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

Kim Grüttner [a,*], Ralph Görgen [a], Sören Schreiner [a], Fernando Herrera [b], Pablo Peñil [b], Julio Medina [b], Eugenio Villar [b], Gianluca Palermo [c], William Fornaciari [c], Carlo Brandolese [c], Davide Gadioli [c], Emanuele Vitali [c], Davide Zoni [c], Sara Bocchio [d], Luca Ceva [e], Paolo Azzoni [f], Massimo Poncino [g], Sara Vinco [g], Enrico Macii [g], Salvatore Cusenza [h], John Favaro [h], Raúl Valencia [i], Ingo Sander [j], Kathrin Rosvall [j], Nima Khalilzad [j], Davide Quaglia [k]

[a] *OFFIS – Institute for Information Technology, Oldenburg, Germany*
[b] *University of Cantabria, Santander, Spain*
[c] *Politecnico di Milano, Italy*
[d] *STMicroelectronics, Italy*
[e] *Vodafone Automotive Telematics, Switzerland*
[f] *Eurotech, Italy*
[g] *Politecnico di Torino, Italy*
[h] *Intecs, Italy*
[i] *GMV, Spain*
[j] *KTH Royal Institute of Technology, Stockholm, Sweden*
[k] *EDALab s.r.l., Italy*

The increasing processing power of today's HW/SW platforms leads to the integration of more and more functions in a single device. Additional design challenges arise when these functions share computing resources and belong to different criticality levels. CONTREX complements current activities in the area of predictable computing platforms and segregation mechanisms with techniques to consider the extra-functional properties, i.e., timing constraints, power, and temperature. CONTREX enables energy ef- ficient and cost aware design through analysis and optimization of these properties with regard to ap- plication demands at different criticality levels. This article presents an overview of the CONTREX European project, its main innovative technology (extension of a model based design approach, functional and extra-functional analysis with executable models and run-time management) and the final results of three industrial use-cases from different domain (avionics, automotive and telecommunication).

1. Introduction

Up to now, mission & safety critical services of electronic 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 to reduce development costs. A basic requirement for this is the absence of interference among applications of different criticalities sharing computing resources. Significant improvements have been achieved supporting the design of mixed-critical systems by developing predictable computing platforms and mechanisms for segregation. Such platforms enable techniques for the compositional certification of applications' correctness, run-time properties and reliability.

The CONTREX European project [1] complements these important activities with an analysis and segregation along specific extra-functional properties: real-time, power, and temperature. These properties will be a major cost roadblock when

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

CONTREX enables energy efficient and cost aware design through analysis and optimization of real-time, power, and temperature with regard to application demands at different critical-

* Corresponding author.
E-mail address: kim.gruettner@offis.de (K. Grüttner).

Published Journal Article available at: http://dx.doi.org/10.1016/j.micpro.2017.03.012

ity levels. To reinforce European leadership and industrial competitiveness the CONTREX approach is integrated into existing model-based design methods that can be customized for different application domains and target platforms. CONTREX focuses on requirements derived from the automotive, aeronautics, and telecommunication domains, evaluates their effectiveness, and drives integration into existing standards for 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 and to reduce cost per system due to a more efficient use of the computing platform.

The CONTREX consortium consists of fifteen partners from six countries. There are six academic institutions (OFFIS, Politecnico di Milano, Politecnico di Torino, University of Cantabria, KTH, and ST-PoliTo), six industrial tool (iXtronics, EDALab, Intel Docea Power) or technology providers (STMicroelectronics and EUROTECH), three industrial demonstrator application providers (GMV, Vodafone Automotive and Intecs), and ECSI. The project started in October 2013 and ended in September 2016.

This article is an extended version of [2] with the following new contributions:

- update with the final results (references to deliverables and recently published papers) of the project
- presentation of evaluation results of the industrial use-cases.

The article is organized as follows: Section 2 provides a some background information on mixed-criticality systems and the associated challenges addresses by the CONTREX project. Section 3 gives an overview of the CONTREX methodology and the demonstrator applications. In the following three sections, the main technical results and contributions of the project are described in more detail: Section 4.1 describes the specification and modeling of extra-functional properties and criticalities in UML-MARTE, Section 5 describes the simulation and analysis of the power consumption and temperature, and Section 6 describes the consideration of power, energy and temperature at run-time. In Section 7 the tools and methods are applied and evaluated on three industrial use-cases. Section 8 closes the paper with a conclusion and summary.

2. Mixed-criticality systems: background and addressed challenges

To close the identified technology gap between custom designed mission- and safety-critical systems and cost-efficient platforms for consumer systems, the main goal of the project is to combine

- platform independent models for (control) applications with different criticalities, represented in domain specific modeling languages and formalisms,
- management and abstraction of multi-core hardware platforms' shared resources to guarantee temporal and spatial segregation for mixed-critical applications,
- management and abstraction of communication network resources to support temporal and spatial segregation to enable system-wide deployment and modularization in networked control applications, and
- cloud infrastructure abstraction and management techniques to support integration with data fusion/filtering for overall monitoring and online optimization of distributed large-scale control systems

with management and control of extra-functional properties, like power and temperature. These properties will limit the capabilities and realization of future ambient intelligent systems with regard to overall energy consumption, mobility (due to limited battery capacities), waste heat discharge, and finally reliability and availability. For this reason, the CONTREX project extends the industrial state-of-the-art in mixed-criticality system design through a holistic design approach that considers extra-functional constraints as first-class citizens. It will represent and expose extra-functional properties under existing segregation and certification techniques (both in the design phase and during system operation), and finally include these properties into local (on the device/network node) and global (information exchange using cloud infrastructure) scheduling and control decisions.

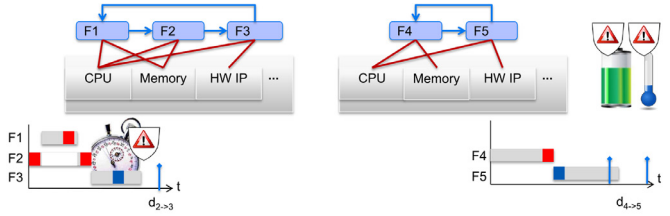
The main goal of the project is to enable cost-efficient design, modeling, analysis, simulation, and exploration of complex networked control systems with mixed-criticality on different levels of abstraction. The project targets a meet-in-the-middle approach for the integration of existing design environments, models, and analysis and simulation tools. The project will extend the state-of-the-art in domain specific control system modeling (top-down) through:

- Separation of design decisions for control application, deployment and underlying hardware/software architecture at device level [3].
- Formalization, annotation, and refinement of constraints/contracts on extra-functional properties: time, power, and temperature [4] [5].

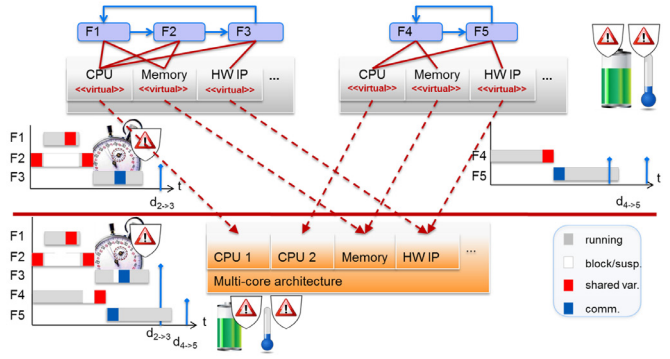
State-of-the-art segregation techniques for shared computing resources (i.e. multi-core systems) cover functional correctness and timing [6], but ignore possible influence and feed-back paths originating from parasitic extra-functional effects [7]. Sharing the same computing platform (as shown in Fig. 1), multiple applications can interfere indirectly through power/energy and temperature properties. Running a hard real-time application and non-timing critical application (best effort) on the same execution platform (e.g. using a static Time Division Multiple Access (TDMA) scheduling), the non-timing-critical application can have an extra-proportional contribution to the overall power consumption. The increased power consumption heats up the whole chip and requires to slow-down (e.g. dynamic voltage and frequency scaling) dedicated cores and the memory subsystem to keep the chip temperature within a range allowing reliable operation. This dynamic reaction to control waste heat and reliability of the chip might have an influence on the core running the hard real-time task. This can be either directly through reducing the clock frequency of the core running the real-time application or indirectly through the effects in the memory subsystem. When designing such systems, all critical applications of the system need to designed with the explicit awareness of possible mode switches due to control of extra-functional properties.
Another example regarding the influence between mixed-critical applications and extra-functional properties can be found in mobile battery powered systems. These systems suffer from limited battery capacities that keep running the system for a determinate amount of time. When running applications with mixed criticalities on mobile platforms the available battery capacity needs to be partitioned among applications and managed at system run-time to keep mission- and safety-critical services running for a determinate time (e.g. to reach the next recharge cycle).

As pointed out, integrating mixed-criticality applications on multi-core and mobile battery-power computing platforms requires additional segregation along extra-functional dimensions, while keeping up classic temporal and special segregation properties.

The project combines top-down (control system modeling) and bottom-up (execution platform modeling) approaches in an integrated design environment establishing a missing link through:



(a) State-of-the-art: Two control applications with different criticalities (left: hard real-time system with strict timing deadline, no power or temperature constraints; right: soft real-time system with no strict deadline, hard power and temperature constraints that might also originate from the systems environment/harsh operating conditions) implemented on two physical separated and/or distributed hardware/-software platforms.



(b) Future mixed-criticality systems: Two independent applications with different criticalities (from Fig. 1a) implemented on a multi-core hardware/software platform that enables temporal and spatial segregation (e.g. through static virtualization using TDMA). CONTREX enables analysis of real-time, power, and temperature properties and to implement segregation techniques regarding power consumption and heat dissipation.

Fig. 1. Mixed-criticality systems now and then.

1. Deployment and mapping of control applications to a network of virtualized hardware/software platforms and network infrastructure abiding extra-functional properties.
2. Simulation infrastructure that scales from detailed subsystem to overall networked control systems, including dynamicity of extra-functional properties.
3. Support for the exploration of different deployment and mapping alternatives to obtain the most cost-efficient solution under the given extra-functional constraints.
4. Cloud services for data acquisition and monitoring of extra-functional properties to obtain an overall health-state of the controlling system and the system under control including the coordination of global compensation actions at run-time.

