To: The High Confidence Software and Systems Coordinating Group
From: Robert Baillargeon -- General Motors Research & Development
Subject: Position Paper for National Workshop on Composable and Systems Technology for High Confidence Cyber-Physical Systems

Introduction

The electrification of vehicle control systems is changing traditionally mechanical-physical systems into cyber-physical systems. This natural evolution is an attempt to produce more valuable (and more complex) controls with greater performance and quality. The automotive industry's competitive environment demands the rapid growth of timely and cost effective methods. These elements form business drivers that are only loosely related to the technical complexities of introducing such features in the physical environment. Technical demands, coupled with business constraints, necessitate new approaches to system design in which systems are not created but are instead composed. System design methods are traditionally "top-down" whereas compositional approaches are "bottom-up". This reversal invalidates many of the traditional techniques and thus requires new techniques that question pervasive assumptions in the domains of system design, verification, and software platforms.

The automotive community is pursuing several techniques to deal with complexity and composition such as model-based methods and software product lines; however neither is fully inclusive to the needs of the future. Model-based methods have been advocated for some time; however multitudes of uses, formality and abstraction have typically limited their value to singular processes or disciplines. Software product lines, and their decoupled development paradigm, have worked to formalize this practice for planned reuse and strategic compositions, but the future indicates more opportunistic or decentralized decisions on compositions where product lines have limited proven solutions. Demands in the automotive realm require new approaches to design and assemble systems using compositional mechanisms that guarantee to maintain certain properties.

Fundamental Limitations and Knowledge Barriers to the Composability of High Confidence Software Systems

Composability by nature is both a way to deal with complexity as well as an introduction to a new dimension of complexity. While it is often viewed exclusively as a value, and an architectural characteristic, the objective of composability has a pervasive effect on process, methods, and designs. It appears that only through the clear definition and management of the dimensions and depths of complexity will a composable environment be achievable.

Much of the difficulty with the ability to reason and implement composable systems is the desire to treat the system composition environment like mechanical building blocks. The problem is that system composability is not restricted by the three mutually exclusive dimensions that are often the foundation in the mechanical world. Rather, the software and systems world is characterized by demands for shared resources (computational capability, memory, …) and desires for shared goals (safety, security, control,…) which are generally not mutually exclusive. With the malleability of software systems there is a common shift between constraints, such as latency, and implementation results, such as worst case execution time, which adds to the elements of confusion by using units with different intent and compositional dynamics. This can be considered a unique element of uncertainty within the science.

While this view of overlapping dimensional complexity may be considered simplistic, it illustrates why there continues to be a gap across system design, verification, and software platforms that inhibits the growth and realization of "truly" composable systems. The lack of a globally acknowledged set of dimensions, or acknowledged even within a particular domain, limits the ability to rationally understand and reason about the formal meaning of composability. Additionally, once the dimensions are defined, methods and mathematics to compose and to compare compositional tradeoffs are lacking. Specifically, objective-based constraints, such as safety, lack explicit techniques for composition and must currently be handled uniquely per application composition as opposed to universally across a class. As a result,

unexpected emergent behaviors arise from conflicts in resource utilization or goals. Until this foundation can be established, composability will remain an ad-hoc practice and lack formality. Within the uncertainty of the physical environment, we strive to reason about the formal composition of the cyber dimension.

Fundamentally, a gap has continued to exist across the domain of systems and formal verification due to the lack of uniformity across usage of description. Unique development techniques and analysis of system utilization and verification has created a discontinuity. Add to this the singular nature of models by their user bases, system synthesis and code generation for system designers and property verification for formal methods users, a discontinuity has arisen in the domain in which continuity and integrity are critical to support the results of formal verification methods to hold in end designs.

Promising Innovations for Composing High Confidence Software Systems

Innovations in composing high confidence software systems will occur when unified perspectives increase the accessibility and capability of the methods and tools. As we look at each of the dimensions we observe promise in their individual growth as well as see promise of the integration in the future.

