



# Innovating a smarter and safer power network

**Managing IoT risk in  
power and utilities**



Smart city IoT projects encompassing utilities and lighting represented among the largest share of global smart city projects in a recent study of current enterprise IoT implementations at

22% and 21%

respectively. Meanwhile, connected building projects, including automation solutions to control energy costs, represent one of the largest-growing IoT segments.<sup>1</sup>

Utilities will spend an estimated

\$61 billion 

on IoT solutions globally in 2019 alone, with a focus on smart grid technology.<sup>2</sup>



# IoT powers productivity and efficiency...

The billions of connected devices that make up **the Internet of Things (IoT)** are forever changing the way utilities manage their operations and interact with energy consumers.

**In homes and offices**, utility-installed smart meters, smart thermostats, connected outlets, and other devices provide the data that utilities need for an increasingly complex ecosystem and the insights to develop new products and services to meet customer demands for fast, personalized service.

Meanwhile, **at power stations and along transmission lines**, sensors help detect outages in real time and allow workers to quickly locate points of failure.

When combined with **advanced analytics and automation**, IoT also is used to rebalance and even predict where and when to direct power along the grid based on weather, workday schedules, and other data. These technologies allow utilities to throttle up and down, providing power when it's needed most and dialing back or storing energy when it's not, for even greater efficiency.

In just one example, the U.K.'s National Grid is looking to maximize the **integration of intermittent renewable energy sources** such as wind and solar.

By working with DeepMind, owned by Google parent company Alphabet, and using artificial intelligence to crunch the data from smart meters as well as from weather-related variables, National Grid seeks to predict supply and demand peaks. While the effort is still in its early stages, DeepMind can point to prior success using AI to reduce the amount of energy used for cooling Google's data centers by 40 percent.<sup>3</sup>

As utilities continue **the shift from traditional power companies into network integrators and participants**, IoT allows them to expand new energy markets, enable resiliency and reliability, and contribute to centralized management of a distribution grid.<sup>4</sup>

Indeed, IoT has the potential to connect the web of conventional regional power stations fueled by traditional sources with a growing number of localized microgrids and renewable sources, spurring the distributed energy transition where energy consumers are also energy producers.

**As useful as IoT is today, it's even more critical for the utility of tomorrow.**

<sup>1</sup> "The Top 10 IoT Segments in 2018—based on 1,600 real IoT projects," IoT Analytics, February 22, 2018.

<sup>2</sup> Worldwide Semiannual Internet of Things Spending Guide, IDC, 2019.

<sup>3</sup> "DeepMind and National Grid in AI talks to balance energy supply," *Financial Times*, March 12, 2017.

<sup>4</sup> Explore more about the Network Integratory journey

# ...if companies are smart about the risks

However, with new technologies can come **new and greater risks**. Power and Utility (P&U) industry leaders see cybersecurity risk as a top-three threat to growth, along with emerging technology and climate change.<sup>3</sup>

As IoT expands P&U connectivity, “bad actor” threats grow. If 10,000 customers on a grid have smart meters, that’s 10,000 **potential entry points** to hack the system, introduce malware, or perpetrate other threats.

More, the use of **third-party technology providers** opens the door even wider. Attempts have already been made to attack the U.S. power grid through contractors who provide software to utilities. According to U.S. intelligence agencies and technology executives, foreign hackers are now even more focused on proving they can disrupt the U.S. power grid than on disrupting elections.<sup>4</sup>

As governments and regulators become more concerned with these risks, they expect the power and utility industry to answer their concerns and **demonstrate security**. Additionally, with expanded customer relationships enabled through IoT technologies, industry leaders increasingly recognize they have a responsibility to **protect personal data** and **maintain the public trust** as well.

Deploying connectivity through IoT without a **unified vision and strategy** can drive up costs and drive down returns, and failing to integrate and manage third parties can render IoT investments obsolete and leave open doors to introduce harm. Introducing IoT technologies without **adequate policies, training, and operational capabilities**—whether built, bought, or borrowed—can leave companies vulnerable.

**In order for P&U companies to remain competitive against innovative upstarts and realize the full business potential that IoT can bring, they must manage the risks that come with innovation.**

<sup>3</sup> 2018 KPMG CEO Outlook: Power & Utilities

<sup>4</sup> “Russian Hackers Appear to Shift Focus to U.S. Power Grid,” *The New York Times*, July 27, 2018.