3. CONTREX methodology overview

Fig. 2 shows an overview of the CONTREX methodology for the design of mixed critical systems under consideration of extra-functional properties (EFP). Some elements of the methodology have been available before the project started, for instance inputs for the methodology like system models from previous and existing hardware or software components shown in the upper part of the figure. In addition, 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 behavior 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 complements this methodology 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. More details about the modeling methodology will be given in Section 4.1 using the avionics demonstrator as an example. 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 in- frastructure for the runtime-monitoring of these properties. These models can be connected to environment models to simulate the entire system. To complete the flow, technical data of the platforms such as IC package descriptions, floor plans, or technology information, as well as hardware-in-the-loop facilities are added to perform more detailed design validation. In Section 5, the virtual platform based simulation and analysis is described by using the telecom demonstrator. Section 6 focuses on the techniques for monitoring and management of extra-functional properties at runtime and their application to the automotive telematics demonstrator.

3.1. Demonstrator applications

The evaluation of the proposed methodology is based on its adoption in three demonstrator applications: a Remotely Piloted Aircraft, a telecom system (Ethernet-over-Radio), and an automotive telematics system.

3.1.1. Avionics demonstrator

The avionic 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. Expected improvements for extra-functional budget analysis will result in reduced weight, power, size, and heat dissipation.

3.1.2. Automotive telematics demonstrator

This demonstrator provides private and/or fleet vehicle drivers with a support service in case of accident. The architecture is based on an end-to-end cloud-based IoT solution that is responsible for data collection, data processing, and automotive services provisioning. In the vehicle the system relies on three main components: a sensing unit for acceleration measurements, a GPS based localization unit, and a data processing and communication unit for identification of accidents and communication of acceleration and position data to the cloud infrastructures, which, in turns, makes such data accessible either to public authorities (hospital, police) or private support providers. CONTREX results help to improve performance, energy efficiency, and cost of the system.

3.1.3. Telecom demonstrator

The Telecom demonstrator is based on the Ethernet-over-Radio System. It is specifically designed and engineered to allow a smooth transition from old digital protocols to new wireless standards up to WDCMA and LTE. It consists of Indoor and Outdoor Units, connected by a Gigabit Ethernet cable which delivers also power. It naturally represents a mixed critical system. Timing guarantees under power and temperature constraints of the hosting equipment, as well as installation weight and space footprint are crucial. The new CONTREX techniques for global optimization over the entire installation greatly enhance cost/performance characteristics.

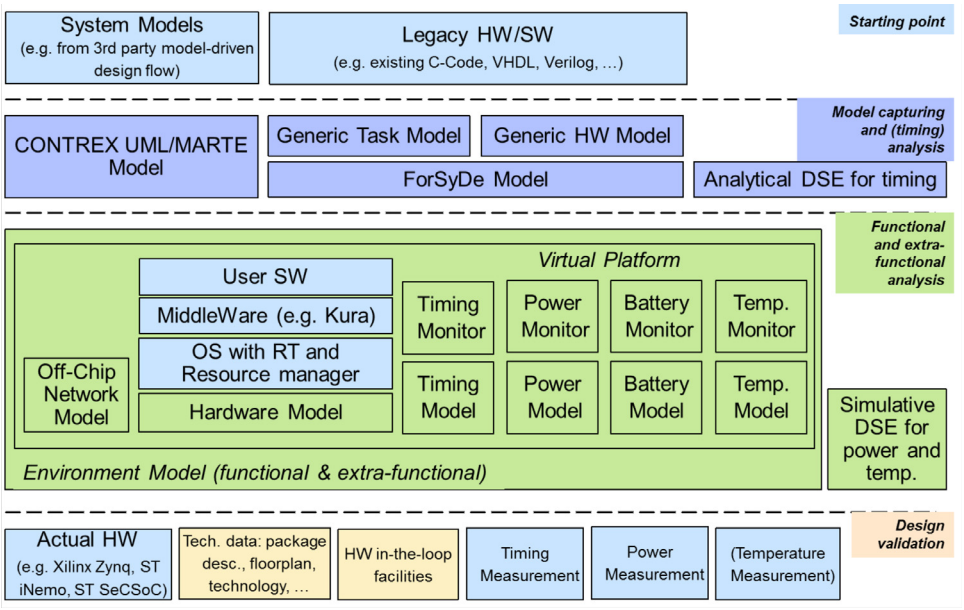


Fig. 2. CONTREX reference architecture.

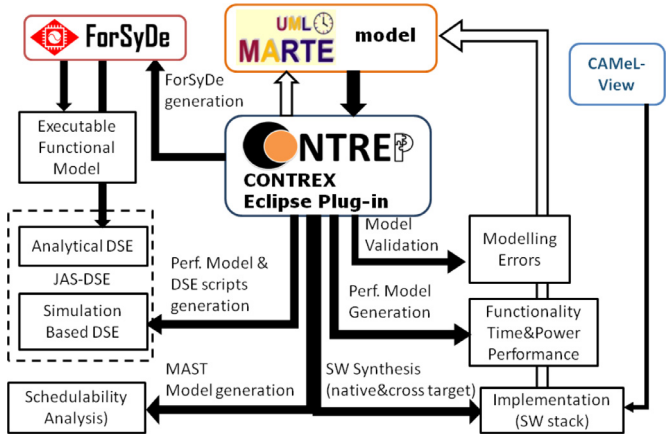


Fig. 3. Languages and design activities in the single-source design approach developed in CONTREX.

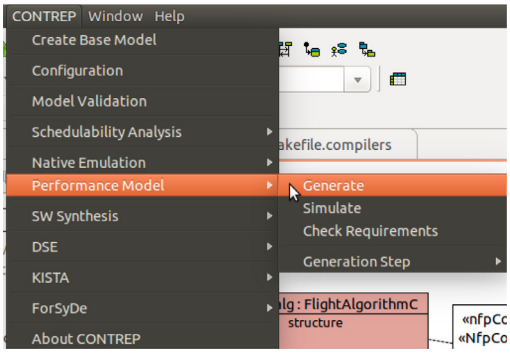


Fig. 4. CONTREP menu (and detail on the automated generation of an executable performance model.

4. Model capturing and analysis

Specifically, CONTREX is providing a design approach covering the aforementioned modeling, analysis, simulation and DSE activities. The main language used in CONTREX for the modeling activity is UML, complemented with the MARTE profile. Moreover, as sketched in Fig. 3, CONTREX connects the UML/MARTE and ForSyDe [8] methodologies, and also relies on CAMeL-View [9] for the capture of complex physical environments, to exercise the simulation-based performance model.

The CONTREX UML/MARTE model captures all the information required for tackling a number of system-level design activities. Thus it is suitable for supporting a *single-source* approach, which leverages the consistency among the different high-level design activities. In CONTREX, a novel single-source, UML/MARTE modeling and design framework, called in short CONTREP (CONTREX Eclipse plug-in) [10] has been developed. Once CONTREP is installed, a specific menu is enabled in the Eclipse-based user front-end (shown in Fig. 4) which facilitates the modeling activity and automates the analysis and design activities shown in Fig. 3.

4.1. Modeling

A former and crucial design activity is a proper capture of the model. CONTREP supports the modeling activity with a model validation facility.

Among the relevant aspects to tackle the challenges mentioned at the beginning of the section, CONTREX supports capturing mixed-criticality in the modeling methodology. A specific novel aspect is the possibility to associate criticalities to extra-functional properties and to requirements on them. This support state-of-the- art and relevant MC modeling and analysis scenarios. Association of criticalities to worst-case execution times (WCET), a specific EFP employed in hard-real time scheduling theory, is required by novel mixed-criticality schedulability analysis algorithms. Association of criticalities to EFP requirements, enables to assign different impor- tance to them in the different analysis activities, as it is illustrated in Section 4.2.

CONTREX proposes a minor extension of the MARTE standard allowing the notation of criticality as a generic attribute which allows the adaptation to different modeling scenarios [11]. This way, the CONTREX UML/MARTE methodology allows to capture criticality and associate it to different model elements. The methodology also supports the annotation of worst-case execution times per criticality, as it is required by recent mixed-criticality schedu-

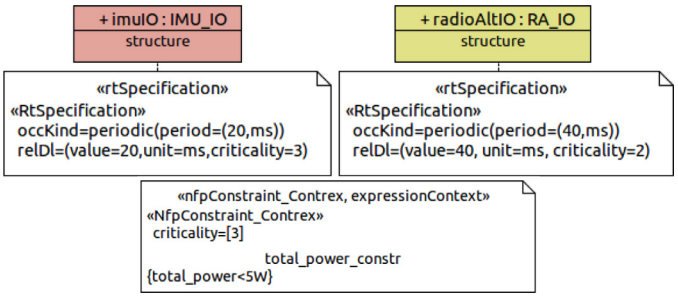
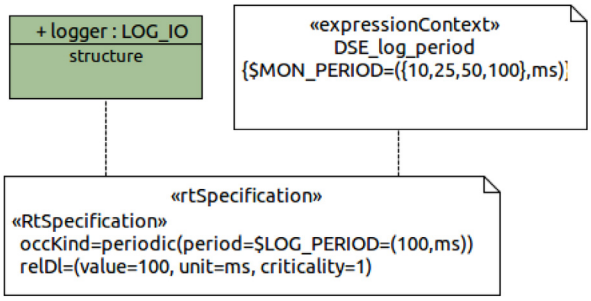


Fig. 5. CONTREX UML/MARTE models enable the association of different criticalities to performance requirements.

(a) Periodicity of a PIM component functionality as DSE parameter.



(b) Parameterization for DSE of processor platform components.

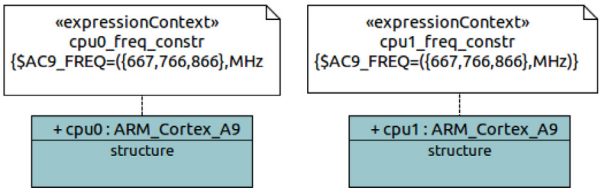


Fig. 6. DSE parameters defined at different model levels.

lability analysis algorithms. Moreover, CONTREX covers a scenario where mixed-criticality refers to the possibility to associate criticalities to performance requirements. For instance, Fig. 5 shows the modeling of timing requirements associated to particular tasks of the RPA IO system (CONTREX avionics demonstrator) and a global power requirement for it too. These time and power performance requirements have associated different criticalities. CONTREX UML/MARTE modeling methodology also supports MARTE-based specification of a design space for supporting an efficient DSE [12,13].

A holistic DSE is enabled because the design space comprises extra-functional parameters which can refer to different levels of the system. For instance, for the RPA IO system, parameters on the application (task periods), and parameters on the platform, i.e. processor working frequencies (shown in Fig. 6), are explored.