Complexity and scale in the formal verification domain are approaching the levels of of scale and complexity in problem space creation. The questions remain more aligned with the description of the problem space (Can the composability constraint be captured?) and the property to be asserted (Can the composability question be formally solved?). Additionally there exists the standing question of accessibility to the methods to the "common" engineer that has remained a barrier of adoption. However, innovations in model representation and model transformation are believed to be eroding this barrier and shortly the utilization of verification for particular dimensions will lead to more formal and capable reasoning to composability of well understood dimensions.

In the systems and software domain, the issues of complexity and scale are demanding new system representations. The promise in this domain is the growth in model representations as well as the growth in aspect methods. The more prevalent usage of models provides more formal representations, which enables verification techniques. The further exploration of aspect approaches, in context of models, provides the opportunity to clearly represent concerns in the problem space about composability. It is critical that these methods preserve concerns and weave dimensions while continuing to grow, progressing to semantic rather than syntactic weaving, to yield property preserving solutions. It is through these paths that "correct-by-construction" methods may be preserved for systems that remain static in deployment.

In the platform domain, the importance of resource and property preservation is growing to address the desire for component technologies and system composability. The platform is responsible for dynamic deployment and system adaptability while still preserving the critical system wide behaviors. It is the development and dynamic enforcement of system properties which will dictate run-time composability and be the key insight into the development of adaptive systems.

Most Important Research Challenges for Composing High Confidence Software

The most important research challenge for composing high confidence software is the ability to transition the questions of composability upward in the design cycle for more flexibility in solution. Composition, by nature, is better suited for proactive methods rather than reactive resolutions. Proactive solutions can be developed in the synthesis of designs and in the core of the infrastructure for run-time support. Although these two approaches trade off capabilities and cost, both are better than purely reactive approaches.

The foundation of "traditional" methods is predicated on the utilization of design and/or implementation constructs to assert the properties of a given system. Fundamentally this is reactive in nature and an ad-hoc method to establish assertion through testing, even though the testing is formal. If the community desires growth in reasoning about composition, it must address this from the position of proactive methodologies. To this there are two important research challenges that are proposed with

respect to the timing of composition. The first is design time composition which asserts the composability properties with design intent and the second is run-time composition which asserts the assurances of composability with collaborative matching of needs and provisions to the system and platform.

The ability to introduce design time composition requires capturing composability in clear dimensions with clear evaluations of the validity of the compositions. These models tend to be unique from previous model-driven methods which are resident in the language of the problem space and constraints, and which contain formal characterizations of the "non-functional" requirements that the system must achieve. This requires a formal description method (models), a distinct description of dimensions (language), and a formal assessment method (composability formula). In conjunction with this, a property preserving integration that maps the system constraints to a valid implementation solution is required. These represent critical research challenges to the design time composability.

The ability to introduce run-time composition requires the capability of the platform to preserve quality of service. While not unknown to the platform space, where measurable elements such as time and memory portioning have been observed and well understood, the growth will be in measuring composability. This enables the composition of elements known today, as well as the applications to be added at run-time in the future. This represents growth in capability to characterize and capture objective based dimensions such as safety as well as domain specific constructs (such as power management) which represent a significant challenge. Growing the competency to control system-wide characteristics established and guaranteed by application-independent platforms places significant requirements on the underlying infrastructure and application services. This can be equated to system regulation which becomes more difficult in decentralized and heterogeneous architectures.

Conclusion

The foundation of building high confidence systems of the future lies in the ability to characterize and reason about of the dimensions of composability. Until a mathematical basis can be established to reason about the dimensions and its compositional relationship with other dimensions, the methods will remain categorized as ad-hoc. The growth in capabilities in the formal methods and modeling domains are providing reasonable hope that ability exists to reason about composing systems. However, there exist significant gaps in system architectures that need to be researched to provide software platforms that support heterogonous and adaptive system compositions.

Acknowledgements

Thanks to my colleagues for discussions and editing suggestions including Alan Baum, Shengbing Jiang, Shige Wang, and Jennifer Black.

Authors

Robert Baillargeon, General Motors Research & Development
Title: Thrust Area Leader, Electrical & Controls Integration Lab
Responsibilities: Development of strategies for the research in model-driven design, systems, and high-integrity development.
Contact: robert.c.baillargeon@gm.com or 586 986 1402