Developing High Confidence Software for Cyber-Physical Systems

Aniruddha Gokhale[1], Sherif Abdelwahed[1] and Nagarajan Kandasamy[2]
[1]Vanderbilt University and [2]Drexel University
Contact: a.gokhale@vanderbilt.edu

Many new and planned cyber-physical systems (CPSs) are realized as distributed real-time and embedded (DRE) systems. Examples of DRE CPSs we are interested in include data computing centers and automated warehouse management systems.

Emergent Traits of DRE CPSs

Next generation DRE CPSs illustrate the following emergent characteristics:

- *Complexity and scale*. As an increasing number of services are moved online, the required computing infrastructure keeps growing in complexity and scale. Effectively managing the performance of these large-scale computing systems subsequently becomes more complex, requiring increasing numbers of skilled personnel to configure, operate, and optimize them.
- *Dynamic and uncertain operating environment*. These systems typically execute in a dynamic and uncertain operating environment caused by multiple factors such as time-varying user workload, hardware and software resource failures, incomplete knowledge of the system operating state, and other vulnerabilities, such as security violations or denial of service attacks.
- *Use of on-demand computing models*. This is an emerging resource provisioning model to efficiently host applications, where computing resources e.g., servers, memory, and storage for data centers or warehouse resources e.g., forklifts and belts for warehouses, are dynamically made available to these applications as needed, and not statically allocated based simply on peak demand

High-confidence is an essential quality of service (QoS) property of these emergent DRE CPSs that must be considered over the entire lifecycle of these systems, including design, development, deployment, and operation. Meeting these demands using today's stovepiped technologies is tedious, error-prone, and costly to develop, optimize, validate, deploy, and maintain.

R&D Needs for DRE CPSs

Realizing high-confidence software for DRE CPSs requires meeting the following criteria.

- *Trustworthiness* – DRE CPSs must be trustworthy, which includes the system's ability to meet performance objectives, and be resilient to failures and security attacks.
- *Autonomicity* – DRE CPSs must be autonomous i.e., self healing, self configuring and self optimizing while maintaining good resource utilization.

- *Analyzability* – The algorithms and technologies used to develop DRE CPSs must be amenable to analyses and verification for different properties, such as timeliness guarantees, fault tolerance, stability and correctness.

Solution Approach

The solution needs of high confidence DRE CPSs can be met by developing novel techniques described below and synergistically integrating them as shown in Figure 1.

- **Model-driven System Execution Modeling** – which requires developing modeling abstractions to obtain high-fidelity system models of DRE CPSs that describe its structure and expected (i.e., correct) behavior at various levels of abstraction e.g., platform independent and platform-specific. These models will be executed concurrently with actual system operation and the results compared. A divergence between the system behavior and that of the corresponding model may be treated as a symptom of an anomaly that must be diagnosed and fixed.

- **Model-based Diagnosis** – which requires developing distributed, model-based diagnosis techniques that use the observed divergence between the actual system and its models to isolate and characterize possible attacks or errors as well as the set of possibly corrupted resources. These algorithms will have to detect, isolate, and estimate the state of corrupted hardware/software components using concepts from continuous and discrete-event diagnosis, and consistency-based causality analysis.

- **Robust and Adaptive Control** – which requires handling complex optimization problems under uncertainty within a *receding horizon control* framework. Based on our earlier work, the notions of uncertainty and risk will be incorporated within these frameworks to cope with unexpected changes to performance goals, dynamic workload, and hardware and software failures. Online parameter tuning and model learning techniques will need to be integrated within the control framework to both improve the quality of partially specified system models and adapt to changes in the system model itself over time (e.g., addition or removal of system components, replacement of components)

