

INDEXYS, A Logical Step Beyond GENESYS

INDustrial EXploitation of the genesYS cross-domain architecture

<http://www.indexys.eu/>

This paper has been prepared under the lead of Andreas ECKEL
andreas.eckel@tttech.com

INDEXYS Coordinator, TTTech Computertechnik AG

in cooperation with the INDEXYS project partners as follows:

Paul MILBREDT (Audi AG)
Zaid AL-ARS (Delft University of Technology)
Stefan SCHNEELE (EADS Deutschland GmbH)
Bart VERMEULEN (NXP Semiconductors Netherlands B.V.)
György CSERTÁN (OptXware Research and Development Ltd.)
Christoph SCHEERER (Thales Rail Signalling Solutions GesmbH)
Neerai SURI and Abdelmajid KHELIL (Technical University of Darmstadt)
Gerhard FOHLER (Technical University of Kaiserslautern)
Roman OBERMAISSER (Vienna University of Technology)
Christian FIDI (TTTech Computertechnik AG)

ABSTRACT

Embedded computing systems have become a pervasive aspect in virtually all application domains, such as industrial, mobile communication, transportation and medical. Due to increasing computational capabilities of microcomputers and their decreasing cost, new functionality has been enabled (e.g., driver assistance systems) and cost savings have become possible, e.g., by the replacement of mechanical components by embedded computers.

Conventionally, each application domain tends to develop customized solutions, often re-inventing concepts that are already applied in other domains. It is therefore expedient to invest into a generic embedded system architecture that supports the development of dependable embedded applications in many different application domains, using the same hardware devices and software modules.

INDEXYS targets to pave the way from the European Commission Framework 7 GENESYS Project reference computing architecture approach towards pilot applications in the automotive-, railway- and aerospace industrial domains. INDEXYS will follow-up GENESYS project results and will implement selected industrial-grade services of GENESYS architectural concepts.

The results of laying together GENESYS, INDEXYS and the new ARTEMIS project ACROSS, which will develop multi processor systems on a chip (MPSoC) using GENESYS reference architecture and services, will provide integral cross-domain architecture and platform, design- and verification- tools, middleware and flexible FPGA- or chip- based devices lowering OEM cost of development and production at faster time-to market.

1. Introduction

The objective of INDEXYS (**IND**ustrial **EX**ploitation of the genes**YS** cross-domain architecture) is to tangibly realize industrial implementations of cross-domain architectural concepts developed in the GENESYS project in three domains: automotive, aerospace and railway, thereby relating to ARTEMIS-JU Industrial Priority: “Reference designs and architectures”, see reference [1]. GENESYS (Generic Embedded System Platform) is developing a cross-domain architecture according to requirements of the ARTEMIS Strategic Research Agenda. The GENESYS architectural style supports a composable, robust, and comprehensible component-based framework with strict separation of computation from message-based communication. So components can be massively reused in differing contexts. In the GENESYS architecture three integration levels of components are distinguished: **chip-level**, where IP cores communicate via a deterministic Network-on-a-Chip (NoC); **device level**, where chips communicate within a device and **system level**, where devices communicate in an open or closed environment. INDEXYS expands the GENESYS approach by implementing and integrating architectural services into prevailing (real-world) platform solutions. A key goal of INDEXYS is legacy integration, for platform providers – by integrating new architectural services into legacy platforms – and for platform users – by supporting legacy applications. INDEXYS addresses robustness w.r.t. design faults and physical faults by diversity and component replication. INDEXYS targets ARTEMIS-JU Sub-Programme 5, see reference [1]: “Computing environments for embedded systems” by developing new concepts for composable component integration, re-usable dependability services, and a cross-domain tool-chain based on OMGs Model Driven Architecture. By fostering development of re-usable, dependable products and associated services, INDEXYS significantly contributes to competitive advantages of European players in the transportation industries.

Proposed in the first call of the ARTEMIS Joint Undertaking, INDEXYS relates to the ARTEMIS SRA industrial priority “Reference Designs and Architectures” and aims at re-using concepts and designs in multiple industrial domains for different types of applications. INDEXYS is conducted by an international consortium of 10 partners, representing SME partners (2), industrial partners (4) and universities (4). The project is partly funded by the ARTEMIS Joint Undertaking and by national governmental funding agencies and the project partners. The effort required for INDEXYS amounts to 667 man months. INDEXYS has started in April 2009 and will be completed in September 2011.

DECOS, GENESYS, INDEXYS, ACROSS – the Coherent R&D Program Chain

INDEXYS addresses actual instantiations of architectural cross-domain services which are defined through the GENESYS reference architecture template, and over ARTEMIS SRA's (see reference [2]) requirements and constraints. INDEXYS is further based on results of the DECOS project – a predecessor project of GENESYS. DECOS focused at finding common composable design concepts across multiple application domains. With ARTEMIS as a basis, GENESYS extended the DECOS concepts by developing a cross-domain architectural reference template. INDEXYS builds on the DECOS / GENESYS foundation to realize these concepts by instantiating architectural cross-domain services defined by the GENESYS reference architecture template. INDEXYS architectural service instantiations targets three domains: automotive, aerospace and railway, leading to domain specific upgrades of existing architectural solutions. Legacy platforms, such as the TAS Control Platform (see reference [3]) in the railway domain or IMA (see reference [4]) in the aerospace domain will serve as the basis for subsequent instantiation of GENESYS' generic platform services.

Complementing and further enhancing the achievements from DECOS, GENESYS and INDEXYS, the ACROSS project has been submitted as a proposal in the ARTEMIS second call in 2009. The project has been selected for funding and is due to start end of Q1/2010. It will develop a multiprocessor system on a chip (MPSoC) providing an on-chip network with flexible composition of components replying to the market's requirement of composable, reliable, embedded networks. In addition, ACROSS will target the development of tailored middleware components and suitable design, development and verification tools to generate a powerful cross-industry platform.

2. R&D Results from Previous Programs Establish INDEXYS Basis

2.1. DECOS Paving the Way for Cross-Domain Architecture Reference Template

As a European Commission Framework 6 Integrated Platform Programme, DECOS (see reference [13]) targeted the development of fundamental technologies facilitating the paradigm shift from federated to integrated design of dependable real-time embedded systems. DECOS provided means for systematic design and development of integrated, electronic sub-systems in embedded applications by (a) cost reduction in electronic hardware, (b) by enhancing dependability by design, (c) by enabling modular certification, (d) special diagnosis and maintenance support, (e) by offering individual intellectual property protection. Applications were deployed in automotive, aerospace and industrial control domains.

The DECOS results offered the first proof of concept for the GENESYS basic idea of developing a cross-domain architecture reference template. The DECOS results fundamentally enhanced the means for design, analysis and tools for integrated, dependable, real time embedded systems (see also Figure 1).

