Tackling Uncertainty for Transportation Cyber-Physical Systems

2014 National Workshop on Transportation CyberPhysical Systems
Position Statement

Betty H.C. Cheng
Department of Computer Science and Engineering
Michigan State University
East Lansing, MI 48824

A dynamically adaptive cyberphysical system (DAS) must be able to monitor its environment, adapt to changing conditions, and be resilient to component failures and attacks. However, the designer of such an adaptive system is faced with a challenging set of tasks: anticipating how and when the system will need to adapt in the future, codifying this behavior in decision- making components to govern the adaptation, and ensuring system integrity during and after adaptation. These tasks are particularly difficult for systems that must operate safely in the face of continuous dynamics and environmental uncertainty.

Our position is to motivate research projects that investigate novel ways to model, analyze, and mitigate uncertainty arising in three different aspects of the system. First, for many systems, uncertainty about the physical environment can lead to suboptimal, and sometimes catastrophic, results as the system tries to adapt to unanticipated or poorly-understood environmental conditions. Second is dealing with uncertainty in the cyber environment, including not only performance metrics (load, traffic, etc.) but also potential threats or overt attacks. Third is uncertainty about components themselves and how they interact upon reconfiguration, including unexpected and unwanted feature interactions. Each of these sources of uncertainty can potentially be identified at different stages, respectively run time, design time, and requirements, but their mitigation might be done at the same or a different stage. Based on the related literature and our preliminary investigations, we argue that the following three overarching techniques are essential to developing enabling technologies to address uncertainty at all three stages.

(1) Model-based development: Model-based development enables developers to manage the increasing complexity of DASs, starting with the requirements, iterative and automated refinement to code, and management at run time. Model-based abstractions are essential to ensuring traceability of dynamic reconfigurations to design decisions and functional objectives of the system.

(2) Assurance: Given the increasing role of cyber-physical systems (CPS) in high-assurance domains, where the computing system is tightly intertwined with the physical components of the system and environment (e.g., transportation, medicine, and critical infrastructure protection), applying a rigorous approach to the assurance of a DAS is paramount. Given the complexity of these systems and their continuously changing requirements and environmental conditions, it is important to use lightweight techniques at run time, perhaps used in conjunction with heavier weight assurance techniques used during development.

(3) Dynamic adaptation: Given the multiple levels and sources of uncertainty, it becomes impossible to determine at requirements or design time to identify all possible conditions under which a CPS will execute. As such, support for dynamically adapting a system in response to real-time monitored events is needed. Also, the adaptation process must be rigorously applied, while ensuring system consistency and acceptable behavior during and after adaptation.

We posit that in order to go beyond incremental improvements to current software engineering techniques, we need to infuse these three areas with successful techniques and inspirations from other disciplines, such as machine learning and biology. For example, we observe that in the biological world, evolution has done a remarkable job of producing systems that adapt to their environment and survive dynamic and adverse conditions. Our preliminary investigations exploit this power by integrating evolutionary computation into the model-based development and run-time support of high-assurance, dynamically-adaptable systems. The open-ended nature of the evolutionary process has been shown to discover novel solutions to complex engineering problems. However, in the case of high-confidence software, this search capability must be coupled with rigorous development tools and run-time support to ensure that the resulting systems behave in accordance with requirements.

Selected References

[1] J. Whittle, P. Sawyer, N. Bencomo, Betty H.C. Cheng, and J.-M. Bruel, "RELAX: Incorporating uncertainty into the specification of self- adaptive systems," in Proc. of the 17th Int. Requirements Eng. Conf. (RE '09), Atlanta, Georgia, USA, September 2009, pp. 79–88.

[2] B. H.C. Cheng, P. Sawyer, N. Bencomo, and J. Whittle, "A goal-based modeling approach to develop requirements of an adaptive system with environmental uncertainty," in ACM/IEEE International Conference on Model Driven Engineering Languages and Systems (MODELS'09), ser. Lecture Notes in Computer Science. Denver, Colorado, USA: Springer- Verlag, October 2009, pp. 468–483.

[3] A. J. Ramirez and B. H. Cheng, "Automatically deriving utility functions for monitoring software requirements," in Proceedings of the 2011 International Conference on Model Driven Engineering Languages and Systems Conference, Wellington, New Zealand, 2011, pp. 501–516.

[4] A. J. Ramirez, A. C. Jensen, B. H. Cheng, and D. B. Knoester, "Automatically exploring how uncertainty impacts behavior of dynamically adaptive systems," in To Appear In the Proceedings of the 2011 Inter- national Conference on Automatic Software Engineering, ser. ASE'11, Lawrence, Kansas, USA, November 2011.

[5] A. J. Ramirez, D. B. Knoester, Betty H.C. Cheng, and P. K. McKinley, "Applying genetic algorithms to decision making in autonomic comput- ing systems," in Proceedings of the Sixth International Conference on Autonomic Computing, Barcelona, Spain, June 2009, pp. 97–106.

[6] A. J. Ramirez, B. H. Cheng, P. K. McKinley, and B. E. Beckmann, "Automatically generating adaptive logic to balance non-functional tradeoffs during reconfiguration," in Proceedings of the 7th International Conference on Autonomic Computing, ser. ICAC. Washington, DC, USA: ACM, June 2010, pp. 225–234.

[7] A. J. Ramirez, E. M. Fredericks, A. C. Jensen, and B. H. C. Cheng, "Automatically RELAXing a goal model to cope with uncertainty," in SSBSE'12: Proceedings of the 4th international conference on Search Based Software Engineering. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 198–212.

[8] "Automatically Exploring How Uncertainty Impacts Behavior of Dynamically Adaptive Systems" (Andres J. Ramirez, Adam C. Jensen, Betty H.C. Cheng and David Knoester,), in Proceedings of 26th IEEE/ACM International Conference on Automated Software Engineering (ASE 2011), pp. 568–571, November, 2011, Lawrence, Kansas.

[9]"A Toolchain for the Detection of Structural and Behavioral Latent System Properties" (Adam Jensen, Betty H.C. Cheng, Heather J. Goldsby, and Edward Nelson), Proceedings of the ACM/IEEE International Conference on Model Driven Engineering Languages and Systems (MODELS 2011), pp. 683–698, Wellington, New Zealand, October, 2011. (Nominated for Best Paper).