Association for Computing Machinery
Advancing Computing as a Science & Profession

*Ubiquity,* an ACM publication
February 2016

## Ubiquity Symposium

# The Internet of Things

## On Resilience of IoT Systems

***by Kemal A. Delic***

### Editor's Introduction

*At the very high level of abstraction, the Internet of Things (IoT) can be modeled as the hyper-scale, hyper-complex cyber-physical system. Study of resilience of IoT systems is the first step towards engineering of the future IoT eco-systems. Exploration of this domain is highly promising avenue for many aspiring Ph.D. and M.Sc. students.*

**Ubiquity Symposium**

# The Internet of Things

## On Resilience of IoT Systems

***by Kemal A. Delic***

The resiliency of a system is defined by its capability (1**) to resist** external perturbances and internal failures; (2) to **recover** and enter stable state(s); and (3) **to adapt** its structure and behavior to constant change. Resilience is carefully studied in various scientific, engineering, and social domains as it has also a great practical importance and value. The first decade of 21st century has witnessed the rise of the ultra-large-scale systems, notably based on advances in information and communication technologies. Global-scale social networks, advertising markets, and global trading and shopping hubs are the prime examples of such ultra, large-scale systems.

We are now experiencing the rise of Internet-of-Things (IoT), as the third wave of the global Internet spreads, which will culminate in 30-50 billion always-connected devices [1]. Such a system will be difficult to monitor effectively and control efficiently. Consequently, the resilience of an IoT system would be of prime importance and it could spawn an entire new branch of research into resilience of hybrid, ultra-large scale, and safety-critical systems.

Study of the structure and behaviors will lead to the creation of resilience models, which will likely be meta-models of the system-of-systems. These models will be used for simulation of all possible behaviors. Once behaviors are recognized, understood, and classified, they will be used as the insights into architecting, designing, and engineering resilient ultra-large-scale systems. Architecting will result in creation of a long-term framework that will in turn guide appropriate design and technology choices. Engineering will explore all possible trade-offs regarding cost/performances aiming to ensure and guarantee system resilience.

This short article will outline the long-term roadmap of research into the resilience of ultra, large-scale systems with a particular focus on the emerging field of IoT.

**Resilience Defined**

The word "resilience" has roots in the Latin word *resilire*, describing capability of the system to resist to various types of perturbances and to recover either fully or partially [2]. Natural scientists have been observing and studying this distinctive quality of nature-born, living systems for a long time. Social scientists study the evolution of human societies and cultures exhibiting resilience and longevity. In modern times, engineers try to emulate such qualities in artificial, man-made artifacts producing long-lasting goods and smoothly functioning systems.

