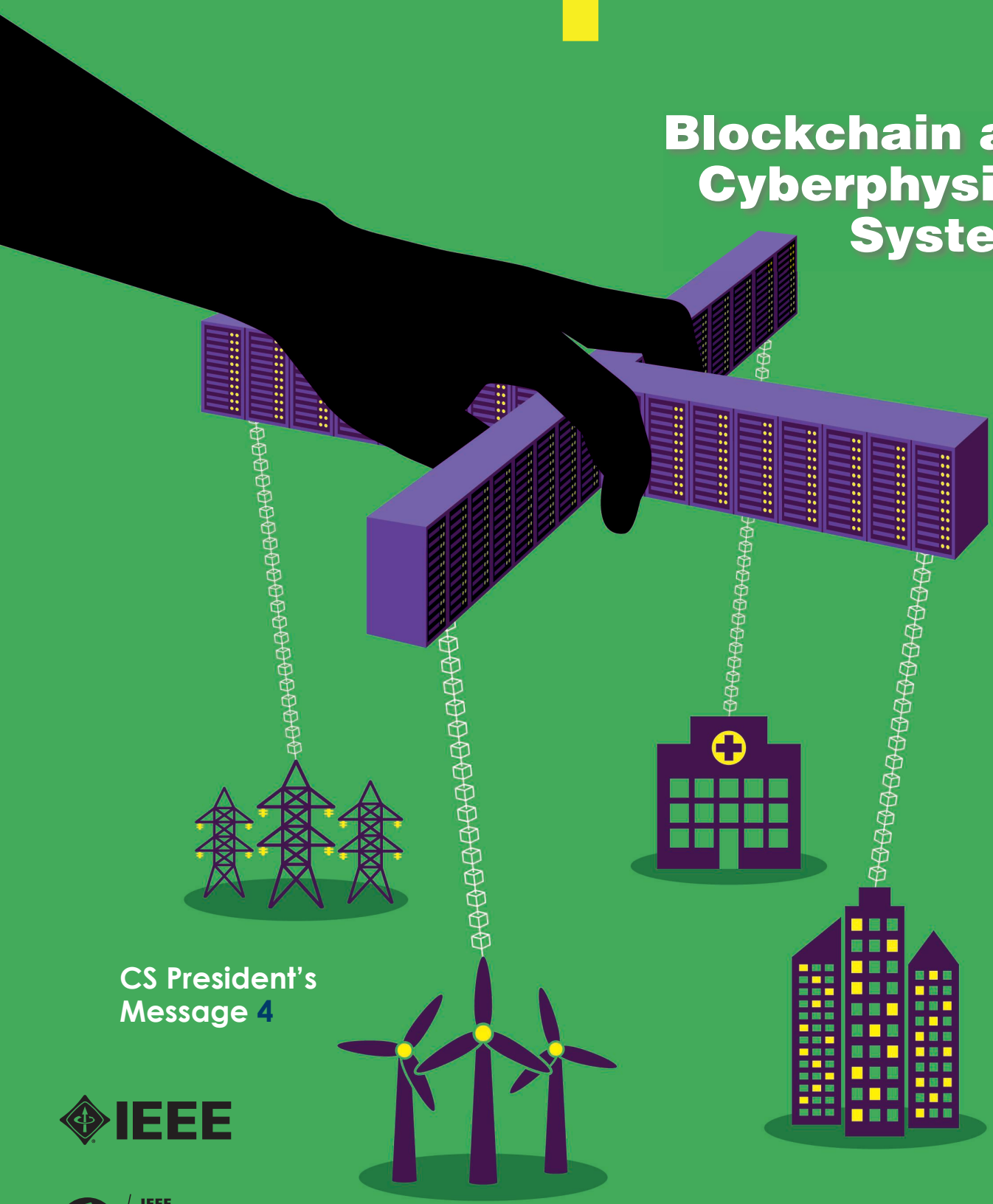
09.20

Computer

Blockchain and Cyberphysical Systems



CS President's Message 4

IEEE

IEEE COMPUTER SOCIETY

vol. 53 no. 9

www.computer.org/computer

Cybersecurity Road Map for Digital Manufacturing

Nektarios Georgios Tsoutsos, University of Delaware
Nikhil Gupta and Ramesh Karri, New York University

Digital manufacturing systems will be enabled by the convergence of ITs with manufacturing systems. Such systems are exposed to risks that require innovative solutions. We present a security road map that includes application-driven research and workforce development.