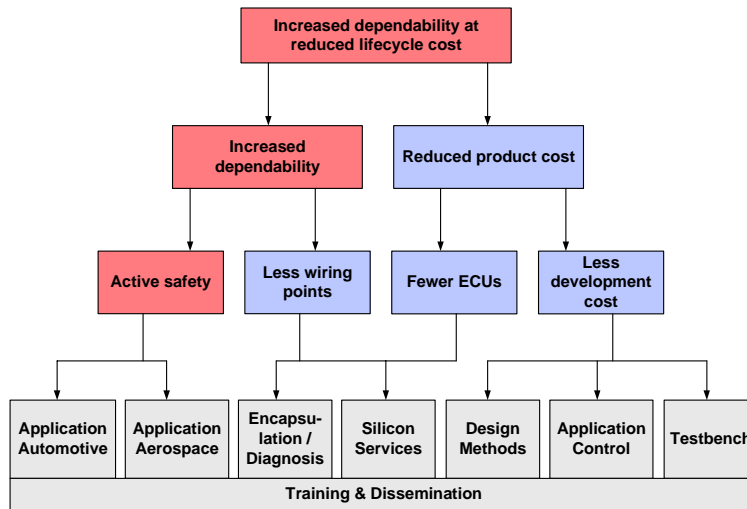


Figure 1: DECOS Results

Detailed information is available in reference [13].

2.2. Introduction on the GENESYS Project

Conventionally, each application domain tends to develop customized solutions, often re-inventing concepts that are already applied in other domains. It is therefore expedient to invest into a generic embedded system architecture that supports the development of dependable embedded applications in many different application domains, using the same hardware devices and software modules. Furthermore, increasing capabilities of microcomputers and decreasing cost foster a change from mechanically to electronically controlled functions in all industrial domains.

The world of embedded systems, in particular when respecting various industrial domains with its different application requirements, is broad and diverse. The technological situation is strongly fragmented and the expectations of the increasing number of users are permanently rising.

In order to take advantage of the economy of scale of the semiconductor industry, designing and developing a cross domain architecture reference template for embedded systems to be used in various industrial domains can easily be justified (this chapter frequently makes reference to [5]) due to faster time to market and reduced design and implementation cost resulting from re-using once developed approaches.

H. Kopetz and R. Obermaisser summarise GENESYS as follows (see reference [5]): Mainly three challenges have driven the development of the GENESYS reference architecture: (a) Complexity Management, (b) Robustness, (c) Energy Efficiency.

GENESYS established a platform architecture providing a minimal set of “core services” and a plurality of optional services (i.e. special communication services, diagnostic services, etc.) predominantly implemented as self-contained system components selected due to the industrial domain application requirements (see Figure 2).

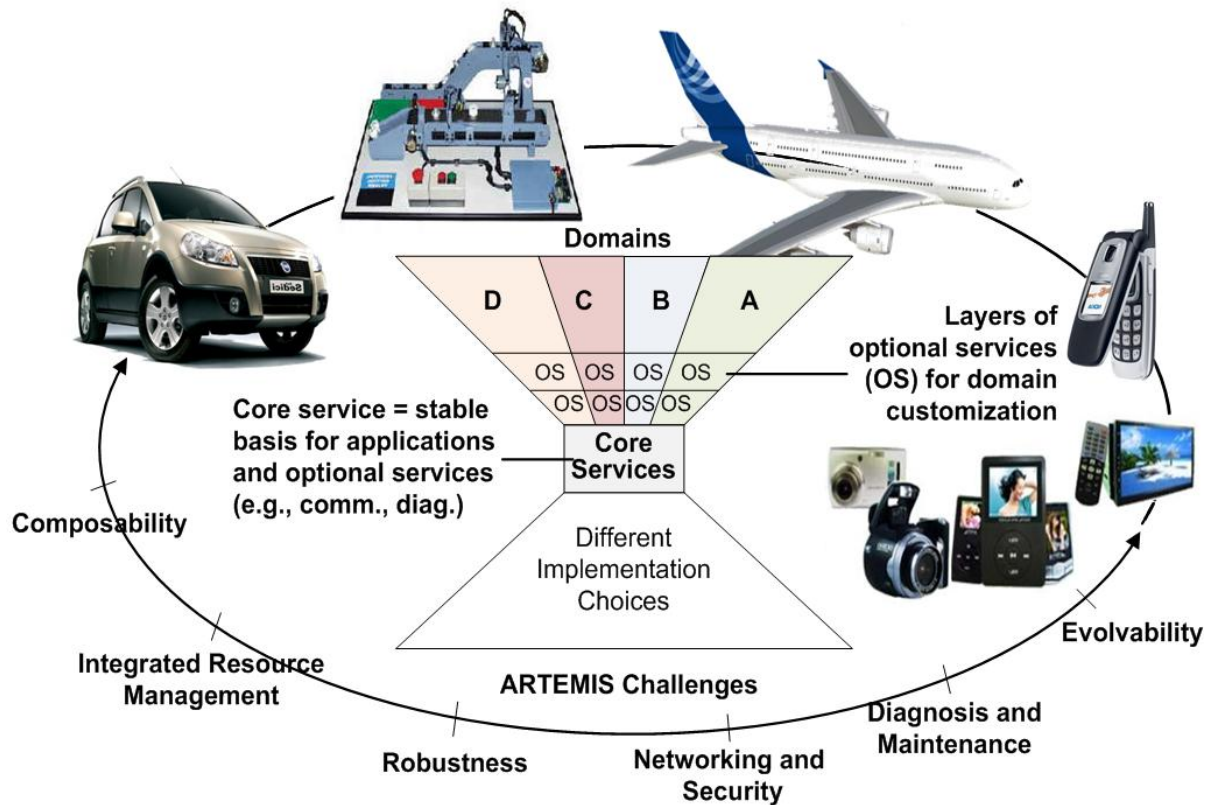


Figure 2: GENESYS overview (see reference [9])

The GENESYS reference architecture targeted to provide (a) a consolidated cross-domain architectural style, (b) a reference architecture template, and (c) a cross-domain development methodology.

The GENESYS Reference Architecture has been described in detail by R. Obermaisser and H. Kopetz, Vienna University of Technology, see reference [5]. The book is available free of charge for download from <http://www.genesys-platform.eu/>.

2.3. Results used from the GENESYS Project

The GENESYS reference architecture template provides architectural services as a baseline for the development of applications. GENESYS distinguishes between core services and optional services.

As illustrated in Figure 3, the GENESYS reference architecture template provides specifications for a comprehensive set of platform services. These platform services can be partitioned into the following three service categories: core services, optional services and domain specific services.