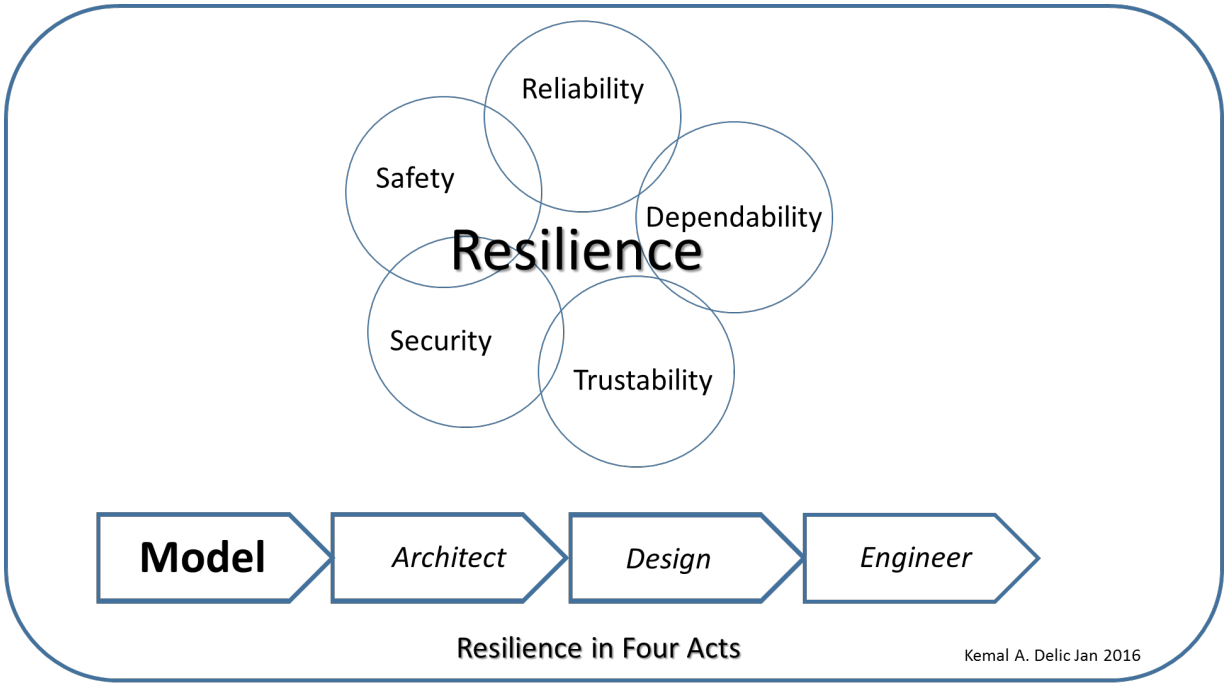


**Figure 1. Resilience Studies and Acts.**

Consequently, studies in fault-tolerant systems, dependable and trustable systems, and reliable and available systems have advanced the creation of resilient infrastructures that serve contemporary humanity well. Each branch of research (see the top of Fig. 1) has a specific angle of interest. So, *reliability* studies aim to understand design faults and usage failures to ensure functionality. *Dependability* studies combine the importance of certain functionality related to the robustness of infrastructure, aiming to provide quantitative measures of dependability. Human dimension of *trust* is transposed into engineering systems having similar qualities. *Security* dimension is especially important for Internet-related commercial activities. In extension to physical security, *safety* is studied in various domains, and especially in domains of large-scale, industrial systems. In an ideal word, we would ensure the construction of system

models, capturing system behavior to guide long-term, strategic architectural plans of the system that aim for long-term, fault-less longevity. Design is actually a detailed work-out of specific architectural aims with an engineering objective to provide measurable, manageable, and controlled system behavior (see the bottom of Fig. 1).

In the recent decades, techno-social systems emerged as the particular instance of hybrid systems combining infrastructures, devices, and people. The IoT is probably the best current embodiment of such system. Challenges to be dealt with resilience of IoT domain can be summarized as scale, speed, and uncertainty**.** Omnipresent, global, high-speed connectivity of billions of devices will certainly bring new dimension of interest in IoT resilience. The first step will be to define and construct **the model for resilient IoT systems.**

## IoT Resilience Modeled

IoT represents a hyper-scale system that can be captured conceptually as the meta-model consisting of the three big models: markets, users, and infrastructure (see Fig. 2). We would aim to create inter-operating models, so that we can run various simulations and explore events and flows relative to resilience concerns and objectives. (Very much in a vein to how a SimCity game works.)