4.2. Analysis

CONTREX methods and tools, and specifically CONTREP, support several types of analysis. A novel and specific aspect is the capability to use and exploit criticality information annotated on the model at several design activities.

The model can be used for the automated generation of an emulation model targeted to run on the host machine (native target).

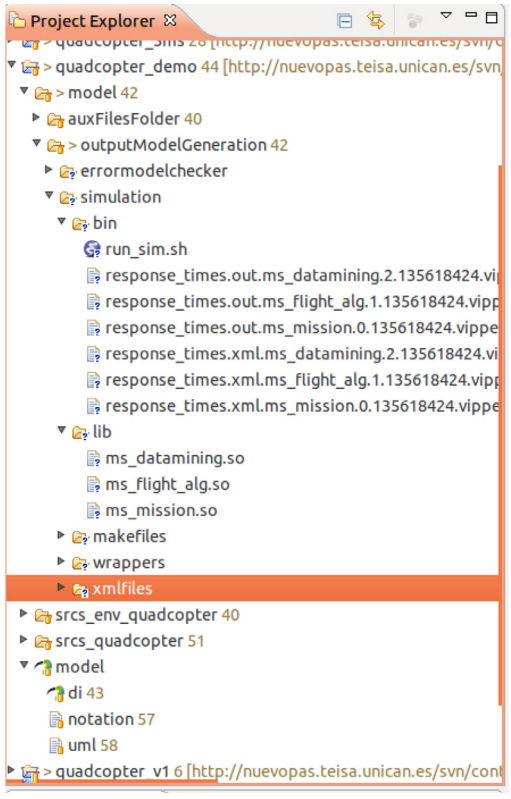


Fig. 7. Files corresponding to the VIPPE executable performance model automatically generated.

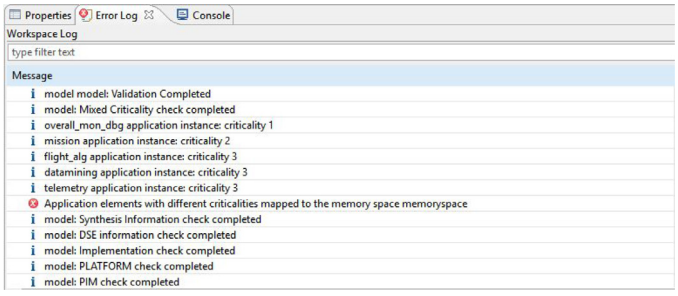


Fig. 8. CONTREP detects modeling errors relying on criticality annotations.

Software synthesis is also supported, as the eSSYN tooling reported in [14] has been adapted and integrated to read the same model.

Finding a suitable and efficient implementation is required before the SW synthesis phase. CONTREP enables an automated generation of a simulatable performance model [15]. Fig. 4 shows the *Generate* menu action used for launching a fully automated genera- tion process. The performance model generated relies on the VIPPE tool (see Fig. 7) [16,17]. VIPPE is based on *native* (or *source-level*) *performance simulation*, a performance estimation technology capable to offer performance estimations close in accuracy, but one or more order of degrees faster, than instruction-set simulators (ISS)
or simulators relying on *binary translation*. This makes native simulation convenient for design space exploration with concern on EFPs.

CONTREP also enables the automated generation of an automated DSE framework, in turn relying on the automatically generated VIPPE model [12]. CONTREP also connects with a schedulability analysis tool [18].

The design framework is capable to exploit criticality information at model validation, to check that mixed-criticality aware modeling rules are fulfilled [19]. For instance, Fig. 8 shows the

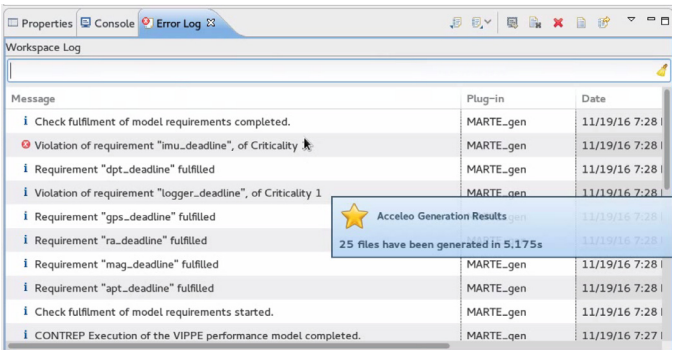


Fig. 9. The severity of a performance requirement violation report depends on the criticality of the requirement.

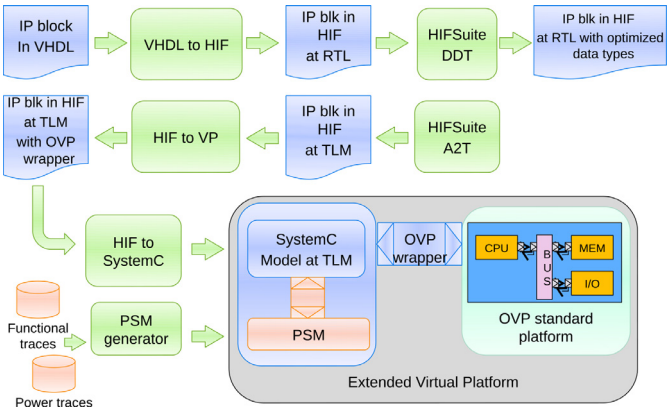


Fig. 10. VP generation flow.

status of the Error Log after CONTREP has passed a model validation. In this case, the violation of one of the mixed-criticality aware rules defined is found (two PIM components of different criticalities are mapped to the same memory space). CONTREP enables the automated validation of performance requirements, and can also use criticality information on that process. Performance requirements captured in the model and their associated criticalities are converted by CONTREP code generators into a XML-based suitable for a post-simulation validation tool. As well as this file, this tool reads the performance metrics (also in XML format) produced after the simulation of the automatically generated performance model. CONTREP configuration enables the association of criticality levels to different severity levels of the Eclipse Error Log. This way, a performance requirement violation can be ignored, just reported, and reported as error or a warning, depending on its associated criticality level [20]. Fig. 9 shows a case where CONTREP finds the violation of a deadline requirement on a safety critical element of the use case 1 of the project (affect an IMU sensor device), and thus the tool is configured to report it as an error. Notice that this report is achieved after the automated generation of the performance model and its simulation (this is not required for the static model validation).

As sketched in Fig. 3, the UML/MARTE methodology has been connected with the ForSyDe methodology [8]. The CONTREX metamodel has enabled the definition of a common base [12], relying on the theory of models of computation (MoCs) [21], which enables to convert MARTE models into ForSyDe-SystemC models [22]. MoC theory ensures relevant functional properties and analyzability for more critical parts of the system functionality. Then, these parts can be converted into ForSyDe-SystemC and simulated.

Moreover, ForSyDe-SystemC models have been enabled as a design entry to an analytical design space exploration tool, called DeSyDe [23]. DeSyDe is a modular tool which uses constraint pro- gramming to find designs that are compatible with design con- straints. DeSyDe supports applications that belong to two differ- ent domains: (i) streaming applications modeled as synchronous dataflow graphs [24,25]; (ii) feedback control applications modeled as periodic tasks [26].

DeSyDe is also used for an initial design space prune in a joint-analytical and simulation-based DSE (JAS-DSE) [27]. In fact, CONTREX contributes to build an JAS-DSE flow where the aforemen- tioned analytical DSE (DeSyDe) is combined with simulation-based DSE, relying on the tools KisTA [28] and MOST [29] tools, to speed up the exploration time by filtering out non-valid solutions. The JAS-DSE flow has been further enhanced including the concept of mixed-criticality either including it within the cost function target of the optimization or by filtering out solutions not respecting analytically detected *interference rules* among tasks at different criticality levels [30]. All the JAS-DSE infrastructure is automatically generated by the previously described modeling and analysis framework.

5. Functional and extra-functional analysis

In this section, the focus is on the extension of a virtual platform by extra-functional models for power and temperature. In this context a virtual platform is an executable model of a real hardware platform that is capable to run the original software stack (full binary compatible) and supports tracing of functional and timing properties when the system is being executed.

5.1. Virtual platforms

The Virtual platform (VP) is an executable model of a system that can be used for early software development and architectural analysis. Every VP includes processor, bus, memory and peripheral models, potentially supporting pre-silicon development of the entire software stack up to the applications level. VPs usually provide a debugging environment to improve software quality and reduce software development costs and time to market.

Imperas Open Virtual Platform (OVP) [31] consists of a set of open source C-based platform descriptions and a closed-source CPU emulator supporting the fast instruction-accurate simulation of several CPU architectures. CPU emulation is based on dynamic binary translation [32]. The CPU emulator and peripheral models are also available as modules written by using Accellera Transaction-Level Modeling (TLM) standard [33].
While OVP and all commercial VPs provide models for standard components, the integration of custom IP blocks is an issue because they are usually described at RTL in VHDL or Verilog while VP models are usually written in SystemC or C/C++ at TLM level. Commercial VPs provide co-simulation mechanisms to handle different languages at the cost of slower simulation while hand-made transactors to connect RTL blocks are inefficient and error-prone. Furthermore, standard VPs do not provide models reproducing the behavior of extra-functional properties (e.g., power and temperature) together with functional behavior. Currently, power and temperature are simulated off-line by using ad-hoc tools without exploring the interaction with embedded software.

5.2. Automatic VP integration supporting EFP

The previously reported issues are solved by extending EDALab's model manipulation tool named HIFSuite to generate extended VPs. The overall flow is reported in Fig. 10. HIFSuite allows to import models described in VHDL or Verilog into a XML-based representation named Heterogeneous Intermediate Format (HIF).

Then the tool allows to manipulate such representation to abstract it at TLM level (DDT [34] and A2T [35]) and to generate the OVP wrapper to connect the module to a standard OVP platform.

The CONTREX project introduced a methodology for the automatic generation of Power State Machines (PSMs) [36] by adopting an approach based on (i) dynamic mining of temporal assertions to extract the IP's functional behaviors from a set of functional traces, and (ii) a calibration process to extract the associated power behaviors from a corresponding set of references power traces. Finally, a Markov model was defined to implement a SystemC executable model of the PSMs to be integrated in a standard VP like a traditional functional description. The power estimation obtained by a system-level simulation of the automatically generated PSMs is up to two orders of magnitude faster than running a state-of-the-art gate-level power simulator like PrimeTime PX without a significant loss of accuracy. This approach enables the efficient simulation of power behavior together with functional behavior to find interferences between applications at different criticality lev els and to test adaptation polices made at software level.