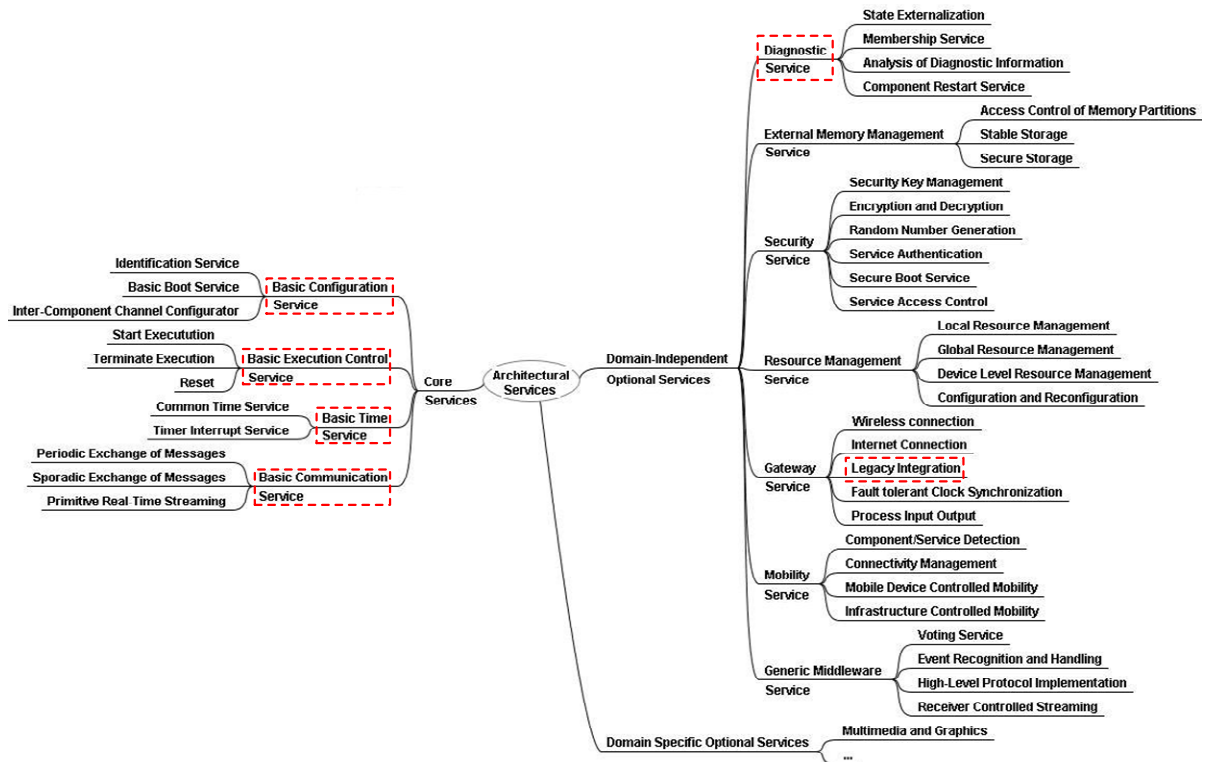


Figure 3: Services of the Reference Architecture Template

2.3.1. Core Services

The core services are mandatory and thus part of any instantiation of the GENESYS architecture. The core services are minimal in the sense that only those services which are absolutely indispensable to build higher-level services or to maintain the desired properties of the architecture are included in the set of core services. In GENESYS the core services must be amenable to certification. For this reason they must be deterministic and simple.

2.3.2. Optional Services

The optional services are built on top of the core services. Optional services are an open set of services that can be extended as needed. All or only a subset of these optional services can be selected for any particular instantiation of the architecture. Most of the optional services are implemented in self contained system components that interact with the generic middleware (GEM) of the application components by the exchange of messages. In case an optional service is mature and stable, it can be implemented in the form of a hardware component, which leads to a significant improvement in the energy efficiency.

2.3.3. Domain Specific Services

The domain specific services are a sub-set of the optional services and support specific features required by the particular domain or application under consideration.

3. The INDEXYS Approach – a Reply to a Market Pull

Generally, market domains such as automotive, aerospace or railway use their specific processes, development technologies, development tools, verification and validation approaches and test methodologies. Various standards have been established and enormous budgets are required to permanently maintain and improve these technologies with respect to their platform components and performance. Increasing cost pressure and the shortening of “time-to-market” requirements caused the large players in the various market domains to “look over the fence” and check whether processes, methods and technologies from other market domains wouldn’t be suitable for their own field of application as well in order to make use of “economy of scale” and reduce cost and time-to market appropriately for their own competitive advantage.

Thus the idea of establishing a cross domain data communication architecture template and a platform approach, such as offered by INDEXYS, definitely replies to market trends of many domains in parallel. INDEXYS shows the flexibility in integrating domain specific services in combination with template based core services allowing the use of “proven” and “existing” design building blocks and thus resulting in the targeted advantage of reducing cost and time to market by using once developed, cross-industrial platform based technologies and proofs concept in their automotive, aerospace and railway domain demonstrators.

In addition, cross domain industrial use will foster permanent improvements and enhancements resulting from different area of application. Thus the potential community will benefit from a higher maturity of the platform in the long run compared to just developing, maintaining and improving such platform internal of one domain only. The likelihood for being confronted with system based errors is therefore reduced to a minimum and the speed and efficiency of development is optimized.

3.1. Overview of the INDEXYS Project

The objective of INDEXYS is to enable industrial exploitation of GENESYS’ cross-domain architectural services, thereby particularly focusing on (but not restraining to) the domains: aerospace, automotive and railway.

The overall strategy of the INDEXYS work plan is defined by three phases, namely Analyze, Implement, and Evaluate, detailed as (see Figure 4):

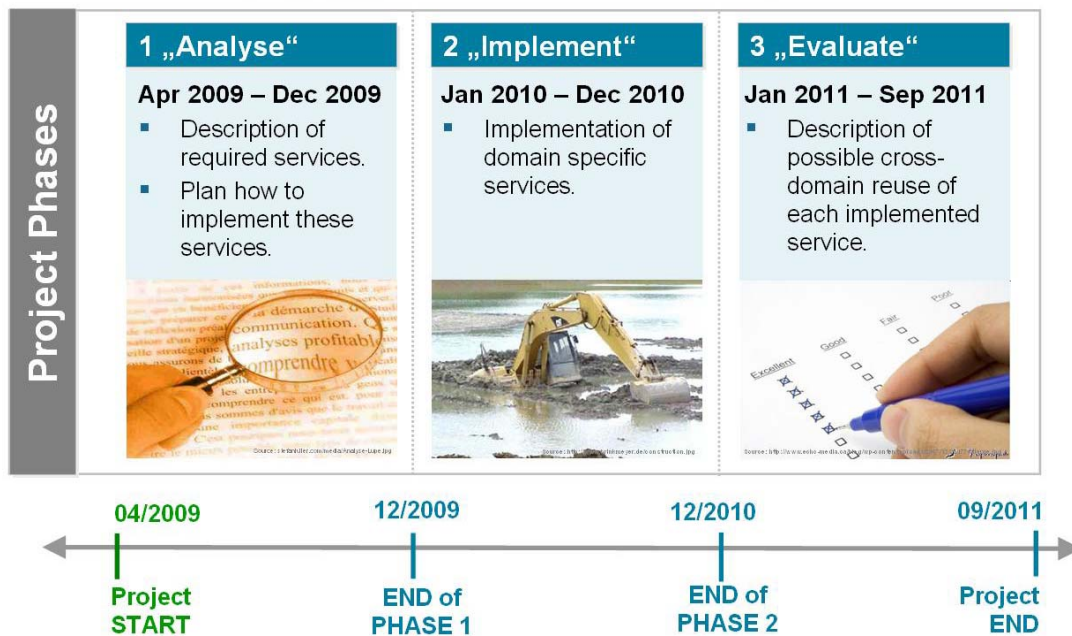


Figure 4: INDEXYS Project Phases

Phase 1: “Analyze”: Analyze and prioritize GENESYS architectural services and create fundamental paradigms, methods and tools supporting embedded system design for a broad range of applications. This phase will investigate on topics such as: general tool-chain concepts, i.e., development of a comprehensive, customizable tool-chain based on OMG’s Model Driven Architecture (MDA), domain specific modeling based on domain specific modeling languages (DSL), support for advanced synthesis solutions based on COTS tools and configurable transformations, and on-line fault handling that copes with increasing transient fault rates in modern embedded devices. The “Analyze Phase” will evaluate the gap between existing, reusable technology and GENESYS architectural services deemed relevant within INDEXYS and summarize the results in an analysis. All required services will be specified and a plan will be developed how to implement them.