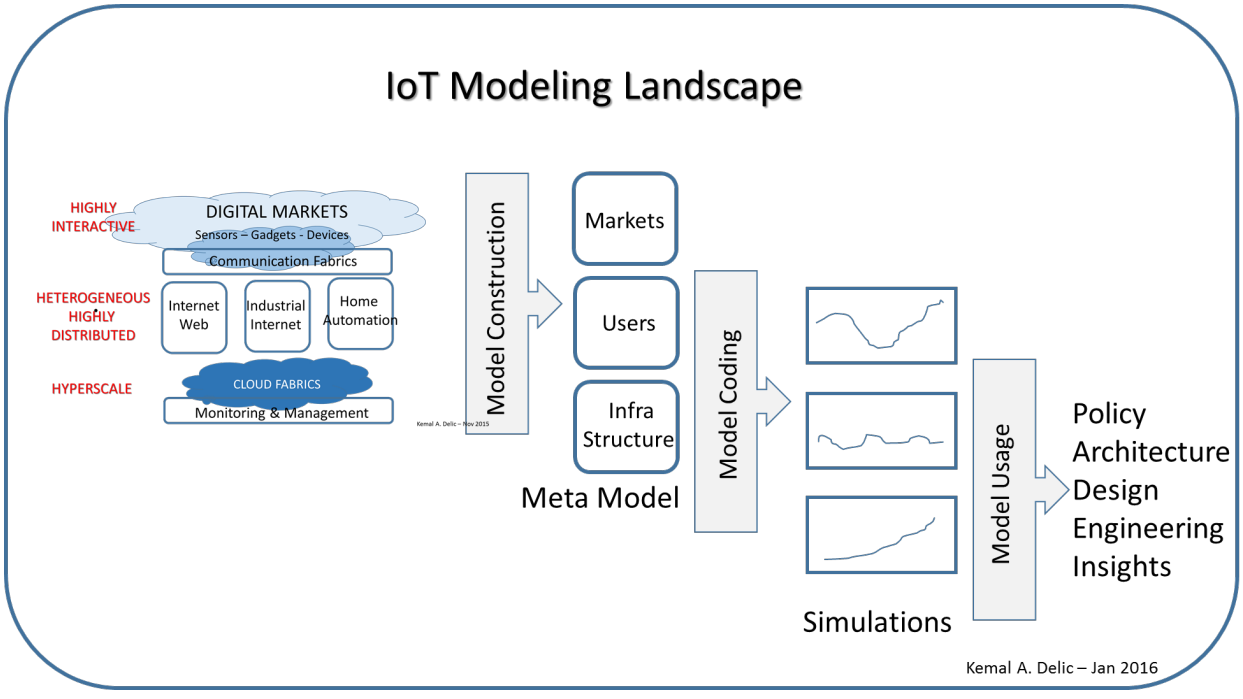


**Figure 2. From hyper-scale system model to practical model usage.**

So, for example, a model of markets may have graph-probabilistic structure where users can be described via agent models and infrastructure might be modeled via causal networks. Once models are coded in programming language, they will be transformed into executable form and exercised over different criteria. The outcome of many simulations will provide insights for architecture, design, and engineering. It will also provide hints about creating policies to ensure system resilience. All this seems to be an area of future research with several interesting topics to address, resolve, and advance. It will be on both levels: fundamental research into phenomenon of resilience, and applied research in architecting, designing, and engineering of resilient systems.

**Future IoT Resilience Research**

A few years ago [3], we had taken position that the useful way of looking into resilience would be to study the resilience of complex systems. We specifically suggested diversity, adaptation, correlation, causation, and renewal are the most promising directions of research investigations. It was observed in nature that diversity of ecosystems is an important explanation of resilience. In that spirit, highly-dependable systems (like avionics) have emulated that behavior in avionics triple systems to ensure diversity in control systems (electronics, fluid, and mechanical control). In the same spirit, imagine a variety of programmers writing code independently, for the same function, so that the outcome of voting system can be applied in control of safety critical systems. In that perspective, diversity in an IoT system would be a very important characteristic and advantage of IoT eco-systems.

Adaptation phenomena are omnipresent in nature, so one would expect that IoT systems will be highly adaptive, always changing, and slowly evolving systems. Correlation is a deep, not well-known process that is important in many areas and has been explored for centuries. In the IoT domain, this will become even more complicated and likely even more difficult to understand and explain. Closely related is causation, which is often confused with correlation. Understanding causes and consequences is objective of many modeling exercises. In the IoT domain, this would be even more difficult—if not impossible. Yet it is another avenue of possible research. Finally, an IoT system will certainly be a constantly evolving system in which we will observe phenomena of renewal of technologies, devices, and IoT uses.

