Volume 2, No. 4 | July–August 2019

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL The Journal of Robotics, Artificial Intelligence & Law

Volume 2, No. 4 | July–August 2019

EDITOR-IN-CHIEF

Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR

Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Miranda Cole
Partner, Covington & Burling LLP

Kathryn DeBord
Partner & Chief Innovation Officer, Bryan Cave LLP

Melody Drummond Hansen
Partner, O'Melveny & Myers LLP

Paul B. Keller
Partner, Norton Rose Fulbright US LLP

Garry G. Mathiason
Shareholder, Littler Mendelson P.C.

Elaine D. Solomon
Partner, Blank Rome LLP

Linda J. Thayer
Partner, Finnegan, Henderson, Farabow, Garrett & Dunner LLP

Mercedes K. Tunstall
Partner, Pillsbury Winthrop Shaw Pittman LLP

Edward J. Walters
Chief Executive Officer, Fastcase Inc.

John Frank Weaver
Attorney, McLane Middleton, Professional Association

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2019 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Copyright © 2019 Full Court Press, an imprint of Fastcase, Inc.

All Rights Reserved.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquires and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Risk and Opportunity with the Industrial Internet of Things

David T. Doot, Steven A. Cash, and James B. Blackburn, IV*

The growth of the Industrial Internet of Things has resulted in benefits to the supply chain, such as greatly improved efficiencies in utility systems. However, those benefits have come with an increase in risk, particularly the vulnerabilities presented by systems that have become ever more communicative. The authors of this article explain.

The Industrial Internet of Things ("IIoT") has increased the connectivity, and correspondingly, the productivity and efficiency of the systems that it brings together. The growth of IIoT has resulted in benefits to the industrial supply chain, such as greatly improved efficiencies in utility systems. However, those benefits have been paired with a commensurate increase in risk, most notably the vulnerabilities presented by systems that have become ever more communicative. Before expanding existing IIoT systems, entities must first be informed and well-equipped to assess the associated benefits and risks presented by new technologies.[1]

IIoT and IoT Are Different

There are important differences between the Internet of Things ("IoT") and the Industrial Internet of Things. The IoT is the network of physical objects, embedded sensors, connections, and computers that permeates much of our everyday life. The IoT consists of helpful gadgets and is becoming prevalent in everyday items from fitness trackers, smart thermostats, and vital medical devices to connected water bottles and shopping monitors. The IoT affects consumers directly and continues to evolve within a largely consumer-driven digital ecosystem. The lineage of IoT devices, and their underlying software, can be traced alongside the development of the internet, smartphones, and the operating systems with which consumers are already familiar.

The Industrial Internet of Things, like IoT, utilizes a network with sensors and various connections; but it grew not out of the

Robotics, Artificial Intelligence & Law / July–August 2019, Vol. 2, No. 4, pp. 257–262.
© 2019 Full Court Press. All rights reserved.
ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

consumer-oriented electronics and operating systems, but alongside large-scale industrial control hardware. Much of the software behind the IIoT was custom developed (going back decades) as an adjunct to big, expensive pieces of industrial hardware: switches, valves, pumps, and other heavy machinery. While the IoT is focused on individual consumers, the IIoT (as its name suggests) serves machines and industrial systems. The IIoT is a fundamental part of the nation's critical infrastructure. It runs our oil fields, our gas pipelines, our water systems, our dams and heavy industry; it underpins the electricity grid, our train systems, our highways, and our ports.

Different Networks, Different Risks, and Benefits

The IIoT presents both opportunity and risk. Opportunities arising from increased adoption of IIoT technologies can include reducing operational expenses, increasing productivity and efficiency, and improving worker safety.[2] Additionally, while the IIoT has been around for some time, new and improved technologies are accelerating opportunities for growth, innovation, and value that can be derived with smart IIoT applications. While the introduction of new IIoT technologies can make the entire system smarter, integration of those technologies into IIoT increases risks. This perhaps can be aptly illustrated by a metaphor comparing two very different living organisms: a human and a fungus. The human has a brain and is capable of intelligent thought. The brain actively and passively connects the entire system (the body) and allows those systems to engage in and accomplish highly complex tasks. A fungus, on the other hand, does not contain a connected system capable of intelligent thought and physical dexterity. But with the human's complex system comes increased risk. A kick to the head or a blow to the spine can severely limit or destroy the entire system. In contrast, a fungus does not face the same risks—it is a simple but generally resilient system. In this regard, consider this metaphor in the context of a connected utility network.

By way of a real-world example, consider the power grid. To keep the lights on, generating stations, high-voltage transmission lines, substations, and distribution lines must all work in tandem to get power from where it is generated to where it is consumed.

Prior to the IIoT, significant human resources and capital needed to be expended to maintain the entire system. When one component failed, operators had to determine its location and assess repair needs; that process took time and money. Now, with the IIoT, sensors connect these assets and give utility operators a real-time view of the entire system. Not only can issues be more quickly detected when they occur, but the system can anticipate failure and proactively deploy resources. This connectivity saves time and money, and contributes to the system's overall resilience.

