Sangiovanni-Vincentelli, Alberto; **Damm, Werner**; **Passerone, Roberto**

Taming Dr. Frankenstein: contract-based design for cyber-physical systems. (English)

Zbl 1264.93152
Eur. J. Control 18, No. 3, 217-238 (2012).

Summary: Cyber-physical systems combine a cyber side (computing and networking) with a physical side (mechanical, electrical, and chemical processes). In many cases, the cyber component controls the physical side using sensors and actuators that observe the physical system and actuate the controls. Such systems present the biggest challenges as well as the biggest opportunities in several large industries, including electronics, energy, automotive, defense and aerospace, telecommunications, instrumentation, industrial automation.

Engineers today do successfully design cyber-physical systems in a variety of industries. Unfortunately, the development of systems is costly, and development schedules are difficult to stick to. The complexity of cyber-physical systems, and particularly the increased performance that is offered from interconnecting what in the past have been separate systems, increases the design and verification challenges. As the complexity of these systems increases, our inability to rigorously model the interactions between the physical and the cybersides creates serious vulnerabilities. Systems become unsafe, with disastrous inexplicable failures that could not have been predicted. Distributed control of multi-scale complex systems is largely an unsolved problem.

A common view that is emerging in research programs in Europe and the US is "enabling contract-based design", which formulates a broad and aggressive scope to address urgent needs in the systems industry. We present a design methodology, and a few examples in controller design whereby contract-based design can be merged with platform-based design to formulate the design process as a meet-in-the-middle approach, where design requirements are implemented in a subsequent refinement process using as much as possible elements from a library of available components. Contracts are formalizations of the conditions for correctness of element integration (horizontal contracts), for lower level of abstraction to be consistent with the higher ones, and for abstractions of available components to be faithful representations of the actual parts (vertical contracts).

MSC:

93C70	Time-scale analysis and singular perturbations in control/observation systems	Cited in **6** Documents
93B51	Design techniques (robust design, computer-aided design, etc.)	
93C95	Application models in control theory	

Keywords:

design methodologies; industrial automation; development schedules; horizontal contracts; mechanical, electrical, and chemical processes; horizontal contracts; controller design; element integration; meet-in-the-middle approach; vertical contracts; platform-based design; contract-based design; subsequent refinement process; complexity of cyber-physical systems; control of multi-scale complex systems

Software:

Metropolis; Ptolemy

Full Text: DOI

References:

[1] Road vehicles—functional safety. Standard ISO 26262.

[2] Balarin, F.; Hsieh, H.; Lavagno, L.; Passerone, C.; Sangiovanni-Vincentelli, A.L.; Watanabe, Y., Metropolis: an integrated electronic system design environment, IEEE computer, 36, 4, 45-52, (2003)

[3] Balarin, F.; Davare, A.; D'Angelo, M.; Densmore, D.; Meyerowitz, T.; Passerone, R.; Pinto, A.; Sangiovanni-Vincentelli, A.;

Simalatsar, A.; Watanabe, Y.; Yang, G.; Zhu, Q., Platform-based design and frameworks: metropolis and metro ii, (), 259

[4] Balarin, F.; Passerone, R., Specification, synthesis and simulation of transactor processes, IEEE trans. computer-aided design integrated circuits syst, 26, 10, 1749-1762, (2007)

[5] Benvenuti, L.; Ferrari, A.; Mangeruca, L.; Mazzi, E.; Passerone, R.; Sofronis, C., A contract-based formalism for the specification of heterogeneous systems, (), 142-147, September 23-25

[6] Berry, G., The effectiveness of synchronous languages for the development of safety-critical systems, (2003), White paper, Esterel Technologies

[7] Booch, G.; Rumbaugh, J.; Jacobson, I., Unified modeling language user guide, The (addison-wesley object technology series), (2005), Addison-Wesley Professional

[8] Broy, M., Compositional refinement of interactive systems, J. ACM, 44, 6, 555-600, (1997)

[9] Damm, W., Controlling speculative design processes using rich component models, ()

[10] Damm, W.; Votintseva, A.; Metzner, A.; Josko, B.; Peikenkamp, T.; Böde, E., Boosting reuse of embedded automotive applications through rich components, (), August 21

[11] Davare, A.; Densmore, D.; Meyerowitz, T.; Pinto, A.; Sangiovanni-Vincentelli, A.; Yang, G.; Zhu, Q., A nextgeneration design framework for platform-based design, ()

[12] de Alfaro, L.; Henzinger, T.A., Interface automata, (), 109-120

[13] Derler, P.; Lee, E.A.; Sangiovanni Vincentelli, A., Modeling cyber-physical systems, Proc. IEEE, 100, 1, 13-28, (2012)

[14] Dill, D.L., Trace theory for automatic hierarchical verification of speed-independent circuits. ACM distinguished dissertations, (1989), MIT Press

[15] Doyen, L.; Henzinger, T.; Legay, A.; Nickovic, D., Robustness of sequential circuits, (), June 21-25