Phase 2: “Implement”: Based on the results of the first phase, three domain specific applications (Aerospace, Automotive and Railway) will be developed. In each of the three domains, a certain set of architectural services will be instantiated. This instantiation will either be by reuse of existing

technology or by new developments, where a strong focus will clearly be on reuse of existing components, methods and tools. At that point it should be mentioned that several project partners have closely cooperated in the DECOS project. It is thus planned to (re)use results, i.e., methods, tools and concepts of DECOS wherever appropriate. The “Implementation Phase” will investigate what is required to instantiate GENESYS architectural services so that these services can be exploited for concrete platforms in the automotive, aerospace and railway domains. As result, INDEXYS will develop the domain specific prototype implementations of GENESYS architectural services.

Phase 3: “Evaluate”: As soon as prototype implementations of architectural services are available, an evaluation will take place to find out if the domain specific architectural service implementations can be reused across other domains targeted by INDEXYS. As it is a key objective of INDEXYS to maximize cross-domain reuse, the objective of this phase will be to enable reuse of as many architectural service implementations as possible. INDEXYS will define the required means for enabling reuse of INDEXYS’ architectural service implementations across further domains. The possible reuse of each service implemented during the second phase will be specified.

3.2. INDEXYS Builds on GENESYS and Enhances the Results Achieved

The reference architecture template generated in the course of the GENESYS project offers four core services summarized below (see Table 1). These services map to several of the domain specific requirements and features. The core services consist of a couple of sub-services. The INDEXYS Demonstrators make use of these services according to the Table 1 below. Please note that throughout all INDEXYS project aspects except the demonstrators all services as identified in the Table 1 are considered and supported.

Core Service Name	Sub-Service Name	Automotive	Aerospace	Railway
Basic Configuration	Identification Service	yes	yes	yes
	Basic Boot Service	yes	yes	yes
	Inter-Component Channel Configurator	yes	yes	yes
Basic Execution Control	Start Execution	yes	yes	yes
	Terminate Execution	yes	yes	yes
	Reset	yes	yes	yes
Basic Time	Common Time Service	yes	yes	yes
	Timer Interrupt Service	yes	yes	yes
Basic Communication	Periodic Exchange of Messages	yes	yes	yes
	Sporadic Exchange of Messages	yes	no	yes
	Primitive Real-Time Streaming	no	no	no

Table 1: GENESYS Core Services in INDEXYS Demonstrators

The optional architectural services of the reference architecture template facilitate the establishment of the identified requirements and features are illustrated in Table 2 (Again, the table refers to the INDEXYS demonstrators while all optional services are considered and supported in all INDEXYS project aspects except the demonstrators).

Service Name	Automotive	Aerospace	Railway
State Externalization	no	yes	no
Membership Service	yes	yes	yes
Analysis of Diagnostic Information	yes	yes	no
Component Restart Service	yes	yes	yes
Access Control of Memory Partitions	no	no	no
Stable Storage	no	no	no
Secure Storage	no	no	no
Secure Key Management	no	no	no
Encryption and Decryption	no	no	yes
Random Number Generation	no	no	no
Service Authentication	no	no	no
Secure Boot Service	no	no	no
Service Access Control	no	no	no
Local Resource Management	yes	yes	yes
Global Resource Management	no	no	no
Device Level Resource Management	no	no	no
Configuration and Reconfiguration	no	no	no
Wireless connection	no	no	yes
Internet Connection	no	no	yes
Legacy Integration	yes	yes	yes
Fault-tolerant Clock Synchronization	yes	yes	yes
Process Input Output	yes	yes	yes
Component/Service Detection	no	no	no
Connectivity Management	no	no	no
Mobile Device Controlled Mobility	no	no	no
Infrastructure Controlled Mobility	no	no	no
Voting Service	yes	yes	yes
Event Recognition and Handling	yes	yes	yes
High-Level Protocol Implementation	no	no	yes
Receiver Controlled Streaming	no	no	no

Table 2: GENESYS Optional Services in INDEXYS Demonstrators

3.3. The INDEXYS Project Consortium

The ten member INDEXYS project consortium coordinated by TTTech Computertechnik AG is well balanced consisting of four industrial partners evaluating the developments in their demonstrators (Audi AG [automotive domain industrial partner], EADS Deutschland GmbH [aerospace domain industrial partner], NXP Semiconductors & Thales Signalling Solutions GesmbH [railway domain industrial partner]), two SMEs providing the technical know-how as the market leaders in the specific technological area (OptXware Research and Development Ltd. & TTTech Computertechnik AG) and four universities representing most relevant academia (Delft University of Technology, Technical University of Darmstadt, Technical University of Kaiserslautern & Vienna University of Technology). The Consortium combines technical excellence of four European countries, Austria, Germany, Hungary and The Netherlands.

3.4. The INDEXYS Project Goals – Progress Beyond the State of the Art

Contrary to the approach of many present platform solutions, which are tailored to a specific domain, INDEXYS aims at the development of reusable architectural services that can be exploited across platforms of different domains. INDEXYS' architectural service implementations will support a gradual shift towards higher reusability of services across different domains (particularly across automotive, aerospace and railway domains) due to lower cost by availability of existing solutions, and by existing experience with these solutions in the engineering community, see reference [7].

INDEXYS will build on prevailing platform solutions such as AUTOSAR for automotive systems, IMA for aerospace systems (i.e. AFDX (see reference [9]), see also SPIDER project, see reference [10]), and TAS Control Platform (see reference [8]) for railway systems with the goal to implement selected GENESYS services within these platforms.

INDEXYS will further observe (and potentially take up) related technical approaches of other domains such as telecommunication or consumer electronics.

Technological Aspects:

In line with the results of GENESYS, INDEXYS will implement architectural services according to GENESYS' cross-domain architectural style. Thereby, the following **technological aspects** will be considered for complementing existing platform solutions (and thereby progressing beyond the state of the art): (a) Networking and Resource Management (i.e. development of scalable, deterministic communication and design methods), (b) Robustness, Diagnosis and Maintenance (i.e. architectural services ensuring the “capability of a system to deliver an acceptable level of service despite the occurrence of faults”), (c) Composability (i.e. architectural support of the constructive composition of large systems out of components and sub-systems without uncontrolled emerging behavior or side effects) and (d) Methodology and Tools (i.e. multi-paradigm tool/methodology approach based on the Model Driven Architecture (MDA) and on the Model Driven Development).

