Energy and Commerce Committee Hearing

Disrupter Series: The Internet of Things, Manufacturing and Innovation

Testimony before the Subcommittee on Digital Commerce and Consumer Protection

United States House of Representatives

January 18, 2018

by

Thomas R. Kurfess, Ph.D., P.E.

Professor and
HUSCO/Ramirez Distinguished Chair in Fluid Power and Motion Control
Woodruff School of Mechanical Engineering
Georgia Institute of Technology
Atlanta, Georgia USA

Chairman Latta, Vice Chairman Harper, Ranking Member Schakowsky and other committee members, I appreciate the opportunity to testify before the subcommittee. My name is Thomas Kurfess and I am a Professor and HUSCO/Ramirez Distinguished Chair in Fluid Power and Motion Control in the George W. Woodruff School of Mechanical Engineering and the Georgia Institute of Technology in Atlanta, Georgia. My background is in advanced manufacturing, and I have over 40 years in manufacturing. I grew up in the Chicago area in a family machine shop working on machines tools with my father, sister and brother. I studied mechanical engineering, and electrical engineering and computer science at the Massachusetts Institute of Technology. I have been a faculty member since 1989, and have had in depth experiences with a variety of companies and organizations including small start-ups, medium sized corporations, large suppliers, and original equipment manufacturers (OEMs). I have worked at national laboratories such as the Lawrence Livermore National Laboratory and the Sandia National Laboratories, and I have participated in a wide variety of national and international organizations that are heavily involved in manufacturing.

As I have previously noted the principle area of my research and its application is in advanced manufacturing, in particular what has come to be known as digital manufacturing. Digital manufacturing relates to the use and integration of Big Data, connectivity (*e.g.*, broadband and the Internet), and high performance computing into manufacturing. Sometimes this is described as the fourth industrial revolution, or Industry 4.0. The first industrial revolution was when water and steam were used to power production operations. The second was when electricity replaced water and steam. The third industrial revolution was when electronics, such as computers, were used to automate production. The fourth industrial revolution takes the third industrial revolution to a completely new level by leveraging high speed connectivity, Big Data, cloud computing, and cloud storage. In particular, I am here to speak about "The Internet of Things and its effect on Manufacturing and Innovation." The Internet of Things, or IoT as it has come to be known, is the network of physical devices that are all around us. For example, we have smart phones that are on line, smart watches and cars that are on line, and so forth. The same is true for the IoT and manufacturing, sometimes known as IoT4MFG, or the Industrial Internet of Things (IIOT). In particular, I will testify about IoT for manufacturing as it relates to Digital Commerce and Consumer Protection. The key points of my testimony are as follows:

1. IoT has come to manufacturing. It is here and cannot be stopped. We need to embrace it, and ensure that our use of IoT in manufacturing leverages all of our strengths in the United States.
2. While IoT for manufacturing provides a variety of significant advantages, and must be embraced by U.S. industry, we must also be aware that there are a variety of security issues that must and can be addressed. These need to be taken seriously and addressed quickly to avoid falling behind our competition in the manufacturing sector.
3. IoT within manufacturing leverages the innovation and forward thinking nature of U.S. culture, and should be used to enable innovation in the United States, allowing U.S. based companies and entrepreneurs to quickly innovate and move their ideas and concepts into large scale production before others can copy and deploy these new concepts and technologies.
4. IoT for manufacturing is a means by which an educated workforce can be highly leveraged and utilized. It can be used to make safer and more productive workplaces, but it does require a more sophisticated workforce.

I will elaborate on these points during the remainder of my testimony.

Many of our manufacturing operations are already connected one way or another to the Internet, or at least to an internal corporate network. For example, typical machine tools and robots that we see in production operations have front end PCs as user interfaces, and these PCs, like most PCs, are on line. Network connections to these front end PCs are typically how information such as the programs is loaded into a machine and/or robot. Furthermore, these machines have a variety of sensors that generate data that are useful for plant operations and maintenance. For example, just monitoring the oil level in a machine is a simple operation. Sending out an e-mail or text over the network when the oil level becomes low is a very useful and simple operation using the IoT. The oil level sensor is ultimately connected via the network to plant operations and maintenance personnel, allowing them to know when to add oil. Of course, this is a very simple concept, and one with which we are familiar, as modern automobiles also inform us when it is time to add oil, or perhaps change the oil. Furthermore, many cars are on line, and it may be that the car schedules an oil change on its own such that the driver or owner of the vehicle is not bothered with the details of an oil change. The same is true for a machine in a plant. The information from the machine may be used to automatically order more oil and oil filters for the machine, and schedule an oil top-off or change, making plant operations even more efficient. Finally, a supervisory system may track oil consumption on a particular machine. If that system notes that the machine is consuming excessive oil, it may order extra maintenance or diagnostics for the machine to determine why it is “burning” or consuming more oil than usual.

