Invited Thoughts on the Internet of Things

Are humans succumbing to, and dumbing themselves down, to each new advance in technology? We ask because today you have no need to learn to spell with accuracy– use a spellchecker. The same goes for grammar. And why learn to type – talk into the microphone and the text will appear. Or why bother with that? Need a conference paper? Allow software to create one, acceptable to a conference, given a few keywords that you feed it. And don't get us started on math. Why learn that? Use a calculator app. The point is that with cars that drive themselves, or at least can auto parallel-park, planes that fly themselves, robots that make our meals, and homes that know our proximity to them and know what we want turned on or off, it is hard to imagine how the "supposed" technology advances offered by the Internet of Things (IoT) will not merely make us more dependent. Why? It is because automation typically suggests increased efficiency through more precise (and quicker) decisions and actions.

The now heavily clichéd "Internet of Things (IoT)" includes devices, sensors, actuators, communication, computational elements, and who knows what else, all tethered to the Internet. However in practice, users of IoT technology will most likely have a private, well-provisioned, and well-purposed network of things addressing tasks they want automated or for which IoT technology is the only solution. There is a great deal of excitement about the seemingly limitless uses for this technology, but as always, the problem is in the details, and with IoT, the nefarious intent could run rampant.

Given that this is an exciting and scary technology simultaneously, let's look at various viewpoints from a set of invited authors on where they believe that IoT technology is today, and where it might head.

Our first article "Requirements Engineering of Reliable IoT Systems : The First Step" by Phil Laplante from Penn State University, introduces the first principles of a specialized approach to requirements engineering for IoT systems.

Our next article, "Secure and Reliable IoT Adoption: 'I think I can, I think I can'", by Steven Rosen and Saeid Abolfazli from YTL Communications and Xchanging Malaysia, focuses on security, privacy, and interoperability issues in the IoT ecosystem. Despite the advancements in IoT enabling technologies, adopting secure and reliable IoT on a global scale is still questionable and therefore the IoT fundamental building blocks require revisiting to ensure security and reliability in the IoT systems.

Further, the article "Considerations for Healthcare Applications in the Internet of Things" by Phillip Laplante from Penn State University, Nancy Laplante from Widener University, and Jeffrey Voas from NIST review an approach to characterizing healthcare applications for IoT and discuss the challenges in eliciting requirements from patients and the privacy issues in this context. Some of these new challenges and issues, such as the obligations to report illegal activity information captured by IoT that run up against privacy considerations, warrant further research by legal scholars.

Finally, the article "Digital Immunity: An Interaging Metaphor" by George Hurlburt from STEMCorp., discusses the concept of digital immune system, which would satisfy the deepening cybersecurity concerns. Considering Complexity Theory, Network Science, and correspondence between threats, biological defenses and potential cyber-analogs, the author discuses early postulated organizing principles for a digital immunity architecture.

Thank you for reading our "Invited Thoughts on the Internet of Things" issue of Reliability. We welcome your comments and perspectives.

Jeffrey Voas is the security column editor for Computer magazine and an IEEE Fellow. You can reach him at j.voas@ieee.org.

Irena Bojanova is Acting Editor in Chief of IEEE Transactions on Cloud Computing, Associate Editor in Chief of IEEE IT Professional magazine, and a Senior Member of the IEEE. You can reach her at irena.bojanova@computer.org.