Towards Formal Framework for Modeling and Evaluation of High-Confidence Criticality-Aware Software for Distributed CPS: A White Paper

Sandeep K. S. Gupta
IMPACT Lab
Department of Computer Science and Engineering
Arizona State University
Email: sandeep.gupta@asu.edu
URL: http://impact.asu.edu

Transportation congestions, Energy scarcity, and Climate change are three most important challenges facing our nation and the world. Cyber-physical systems (CPS) – engineered systems in which physical, computation and control components are closely integrated - have a great potential to address these (infrastructure) challenges in a novel and integrated manner. Emerging technology, e.g. embedded distributed sensors, and algorithmic innovations is helping to foster infrastructure solutions to enhance efficiency, safety, dependability, manageability, and sustainability of CPS systems. However, much is needed from the perspective of developing formal software foundations towards the development of CPS systems to ensure *criticality-awareness* – the ability of the system to respond to unusual situations, which may lead to disaster (with the associated loss of life and/or property), in a proactive and autonomic manner. Although existing software technology, especially in the domain of real-time embedded systems, is designed to be cognizant of the physical environment they operate in, such systems are mainly designed to address the physical and economical constraints while meeting the functional goals. However, as more and more CPS systems would be deeply embedded in the physical infrastructure and as we as a society become increasingly reliant on these CPS systems – what is needed is that the software systems should be designed to be more criticality-aware to address unexpected events and potentially save lives and prevents loss of property. Such criticality-aware systems should be able to detect abnormal situations and respond appropriately.

For example, imagine a futuristic smart sky-scraper building (almost a small city) designed to address the aforementioned challenges. It is but natural that a large number of novel technologies from construction material to design to sensing, computation, and control would be needed to make such a building energy-efficient, safe, and habitable. The question is how should the CPS software monitoring and controlling the status of the building at all times be designed and tested for unusual situations like fire or terrorist attack? How should it interact with the first-responders to ensure safe evacuation of the inhabitants? And more importantly, how can we design, develop, and test such software systems? Finding solutions for the last question is the focus of this white-paper. As another example consider futuristic cars (transportation vehicles), on a futuristic high-away which is capable of "interacting" with the smart high-away infrastructure to enable important functionality e.g. help in mitigating the congestion problem with the help of real-time traffic and accident updates, assist in timely and safe routing of first-responder vehicles, meeting the personal QoS of vehicle drivers e.g. minimizing travel time or maximizing fuel-efficiency, in collaboration with the smart high-way. In this context, a similar challenging question is whether we could design and develop scalable and

dependable CPS software to meet these diverse demands while being criticality-aware. As these two examples illustrate, despite diverse domains, there is commonality in the need for criticality-aware CPS software.

Towards this goal, we in the IMPACT lab at Arizona State University, have been developing formal framework for developing criticality-aware software for CPS. It is based on the observations that there exists a *window-of-opportunity* to respond to a critical situation before it leads to a disaster. Within this event-dependent window-of-opportunity certain mitigative interdependent actions need to be performed to avoid disaster. The efficacy of these actions depends on such diverse parameters such as the availability of resources and the expertise (and mental state) of humans who perform these actions. In our criticality-aware framework, the concept of *Criticality* is used to characterize crises in smart-infrastucture [1][2][3]. The changes in the system's environment which lead the system into a crisis/disaster are called *critical events*. The *resulting effects* of the critical events on the smart-spaces are defined as criticalities. Two verifiable properties of criticality management – *Responsiveness* to criticalities, and *Correctness* of criticality response – are identified and analyzed. A *controllability condition* is established based on the real-time requirements of the criticalities. This condition encompasses the level of responsiveness to give an upper bound on the time taken for detecting and responding to the critical events. *Manageability* metric characterizes how *effectively* the crisis management can respond maximizing inhabitants' safety. This is measured in terms of the *Q-value* or the *Qualifiedness* of the response actions. The Q-value depends on the controllability condition and the uncertainties involved in performing the response actions due to possible human involvement. A *state-based stochastic model* is established in this regard where critical states are considered when the system is under one or more criticalities. Using the stochastic model a generic modeling framework is developed i) to evaluate the effectiveness of the crises management in smart-spaces; and ii) to select appropriate crises response actions accordingly [1].