The next generation of the manufacturing revolution is taking shape by integrating IT with modern manufacturing systems. Within the manufacturing domain, additive manufacturing technologies are being developed toward moving manufacturing to a digital domain where the skills of the operator are less relevant while the skills of the designers are more valuable. New manufacturing platforms are coming online that integrate additive and subtractive technologies in the same hybrid system. Moreover, automation allows traditional manufacturing methods, such as computer numerical control machines, to go online and make their remote operation and control possible. These advances are augmented by machine learning methods revolutionizing product design and qualification processes, sensors and data analytics making these processes streamlined, and imaging and testing methods automating testing procedures.

This digital manufacturing (DM) ecosystem is fundamentally different from traditional manufacturing, especially due to the digital information flows, including design and manufacturing data, from product design to manufacturing and the final testing stages. Furthermore, network and communication systems are essential in these emerging scenarios. Thus, DM requires a new cybersecurity strategy since the traditional approach of creating silos of manufacturing plants or confining the system to a small group of trusted parties [Figure 1(a)] is no longer possible. To benefit from the possibilities afforded by DM, systems should be open, secure, and collaborative: each step of the process must integrate security as a fundamental requirement or constraint [Figure 1(b)] to enable free sharing of

Digital Object Identifier 10.1109/MC.2020.3003432
Date of current version: 4 September 2020

EDITOR **DIMITRIOS SERPANOS**
ISI/ATHENA and University of Patras; serpanos@computer.org

information among designers, manufacturers, and customers.

Developing cybersecurity methods and strategies for the manufacturing cyberphysical systems (CPSs) remains challenging. Some applicable threats are similar to those in most connected systems, such as denial of service, viruses, malware, and ransomware. Other threats are unique to DM, such as inserting undetectable defects in parts during manufacturing to cause in-service failure,[1] reverse engineering and counterfeit production, or developing competing products by modifying designs from stolen/pirated digital files. The available security methods should be tailored for the requirements of DM.

CYBERSECURITY RISKS IN THE DM WORKFLOW

A typical DM process workflow is illustrated in Figure 2. All steps can be conducted by a single entity, or each step can be conducted by a separate entity within a company or across multiple companies. A large portion of the process before the actual manufacturing step is completely digital and relies on computational and network resources for part design, simulation, and programing the controllers of the manufacturing machines. Apart from the flow of Figure 2, which mostly represents large companies for mass production, DM also enables collaborative cloud design platforms, design marketplaces, and general-purpose manufacturing facilities where people can print their designs (for example, individually customized designs manufactured in batches of one or small production runs).

The launch of two astronauts aboard the SpaceX Dragon capsule in May 2020 marked a major milestone for the U.S.-based space exploration programs. DM has played a key role in the rapid development of private space programs in the United States, where the component development lifecycle is significantly shortened by digital design and manufacturing methods. The reusable rocket boosters and crew capsule are made possible largely by rapid manufacturing of worn-out and damaged parts using 3D printing on an as-needed basis at low cost. Other aerospace companies and NASA are using DM to develop next-generation aviation and space technologies. The aerospace industry is an example where nation-state actors and highly skilled professionals may engage in extensive hacking, sabotaging, and reverse engineering the available resources. Likewise, online repositories of DM designs, such as recreational drone replacement parts, are subject to attackers stealing individual design files for personal use. These scenarios require novel cybersecurity design and implementation methodologies.

One aspect that differentiates a CPS from the IT sector is that many attacks can be implemented without ever interacting with the manufacturing process or supply chain of a genuine product. For example, a legally acquired part can be used for reverse engineering[3] and unauthorized production for personal use or sale in the gray market. Hence, the product itself needs to incorporate antireverse engineering or counterfeit identification technologies embedded within.[4] Mitigations can use novel materials that cannot be scanned using most commercial 3D scanners