5.3. Stream-based simulation and tracing framework

To enable the seamless integration of extra-functional property models into virtual platforms, a framework for stream-based simulation and tracing has been developed [37]. It allows the instrumentation of virtual platforms to access functional and extra-functional aspects at simulation runtime, as well as pre-processing, monitoring, and recording of these properties.

The underlying technique is based on *timed value streams*, i.e. , a sequence of `(value,duration)` tuples. A *stream writer* is a source of such a stream, *a stream reader* a sink. A *stream processor* is both, sink of one or more streams and source of one or more streams. The basic idea of using the framework is that leaf annotations in the functional model push tuples according to the current local simulation time and status or activity of the producing process to a stream. These incoming tuples are buffered within the stream without advancing the stream's local time. Once the stream writer explicitly commits its updates, the stream's local time is advanced and the pending tuples are forwarded to the stream readers. Stream processors can be used for online pre-processing, filtering, or temporal or structural abstraction. Then, stream sinks can be used for online monitoring or generation of trace files.

The main advantages of this framework over others such as `sc_trace` are:

- high flexibility due to composability of streams and dynamic adaptivity of parameters at runtime,
- support for physical quantities, e.g. with Boost.Units, and
- distributed time model to support temporal decoupling.

Fig. 11 shows the application of this concept within the CONTREX project. The application is running on an OVP-based virtual multi-processor platform representing the Xilinx Zynq SoC. The OVP API gives access to the basic parameters of the platform activity, such as each processor's workload or the number memory accesses in a certain period of time. These basic parameters are fed to a set of *primary streams*. A stream processor reads these primary streams, and, together with some further parameters like supply voltage and processor frequency, it calculates the power dissipation per processor. Then, the power values are written to *secondary streams*. Finally, the secondary streams are connected to a VCD sink that outputs the power over time traces as VCD file.

With this, the result of the virtual platform simulation is not only the functional behavior but as well a component level power trace for an application running on that platform. In addition to the power analysis, we can locate the power dissipation to corresponding areas in the SoC's floor plan, and, together with a thermal model off the SoC package, we can simulate the thermal behavior of the chip as well.

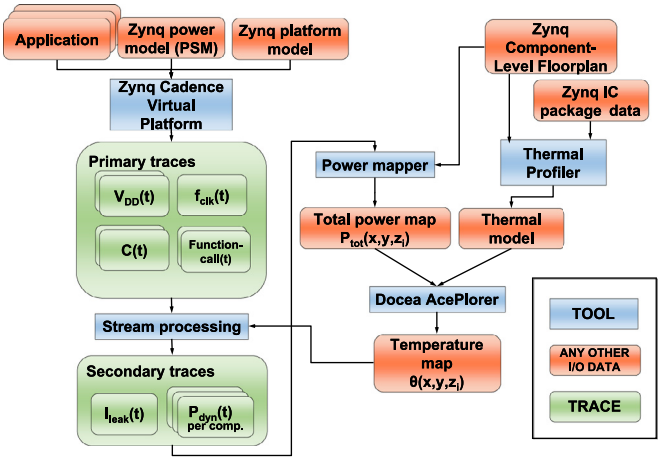


Fig. 11. Stream processing flow.

More details of this simulation framework and its application to a mixed-criticality multi-rotor system [38] and be found in [39].

5.4. Integrating of power models into an instruction accurate Xilinx Zynq virtual platform

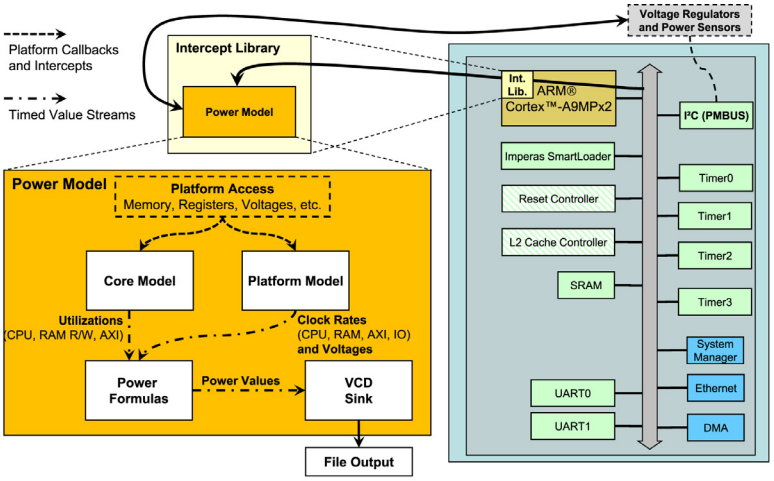
The timed value stream based power model has also been successfully integrated into an stand-alone Imperas Open Virtual Platform (OVP) of the Xilinx Zynq platform. As a proof of concept, an OVP Xilinx Zynq virtual platform has been equipped with a dynamic voltage and frequency scaling (DVFS) compatible power model. Software on the virtual platform can access the actual power consumption and perform power management through DVFS. The Xilinx Zynq platform consists of two subsystems: a processing system with an ARM Cortex-A9 dual-core processor and a programmable logic fabric for custom hardware or additional soft-core processors. With this power model integration the usage of the OVP technology for functional software testing, debugging and non-intrusive analysis of performance metrics is extended through:

- Instructions per Cycle (IPC) based power model structure and measurement based power model calibration for an ARM Cortex-A9 dual core processor
- Extension of the timing and power model towards dynamic frequency and voltage scaling (DFVS)
- Integration of the power model into the virtual platform and software access for testing of dynamic power management.

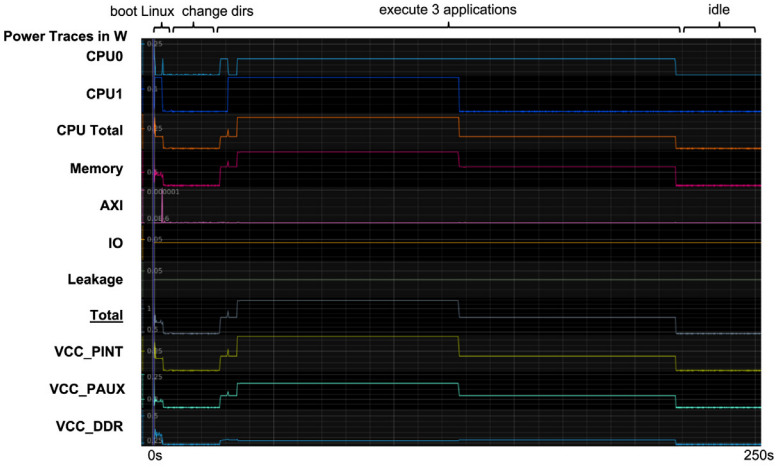
The implementation has been demonstrated at [40]. Fig. 12 depicts the OVP integration of the trace based power model and a power trace of a Linux system executing three benchmark applications.

6. Run-time management

The Automotive Demonstrator has been defined to stress the run-time part of the CONTREX methodologies. In addition to that, it includes also the concept of a distributed system where sensor nodes and remote control units deployed on the cars have to communicate with remote infrastructure for data collection. Thus, this use case not only considers node-level extra-functional modeling, monitoring and management but also the remote services abstractions.



(a) Overview of the Power Model and the Zynq ARM Dual Core Platform: The Power Model is instantiated in the OVP intercept library, it accesses the platform information via defined memory callbacks and I2C intercepts are used for transmitting new voltage parameters or returning power values. The Platform model is responsible for recognizing all platform values, like frequencies and voltages, as well as the intercepted I2C communication with the Voltage Regulators and Power Sensors. Both ARM cores have a single Core Model. It is responsible to calculate all core specific data, like CPU utilization, Memory Read and Write rates and AXI Load (both with memory read and write callbacks). All calculations for the utilization are called periodically. The Power Formulas, based on the Xilinx Power Estimator (XPE), calculate all power streams for CPU, Memory, AXI, IO, Leakage, etc. The VCD Sink writes all traces and data to a trace file.



(b) Exported VCD power traces from the Xilinx Zynq platform above. The traces show the Linux (running in SMP mode) boot phase, a user interaction through a terminal (changing directories) and the execution of three benchmark applications. CPU0 and CPU1 is the power consumption of each CPU. Memory is the power consumption of the external memory. AXI is the power consumption of the on chip bus. IO is the input output power consumption. VCC_PINT, VCC_PAUX and VCC_DDR is the power consumption at the different power rails.

Fig. 12. Xilinx Zynq OVP model with stream based power model [40].

6.1. Cloud service abstraction

The concept of connected devices is changing the embedded systems world. Machine to Machine (M2M) and Internet of Things (IoT) follow a common technological paradigm: intelligent devices, seamlessly connected to the Internet, enable remote services and provide actionable data. The IoT acronym is more adopted in the consumer space while M2M has a stronger industrial connotation, such as for the automotive scenario. One of the most important aspects of the IoT/M2M vision is that smart objects communicate effectively with each other and possibly with applications residing in data centers or the cloud. This however creates a need of a standardized software layer involving both the *Device-to-Cloud* related part and the *Cloud Platform* (see Fig. 13).

The concept of the *device to cloud* proposes an end-to-end solution that includes purpose-built hardware, connectivity and embedded device management through a pervasive software framework and a cloud client, running on the devices, and a set of machine to machine (M2M) cloud-based services. The objective of this

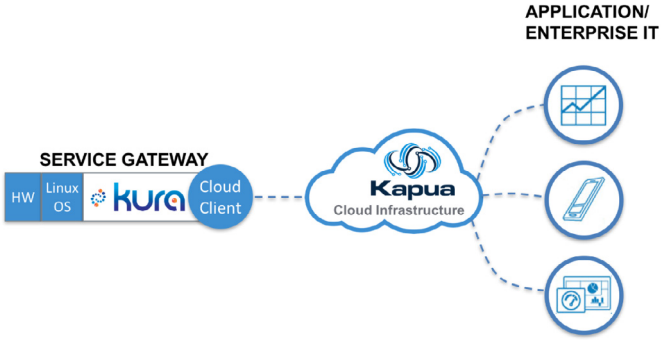


Fig. 13. Device to cloud approach.

solution is to deliver actionable data from the field to downstream applications and business processes, dashboards and reports. The Kura pervasive framework [41] proposed in CONTREX offers the

technical building blocks required to assemble distributed systems of devices and sensors which are effectively connected to IT infrastructures. This solution is based on a combination of hardware, firmware, operating systems, programming frameworks that dramatically accelerate the time to market of M2M / IoT projects and enable future potential customers to layer their added-value components on a reliable ready-to-use infrastructure. Kura is responsible to manage the edge of the IoT system and provides a Java/OSGi-based framework for multiservice gateways that offers access to the underlying hardware (serial ports, GPS, watchdog, GPIOs, I2C, etc.), management of network configurations, gateway management and communication with the M2M/IoT cloud platform.

