High-Quality Customizable Embedded Software from COTS Components

Farokh B. Bastani
Department of Computer Science
University of Texas at Dallas
Richardson, TX 75083-0688
Email: bastani@utdallas.edu

Dramatic advances in computer and communication technologies have greatly promoted the growth of embedded telecommunication systems. More and more critical applications, such as banking and financial services, remote patient monitoring systems, transportation, etc., are being developed. The software for these applications is becoming increasingly sophisticated and complex and this trend will accelerate over the next few years with the development of "software-defined telephony". To support these critical applications, it is necessary to achieve high quality and rigorously demonstrate that high quality has in fact been achieved. In today's highly competitive environment, it is also essential to have accelerated development schedules and the capability to quickly customize and adapt products for niche markets and to satisfy diverse regional standards and procedures.

To meet all these challenges, software development technology is rapidly shifting away from low-level programming issues to automated code generation and integration of systems from components, either Commercial-Off-The-Shelf (COTS) components or specially developed in-house components. This is made possible by numerous recent breakthroughs in software technology, including web-based cooperative software development, in-process monitoring, agents, Java, scripting languages, and, especially, industry-driven standardization efforts, such as CORBA, TINA, TL 9000, and XDAIS. The use of COTS components can significantly reduce software development time and cost. However, the downside is loss of control over the quality of the system, especially with the use of third party software components. Rigorous techniques for rapidly constructing highly reliable software for embedded systems must emphasize modular design & software engineering principles, use of standard software frameworks, downloadable and updatable code modules, and complex and dynamically changing software configurations.

The UT-Dallas Embedded Software Center is developing the iAPEX (Infrastructure for Advanced Programming for Embedded Computer Systems) environment to facilitate the use of COTS components and third party software. iAPEX includes automated code transformation and synthesis, automated qualification, and a framework for adapting a system to changes in its environment without sacrificing performance. iAPEX is sharply focused on embedded systems, but the infrastructure encompasses a comprehensive, integrated solution that spans the entire product life-cycle.

At the heart of iAPEX is the Online Repository for Embedded Software (ORES), a distributed collaborative web-based repository system connecting application developers with component vendors. A vendor’s site offers support for component customization while a developer’s site contains technical data regarding the components. The development process starts with a new COTS aware requirements engineering methodology to adapt a product concept to maximize the use of available COTS components in its implementation. A new design method is used to decompose the application into a set of independent subsystems that can be independently evaluated and composed together. Each subsystem is developed using code synthesis utilities that interact with the vendor’s web-site to customize components and mine the developer’s ORES to generate glue code from existing design patterns and code templates. Each subsystem is then tested using a set of powerful simulation and analysis tools that interact with the vendor’s web-site to generate instrumented versions of the components for performing coverage and other quality analysis. Once the subsystems have been independently validated, they are automatically composed together by a preprocessor that generates a customized real-time operating system for the application based on its specification. The final step in the development life-cycle is to strengthen the reliability and security of the application.
The iAPEX infrastructure is unique in several ways.

- **Think COTS from the first step.** It is very difficult to try to achieve a good COTS-based design for an arbitrary set of requirements. Instead, iAPEX emphasizes the “front-end” aspects of software engineering to facilitate the effective use of COTS components and quality assurance during the later stages. An application-specific knowledge base of COTS components is being developed to guide the selection of functional and nonfunctional requirements that are amenable to implementation using the currently available suite of COTS components.

- **Think COTS throughout.** There has been some work on different aspects of COTS components, such as how to harden COTS components and how to assess the reliability of COTS components. The problem is that this type of focus makes it difficult to assure that any assumptions made will be satisfied in practice. For example, reliability assessment models usually assume that the COTS components have independent failure rates, but this may not be true in practice. Instead, iAPEX is targeted at a narrow application area (embedded software) but encompass all aspects of the life-cycle process, including requirements specification and analysis, design, implementation, refinement, and evaluation. In this way, iAPEX ensures that, for example, the assumptions made by an analysis technique will be guaranteed during the design and implementation steps.

- **Shift from a monolithic design to multiple, composable designs.** We are developing a method of decomposing embedded software systems into a set of Independently Developable End-user Assessable Logical (IDEAL) “micro-services” that can be automatically composed together to form the system. The micro-services will span both functional as well as nonfunctional aspects (repository, privacy, secrecy, authentication, etc.) and will be designed to insulate the application from changes in the set of available COTS components. The composition framework will be designed to guarantee that the properties of a system of micro-services can be inferred easily from the corresponding properties of the micro-services.

- **Quantitative reliability assessment.** iAPEX emphasizes quantitative reliability assurance techniques. Models will be developed to strengthen the statistical reliability analysis by incorporating structural and functional information to achieve high confidence bounds. A framework will be developed to allow system-level properties to be inferred from component-level properties.

- **Application-specific focus.** iAPEX is a powerful, scalable technology for a specific but important application domain, namely, embedded telecommunications software. This narrow focus enables us the special characteristics of telecommunications systems to be leveraged to develop deep knowledge bases, tools, and techniques for achieving accelerated development schedules and high quality assurance. The technology will address the special characteristics of telecommunications software, especially performance/real-time emphasis, low cost, small footprint solutions, heterogeneous dual/multi processor implementations, use of media accelerators and use of attached special purpose processors.