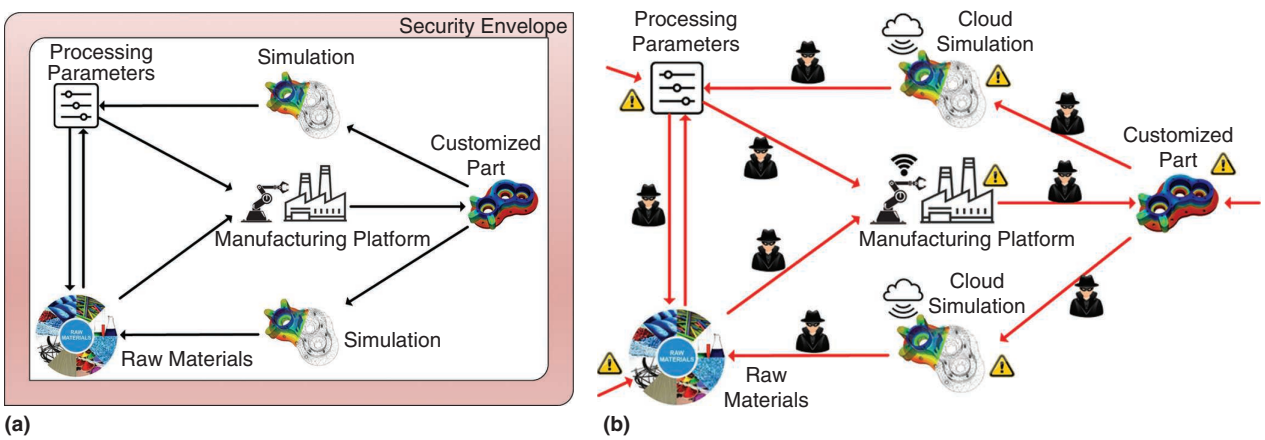


FIGURE 1. (a) An individual manufacturing facility or a small set of trusted parties, siloed in a security envelope. The external communication network is isolated from the manufacturing network. (b) A future DM framework based on open collaboration among designers, manufacturers, and customers, where each step needs to be secure and trustworthy. Data from sensors, actuators, and modeling tools within a plant may be shared widely, including outside of the manufacturing facility to make the entire DM ecosystem efficient.