The *cloud platform* is a M2M integration platform that simplifies device and data management by connecting distributed devices over secure and reliable cloud services. The devices can be IoT modules deployed in the environment, e.g. the embedded systems installed in the car. The data are the functional and extra functional properties monitored by these devices. The cloud service abstraction is responsible to provide full control over the embedded systems hardware, software and acquired data with a simple service model. The objective is to completely hide the complex details that stand behind the remote management procedures, remote data acquisition and transmission. The cloud service abstraction id based on Eurotech EDC, an industrial grade cloud platform for IoT application that has been recently released open source with RedHat and Eclipse with the name Kapua [42].

6.2. Extra-functional properties management at run-time

Power management at node level is of particular interest in battery powered sensor-node. In detail, the main idea within the sensor-node of the automotive use case has been to configure the node's hardware devices and software activities (functions and tasks) according to functional and extra-functional considerations, by exploiting accurate operating condition profiles derived at design-time. However despite this object seems to be simple, run-time actions are based on three classes of information, namely: *functional status, extra-functional status* and *design-time configurations*.

Functional Status. The application's functional status is also referred as *operating-mode*. Given the requirement of the automotive application, a completely autonomous management system solely based on non-functional properties will not satisfy availability and functional needs. For this reason it is necessary to introduce the notion of operating mode, that expresses the current functional status of the system, e.g. the motion status of the vehicle or the status of the dashboard key. Associated to such states, different sets of functions shall be mandatorily enabled/disabled or properly configured, leaving to the non-functional manager the role of managing power (and other) optimizations, possibly at the cost of a processing quality degradation.

Extra-functional status. This information consists in the collection of metrics exposed by the extra-functional monitoring infrastructure. The framework provides to an application the ability to monitor at run-time the desired metrics with a function-level granularity. The CONTREX monitoring framework is based on four main concepts. (i) Device. It is a physical component of the system that can be profiled in terms of extra-functional properties; (ii) Metric. It is any extra-functional property relevant for the application, such as time and energy, amount of data transferred by the system; (iii) Measure. It is defined by the metric, a numeric value and the related device. The metrics and the devices must be defined in the configuration of the framework. (iv) Event. It is meant to express concepts such as "an interrupt from the accelerometer has been acknowledged" or "the idle task is executing". Additionally, in order to gather the measures, the developer must instrument the region of code that he wants to observe. In this way, the framework automatically senses the system and stores the ob- servation values making them available to specific portions of the application responsible to implement local run-time management and to export them up to the cloud.

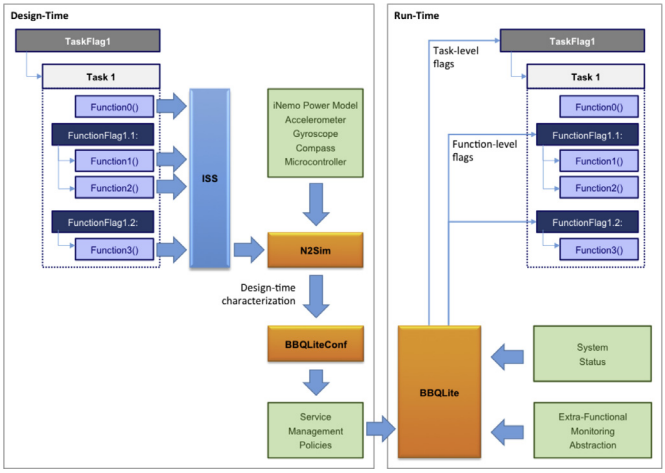


Fig. 14. Overview of the EFP rum-time management framework.

Design-time configurations. The design-time configuration depends on the results of application and node event-driven simulation, combined with user-defined policies explicitly specified by the application's developer. A system characterization framework of both hardware and software components has been developed and integrated in a sensor node-simulations. The characterization phase has been based on models, simulations and measurements on sub-systems and components.

Fig. 14 shows the structures of the run-time management framework implemented. The figure can be split in two: on the right-hand side there is the design time flow, while on the left-hand side there is the actual run-time part.

6.3. Battery modeling

Energy storage devices have a crucial role in determining the *lifetime of a system*, i.e., how long the system can operate au tonomously from the grid or from power sources. This makes the modeling and simulation of energy systems, and of batteries in particular, an important dimension in system design. Monitoring or simulating the energy flows in the system would indeed allow an accurate estimation of energy consumption, and it would provide a forecast of system lifetime. Battery models can be easily integrated inside of the proposed monitoring framework. The adopted imple- mentation language is SystemC, with its AMS extension [43], that can be easily integrated in C++ environments [44].

The battery is modeled as a SystemC module (`SC_MODULE`). The *interface* is standardized, so that it exposes all relevant information. This allows to preserve flexibility, as the interface is independent from the implemented model. The ports, declared as SystemC-AMS TDF ports, are: `V` (voltage level of the battery), `I` (current demand), `SOC` (battery state of charge in percentage), `E` (battery capacity), and `En` (an enabling signal used to implement battery management policies).

Battery model implementation strictly depends on the chosen level of detail. *Functional models* implement a generic evolution of the energy flow through a function, such as an equation or a power state machine [45,46]. This kind of models are implemented as a C++ function, repeatedly executed at fixed time steps. *Circuit models* emulate the behavior of a battery through an equivalent electri-

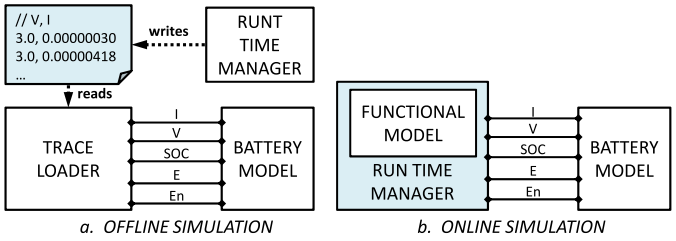


Fig. 15. Possible alternatives for the integration of the battery model.

cal circuit made of electrical components (e.g., resistors and capacitors) [47]. This kind of models is realized through the instantiation and connection of SystemC-AMS ELN primitives, that natively represent electrical linear elements. Note that all battery models must be populated with appropriate parameters, either derived with empirical measurements or extracted from battery datasheets [47].

The generated battery model can then be easily *integrated with the run-time management infrastructure*. Two alternatives are possible, depending on the desired level of interaction (see Fig. 15). *Offline simulation* allows to simulate the battery model stand alone on consumption traces generated by the functional simulator. Trace files contain voltage and current samples equally spaced in time, and they are loaded by a SystemC module, in charge of writing onto the battery model interface. On the contrary, *online simulation* allows incapsulating the equations of the model into the extra-functional properties monitoring infrastructure. This is possible since the concept of metric, as defined by the monitoring infrastructure, is hierarchical in nature: the battery state of charge, in fact, can be described as a higher-level metric based on time, voltage and current metrics. Once the model is integrated in the framework, the run-time manager can react instantaneously to the evolving operating conditions of the battery (e.g., to change system operation when battery state of charge is too low).

7. Use-cases and evaluation

7.1. Avionics use-case and CONTREX MDE tool integration

7.1.1. Use-case description

For the avionics use case, a demonstrator based on the Flight Control Computer (FCC) of a medium-sized Remotely Piloted Aircraft (RPA) was used. The FCC, in charge of the guidance, navigation & control of the RPA, has a mixed-criticality nature for which extra-functional property behavior is of the highest relevance.

Taking into account that size, weight and power (SWaP) constraints are a key factor for modern RPA equipment, the Flight Control Computer (FCC) software is susceptible of being reused in diverse commercial all-purpose MPSoCs and low-cost avionics sensors, that could be integrated into increasingly lighter RPA platforms.

7.1.2. Design challenges and status before CONTREX

The main challenge posed by this scenario is to find those optimal designs that minimize cost, size, weight and power consumption without compromising the safety and overall performance of the system. For it, a flexible approach that enables the early assessment of system performance on different (COTS) platforms and the efficient exploration of wide design spaces is required.

The state-of-play avionics development flow consists of a typical V-cycle geared to custom platforms for systems under construction, where the HW/SW partitioning decision is taken at an early stage of the cycle then evolving HW and SW developments in parallel to the integration phase. This approach presents important difficulties to its applicability to the new context above discussed.

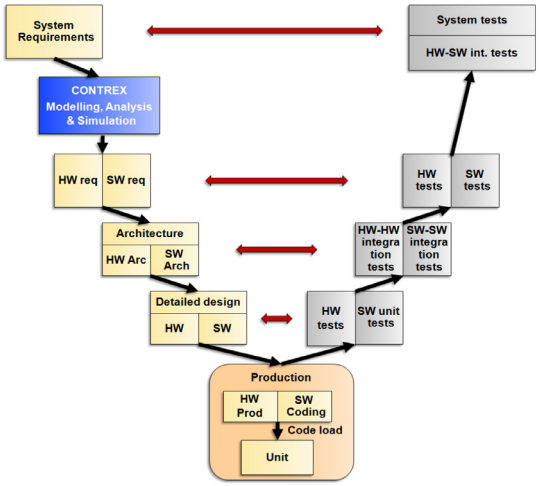


Fig. 16. Integration of the CONTREX modeling, analysis, simulation and DSE methods and tools in the avionics industrial flow.

Firstly, in order to avoid late integration issues, the design space is strongly limited, which prevents from exploring wide spaces that would increase the probability of finding the optimal design solutions. Secondly, the quantity and capacity of resources are usually oversized (especially in the case of mixed criticality systems due to the spatial and temporal isolation principle), which leads to larger, weightier and more power-consuming designs.

7.1.3. New design flow and application of the CONTREX MDE tools

In order to overcome previous issues, the CONTREX approach was evaluated by applying its methodology to the avionics demonstrator. In essence, CONTREX methodology enhances the avionics development flow by introducing extra activities for system modeling, model-based analysis and simulation and automatic Design Space Exploration (DSE) during the design phase, as shown in Fig. 16

7.1.4. Main evaluation results

The results gathered from these activities are used to make better-informed architectural decisions (such as platform selection and HW/SW mapping) based on reliable figures that may range from timing and power estimations to thermal properties of the system running on different platforms. This approach helps minimize design errors and thus reduce the chance for re-design work at late stages without having to limit the design space or oversize platform resources.

