Analysis of Cyber-Physical Systems

Warren A. Hunt, Jr.
Department of Computer Science
2317 Speedway, M/S D9500
The University of Texas
Austin, TX 78712-1757

E-mail: hunt@cs.utexas.edu
Tel: +1 512 471 9748
FAX: +1 512 471 8885
http://www.cs.utexas.edu/users/hunt

My interest concerns our ability to be rigorous in specifying and analyzing cyber-physical systems (CPS). Over the last century, we have developed very sophisticated systems such as aircraft, powered automotive vehicles, and electric power systems whose complexity goes well beyond anything we can now rigorously specify and analyze. I see several problems in making these systems secure:

1. We lack adequate mathematics to specify the behavior imposed by digital controls on analog systems;

2. We have few, if any, formal models of CPS artifacts;

3. We lack of computational tools suitable for analysis of realistic CPS devices; and

4. We lack suitable education programs to train engineers and scientists to apply such mathematics and tools.

We, as a nation, are currently unable to validate combined computational-physical systems with any degree of rigor.

The community with which I work most closely seeks to model and validate various digital artifacts such as processors, assemblers, and compilers. We seek to assure that such systems meet their specifications. However, carrying out this work has required scientists to painstakingly to specify the very devices we use. For instance, our group has been developing a formal, executable model of the Intel X86 instruction-set architecture. Although still incomplete, our specification already exceeds 40,000 lines of formal mathematics. Nevertheless, this formal model is already sufficiently complete to verify the correctness of binary programs produced by modern compilers. In addition, we are also deeply involved in an ongoing effort to verify mechanically that the VIA Nano (a X86-compatible microprocessor) is correctly implemented. Our dual involvement in efforts to prove both hardware and software correct provide twin means to validate our X86 specification; further, our X86 ISA model can be used to execute X86 binary programs. Thus, our X86 specification is validated by co-simulation, its use in software verification, and by our work to prove that the the hardware design of the VIA Nano correctly implements our X86 ISA-level specification.

To extend our X86-focused hardware specification for analyzing the

behavior of a CPS device containing an X86 microprocessor will require us to augment our specification to include the I/O devices with which an X86 can sense and control an external environment. Modeling such I/O devices and their effect on an external environment is itself a major research topic that will require years of dedicated effort to produce an operational system model that can be used to specify and mechanically validate a CPS.

One of my PhD students, Shant Harutunian, did indeed complete the specification and mechanical verification of a very simple CPS. By mechanically proving a correctness condition as specified by a Lyapunov stability condition, my student proved that a computer program could faithfully keep a dynamic CPS system in its stable region. His effort developed a system model of both the control system and its environment, as well as a model of sensing the analog values of the physical system, and a digital control algorithm to respond to changes in external inputs. With these models he constructed a proof, checked by the ACL2r theorem-proving system, thus proving that the overall system would indeed have the desired properties. There have been very few such undertakings because of the level of mathematical sophistication required; such efforts require an enormous amount from those engineers and scientists who undertake them.

My wishes for the CPS community include the development of rigorous methods to model, simulate, analyze, and verify cyber-physical systems. Carrying out the development of such tools and infrastructure will require years of research. I recommend that funding agencies supporting such research work both with academia and with organizations that have critical needs for improved CPS analysis tools. An interested funding agency should be able to get cooperation from a provider of CPS products, such as the auto industry, for working with researchers focused on CPS.

Without advances in the modeling, analysis, and verification of CPS artifacts, society will continue to produce and use flawed, and even dangerous, products. Our safety and security depends on our ability to make CPS engineering as rigorous a discipline as mathematics while making analysis solutions effective enough to reduce the costs of deploying such technology. There is already much evidence that computerized mathematical modeling has greatly advanced the range of products that can be designed and built. We need to go a full-step farther and construct the theory and tools required to assure the safety, security, and operational characteristics of CPS products.