3.5. The INDEXYS Developments

INDEXYS will first of all develop methodologies (tool chain, modelling, verification and validation, on-line fault handling and complexity management) and then focus on the industrial domains (Automotive, aerospace and railway) and conclude the project in a cross-domain integration phase. As usual in European Commission projects this is accompanied by a dissemination/exploitation and standardization work package and project management activities (see Figure 5).

3.5.1. Methodology

The objectives within this INDEXYS topic will analyze and prioritize GENESYS architectural services and thereby create fundamental paradigms, methods and tools supporting embedded system design for a broad range of applications. Furthermore, an initial project alignment according to the final GENESYS results is performed. Analysis and implementation of exploitable cross-domain services is provided. INDEXYS Methodology covers (a) general tool-chain concepts, (b) domain specific modeling and synthesis support, (c) design time verification and validation, (d) on-line fault handling and (e) complexity management.

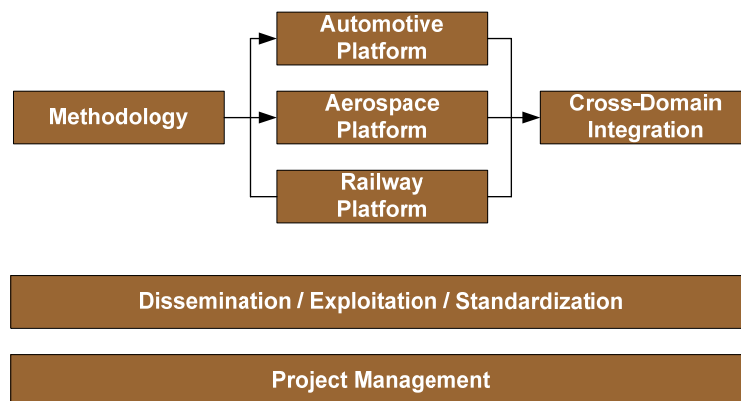


Figure 5: INDEXYS Development and Work Plan Overview

3.5.2. Industrial Platforms

An overview on the three industrial domains and their innovation is provided in Figure 6.

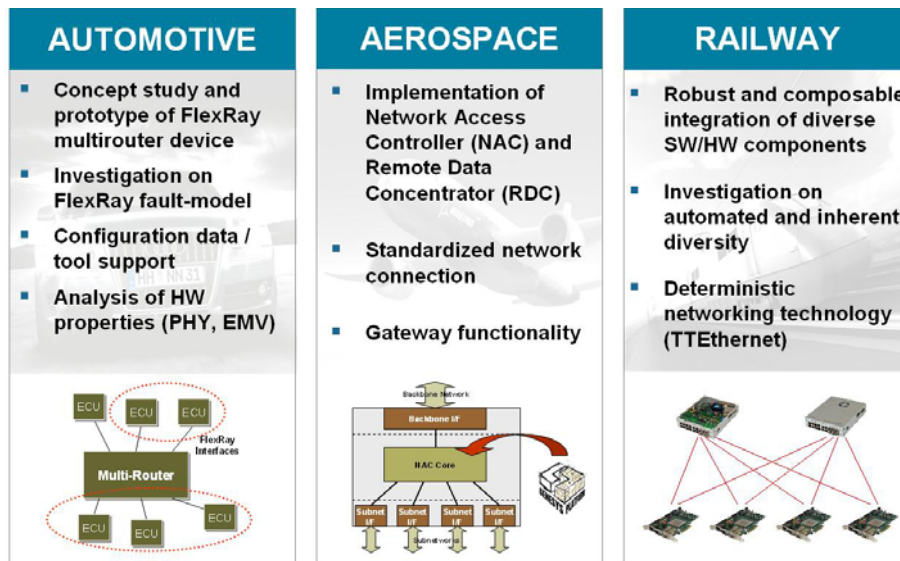


Figure 6: INDEXYS Innovation per Domain

Automotive Platform

The objective of the automotive platform takes under consideration the increasing complexity of current and future automotive systems requiring composable subsystem integration. Composable subsystem integration guarantees that properties which have been established at subsystem level are not invalidated through the integration of these subsystems into a larger system. It is the objective of this work package to investigate on and to enable composable integration of real-world in-vehicle network technology of prevailing automotive networks, such as CAN and FlexRay, also considering Functional Safety. The prototype implementation will be validated also for their composability by thorough validation in a target vehicle network.

With respect to multiple CAN networks required in automotive industry, INDEXYS will elaborate a completely new integration concept. This integration concept will be based on a GENESYS conformant composable CAN interconnect that supports the legacy CAN interface of existing ECUs, increases the CAN network performance and will provide a programmable gateway service between different CAN networks.

In INDEXYS the concept of a FlexRay multi-switch will be investigated and prototypically implemented. A multi-switch device directly connects to FlexRay end-systems in a star topology and allows parallel transmission of messages from different senders at the same time (given that the receivers are disjunctive). The methodology for cross-domain reusable safety modules will be applied in selected areas on the prototypes. This means: (i) early definition and consideration of safety requirements, (ii) ongoing coaching of the development for functional safety needs, and (iii) evaluation of safety, including reachable Hardware Safety Integrity.

Demonstrator Automotive - FlexRay Multi-Switch

The FlexRay “multi-switch” is a cut-through switch for FlexRay networks. It switches a number of FlexRay branches according to a pre-defined static schedule. The communication elements are forwarded with minimal delay and are not stored and forwarded at a later point in time.

A FlexRay multi-switch is a device which is physically similar to the FlexRay Active Star device, but in contrast to the Active Star, it implements a selective switching of the communication paths according to a configured switching schedule. The multi-switch is able to provide additional functionality of complex data traffic paths and also isolation of branches Figure 7.