During the evaluation activity, the avionics use case focused on UML/MARTE modeling, native simulation technology and simulation-based DSE.The CONTREX modeling language exhibited a fair balance between expressiveness and complexity, although it was found somewhat restrictive in some aspects. The tools being part of the CONTREX's avionics use case tool-set were smoothly integrated and demonstrated their potential to perform early assessments of system's performance on new platforms, providing a fair trade-off between speed (that enables to explore a wide design space in a reasonable amount of time) and accuracy (that enables to make design decisions based on reliable figures). In order to improve their applicability to operational developments, they should progressively add support for additional commercial MPSoCs and applications using non-POSIX APIs (e.g. FreeRTOS).

In summary, CONTREX project allowed the development of a demonstrator that served as a prototype for evaluation purposes and enabled the preliminary assessment of the applicability of CONTREX approach to the avionics flow. Although further developments need to be performed in order to apply the activities to real

operational developments, CONTREX supposes a solid base towards an enhanced design flow that improves the capability to tailor the existing FCC system to increasingly lighter RPA platforms, leading to maintain a competitive supply base in Europe for new markets and countries.

7.2. New low-power telematics box

7.2.1. Use-case description

Car Black Box (also called Event Data Recorder) is gaining an important role not only in investigation of car accidents or to track driver behavior, but also for a more direct user support. In fact, while it is true that it can be used to record the events and actions of the driver including speed, braking, turning, etc. seconds before a collision, thus possibly helping both the police and insurance companies in accident reconstruction, it can be also used to trigger an event when this negative events happens. In this direction, several non-automotive companies provide private and/or fleet vehicle drivers with a support service in case of accident [48]. This can happen calling directly either the mechanical support or an ambulance depending on the crash entity, or notifying the car owner if something happened to the car while it was in a parking area. From more technical point of view, the architecture is based on four main components: (i) a sensing unit for acceleration measurements, (ii) a GPS unit for speed and position measurements, (iii) a data processing unit accidents and minor impacts identification, and, (iv) a communication unit for transmitting data to the cloud infrastructure either for further processing or for providing crash information to public authorities, insurance companies or private users.

The Automotive Telematics Demonstrator of CONTREX extends this type of commercial solutions trying to provide more functionalities and better performances/power trade-off.

7.2.2. Design challenges

To cope with the constraints and requirements of the application scenario, several challenges have to be faced. We can identify several classes of challenges, which have been addressed by the CONTREX extended tool flow as described in the following.

- Design-time. When starting a new design - as it has been the case of the demonstrator described here - it is crucial to have the possibility to rapidly model the main system hardware/software components and simulate the system's non-functional behavior, mainly execution times and power consumption. By simulating the system in different "operating conditions" (e.g. different data sampling rates, different sets of enabled functions, different CPU power modes, ...) an optimal set of operating modes can be defined. Such design-time defined modes will be used at run-time. The CONTREX flow has been extended with a non-functional hardware/software node simulator (N2SIM) and a set of post-processing utilities to analyze simulation results and to define a set of "policies" that will be used at run-time (BBQLiteCongif).
- Run-time. The main challenge at run-time is to manage the system to balance power consumption and quality of service. To this purpose it is necessary to sense the instantaneous non-functional status of the system (e.g. bandwidth usage, battery state of charge) and to know the operating condition of the vehicle (e.g. driving, parked, key status) and, based on this information, switch to one of the operating modes defined at compile time. To this purpose the extra-functional properties monitoring infrastructure (EFPM) and the run-time manager (BBQLite) have been implemented and integrated into a traditional design-flow while limiting their intrusiveness in the target code.

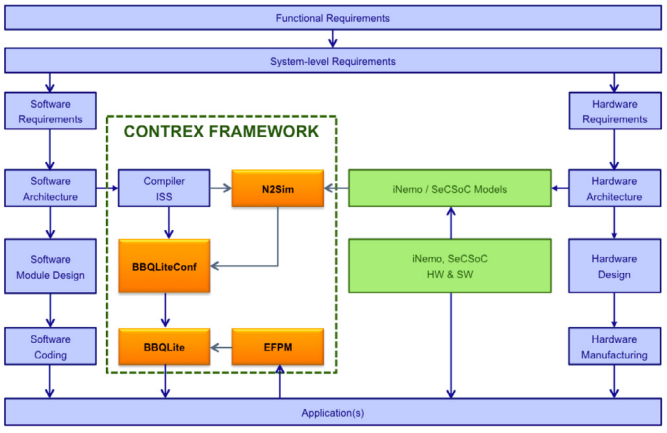


Fig. 17. Automotive demonstrator extended design flow.

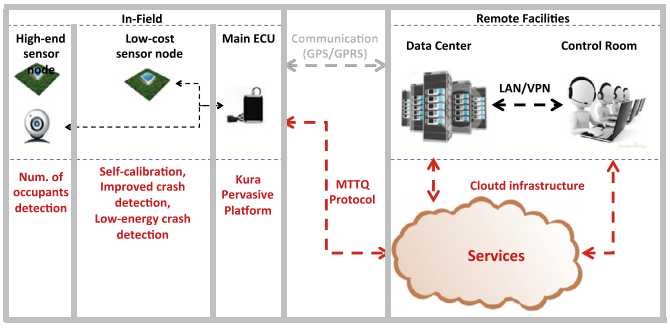


Fig. 18. Overview of the automotive demonstrator.

- Product life. During the life of a telematics box is very common to receive requests from business customers (e.g. insurance companies, public authorities) to modify existing functions or to add brand new ones. In this situation it is crucial to allow for the changed/added functionality to be integrated into the existing system without redesigning the entire functional and non-functional management code. By exploiting the tools and the methodology described above, such requests for change can be dealt with by performing new simulations and define new operating points (at design-time) and to make minor modifications to the code, i.e. changing the policy description table used by BBQLite.

Fig. 17 shows the complete CONTREX flow: the blue boxes represent the tools in the original design-flow, while the orange ones are the new CONTREX tools and frameworks.

7.2.3. Functional improvements

From the functional point of view the enhancement in the system architecture introduced by the CONTREX project are multiple (see Fig. 18).

First, the car sensing unit has been enhanced by using new platform hardware and enhanced algorithms for event detection and analysis. From the hardware point of view, the platform of the sensing unit have been migrated on the iNEMO-M1 [49], a 9-axis motion sensing System-on-Board (SoB) guaranteeing high-definition digital acquisitions and low-power modes. From the software point of view, the new capability introduced by the hardware platform has been exploited introducing new functionalities. In particular, a novel self-calibration algorithm has been defined to reduce the cost of installation. The device is now capable to auto-detect its orientation relative the car cinematic reference system and autonomously auto-adapt the computation. This allows devices

to be installed by non-specialized personnel and dramatically reduces the effort for maintenance. In addition, the new combination of the hardware and novel algorithms, enabled the possibility to detect low-energy events, such as minor crashes and acts of vandalism, while the car is parked and unattended.

Second, a high-end video sensing node - based on the ST SeC-SoC ultra low-power computing platform - has been added to collect visual information from inside the car, in particular to detect the number of car occupants at the moment of an accident. The automatic detection and counting of vehicle occupants is a challenging problem within the automotive demonstrator since it gives the possibility either to tailor the assistance in case of a crash based on the number and condition of vehicle occupants or to detect fraudulent behaviors.

Third, on the communication and data processing side, a new automotive gateway [50] has been included on-board to collect and transmit remotely the data gathered from the previously two described sensing nodes. This new device is a compact size device designed to support M2M applications and to host the Kura framework as described in Section 6.1.

Fourth, a cloud infrastructure substitutes a custom data-center to enable services scalability. In fact, being the number of customers and the amount of data to be collected per customer expected to significantly grow in the next few years, a switch from a dedicated server infrastructure to a flexible and scalable cloud-based solution is necessary, also considering the additional services highlighted in Section 6.1.

7.2.4. Extra-functional improvements

In addition to the reduction of the installation cost given by the novel self-calibration algorithm mentioned in the previous section, other extra-functional improvements have been integrated in the automotive use case at the sensing-node level. In particular the introduction of the extra-functional property management framework described in Section 6.2, while considering also the effect of the battery (Section 6.3), enabled to autonomously manage and optimize the power consumption and thus improve the availability of the sensing devices, especially when the car is switched off.

7.2.5. Main results and impact to future products

The main results obtained thanks to the CONTREX approach and tools are the following:

- Improved quality of the sensor data, namely: higher sampling frequency, 9-axes instead of 3;
- New functionality, namely: self-calibration, improved crash detection, low-energy event detection, more detailed trip reporting (once a second instead of once a minute);
- Power consumption reduction: 50% reduction when in full-operating mode, 80% reduction when in low-power mode.
- Shortened design time needed to implement and integrate new functions: from 6 to 2 weeks;

Thanks to the CONTREX flows, in addition, new market opportunities have been opened and are being investigated. In particular, the development of a new class of devices for the motorbike market has been started. This application is especially critical both in terms of functionality, availability and power consumption. A prototype is expected to be on the field for a first test on 1000 vehicles in Q2 2017.

