Dependable By Construction: Cyber-Physical Systems to Bet Your Life On

Rance J. DeLong
LynuxWorks, San Jose, CA

John Rushby
SRI International, Menlo Park, CA

October 21, 2008

Abstract

Cyber-physical systems will touch many aspects of life, and lives will depend on them: on the road, in the air, on rails, and in the operating room. We are concerned with the efficient construction of cyber-physical systems, and of the assurances required to place lives within their scope of control.

We have been investigating a framework for an approach to safety- and security-critical systems known as Multiple Independent Levels of Security/Safety (MILS). We are optimistic that the concepts will be applicable to cyber-physical systems in general. Our approach includes the use of an explicit assurance case, decomposed along architectural lines, supporting system-level claims of safety and security, that leverages the previously established claims for the components and for the architecture. We pose a grand challenge for cyber-physical systems based on a vision that has emerged from our work with MILS.

Introduction

We present a vision for the development of trustworthy cyber-physical systems that are dependable-by-construction, for their rapid and inexpensive construction, as well as their rapid and inexpensive certification. The envisioned approach employs:

- an explicit assurance case,
- architectural decomposition corresponding closely to that of the assurance case,
- a basis set of well-understood components that can be extended or changed,
- a theory of composition for functional and non-functional properties,
- an automated method for synthesis of systems from the components, and
- an automated method for producing the certification evidence and checking that evidence against the certification requirements.

Elaborating the Vision

We envision a computer aided design system ("CPS-CAD") that will support the development of a design for a target cyber-physical system, and that will produce the realization of the "cyber portion" (software, firmware, hardware netlists) of the cyber-physical system. The desired properties of such systems will be behaviors and constraints on behaviors. The CPS-CAD system would embody knowledge of engineering principles and methods necessary to produce the cyber artifacts and to "understand" their relation to the physical artifacts.

Existing methods for systems-on-a-chip suggest the feasibility of this vision. The entire design of a system-on-a-chip may be done today with computer aided design tools, with the overall workflow process, and the "driving" of the tools under the control of a person. It is not far fetched to image the role of the person reduced to what the person does best: the production of the high-level specification of the desired system, with the other steps in the workflow carried out by automation.

Already, in the realm of software, code is generated for applications based on high-level model-based designs, using standard frameworks and component libraries. The envisioned CPS-CAD system would combine silicon design and software generation to produce the cyber portions of cyber-physical systems.

A design developed under CPS-CAD may include the specification of physical layout, physical properties, behavioral properies, and non-functional logical properties. The artifacts produced by CPS-CAD will include firmware and software (and potentially, hardware specifications) to form the cyber components of a complete system that realizes the design, and the the evidence for certification of the system.

An Approach to Construction in CPS-CAD

For MILS we are defining an integration framework and a collection of components that have been constructed with high assurance to have well understood properties, and providing a method for their composition that provides the assurance of the properties of the composite. In CPS-CAD the objective would be to combine the components in such as way that the composite satisfies specified properties. Construction would employ existing components, but also the synthesis of additional components or "glue-ware" to mediate the interactions among components, and the interactions of the components with the environment. The difference is that the components would not be just "wired-up" to create the system, but that the system would be synthesized with "holes" into which instances of the components are placed.

An Approach to Certification in CPS-CAD

Historically, certification has been conducted as a monolithic process that scrutinizes every aspect of a system. As systems grow in complexity[1], but have increasing integration, existing

[1] modern luxury cars have 100 million lines of code!

certification regimes are under stress to operate more quickly, more economically, and more flexibly.

Tim Kelly[2] made the point that "the difficulty in compositional assurance is that the assurance case may not decompose on architectural lines." So the question we have asked in the context of MILS, and it is applicable also in CPS-CAD, is: what is an architecture? Surely, a good one is one that does promote decomposition of the assurance case on architectural lines. We think we have this for security properties in the MILS architecture, and the similarity of MILS and IMA[3] makes us hopeful this can be extended to safety, and transportation systems in particular.

The envisioned CPS-CAD certification approach is integrated with the development process, whereby the evidence required for certification is produced directly from the target system itself (product-based) and the method of its construction (process-based). Unlike traditional process-based certification, however, the methods of construction play an explicit, integral and indispensable role in the assurance case.

CPS-CAD would support certification, including:

- incremental certification as vehicular subsystems are integrated
- intra-vehicle certification of behaviors and non-functional properties such as safety and security
- certification of inter-vehicle and vehicle-infrastructure coordinated behaviors and non-functional properties

Some of these cannot be achieved by purely *a priori* certification methods, and will require both incremental and continuous runtime certification.

Summary and Challenges

We propose the development of dependable-by-construction cyber-physical systems by extensively automated means, and their certification in an incremental way during construction, integration, deployment, and at runtime. We presented a vision of CPS-CAD that would largely automate the construction and certification of such cyber-physical systems.

There research and engineering challenges inherent in our vision for CPS-CAD, include:

- functional composition theory
- non-functional property composition theory
- automating CPS construction based on the composition theories
- automating certification evidence generation and management of the assurance case
- infrastructure for incremental certification and runtime certification.

[2]Tim Kelly, senior lecturer, University of York

[3]Integrated Modular Avionics