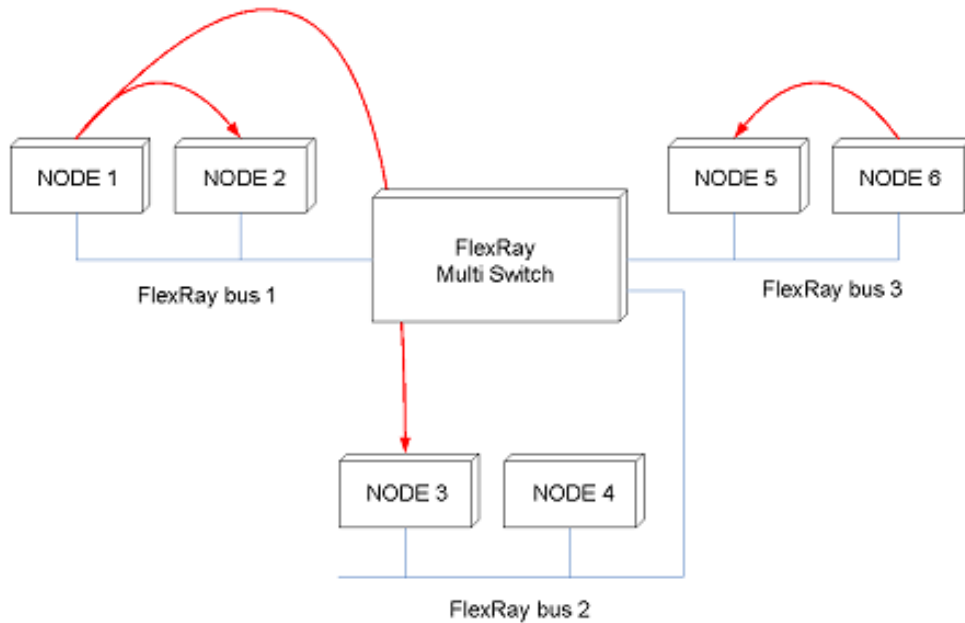


Figure 7: Automotive Platform FlexRay Cluster with FlexRay Multi-Switch

Aerospace Platform

The objective of the Aerospace Platform deals with Integrated Modular Avionics (IMA), where distributed functional computations are centralized on a group of Central Processing Modules with powerful CPUs interfacing small, easy to maintain and reliable Remote Data Concentrators. This state-of-the-art platform concept is widely used for safety-critical control functions of the airplane, but currently not for cabin control applications. The objective is to extend the IMA approach due to enhancements of a Remote Data Concentrator and of a Network Access Controller (NAC) for cabin control applications.

INDEXYS will specify and develop a simple System-on-a-Chip solution of a Remote Data Concentrator for transducer interfacing in distributed aerospace applications. The Remote Data Concentrator will offer a standardized network connection to a time-triggered field bus (e.g., TTP).

The task of Network Access Controller (NAC) is to provide Gateway functionality between a high-speed backbone (e.g., Ethernet) network and up to eight linear buses with several passenger oriented devices. A main focus within aircraft cabins is the development of a system wide cabin-communication architecture that incorporates all electronic cabin systems. Currently, there exist three separate cabin systems: CIDS (cabin interconnection data system), ALNA (airline network architecture), and IFE (in-flight entertainment).

A cabin backbone network (e.g., Fast Ethernet, TTEthernet) interconnects the various components of the cabin management system. The Network Access Controller (NAC) with smart wireless interfaces provides redundant and secure links. Moreover, the network must provide sufficient reliability, fault tolerance, guaranteed bandwidth, high-integrity, bounded latency and jitter, security, scalability, reconfigurability, and interoperability for various heterogeneous components. INDEXYS will specify and develop a Network Access Controller based on architectural and modular principles. Thereby, the focus will be on device level integration.

Several GENESYS principles will be addressed such as complexity management (i.e., reduction of cognitive complexity is achieved through small and easily understood interfaces between core processing modules and associated transducers), component based design (i.e., separation of processing devices and input/output devices and communication over linking interfaces), hard and soft components (i.e., FPGA based implementation of Remote Data Concentrator), message passing (i.e., message based Remote Data Concentrator interface), composability (i.e., deterministic communication over time-triggered network) and the concept of a common time (i.e., global time which is shared across the network).

Demonstrator Aerospace - Network Access Controller (NAC)

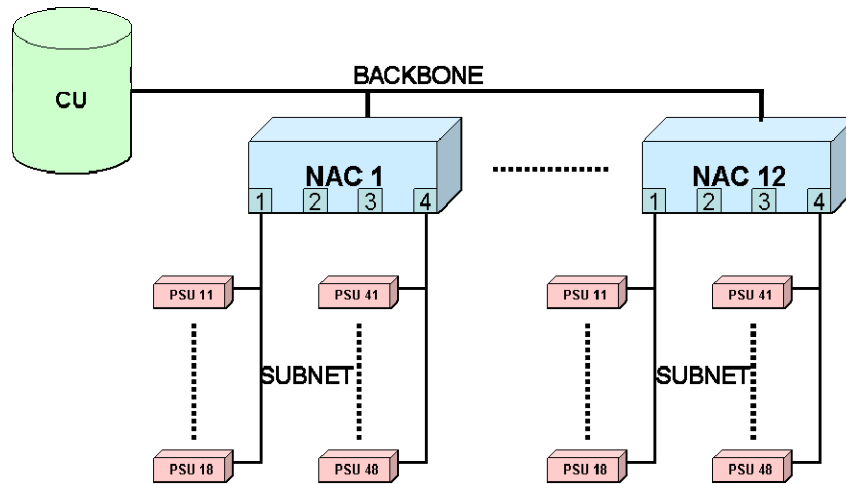


Figure 8: Cabin communication network architecture

Figure 8 shows the principle structure of a network architecture used to provide connectivity from a central unit like a server to passenger oriented devices like a PSU in an aircraft cabin for cabin control applications. This cabin communication architecture should incorporate all electronic cabin systems.

The network consists of one or more Central Units (CU), Network Access Controllers (NAC) and Passenger Service Units (PSU). A high data rate backbone connects up to 12 NACs with the CU. Each NAC provides at least four subnets for connecting to the network up to eight PSUs per subnet.

With this configuration it is possible to connect 32 passenger oriented devices to one NAC. In total up to 384 passengers oriented devices are possible with the use of 12 NACs.

The NAC itself connects the high data rate backbone with the sub-networks. Figure 9 shows the block diagram of a NAC. The NAC has a modular based structure with generalized interfaces to the backbone and to the sub-networks. The NAC Core Module provides gateway functionality between the backbone and the sub-networks. The backbone network is based on Ethernet communication protocol whereas the sub-networks can be implemented to handle protocols like CAN, Ethernet, etc.

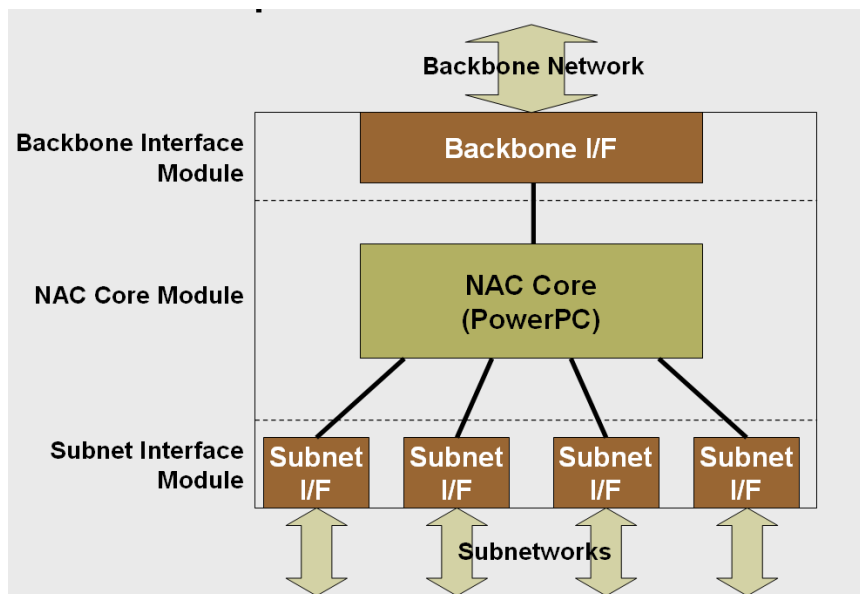


Figure 9: Block diagram of Network Access Controller (NAC)

Demonstrator Aerospace - Remote Data Concentrator (RDC)

The task of a Remote Data Concentrator (RDC) is to interface transducers (i.e., sensors and actuators) in the aircraft. Remote Data Concentrators are connected via communication systems to the Central Processing Modules. To achieve a highly deterministic behavior for the RDC communication a time triggered communication protocol (TTP) has to be used.

