Whitepaper on the CHARIOT Project[1]

Abhishek Dubey, Aniruddha Gokhale, Will Otte, Janos Sallai, Doug Schmidt
Vanderbilt University

Martin Lehofer, Raj Varadarajan, Monika Sturm
Siemens Corporation, Corporate Technology

Ultra Large Scale Extensible Cyber-Physical Systems

Recent advances in mobile networking as well as availability of commodity single board computers and other integrated devices provide a platform where edge devices along with traditional cloud computing can revolutionize how Cyber-Physical Systems (CPSs) are constructed. These advances allow us to move away from traditional single use vertical CPS towards an extensible horizontal platform of CPSs that can host different applications along different verticals, which we refer to as extensible CPS.

Smart Cities are a use case for extensible CPS

In addition to satisfying the requirements of traditional CPSs – such as strict consideration of physical properties, timing properties and resource requirements – extensible CPS also must consider the high degree of heterogeneity related to hardware and software of entities that comprise these dynamic systems. Accounting for these requirements requires appropriate design-time and run-time solutions to design, analyze, deploy and maintain these systems. Design-time tools are important because they allow application developers and system architects to model their applications and systems before deploying them; thereby allowing them to perform a variety of design-time analysis as well as automatic code generation whenever applicable.

Finally, like traditional CPS, dependability is a key requirement for extensible CPS. Additionally, unforeseen environmental conditions or faults in the hardware can trigger latent defects in the software with potentially negative consequences. Thus, failures are likely in both the system and the software running on the platform. The dynamics stemming from the composition of heterogeneous systems and their individual failure models bring about a new dimension of challenges for extensible CPS where uncertainty is a key property that must be accounted for. Thus, the framework must have the provision for monitoring the system parameters, identifying anomalies and then mitigate them.

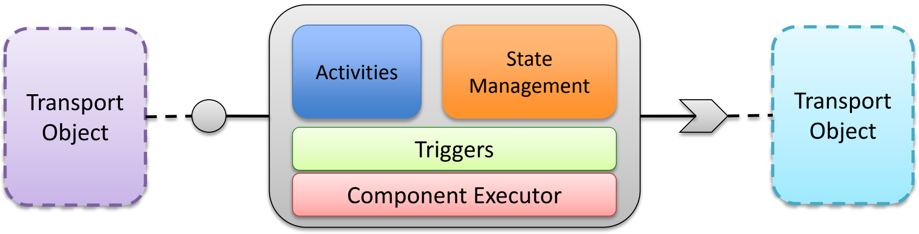
The CHARIOT Project

The CHARIOT (Cyber-pHysical Application aRchItecture with Objective-based reconfiguraTion) project, aims to address the challenges stemming from the need to resolve various challenges within extensible CPS. CHARIOT is an application architecture that enables design, analysis, deployment, and maintenance of extensible CPS by using a novel design-time modeling tool and run-time computation infrastructure. In addition to physical properties, timing properties and resource requirements, CHARIOT also considers heterogeneity and resilience of these systems. The CHARIOT design environment follows a modular objective decomposition approach for

[1] Acknowledgement: This research has been funded under a grant from Siemens Corporation, Corporate Technology

developing and managing the system. Each objective is mapped to one or more data workflows implemented by different software components. This function to component association enables us to assess the impact of individual failures on the system objectives.

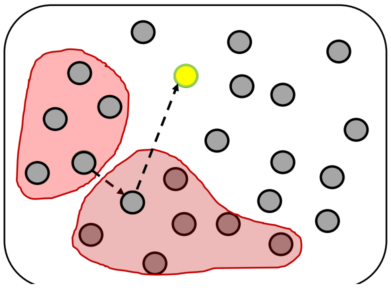
The runtime architecture of CHARIOT provides a universal cyber-physical component model that allows distributed CPS applications to be constructed using software components and hardware devices without being tied down to any specific platform or middleware. It extends the principles of health management, software fault tolerance and goal based design.



A chariot component abstracts the communication and middleware aspects

CHARIOT provides inbuilt mechanisms to deploy software components across different computing nodes in different redundant patterns. The redundancy-based fault tolerance aims to improve the reliability of the system by using redundant parts, with the assumption that failure of each part is independent of the other. Hence, the failure probability of the overall subsystem/system is lower as it is a product of the failure-probability of the individual parts. While redundancy-based techniques are good for masking failures, often it is necessary to detect and diagnose faults in the system followed by repair and reconfiguration efforts to recover the system functionality. The effectiveness of this strategy depends on the support available in the system for monitoring and detecting anomalies (hardware and software watchdogs, comparison to preset values/ thresholds or expected behaviors). For this purpose CHARIOT supports specification of invariants, preconditions, and post-conditions for all system activities. Deviations from these specifications are marked as anomalies, and such deviations can be detected.

In the runtime, all components follow a two level mitigation scheme once the failures have been detected. In the first scheme, each component is associated with modes which capture the internal redundancy in the component's workflow. Thus, each component can autonomously switch modes as part of a preconfigured reactive logic. Dynamic system reconfiguration in the event of failures is formulated as an SMT problem, where we use the Microsoft Z3 solver for it. The problem encoding and solver invocation is built into the CHARIOT runtime architecture.



A representation of the modeled configuration space.

The Smart Parking Scenario

Increasing traffic density, especially in metropolitan areas like Nashville, make finding an appropriate parking space a challenging task. We describe a scenario where we combine several physical sensors and distributed software applications to provide a smart parking solution. The system works in combination with a smart phone application and enables drivers to navigate to the nearest available parking lot. Once the vehicle is in the range of the parking lot, the smartphone application in combination with various sensors and the backend applications finds a suitable empty parking spot and creates a reservation. Thereafter, the driver enters the parking lot where they get a specialized parking ticket with a smart tag, which enables the parking lot to use multi modal indoor localization techniques in order to guide the driver to their reserved spot in the parking lot. Key elements of the demonstration scenario include a client, a localization service, a navigation capability, and occupancy checking.