Editorial: Industry 4.0 – A Confluence of Embedded Artificial Intelligence, Machine Learning, Robotics and Security

Hindustan Aeronautics Limited (HAL) is an Indian manufacturer of aircrafts and airborne vehicles. Most of their manufacturing is based on previous-generation technology for the Indian Air Force, licensed from foreign countries—Germany and Russia, in particular. However, more recently, they have started making an indigenously developed fighter Jet named “Tejas” and also ventured into commercial aviation. Recently, I had the opportunity visit one of their facilities to deliver a lecture on cyber security issues in Industry 4.0. They wanted this specific topic because they have been considering moving to next-generation manufacturing processes and instrumentation, and they wanted to decide whether doing so would have any cyber security repercussion. Surely there would be, as industry 4.0 is considered the new (r-)evolution of the industrial automation which will be better instrumented, more effectively automated, and certainly will be better monitored, and continually optimized based on the data collected and processed through machine learning techniques. The idea is to bring together technologies such as natural language processing for better human-computer interaction, more machine-to-machine (M2M) communication-driven hand-off of tasks, pervasive use of robotics, flexible and custom manufacturing, dynamically customizable assembly process. The science of Cyber Physical Systems (CPS) is the core idea in Industry-4.0 so that physical processes of manufacturing and software/hardware-based adaptive control, informed by advances in deep learning, computer vision, intelligent sensor data and data fusion, and artificial intelligence (AI) may work in harmony.

However, given the business intelligence will also inform the manufacturing decisions and customization of products, the business process will be intricately connected to the automation, leading to the IP-convergence. What that implies is that industrial automation, and supervisory control and data acquisition system (SCADA) will be connected to the enterprise network mediated by demilitarized zones and loosely connected via firewalls. This provides the exposure of the manufacturing systems to the outer world. On the other hand, even if IP-convergence is avoided, the insider attacks, or attacks by insiders induced by social engineering could expose an air-gapped industrial information system to attacks as was amply demonstrated by the Stuxnet worm. Insider attack seems to be one of the topmost concerns of CISOs according to contemporary cyber security surveys. As more embedded control, communication, and intelligent electronic devices are embedded into the manufacturing system—broader will be the attack surface, and higher will be the risk.

Does that mean that Industry-4.0 is not a good idea? The way one should look at it is that it is inevitable. AI and machine learning techniques are getting sophisticated at an extremely rapid rate—thereby creating incentive for industrial processes to leverage them. All pervasive sensors provide better monitoring, control, maintainability, and even self-repairing of the systems. One cannot avoid moving to such advanced manufacturing systems without being imperiled by the possibility of obsolescence. This also provides opportunities for further innovations in AI, machine learning, robotics, and robust and resilient control.

2018 Copyright is held by the owner/author(s).

1539-9087/2018/04-ART29

<https://doi.org/10.1145/3194944>

As we are interested in embedded computing systems, this is a ripe field for us. We have a lot to contribute. Cyber security, resilient design of cyber physical systems, embedded AI, compact machine learning hardware design, micro- and nano-robotics and faster and more secure communication protocols for communication within the manufacturing system components, are some of the topics that come to mind. Block chain technology also has an important part to play as one can consider the confidentiality and integrity of the M2M communication, the infrastructure for immutable and tamper-resistant logging of high-privileged insiders, and many other applications of the block chain technology can be envisaged in this context.

So, I would appeal to the readers of ACM TECS to consider planning a special issue in the near future on embedded-system topics relevant to Industry-4.0. There is a set of opportunities, and a set of challenges, that we must solve together.

Now we are ready with the second issue of Volume 17. Volume 17: 2 features a special section on formal methods and models for system design based on the ACM/IEEE Formal Methods and Models for System Design (MEMOCDE 2016) conference. I thank the guest editors of the special section for the enormous effort they have put in to get the submissions reviewed and make the selections. We also have many regular papers on a variety of topics.

Sandeep K. Shukla
Indian Institute of Technology Kanpur
March 5, 2018
Editor-in-Chief