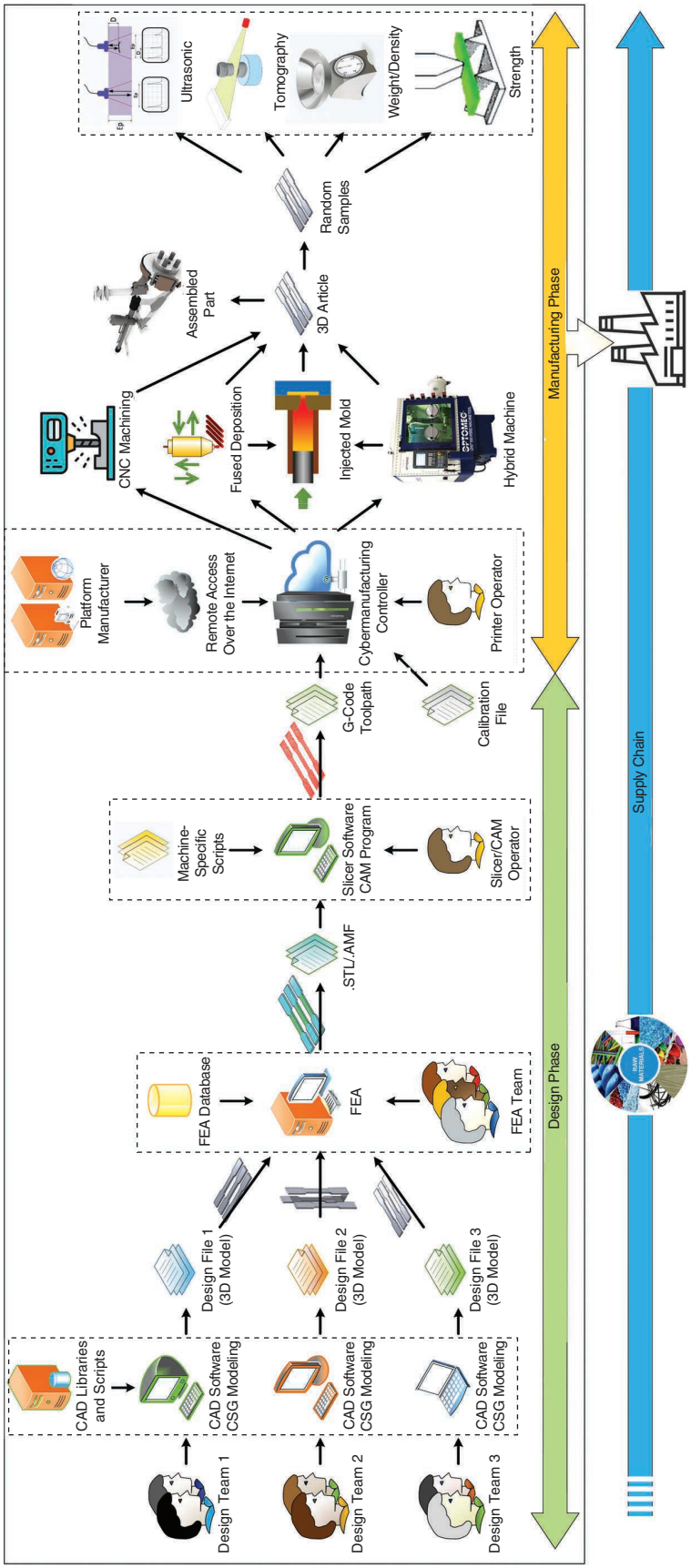


FIGURE 2. The DM process showing design, manufacturing, and product qualification steps. All steps can be conducted by a single entity or each step can be conducted by a separate entity within a company or across multiple companies. The overall supply chain includes raw material and tools acquisition, shipping and logistics, and after-life recycling.[2] CNC: computer numerical control; CSG: constructive solid geometry; FEA: finite element analysis.

or employ specialty materials with a spectroscopic signature that cannot be easily acquired. However, the cybersecurity and hardware-based security solutions need to work collectively to develop the security solutions for DM.

CLASSIFICATION OF THREATS IN DM

The threats applicable to DM can be classified into four main classes: side channel attacks, sabotage, reverse engineering, and counterfeiting.[5] Side channel attacks employ characteristics of the physical implementation (for example, power consumption, acoustic data, and toolpath data) to extrapolate information about the manufacturing process (such as identifying the part being manufactured). Sabotage entails deliberate manipulation of the process and/or design files to cause destruction, safety issues, and the premature failure of a part. This can lead to a financial and reputational impact for the manufacturer. Reverse engineering focuses on analyzing a manufactured part to extract knowledge and reveal its internal architecture. Likewise, counterfeiting entails the manufacturing of fake products, typically using inferior materials and less strict tolerances, shortening lifetime before failure. All these threats can lead to safety issues (risk of human lives), financial costs, and reputational impact to the original part manufacturer.

MITIGATION OF RISKS

Mitigating most of these DM risks is possible using available cybersecurity methods. For example, strengthening network security for all partners using network access controls, keeping virus and malware detection tools updated, and monitoring traffic can protect against certain side channels and direct sabotage. Moreover, strong password protection, the use of encryption methods for the

stored and transmitted files, digital rights management, and watermarking can protect individual files against intellectual property theft and counterfeit production. Protecting against reverse engineering, however, is challenging. Proposed methods use QR codes that are embedded during layer-by-layer 3D printing in DM, and these codes can be further obfuscated by dividing them into a large number of small segments.[5] This cloud of segments distributed over many layers in the manufactured part makes them look meaningful from several angles, obfuscating the view of the real code.

Education and workforce development

Emerging fields such as DM become a major challenge for traditional education models. DM's cyberphysical nature requires strong foundations in design and manufacturing and materials characterization methods as well as proficiency in programming, cybersecurity tools, machine learning, and simulation methods. While graduate majors in DM can be developed to include manufacturing methods, cybersecurity fundamentals, and computer networking, it remains a question whether industrial careers are evolving to benefit from such interdisciplinary education. In most companies, the manufacturing and IT departments are segregated and rarely collaborate. We envision that this scenario is slated for a major change, and workforce development toward DM cybersecurity will become a priority. Toward that end, specialty courses can educate both manufacturing and cybersecurity professionals on DM assets and how they can be protected as well as the best practices to be adopted by professionals on both sides. The development of continuing education resources is a priority for the workforce that will naturally transition from traditional to DM and cybersecurity professionals whose employers will adopt this manufacturing paradigm.