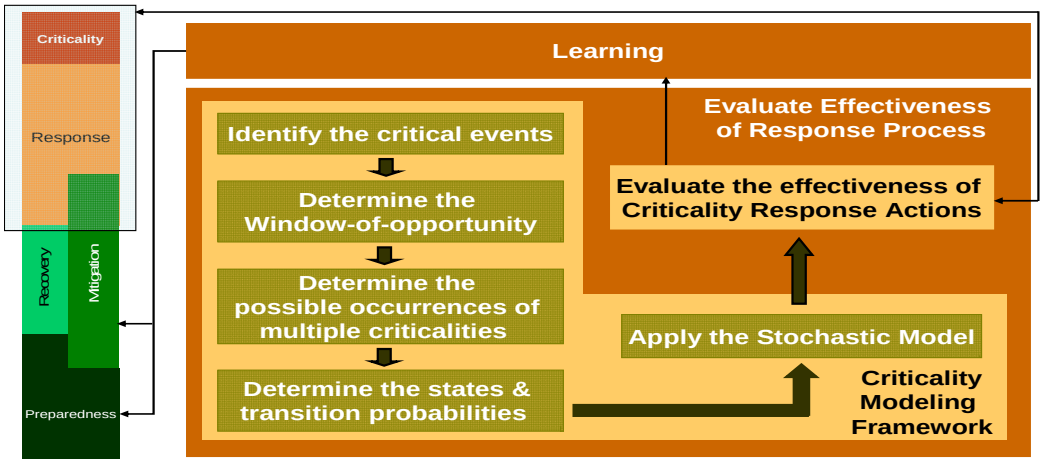

Figure 1: Criticality-Aware Framework for CPS

Figure 1 depicts the modeling framework and its applicability to various phases of crises management.

Such framework is a promising solution to develop criticality-aware future automotive (and transportation) CPS to save numerous lives – 42000 per year in US alone. For example, in case of a forward collision warning in smart vehicle such as Volvo XC 90, the identified criticalities may include – the collision warning itself, the health hazards (e.g. heart-attack of the driver), and so on. The window-of-opportunity to avoid accident depends on the distance of the possible forward collision and the speed of the vehicle, whereas for heart-attack the window-of-opportunity is the golden hour after the attack. Both the criticalities can occur simultaneously. The criticality-aware framework can evaluate the effectiveness of different response actions and their order of actuation based on the maximum Q-value achieved, and thereby enable proper facilities and context-sensitive services to maximize the passenger safety.

Acknowledgements

Thanks to T. Mukherjee and K. Venkatasubramanian for their technical contributions; and Intel Corp. and the Consortium of Embedded Systems for their support.

References

[1] T. Mukherjee, S. K. S. Gupta, ***A Modeling Framework for Evaluating Effectiveness of Smart-Infrastructure Crises Management Systems***, IEEE Tech. for Homeland Security 2008.
[2] T. Mukherjee, K. Venkatasubramanian, S. K. S. Gupta, ***Performance Modeling of Critical Event Management for Ubiquitous Computing Applications***, ACM MSWiM, 2006.
[3] S. K. S. Gupta, T. Mukherjee, K. Venkatasubramanian, ***Criticality Aware Access Control Model for Pervasive Applications***, PERCOM, 2006.

BIO:

Sandeep K.S. Gupta is a professor in the Department of Computer Science and Engineering, ASU, Tempe, USA. Before joining ASU, he has served on faculty of Colorado State University, Ohio University and Duke University. He has Phd from Ohio State University, MTech from IIT Kanpur and BTech from IT-BHU. His research is focused on dependable and adaptive mobile and pervasive distributed systems with emphasis on cyber-physical systems such as datacenters and body-area networks. Gupta's research has been funded by the National Science Foundation (NSF), the Science Foundation of Arizona (SFAz), the Consortium for Embedded Systems (CES), the Intel Corp. and Mediserve Information Systems. His current NSF projects are titled "CSR-DMSS, SM: Next-Generation Thermal-Aware, Energy-Efficient Resource Management for Data Centers" and "CT-ISG: Physiological Value based Security for Body Area Networks". He has authored/co-authored over 100 peer-reviewed conference and journal articles in venues such as IEEE ICDCS, ACM Mobicom, IEEE/ACM ToN, IEEE TPDS, and IEEE TBE. He has served on program committee for various conferences such as IEEE Percom and Symp. on Parallel and Distributed Systems. He is currently on the editorial board of IEEE Communication Letters. Gupta is co-author of the book "Fundamental of Mobile and Pervasive Computing, McGraw Hill. His work has won numerous awards including a Best Paper Award, NSF-ITR, and NSF-NMS. Dr. Gupta was TPC Chair for **BodyNets**'08– http://impact.asu.edu/bodynets, Tempe, AZ, March 2008 and GreenCom'08 (http://impact.asu.edu/greencom). He is a senior member of the IEEE and heads the IMPACT lab at Arizona State University (http://impact.asu.edu).