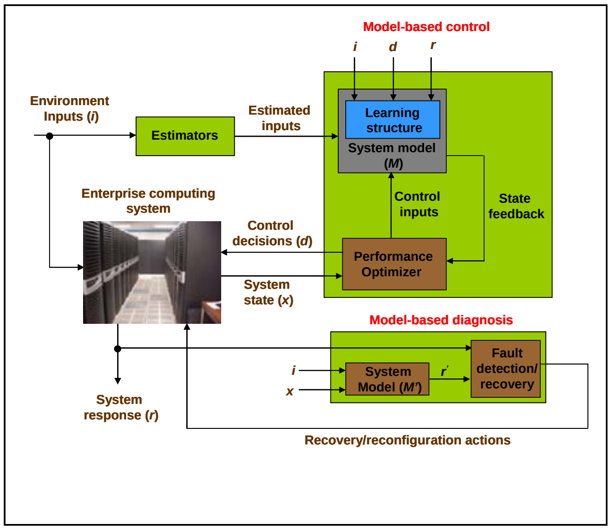

Figure 1: Architecture for DRE CPSs

- **Trustworthy Middleware Infrastructure** – which requires developing QoS-enabled, fault tolerant and self-healing middleware that (a) provides real-time system monitoring capabilities that collect the desired parameters of interest, and (b) can dynamically integrate the artifacts synthesized by the model-based diagnostics and control algorithms, and deploy these software artifacts optimally to assure continuous operation of DRE CPSs.

Leveraging Existing Capabilities

Realizing the vision of high confidence DRE CPSs need not start from scratch. A substantial set of early capabilities exist that can be leveraged to meet the emergent demands of DRE CPSs. For example, as shown in Figure 2, existing capabilities developed at Vanderbilt, such as the PICML modeling language, can be used to model the assembly and deployment of DRE CPSs. Generative tools associated with PICML can synthesize the configuration and deployment artifacts necessary to automate the deployment of these systems via the DAnCE middleware. Distribution component middleware, such as CIAO, already provide the capabilities to support real-time component-based applications. The resource and allocation engine (RACE) is a framework that enables the plugging in of different control algorithms that promote runtime adaptation.

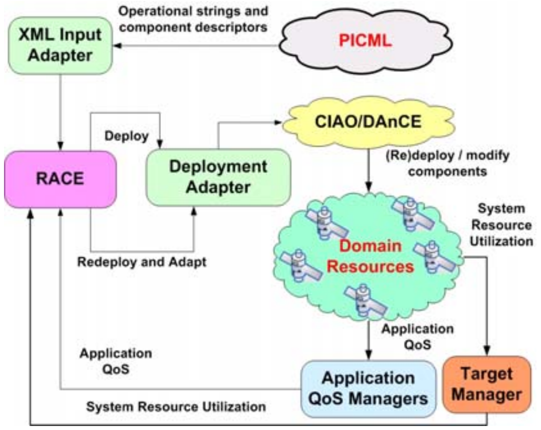

Figure 2: Existing Capabilities

Additional capabilities, including analyses, model-based diagnostics, robust control algorithms, system behavioral modeling, and trustworthy and self-healing middleware must be developed to enhance these existing frameworks and meet the objectives of high confidence software for DRE CPSs.

Author Bios

Aniruddha S. Gokhale is an Assistant Professor in the EECS department and a Senior Research Scientist at ISIS, both at Vanderbilt University. His research interests are in real-time component middleware optimizations, Model-driven Engineering platforms, fault tolerance and distributed resource management. He was the lead investigator for the DARPA PCES program at Vanderbilt, which realized the CoSMIC MDE tool suite of which PICML is a part. He has also contributed to the R&D on DAnCE, CIAO and RACE. He can be reached at (615) 322-8754 and by email at a.gokhale@vanderbilt.edu.

Sherif Abdelwahed is a Research Assistant Professor and a Research Scientist at ISIS, both Vanderbilt University. His research interests include modeling, verification, and control and diagnosis of discrete-event and hybrid systems. He was involved as a co-PI in the DARPA MoBIES program, where he developed a model-based control framework called DQME for dynamic QoS adaptation. He can be reached at (615) 343-7555 and by email at sherif@isis.vanderbilt.edu.

Nagarajan Kandasamy is an Assistant Professor in ECE at Drexel University with research interests in dependable computing, self-managing systems, and embedded systems. He has developed algorithms based on model-predictive control for runtime QoS adaptation in enterprise data centers. He can be reached at (215) 895 1996 and by email at kandasamy@ece.drexel.edu.