Crowdsourcing cybersecurity assessments

The use of statistical methods is often insufficient to analyze the strength of security methods in the CPS area, where sophisticated attackers leverage numerous concurrent attack vectors. Single-discipline defense teams are simply not well equipped to retaliate against such skilled attackers. A red-team/blue-team approach and crowdsourcing of security assessments to people with broad skill levels and backgrounds present a massive opportunity. New York University launched a global DM hacking competition called Hack3D in 2018,[6] resulting in several interesting benchmark examples. One challenge included a damaged photograph of a product and a partial G-code file (that is, the toolpath instructions for 3D printers) for reverse engineering.[3] Teams with a mechanical engineering background measured the part dimensions, recreated its CAD model, and iteratively improved on the design using measurements of the printed artifact. Notably, teams with computer engineering and cybersecurity backgrounds tackled the problem very differently. One team used cyberforensic tool chains to extract metadata and hack the file storage server for further clues. Other teams employed signal processing and machine learning methods to recover the damaged design with high accuracy. This diverse set of approaches cannot be gauged on a single scale to conduct statistical analysis, so crowdsourcing is a great way of measuring the security strength. Further, crowdsourcing can engage the community in assessing the security risks of DM, and the emerging benchmarks can be used in training and education.

Integrating manufacturing with ITs has created DM and revolutionized product development and production. Nevertheless, the interdisciplinary and collaborative nature of DM also creates unique security challenges that must be addressed to expand these methods into new domains. Education and workforce development programs should rapidly evolve to prepare the workforce of the next generation of manufacturing. While moving from one technology generation takes decades in the manufacturing sector, the adoption of DM has been rapid, taking advantage of teleworking, virtual testing, and onsite/on-demand production.

> Developing cybersecurity methods and strategies for the manufacturing cyberphysical systems remains challenging.

ACKNOWLEDGMENTS

The authors acknowledge the National Science Foundation grants 1931724 (DGE), 1932264 (CMMI), and 1931916 (CMMI) to enable this article. The opinions expressed in this paper are those of authors and not of the funding agency.

REFERENCES

1. S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and security challenges in 3D printing," *J. Miner. Met. Mater. Soc.*, vol. 68, no. 7, pp. 1872–1881, doi: 10.1007/s11837-016-1937-7.
2. N. Gupta, A. Tiwari, S. T. S. Bukkapatnam, and R. Karri, "Additive

manufacturing cyber-physical system: Supply chain cybersecurity and risks," *IEEE Access*, vol. 8, pp. 47,322–47,333, 2020. doi: 10.1109/ACCESS.2020.2978815.
3. N.G. Tsoutsos, H. Gamil, and M. Maniatakos, "Secure 3D printing: Reconstructing and validating solid geometries using toolpath reverse engineering," in *Proc. ACM Workshop Cyber-Physical System Security*, 2017, pp. 15–20. doi: 10.1145/3055186.3055198.
4. F. Chen, J. Zabalza, P. Murray, S. Marshall, J. Yu, and N. Gupta, "Embedded product authentication codes in additive manufactured parts: Imaging and image processing for improved scan ability," *Addit. Manuf.*, vol. 35, p. 101319, Oct. 2020. doi: 10.1016/j.addma.2020.101319.
5. N. Gupta, F. Chen, N. G. Tsoutsos, and M. Maniatakos, "INVITED: ObfusCADe: Obfuscating additive manufacturing cad models against counterfeiting," in *Proc. 54th ACM/EDAC/IEEE Design Automation Conf. (DAC)*, 2017, pp. 1–6. doi: 10:1145/3061639:3079847.
6. "Hack3D," CyberSecurity Awareness Worldwide, Brooklyn, NY. Accessed: July 24, 2020. [Online]. Available: https://www.csaw.io/hack3d

NEKTARIOS GEORGIOS TSOUTSOS is an assistant professor of electrical and computer engineering at the University of Delaware. He is a Member of IEEE. Contact him at tsoutsos@udel.edu.

NIKHIL GUPTA is a professor of mechanical and aerospace engineering at New York University. He is a Member of IEEE. Contact him at ngupta@nyu.edu.

RAMESH KARRI is a professor of electrical and computer engineering at New York University. He is a Fellow of IEEE. Contact him at rkarri@nyu.edu.

Digital Object Identifier 10.1109/MC.2020.3013584