7.3. Virtual platform integration into telecom equipment development

7.3.1. Overview of Ethernet-over-Radio system

Radio relay systems have unique competitive features, such as quick deployment and fast network roll-out with simple civil works, that strongly justify a modern telecommunications network

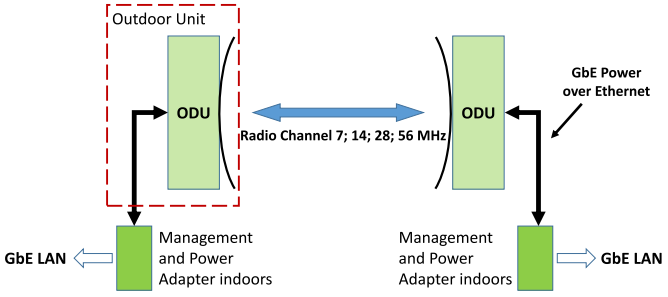


Fig. 19. Overview of Ethernet-over-Radio system with highlighted outdoor unit (ODU).

scenario in which radio systems and fiber optic systems will complement and support each other in a very effective mixed me- dia approach. The wireless family is made of a variety of sys- tems for different applications: i.e. base stations for mobile net- works (GSM, UMTS, GPRS), terminals for nomadic usage (Wi-Fi and Wi-Max), terminals for unidirectional broadcasting (TV and DVB), bidirectional Point-to-Point and Point-to- Multipoint systems for fixed networks. Within the CONTREX project Intecs Telecom focuses its attention on the Point-to-Point (P2P) Ethernet-over-Radio Microwave Wireless System (see Fig. 19). The Ethernet- over-Radio System is specifically designed and engineered for such situations where it is required to transport E1 signals. It allows a smooth transition from the previous generation of transport (PDH) networks, encapsulating the E1 signal into an Ethernet frame. The Ethernet-over-Radio System is particularly suited to cover mobile broadband infrastructure data growth from GSM to WDCMA to LTE and many other needs of high data transport. In other words, it provides smooth migration path from legacy to modern systems, an essential capability in the telecom area. A key element of the system is Automatic Transmit Power Control (ATPC), allowing the modulation of transmission power according to the amount of noise, in order to ensure a lower bit error rate (while sacrificing transmission velocity). This capability also permits the mixing of transmission modes, such as high criticality (e.g. business or emergency response traffic) mixed with lower criticality traffic such as voice grade telephone. Thus, adaptive technologies such as ATPC constitute a key asset in this family of telecom products.

7.3.2. Design challenges and status before CONTREX

Several challenging extra-functional property requirements apply to such telecom systems. The assurance of thermal and power properties is challenging from the environmental point of view, because components are often characterized by outdoor placement. The electronic circuits present challenges because the clock rate is heavily influenced by the technology used for CPU, busses, and FPGA components. Likewise, the assurance of timing properties is difficult because of extreme variation in traffic loads that render analysis complex or even intractable, due in great part to the adaptive technologies described above. These challenges can lead to costly errors in the dimensioning of systems that are only discovered after deployment. At the end of the development phase of the Ethernetover-Radio some significant problems occurred mainly in terms of power consumption. The entire development environment was clearly inadequate for new product development in a broad area of dynamic transmission management products. The primary weaknesses included:

- No mechanisms for handling extra-functional aspects within the specifications;
- No pre-development modeling whatsoever;
- System validation began only at the end of the integration phase;

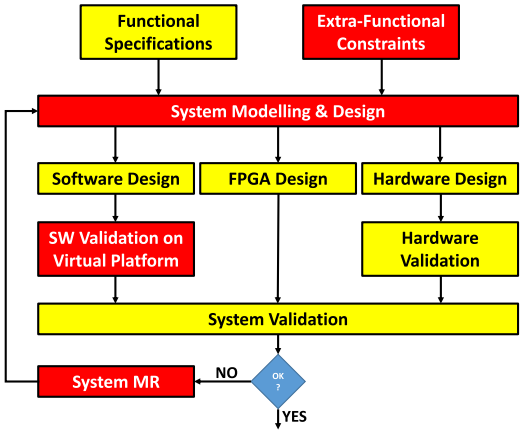


Fig. 20. Improved work flow.

- Lack of any early modeling or simulation tended to lead to costly iterations, usually due to extra-functional concerns.

In view of these weaknesses, the primary goal of the telecom demonstrator became the modernization of the product development environment.

7.3.3. New design and used CONTREX technology

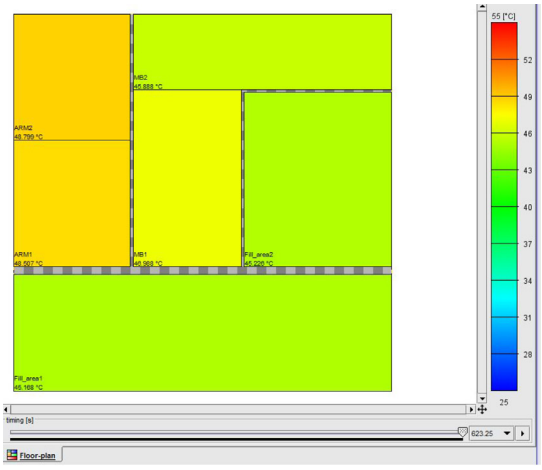
The new design flow is illustrated in Fig. 20. It contains:

- Mechanisms provided to capture extra-functional properties / constraints
- A layer of pre-development modeling capacity
- Early validation capability provided through a virtual platform for the software
- Uplifting of individual SW / HW / FPGA Modification Requests (MR) to System MR, capable of being treated in the system modeling layer.

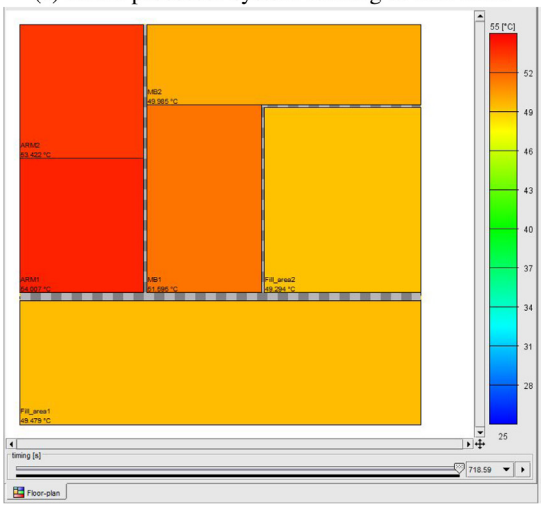
ForSyDe of KTH was selected as the principal software application modeling formalism. The objective was to be able to model (extra-functional) concurrency / timing aspects and enable Design Space Exploration. HIFSuite of EDALab provided the modeling formalism for abstracting legacy IP components so that the application could be faithfully ported to the simulation environment. The principal platform service abstraction is the coupling of the real and virtual platforms with appropriate extensions (e.g. power traces) enabling validation loops, in particular for thermal and power modeling (the real platform being implemented by Intecs, and the virtual platform by OFFIS).

7.3.4. Main evaluation results

A virtual prototyping environment on the host processor makes it possible to test the functional and extra-functional behavior of the system under development. The real hardware prototype can be delayed to later design phases, permitting early, low cost evaluation of the system's timing behavior. Using estimation tools operating in the simulated environment, it also permits exploration of different hardware architecture configurations that optimize thermal and power characteristics. Specifically, the objective was the exploration of the tradeoffs of moving from a legacy PowerPC CPU to a modern Xilinx Zynq architecture with higher performance but also higher power consumption and thermal dissipation. To this end, the application was simulated in the OVP environment. Given the adaptive algorithms that regulate the transmission according to the importance of transmitted data and to channel condition, it needed to be simulated in a full and realistic network scenario to test the behavior of transmission control tasks as a function of time-varying transmission condition. The network interface is a



(a) ARM processor system running at 222 MHz



(b) ARM processor system running at 666 MHz

Fig. 21. Typical heatmap.

legacy HW component written in VHDL, which was abstracted and translated into SystemC/C++ to be integrated into the OVP scenario by using HIFSuite. The OVP top-level configuration was automatically generated by HIFSuite. The bridging elements to allow co-simulation between OVP and SystemC/C++ components were automatically generated by HIFSuite. The power and thermal analysis was used for comparative estimates of power consumption and thermal behavior of the demonstrator application in different configurations on the Zynq architecture, both in the simulated and the real environments. The resulting heatmaps of the ARM CPU at 222 and 666 MHz clock speed (see Fig. 21) exhibited extremely faithful correspondence between simulated and real platform characteristics.

7.3.5. Future use and impact on future products

The CONTREX environment enables migration of key use case IPR into new product areas, in particular by migrating the key ATPC and adaptive modulation techniques of current telecom products onto more powerful, modern processors. There are a number of prospective exploitation areas. Wireless Ethernet is used in LTE base stations to optimize low power consumption and offer mixed criticality transmission. It provides the wireless backhaul link of traffic to the core network. In addition, the European Union has been preparing calls for proposals for bringing broadband to remote areas of the EU (also known as C & D zones). The principal

problem is not technological, but rather commercial: with few potential customers, the fiber optics providers are reluctant to lay the cables in the face of low potential economic returns. One promising alternative solution is to exploit Ethernet-over-Radio technology to create a sub-backhaul bringing internet from the core fiber network to the street cabinet, where the transition to existing copper lines can take place. Modern VDSL technologies over copper wire can then provide highly performant internet service within the remote sites.

8. Conclusion

In this article, we presented the main results of the European project CONTREX. The developed tools and methodology extensions have been described as well as their application to the industrial demonstrators to show the benefits for the design of embedded mixed-criticality systems. This article gave an overview of the main technologies and tools. The *main success stories* of the project are:

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

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, modeling 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.

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

The experimental platform consists 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 CAMeL-View tool.

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.

Insurance telematics for reduced cost of ownership

It is now possible to analyze 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 field by 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 Politecnico di Milano team have created a start-up in July 2016, 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.

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

The Eurotech 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^{TM}Cloud, Eurotech's IoT Integration Platform. The exploitation of R&D activities performed on Kura allowed developing a new version of ESF that was available since the fourth quarter of 2016

Virtual platform introduction for the development of telecommunication equipment

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 fiber 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

More details about the project and its outcomes can be found in the deliverable section of the project website [1].

Acknowledgments

The work leading to these results has received funding from the European Community's Seventh Framework Programme FP7/2007-2011 under grant agreement no. 611146.

References

[1] OFFIS, CONTREX FP7 project website, 2015, [Online]. Available: https://contrex. offis.de/home/.

[2] R. Görgen, K. Grüttner, F. Herrera, P. Peñil, J.L. Medina, E. Villar, G. Palermo, W. Fornaciari, C. Brandolese, D. Gadioli, S. Bocchio, L. Ceva, P. Azzoni, M. Poncino, S. Vinco, E. Macii, S. Cusenza, J. Favaro, R. Valencia, I. Sander, K. Rosvall, D. Quaglia, CONTREX: design of embedded mixed-criticality control systems under consideration of extra-functional properties, in: P. Kitsos (Ed.), 2016 Euromicro Conference on Digital System Design, DSD 2016, Limassol, Cyprus, August 31, - September 2, 2016, IEEE Computer Society, 2016, pp. 286–293, doi:10.1109/DSD.2016.95.

[3] Object Management Group (OMG), UML Profile for MARTE: Modeling and Analysis of Real-Time Embedded Systems, 2011.

[4] G. Nitsche, K. Grüttner, W. Nebel, Power contracts: a formal way towards pow- er–closure?!, in: Proc. of the 23rd Intl. Workshop on Power and Timing Mod- eling, Optimization and Simulation (PATMOS), 2013, pp. 59–66.