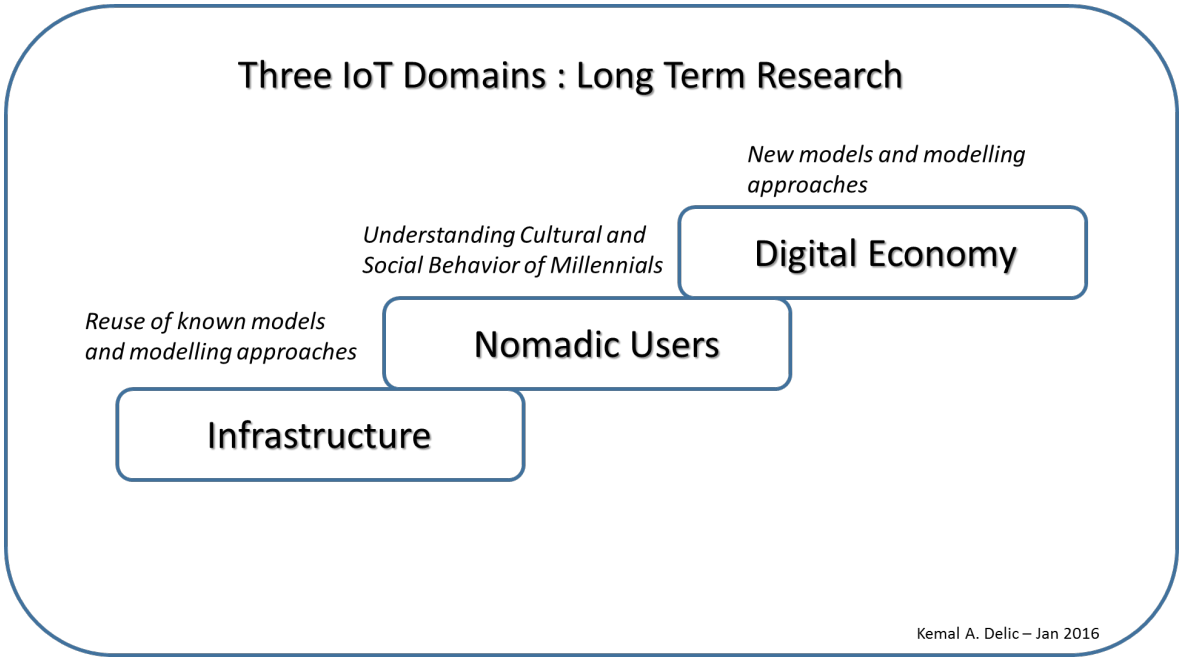


**Figure 3. Three domains for long-term research in IoT.**

Thinking about sub-models of the entire field, we could envision (at least) **three large domains** of research (see Fig. 3) covering IoT in a generic manner, so that some reuse and creation of new models is most likely path of advances. Innovative thinking will be necessary, as we pointed at huge challenges in the IoT field being summarized as scale, speed, and hyper-complexity. As always, great challenges are also big opportunities to make great discoveries and contribute to the scientific progress of human kind.

To conclude this exciting new opportunity of studies in resilience of hyper-scale systems has the potential for many Ph.D. and M.Sc. theses along lines of research outlined above, and possibly creating necessary deep insights for the engineering community that aims to provide devices, infrastructure, and services to the growing field of the digital economy [4]. This may well trigger another wave of economic activities and circle of wealth creation and generational prosperity.

## About the Author

Kemal A. Delic is an associate editor for *Ubiquity Magazine*. He is also a senior technologist with Hewlett-Packard Co. He serves as an adjunct professor at PMF University in Grenoble, advisor to the European Commission FET 2007-2013 Programme, and expert evaluator for Horizon 2020. He can be found on Twitter @OneDelic.

**DOI:** 10.1145/ 2822885

## References

[1] Delic, K. Siren's Song of Internet of Things. ACM Ubiquity. Blog. December 2, 2015.

[2] Strigini, L. Resilience: What Is It, and How Much Do We Want? *IEEE Security and Privacy* 10, 3 (May/June 2012), 72-75.

[3] Delic, K. A. and Bourgine, P.M. Resilience of Complex Systems. ECCS13–Barcelona. Sep 2014.

[4] Delic, K. A. Resilience of IoT Systems. World Wide Web Consortium, Berlin, 2015.