In the past TTTech developed a table driven communication layer (TD-COM Layer, see Figure 10) for TTP in software to make use of the reduced certification effort during reuse. The TD-COM Layer implements a high-performance communication layer between TTP networks and host applications. The TD-COM Layer can support up to two TTP networks, each being connected by a separate TTP controller.

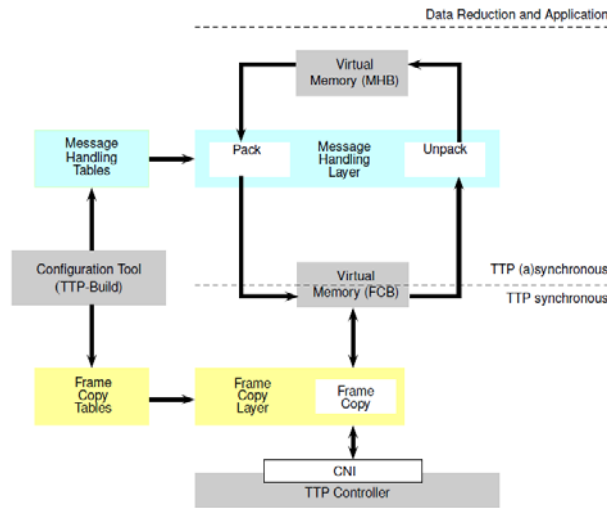


Figure 10: TD-COM Layer overview

For simple distributed communication nodes as Remote Data Concentrators are a solution with the TD-COM layer requires a lot of CPU power for executing the packing and unpacking of messages. This hints to a TD-COM implementation based on a FPGA or moreover as ASIC.

Railway Platform

The majority of Thales Rail SIL4 signaling and train protection system products worldwide is based on a generic fault-tolerant computer platform (HW, OS, Middleware), which has been developed during the last decade by the competence centre of Thales Rail Signaling Solutions Austria (former Alcatel Transport Automation Solution). After the successful rollout of the first generation of the system (called "TAS Control Platform") in more than 20 countries on 4 continents, the TAS Control Platform is now going for the second generation. Major items on the roadmap of TAS Control Platform 2.x is the architectural support for application binary diversification and the increasing use of COTS components.

INDEXYS will develop mitigation strategies to cope with unknown faults in reused components to make the use of off-the-shelf components possible. The CENELEC standards highly recommend the use of diversity to mitigate the risk of undetected faults and to increase robustness in complex components, i.e., the implementation of diverse hardware/software components. In addition, INDEXYS will develop a novel concept for the implementation of fault-containment regions as defined in GENESYS. Conventionally, fault-containment regions w.r.t random hardware faults are formed by active redundant hardware components. INDEXYS seeks to implement fault containment regions on a single hardware channel running diverse application software channels. These software channels are being deduced automatically from legacy source code. The motivation for this approach is to save hardware costs in high volume applications without having the burden of N-Version programming during development.

The integration of these diverse hardware/software components must be composable so that the properties of each independently developed component are not invalidated by its integration into a larger system. The key pre-requisite for composability is deterministic system behavior.

TTEthernet is a novel communication protocol that has been designed with the requirements to provide temporal deterministic communication and to support standard Ethernet communication without the need to change or configure higher level communication protocols, like IP, TCP, UDP, FTP. A TTEthernet system consists of a set of computer nodes interconnected by a specific switch called TTEthernet switch. A node can be either a standard Ethernet node or a TTEthernet node. A standard Ethernet node consists of a COTS Ethernet controller and a host computer. A TTEthernet node consists of a TTEthernet communication controller that executes the TTEthernet protocol and a host computer that executes the user application.

TTEthernet nodes (end systems) can be implemented either in hardware (FPGA based TTEthernet communication controller is available) or by using a COTS Ethernet controller and by implementation of the TTEthernet stack on top of a COTS Ethernet controller. In the INDEXYS project, it is planned to implement a SW based end system for TAS Control Platform hardware (Intel PC based).

Demonstrator Railway – TTEthernet Integration into TAS Platform

The TAS Control Platform is an open, scalable software architecture oriented towards established industrial computing standards. The communication system offers a number of standard communication services, such as Internet Protocol (TCP/IP family), serial lines and field buses (CAN controller area network, TTP time triggered protocol, PROFIBUS Process Filed Bus), as well as specific safe communication services conforming to European Committee for Electro technical Standardization (CENELEC) standards, see reference [12].

At the hardware level, the TAS Control Platform uses commercial off-the-shelf components, which are supplemented by added-value services for railway control systems.

TAS Platform Architecture Overview

Figure 11 shows the component architecture of TAS Platform. A “Computing Node” (CN) is the logical target computer. It may consist of 1 up to 3 individual “Computing Elements” (CEs), depending on the application systems replication degree. A CE refers to a physical computer that is synchronized with other CEs of the same CN. A “Task Set” (TS) is a set of tasks forming a logical application software entity.

The synchronization medium serves inter replica synchronization and is implemented as point-to-point network based on Ethernet.

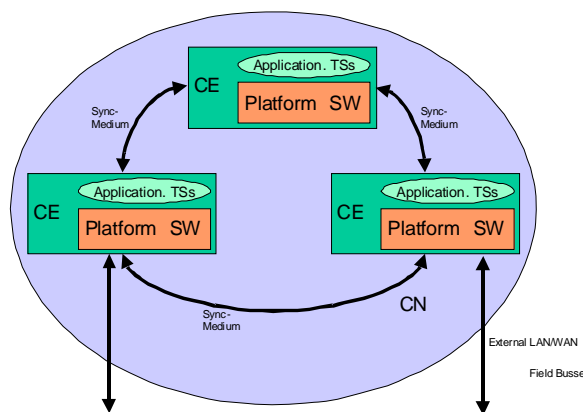


Figure 11: TAS Platform Component/System Architecture

Implementing the Software-based TTEthernet protocol into diverse computing elements of a computing node on TAS Platform will increase the deterministic behavior of the communication system with the advantages of a Time Triggered Communication system.

The Software-based TTEthernet specifies a special implementation of TTEthernet which was created to make use of the time-triggered communication benefit implemented in software without the fault tolerant features of the hardware-based solution enabling also high throughputs for much lower costs. If the use case requires fault tolerance mechanisms then they have to be implemented in the application on top of the TTEthernet API Library.

Figure 12 shows the layered structure of the software-based TTEthernet implementation on a host without an operating system including the TTEthernet protocol core layer embedded between the hardware layer and the API library.

