available for sale in the fourth quarter of 2016. The ESF (Everyware Software Framework) is a commercial, enterprise-ready edition of Eclipse Kura. ESF adds advanced security, diagnostics, provisioning, remote access and full integration with Everyware™ Cloud, Eurotech's IoT Integration Platform. The exploitation of R&D activities performed on Kura allowed developing a new version of ESF that will be available from the fourth quarter of 2016.

Contact information: paolo.azzoni@eurotech.com

NAME

Virtual platform introduction for the development of telecommunication equipment

DESCRIPTION

Ethernet over Radio is part of a family of important bridging technologies that occupy a significant niche in telecom service linking and migration. Central functionalities like Automatic Transmit power Control and adaptive modulation can vary power and bitrate according to signal-to-noise ratio to provide both low-grade (e.g. POTS) and high-grade connections (e.g. emergency response). However, their highly dynamic behaviour has made it difficult to capture and analyse power and thermal characteristics (an important factor in the commercial offering), leading to budget and time overruns. The CONTREX Virtual Platform has introduced a new simulation environment making it possible to obtain reliable, fine-grained traces of power and thermal evolution and iteratively perfecting these extra-functional characteristics before committing to the final platform in silicon. In addition, the simulation environment of the Virtual Platform is aiding the transition to more powerful multicore technologies used in the higher end of the wireless bridging product families.

IMPACT

The provision of the Virtual Platform is enabling Intecs to seek opportunities in emerging telecom markets that use adaptive transmission functionality, including Long-Term Evolution (LTE) base stations that offer wireless backhaul linking of traffic to the core network, but must offer lower power consumption to be competitive. In addition, Intecs is pursuing opportunities in the growing market for broadband introduction to Class C & D zones of Europe where fibre is considered uneconomical, but Ethernet over Radio can bridge from the core network to the street cabinet and permit reuse of the existing copper infrastructure with VDSL technologies.

Contact information: silvia.mazzini@intecs.it, kim.gruettner@offis.de, info@edalab.it