[5] G. Nitsche, K. Grüttner, W. Nebel, Towards satisfaction checking of Power Con- tracts in Uppaal, in: E.E.E. Chips, S. design Initiative (Eds.), Proceedings of the 2014 Forum on Specification and Design Languages (FDL), ECSI - European Electronic Chips and Systems Design Initiative, Munchen, 2014.

[6] A. Burns, R.I. Davis, Mixed Criticality Systems—A Review, 2015. http://www-users.cs.york.ac.uk/burns/review.pdf

[7] S. Trujillo, R. Obermaisser, K. Grüttner, F.J. Cazorla, J. Perez, European Project Cluster on Mixed-Criticality Systems, 3PMCES Workshop (Performance, Power and Predictability of Many-Core Embedded Systems) at DATE'14, Electronic Chips & Systems Design Initiative (ECSI), 2014.

[8] I. Sander, A. Jantsch, System modeling and transformational design refinement in forsyde, IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. 23 (1) (2004) 17–32, doi: 10.1109/TCAD.2003.819898.

[9] CAMeL-View Website, 2016 (http://www.ixtronics.com/21/index.html). Last visited on 06/04/2016.

[10] D2.2.2: CONTREX System modelling methodology (final), CONTREX Consortium, Technical Report, 2016. [Online]. Available: https://contrex.offis.de/home/index.php/dissemination/deliverables.

[11] CONTREX System Metamodel, CONTREX Consortium, Technical Report, 2015. [Online]. Available: https://contrex.offis.de/home/images/publicdeliverables/Deliverable%20D2.1.1%20v1.0.pdf.

[12] F. Herrera, P. Peñil, E. Villar, UML/MARTE modelling for design space explo- ration of mixed-criticality systems on top of predictable platforms, Jornadas Sarteco-JCE (JCE'15), 2015.

[13] F. Herrera, H. Posadas, P. Peñil, E. Villar, F. Ferrero, R. Valencia, G. Palermo, The complex methodology for uml/marte modeling and design space exploration of embedded systems, J. Syst. Archit. 60 (1) (2014) 55–78, doi:10.1016/j.sysarc.2013.10.003.

[14] H. Posadas, P. Peñil, A. Nicolás, E. Villar, Automatic synthesis of embedded SW for evaluating physical implementation alternatives from UML/MARTE models supporting memory space separation, Microelectronics J 45 (10) (2014) 1281–1291. http://dx.doi.org/10.1016/j.mejo.2013.11.003.

[15] F. Herrera, P. Peñil, E. Villar, A model-based, single-source approach to design-space exploration and synthesis of mixed-criticality systems, in: Proc. of the 18th Int. Workshop on Software and Compilers for Embedded Systems (SCOPES'15), 2015, pp. 88–91, doi:10.1145/2764967.2784777. New York, USA

[16] L. Diaz, P. Sanchez, Host-compiled parallel simulation of many-core embedded systems, in: Proc. of Design Automation Conference, DAC'14, 2014.

[17] VIPPE Website, 2016 (http://vippe.teisa.unican.es). Last visited on 22/04/2016.

[18] P. Penil, H. Posadas, J. Medina, E. Villar, UML-based single-source approach for evaluation and optimization of mixed-critical embedded systems, DCIS'15, 2015.

[19] F. Herrera, UML/MARTE modelling for mixed-criticality systems, 2016. (in CONTREX:Virtual Integration Testing for Mixed-Criticality Systems under Consideration of Power and Temperature Constraints tutorial at HIPEAC'16), [Online]. Available: https://www.hipeac.net/events/activities/7330/contrex/#fndtn-program.

[20] F. Herrera, E. Villar, CONTREP: A single-source framework for UML-based modelling and design of mixed-criticality systems, DATE'16 University Booth, 2016 https://www.date-conference.com/system/files/file/date16/ubooth/37929.pdf. Dresden, Germany.

[21] E.A. Lee, A. Sangiovanni-Vincentelli, A framework for comparing models of computation, IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. 17 (12)(1998) 1217–1229.

[22] S. Attarzadeh Niaki, M. Jakobsen, T. Sulonen, I. Sander, Formal heterogeneous system modeling with SystemC, Forum on Specification and Design Languages (FDL 2012), 2012. Vienna, Austria.

[23] desyde, DeSyDe, (https://github.com/forsyde/DeSyDe). Accessed: 2016-12-15.

[24] K. Rosvall, I. Sander, A constraint-based design space exploration framework for real-time applications on MPSoCs, Design Automation and Test in Europe (DATE '14), 2014, doi:10.7873/DATE.2014.339. Dresden, Germany.

[25] K. Rosvall, N. Khalilzad, G. Ungureanu, I. Sander, Throughput propagation in constraint-based design space exploration for mixed-criticality systems, Work- shop on Rapid Simulation and Performance Evaluation: Methods and Tools (RAPIDO'17), 2017. Stockholm, Sweden.

[26] N. Khalilzad, K. Rosvall, I. Sander, A modular design space exploration frame- work for multiprocessor real-time systems, Forum on specification & Design Languages (FDL'16), 2016. Bremen, Germany.

[27] F. Herrera, K. Rosvall, I. Sander, E. Paone, G. Palermo, An efficient joint analyt- ical and simulation-based design space exploration flow for predictable mul- ti-core systems, Workshop on Rapid Simulation and Performance Evaluation: Methods and Tools (RAPIDO), 2015. Amsterdam, The Netherlands.

[28] F. Herrera, I. Sander, An extensible infrastructure for modeling and time anal- ysis of predictable embedded systems, FDL 2014), 2014. Munich, Germany.

[29] V. Zaccaria, G. Palermo, F. Castro, C. Silvano, G. Mariani, Multicube explorer: An open source framework for design space exploration of chip multi-processors, in: 23rd International Conference on Architecture of Computing Systems 2010, 2010, pp. 1–7.

[30] E. Vitali, G. Palermo, Early stage interference checking for automatic design space exploration of mixed critical systems, Workshop on Rapid Simulation and Performance Evaluation: Methods and Tools (RAPIDO'17), 2017. Stockholm, Sweden.

[31] Open Virtual Platform, [Online]. Available: http://www.ovpworld.org/.

[32] K. Ebcioglu, E. Altman, M. Gschwind, S. Sathaye, Dynamic binary translation and optimization, IEEE Trans. Comput. 50 (6) (2001) 529–548, doi:10.1109/12.931892.

[33] L. Cai, D. Gajski, Transaction level modeling: An overview, in: Proceedings of the 1st IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, in: CODES+ISSS '03, ACM, New York, NY, USA, 2003, pp. 19–24, doi:10.1145/944645.944651.

[34] N. Bombieri, F. Fummi, V. Guarnieri, F. Stefanni, S. Vinco, Hdtlib: an efficient implementation of systemc data types for fast simulation at different abstrac- tion levels, Des. Autom. Embedded Syst. 16 (2) (2012) 115–135, doi: 10.1007/s10617- 012- 9092- z.

[35] N. Bombieri, F. Fummi, G. Pravadelli, Automatic abstraction of RTL IPs into equivalent TLM descriptions, IEEE Trans. Comput. 60 (12) (2011) 1730–1743, doi:10.1109/TC.2010.187.

[36] A. Danese, G. Pravadelli, I. Zandoná, Automatic generation of power state ma- chines through dynamic mining of temporal assertions, Design Automation and Test in Europe (DATE '16), 2016. Dresden, Germany.

[37] P.A. Hartmann, K. Grüttner, W. Nebel, Advanced systemc tracing and analysis framework for extra–functional properties, The 11th International Symposium on Applied Reconfigurable Computing (ARC'15), 2015.

[38] H. Schlender, S. Schreiner, M. Metzdorf, K. Grüttner, W. Nebel, Teaching mixed- criticality: Multi-rotor flight control and payload processing on a single chip, in: M. Törngren, M. Grimheden (Eds.), Proceedings of the Workshop on Em- bedded and Cyber-Physical Systems Education, WESE 2015, Amsterdam, The Netherlands, October 4–9, 2015, ACM, 2015, pp. 9:1–9:8, doi: 10.1145/2832920. 2832929.

[39] K. Grüttner, Model-Implementation Fidelity in Cyber Physical System Design, Springer International Publishing.

[40] R. Görgen, D. Graham, K. Grüttner, L. Lapides, S. Schreiner, Integrating power models into instruction accurate virtual platforms for arm-based mpsocs, 2016. (ARM TechCon 2016). [Online]. Available: http://www.imperas.com/documents/ARM_TechCon_2016_Imperas_OFFIS_Paper_Integrating_Power_Models_into_Instruction_Accurate_Simulation.pdf.

[41] Kura website, 2016. [Online]. Available: http://www.eclipse.org/kura.

[42] Kapua website, 2016. [Online]. Available: http://www.eclipse.org/kapua/.

[43] IEEE-1666, IEEE Standard SystemC Language Reference Manual, 2012. doi:10.1109/IEEESTD.2012.6134619 (IEEE Std. 1666–2011, IEEE Computer Society). ISBN 978-0-7381-6801-2.

[44] S. Vinco, A. Sassone, F. Fummi, E. Macii, M. Poncino, An open-source frame- work for formal specification and simulation of electrical energy systems, in: IEEE/ACM ISLPED, 2014, pp. 287–290.

[45] D. Lorenz, K. Grüttner, N. Bombieri, V. Guarnieri, S. Bocchio, From RTL IP to functional system-level models with extra-functional properties, in: Proceedings of the Eighth IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, in: CODES+ISSS '12, ACM, New York, NY, USA, 2012, pp. 547–556, doi:10.1145/2380445.2380529.

[46] D. Lorenz, K. Grüttner, W. Nebel, Data- and state-dependent power characteri- sation and simulation of black-box RTL IP components at system level, in: 17thEuromicro Conference on Digital Systems Design (DSD 2014), 2014.

[47] M. Petricca, D. Shin, A. Bocca, A. Macii, E. Macii, M. Poncino, An automated framework for generating variable-accuracy battery models from datasheet in- formation, ACM/IEEE ISLPED, 2013.

[48] Vodafone Automotive—Telematic Services, 2016. [Online]. Available: http://www.cobra-group.com/vodafone-automotive.

[49] iNemo website, 2016. [Online]. Available: http://www.st.com/inemo.

[50] EUTH IoT gateways website, 2016. [Online]. Available: http://www.eurotech.com/en/products/devices/iot+gateways.