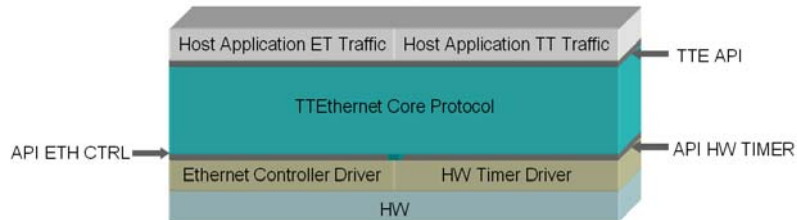


Figure 12: Software-Based TTEthernet detailed architecture

Setting up an application with software-based TTEthernet on a platform with an operating system a driver has to be established on top of the TTEthernet core protocol to get access to the core functions (see Figure 13).

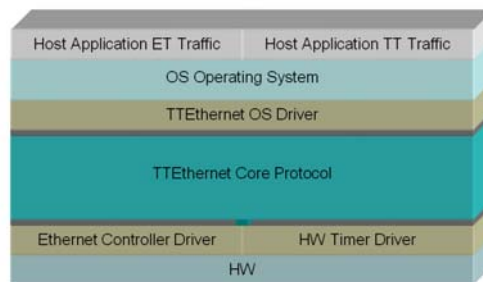


Figure 13: Software-Based TTEthernet with Operating System Driver

3.5.3. Cross-Domain Integration

A key goal of INDEXYS is to enable cross-domain reusability of architectural service implementations which are instantiated for platforms in the automotive, aerospace and railway domains. Cross-domain reusability is the ability to reuse architectural service instantiation which have been implemented for one of the targeted domains (i.e., automotive, aerospace, railway) in other domains. Cross-Domain Integration will focus on analyzing, steering, and evaluating cross-domain reusability during the actual project work. A particular focus will be the reusability within the other targeted domains of INDEXYS. However, reusability can also apply for domains which are not directly in the scope of INDEXYS such as consumer electronics or industrial control systems.

Reusability of safety-related modules across different domains will be supported by deriving a generic methodology for managing reuse of safety-related modules. The methodology shall be applied to one implementation to test its usability in real life. This will allow improvement of the concept. The so improved concept and the experience gained from applications will be investigated with experts from other domains. If suitable the generic methodology can be published and brought into domain standardization groups for further propagation. A good methodology for reuse will allow sustaining advantages from the considerable investments made by companies in developing safety modules with the appropriate safety evidence. This enables a considerable competitive advantage for safety-related developments.

4. ACROSS – Closing the Gap

The objective of the ACROSS project to develop and implement an ARTEMIS cross-domain architecture for embedded MPSoCs based on the architecture blueprint developed in the FP7 project

GENESYS (Generic Embedded System Architecture). ACROSS will result in the design of a generic Multi-Processor Systems-on-a-Chip (MPSoC) and a first implementation in an FPGA. The ACROSS MPSoC will provide a stable set of core services as a foundation for the component-based development of embedded systems with short-time-to-market, low cost and high dependability. The ACROSS-MPSoC will be demonstrated as a universal platform for automotive, aerospace and industrial control systems in order to realize the benefits of the economies of scale of the semiconductor technology. Additionally, the ACROSS-MPSoC platform provides significant potential for being adopted by other industries with safety-critical data communication requirements such as applications in the medical-, power generation -, (i.e. atomic power plant control equipment), space-domains, to mention just a few. Using the core services of the ACROSS-MPSoC, a library of middleware services will be realized in the ACROSS project. Generic middleware will offer services to be used in multiple application domains (e.g., fault-tolerance, diagnosis, security), while domain-specific middleware will implement domain-specific services for specific domains (e.g., AUTOSAR services for the automotive domain, IMA services for the avionic domain). Another significant result of the project will be a general design methodology, supported by appropriate adaptable tools, for the implementation of ACROSS-based applications. The benefits of the cross-domain architecture will be shown in demonstrators from the targeted application domains. It is planned to set up demonstrators for the automotive-, the aerospace- and the industrial control domains.

5. Conclusion

The introduced projects DECOS, GENESYS, INDEXYS and ACROSS do perfectly complement each other. Initially, the DECOS project demonstrated the advantages of the design, development and validation of an embedded platform for dependable, integrated systems.

The next step beyond was taken in GENESYS providing a flexible, cross domain reference architecture defining the fundamental architectural principles required. GENESYS specified, developed and designed the core services and a set of initial optional services allowing a start in applying the results in industry.

INDEXYS now provides the first implementation and proves the feasibility in establishing demonstrators for the automotive-, the aerospace- and the railway sectors using the GENESYS reference architecture platform approach.

To finally provide means for industrial series production visions, ACROSS designs, develops and verifies a FPGA based device integrating a GENESYS architecture on one chip. This will bring development cost further down and will enable the large scale application of the technological step taken in GENESYS and INDEXYS.

As a final step in a R&D project family industry will obtain all tools, methodologies and embedded building blocks to efficiently and competitively implement systems based on the GENESYS reference architecture. The fact that the entire platform is available will pave the way and significantly improve the chance that different industries will pick up the technology for some of their visionary projects in close future.

6. References

- [1] The ARTEMIS Joint Undertaking Annual Work Programme 2008, ARTEMIS-PAB-17/08
- [2] ARTEMIS Joint Undertaking Strategic Research Agenda, Reference Designs and Architectures, Edition May 2006 (ARTEMIS SRA Working Group)
- [3] H. Kantz, N. König, TAS Control Platform: A Vital Computer Platform for Railway Applications. Technology White Paper, 2004
- [4] Aeronautical Radio Incorporated (ARINC), Annapolis, MD, USA. ARINC Specification 651: Design Guide for Integrated Modular Avionics, November 1991.
- [5] R. Obermaisser, H. Kopetz, “GENESYS: An ARTEMIS Cross-Domain Reference Architecture for Embedded Systems“, Südwestdeutscher Verlag für Hochschulschriften Aktiengesellschaft & Co.KG, Saarbrücken, Germany, 2009, ISBN 978-8381-1040-0. The book can be downloaded free of charge: <http://www.genesys-platform.eu/>
- [6] Presentation on GENESYS by Roman Obermaisser, Vienna University of Technology

- [7] The information refers to the INDEXYS Description of Work (according to the contractual agreed content of project work).
- [8] As for AUTOSAR and IMA, summary descriptions are contained from the GENESYS description of work (DoW). The summary of the TAS platform is taken from the technology white paper: “H. Kantz, N. König, TAS Control Platform: A Vital Computer Platform for Railway Applications”.
- [9] Avionics Full-Duplex Switched Ethernet. (2008, October 22). In Wikipedia, The Free Encyclopedia. Retrieved 13:13, November 10, 2008, from http://en.wikipedia.org/w/index.php?title=Avionics_Full-Duplex_Switched_Ethernet&oldid=246938506
- [10] <http://shemesh.larc.nasa.gov/fm/spider/>
- [11] Cf. Simulink-based MPSoC Design: New Approach to Bridge the Gap between Algorithm and Architecture Design; Atat, Y.; Zergainoh, N.-E. VLSI, 2007. ISVLSI apos; 07. IEEE Computer Society Annual Symposium, 9-11 March 2007
- [12] Refer to the following homepage for further information about CENELEC and related standards: <http://www.cenelec.eu>
- [13] DECOS homepage: <http://www.decos.at>