But the network that connects the entire system creates a new type of risk. Whereas the old, unconnected system was subject to a physical attack, it was unlikely that the failure of any one aspect would result in significant consequence to the entire system. Now, however, if the network fails (or is attacked), the entire system is subject to failure; and that attack may be digital, and thus can be more subtle than a physical attack. Indeed, this was precisely what happened in 2015, when the Ukraine bulk power system was the victim of a cyberattack and shut down for several hours.[3]

Assessing Risks and Benefits

IIoT systems are continually evolving, driven by new technology and needs. That technology can add to, leverage, or modify the core IIoT technology that currently exists, and can increase the existing benefits inherent with the IIoT and/or diminish the risks that come with a more connected system. Any evaluation of the value of new IIoT technology must include the critical assessment of the impact of that technology on those risks and benefits.

An effective risk analysis framework is key to evaluating where technology investors and purchasers should focus limited resources. The risk assessment approach used by the United States Department of Homeland Security ("DHS") provides a useful framework through which to evaluate IIoT and the value of technologies that seek to minimize that risk.[4] Risk (R) is a function of Threats (T) × Vulnerabilities (V) × Consequences (C); R = TVC.

Threats

Threats, at least those that flow from the nefarious activities of human beings, are a combination of intent and capability led by sophisticated state and criminal actors that seek, in the example of utilities, to infiltrate the U.S. electric grid. These types of threats are best dealt with at the national and international levels through the coordination of the public and private sectors. Threats can also derive from natural sources (hurricanes and earthquakes), or from human operator failure. The analytic framework remains helpful, replacing “intent” with “probability” as a guide.

Vulnerabilities

These represent avenues for attack or system failure, and include the attack surface (access points that an unauthorized user can exploit to enter or extract data). While a number of access points on the IIoT systems may provide more avenues for attack, the vulnerability can depend more critically on the protections from attack embedded in each access point and how those access points integrate with the broader system.

Consequences

This represents the severity of a given issue if it were to occur. For example, if one power plant goes down, does the entire system shut down or are there redundancies that minimize the effects of that loss? What would be the loss, in terms of dollars, or lives, or both?

To complete the cost-benefit analysis, we submit that a similar assessment can be made for the benefits of IIoT technologies, such that Benefit (B) is a function of Opportunity and Value. For example, transmission utilities recognized the opportunity and value of applying IIoT technology to substations and switching stations, thereby allowing the utilities to maximize the use of those assets while monitoring their operational efficiency in real time. Conversely, a given IIoT technology may be able to allow for more information to flow, but that information may not provide any value. For example, attaching a sensor to a transmission line that provides information about the ambient air quality may be an opportunity, but it provides little value to the system and therefore little overall benefit.

Evaluating New Technologies

In evaluating new technologies, investors and policymakers should focus on the effects on the variables set forth above. Keeping the focus on the R = T × V × C formula as a framework, risk reduction can be achieved by reducing any of those three variables (conversely, Benefits can be achieved by increasing Opportunity or Value). A technology may be focused on reducing consequence, such as an approach to an integrated network that can quickly isolate and bypass a system failure before it spreads to the rest of the system (for example, new grid technology that can contain and bypass a transmission failure before that failure trips the rest of the system). In contrast, a technology could have the effect of reducing vulnerability. And, of course, some technologies could do both.[5]

The IIoT Players

All stakeholders investing in the IIoT should understand how to assess these new technologies. Technologists should assess their own processes and understand where to invest further resources to improve their product. Investors and owners of an IIoT-connected critical infrastructure are best to focus their limited resources on those technologies that provide the greatest benefits and most effectively reduce risks. Policy makers and lawyers must be able not only to assess these technologies, but also to understand how they work together to reduce the risks to—and increase the opportunities of—the integrated IIoT system.

Notes

[*] David T. Doot (dtdoot@daypitney.com) is a partner at Day Pitney LLP and chair of the firm's Energy and Utilities industry group, counseling businesses around the country on wholesale and retail arrangements for the purchase and sale of electricity and advocating on their behalf before federal and state energy regulators. Steven A. Cash (scash@daypitney.com) is counsel at the firm, representing individual and corporate clients in criminal, commercial litigation, and national security matters. James B. Blackburn, IV (jblackburn@daypitney.com) is an associate at the firm, handling a range of

energy matters, including regulatory litigation focused on both electricity and natural gas matters.

[1] For more background on the Industrial Internet of Things, see "The Industrial Internet of Things: The Railway Law Revolution of Our Time," *Bloomberg BNA Privacy and Security Law Report,* Nov. 20, 2017.

[2] For example, IIoT systems now allow utilities to continuously understand how demand is changing in real time and can assist utilities in managing maintenance costs associated with managing their power-generating, transmission, and distributing resources. Crews can be deployed in real time or at convenient times prior to predicted failures, efficiently using human and capital resources and reducing the overall costs.

[3] In December 2015, Russian hackers were able to use phishing emails to gain control of Ukraine's electric grid and cause blackouts across the country. *See* "Critical Infrastructure and the Internet of Things," Tobby Simon (Jan. 2017), *available at* https://www.cigionline.org/sites/default/files/documents/GCIG%20no.46_0.pdf.

[4] *See, e.g.,* "Homeland Security National Infrastructure Protection Plan 2013," *available at* https://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf.

[5] Although possible, it is unlikely that technologies would reduce threat, either human or natural, with one significant exception: it is possible that intent could be affected if nefarious human actors are aware of decreased vulnerability or consequence—bank robbers are less likely to want to rob a bank if they know it has high-quality locks or little money in the safe.