The example that I have just given is related to a single machine. However, there are plants in the U.S. where we have thousands, or maybe even tens of thousands of machines. The ability to monitor those machines to ensure that they are operating most effectively is exactly one of the capabilities that IoT for manufacturing enables. This requires significant infrastructure within plants and between plants. This infrastructure consists of, but is not limited to, broad band connectivity, large data storage capacities (e.g., cloud storage) and advanced high performance computing capabilities to process the large quantities of data. Such infrastructure is readily available in the U.S. and provides us with a significant advantage over less developed parts of the world. Indeed, such infrastructure can offset the advantages of lower labor costs in less developed sectors of the international market. We should be leveraging this advantage, and continuing to support these critical manufacturing relevant technical infrastructures to ensure that the United States preserves and extends its advantage in this area.

With respect to security and safety, the IoT for manufacturing does provide for a safer and more secure workplace. There is no doubt that added sensors and monitoring will lead not only to enhanced productivity, but also to enhanced workplace safety for the labor force. However, with added connectivity and more computing capability comes the threat of cyber-attacks and cyber security issues. As with all sectors that are integrated tightly into the Internet, we must be vigilant with respect to cyber security. This requires that the Nation invests accordingly in cyber security initiatives and standards, and that our workforce is properly trained in best practices for cyber security.

IoT for manufacturing also enables our manufacturing operations to rapidly change and upgrade. This has two major effects. First, such rapid change capabilities enable the latest technologies to be implemented, ensuring that production operations are continuously improving and remain competitive. This capability also permits quick and effective product launch, which allows new products to be quickly produced at scale for deployment into the market. In short, IoT for manufacturing enables the innovations from the proverbial drawing board to migrate quickly to the market. Others may copy new U.S. innovations, but when that happens, we will be able to deploy even newer innovations, constantly keeping ahead of our competition. Thus, IoT for manufacturing complements the highly touted U.S. ability to innovate by rapidly and efficiently bringing those innovations to market.

Finally, as I have already stated, to fully utilize IoT for manufacturing, a strong and well trained workforce is needed. I am talking about training both the next generation workforce, as well as the current generation workforce. The reality is that most of our workforce is well aware of the Internet of Things. Many have products like Fit Bits, smart phones and tablets. Thus, I am not talking about a significant technical leap for our workforce. Rather, I am speaking of having them apply what they are experiencing in their everyday lives to the manufacturing floor. What we need to do is ensure that our workforce understands that the diagnostic and prognostic functions that are now viable for systems, such as robots in a plant, make use of sensors that are already on board the robot. The concept is fairly straightforward. We have Fit Bits for humans. We can also have Fit Bits for robots and machines. Of course, the analogy goes much further than this; however, culturally, the general population has, for the most part, accepted the IoT in their daily lives, and transitioning the IoT to their lives at work in a manufacturing operation is a path that is easily pursued. That being said, there are a number of universities, schools and professional societies that are developing training material to aid in this transition. There is no doubt that IoT in manufacturing will help to grow our manufacturing operations and will generate new and higher paying jobs. However, those jobs will be filled by individuals that are highly trained. Furthermore, those individuals will need to be continuously trained in the latest and state-of-the-art technologies to keep U.S. manufacturing operations at the forefront of this rapidly advancing technology wave. Thus, a culture of lifelong learning must be instilled and supported in our workforce.

In conclusion, the Internet of Things for manufacturing is a technology and capability that is vast, rapidly changing, and plays well to American strengths in high tech, innovation, and a strong manufacturing infrastructure. To fully leverage the opportunities presented by the IoT for manufacturing, we must have a strong high tech industry in place with a well and continuously trained workforce. The United States has all of the elements to fully utilize and leverage the IoT in manufacturing. What is needed is a strong manufacturing infrastructure, new manufacturing technologies and capabilities, and a well trained workforce with a culture that is amenable to lifelong learning. Programs such as Manufacturing USA that bring together collaborative teams from industry, government and academe are not only bringing the Internet of Things into the manufacturing world, they strengthening U.S. manufacturing capabilities by engaging highly diverse and technically savvy teams to rapidly deploy next generation capabilities to our manufacturing operations. Such partnerships not only ensure that the United States domination of the manufacturing sector will continue well into the future, they also ensure that U.S. manufacturing will keep pace with, and lead, our competition no matter how rapidly change occurs. IoT for manufacturing promises to provide a strong, secure and vital manufacturing base for the United States, ensuring national security and strengthening the nation’s economy.