[16] Eker, J.; Janneck, J.W.; Lee, E.A.; Liu, J.; Liu, X.; Ludvig, J.; Neuendorffer, S.; Sachs, S.; Xiong, Y., Taming heterogeneity - the Ptolemy approach, Proc IEEE, 91, 1, 127-144, (2003)

[17] Fleurey, F.; Muller, P.A.; Jzquel, J.M., Weaving executability into object-oriented meta-languages, ()

[18] Fritzson, P., Principles of object-oriented modeling and simulation with modelica, 2.1, (2003), Wiley

[19] Glabbeek, R.; Weijland, W.P., Branching time and abstraction in bisimulation semantics, J ACM, 43, 3, 555-600, (1996) · Zbl 0882.68085

[20] Harel, D.; Kugler, H.; Marelly, R.; Pnueli, A., Smart play-out of behavioral requirements, Fmcad, 378-398, (2002) · Zbl 1019.68622

[21] Harel, D.; Marelly, R., Come, Let's play: scenario-based programming using LSCs and the play-engine, (2003), Springer-Verlag, http://www.wisdom.weizmann.ac.il/~harel/.ComeLetsPlay.pdf

[22] Harel, D.; Segall, I., Planned and traversable play-out: A flexible method for executing scenario-based programs, TACAS, 485-499, (2007)

[23] Karris, S., Introduction to simulink with engineering applications, (2006), Orchard Publications

[24] Karsai, G.; Sztipanovits, J.; Ledeczi, A.; Bapty, T., Modelintegrated development of embedded software, Proc IEEE, 91, 1, 145-164, (2003)

[25] Kesten, Y.; Piterman, N.; Pnueli, A., Bridging the gap between fair simulation and trace inclusion, Information and computing, 200, 1, 35-61, (2005) · Zbl 1082.68055

[26] Kopetz, H., Composability in the time-triggered architecture, (), 6-9, March 2000

[27] Larman, C.; Basili, V.R., Iterative and incremental developments: a brief history, Computer, 36, 6, 47-56, (2003)

[28] Lee, E.A., Cyber physical systems: design challenges, (), 363-369

[29] Negulescu, R., Process spaces, \textit{CONCUR}, of lecture notes in computer science, 1877, (2000), Springer-Verlag · Zbl 0999.68140

[30] Object Management Group (OMG). Model driven architecture (MDA) FAQ. [online], http://www.omg.org/mda/.

[31] Object Management Group (OMG). Unified Modeling Language (UML) specification. [online], http://www.omg.org/spec/UML/.

[32] Object Management Group (OMG). A UML profile for MARTE, beta 1. OMG Adopted Specification ptc/07-08-04, OMG, August 2007.

[33] Object Management Group (OMG). System modeling language specification v1.1. Technical report, OMG, 2008.

[34] The Design Automation Standards Committee of the IEEE Computer Society, editor. \textit{1850-2010—IEEE Standard for Property Specification Language (PSL)}. IEEE Computer Society, 2010.

[35] Hudak, J.; Feiler, P.; Gluch, D., The architecture analysis and design language (AADL): an introduction, Software engineering institute (SEI) technical note, (February 2006), CMU/SEI-2006-TN-011

[36] Passerone, R.; de Alfaro, L.; Henzinger, T.A.; Sangiovanni-Vincentelli, A., Convertibility verification and converter synthesis: two faces of the same coin, ()

[37] Passerone, R.; Hafaiedh, I.B.; Graf, S.; Benveniste, A.; Cancila, D.; Cuccuru, A.; Gérard, S.; Terrier, F.; Damm, W.; Ferrari, A.; Mangeruca, L.; Josko, B.; Peikenkamp, T.; Sangiovanni-Vincentelli, A., Metamodels in Europe: languages, tools, and applications, IEEE design test computers, 26, 3, 38-53, (2009)

[38] Sudarsan, R.; Fenves, S.J.; Sriram, R.D.; Wang, F., A product information modeling framework for product lifecycle management, Computer-aided design, 37, 1399-1411, (2005)

[39] Raclet, J.-B.; Badouel, E.; Benveniste, A.; Caillaud, B.; Legay, A.; Passerone, R., Modal interfaces: unifying interface automata and modal specifications, (), 87-96, October 12-16

[40] Raclet, J.-B.; Badouel, E.; Benveniste, A.; Caillaud, B.; Legay, A.; Passerone, R., A modal interface theory for component-based design, Fundamenta informaticae, 108, 1-2, 119-149, (2011) · Zbl 1242.68147

[41] Sangiovanni-Vincentelli, A.; Shukla, S.; Sztipanovits, J.; Yang, G.; Mathaikutty, D., Metamodeling: an emerging representation paradigm for system-level design, Special section on meta-modeling, IEEE design and test, 26, 3, 54-69, (2009)

[42] Functional safety of electrical/electronic/programmable electronic safety-related systems. Standard IEC 61508.

[43] Sztipanovits, J., Composition of cyber-physical systems, (), 3-6

[44] Törngren, M., Timing problems and opportunities for embedded control systems modeling and co-design, (), September 16