<sup>7</sup> The GE Digital Industrial Evolution Index, October 2017.

<sup>8</sup> 2018 KPMG CEO Outlook

40% 

of utilities surveyed said system security concerns were their largest barrier to digital transformation through the Industrial Internet of Things.<sup>7</sup>

Only 58% of P&U CEOs feel prepared to identify cyber threats, and

63% say they are confident they can contain the impact on their strategic operations.<sup>8</sup>



# IoT in action

IoT is the key to creating a truly smart power grid. The following examples illustrate how connected devices bring about big business benefits across the sector when risk is properly managed.

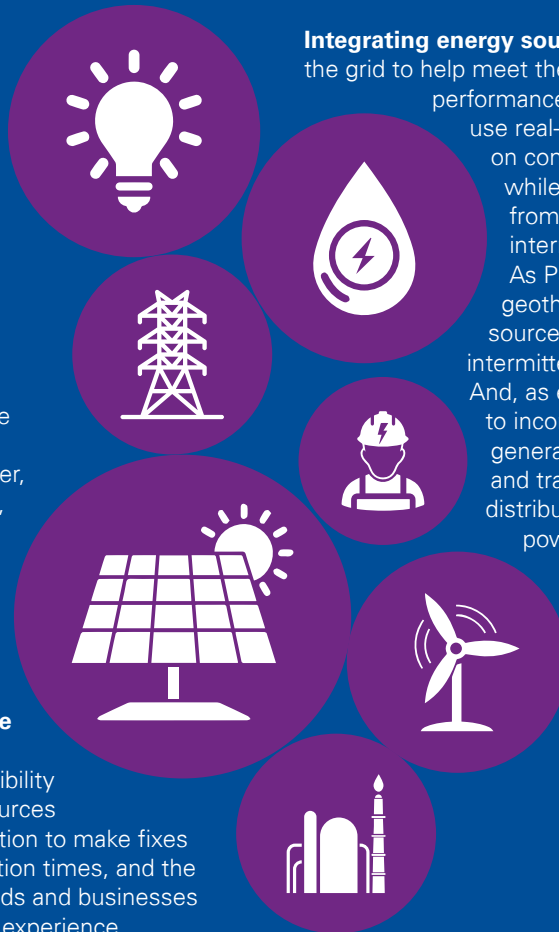
**Supporting energy distribution efficiency.** Utilities typically must invest in network capacity in order to accommodate peak loads, despite knowing that the network will operate well below capacity most of the time. Indeed, the net system load profile for one utility's electricity consumption indicates that its network operates at loads of 60 percent or less than peak approximately two-thirds of the time. Now IoT solutions enable distribution flexibility around both peak and nonpeak demands. This not only helps companies meet goals around cost of operations, but it allows them to remotely monitor and manage the physical impact of demand fluctuations on the hard assets. Energy providers also can implement demand response agility by leveraging sensor technology and data to engage customers in shifting their energy usage.

**Managing network integrity.** Sensors can improve risk management by gathering the real-time data necessary to evaluate asset health and security, both physical and cyber. For example, an IoT-based monitoring and predictive analysis platform may significantly reduce the likelihood of a major failure in a key network asset, such as a zone transformer, helping a utility avoid significant financial, safety, and reputational consequences. IoT-generated data also provides earlier insights into operations, allowing companies to take faster action to prevent and control incidents.

**Boosting productivity and safety in the field.** IoT is helping employees do more, better, by increasing an organization's visibility into network operations to dispatch resources more quickly with more granular information to make fixes and updates. The resulting faster restoration times, and the ability to reduce the number of households and businesses disrupted, vastly improves the customer experience. IoT-gathered data also can be used to optimize the workforce by shifting some maintenance activities away from a cyclical model to a predictive maintenance approach. Meanwhile, IoT sensors incorporated into hats, boots, gloves, and other wearables, in addition to sensors on vehicles and at work sites, collect and monitor data important for protecting the health of employees.

**Driving new business and customer loyalty.** The data collected by P&U companies is extremely valuable for formulating new and improving the delivery of customer services when managed securely and in accordance with privacy laws. Tailored, data-informed energy offerings allow providers to deepen their customer relationships, potentially improving retention and generating additional revenue streams. Moreover, certain data has its own value to potential buyers outside the traditional P&U customer base, such as environmental measurements from across a geographically dispersed network of IoT sensors.

**Integrating energy sources.** Utilities can use sensors along the grid to help meet the challenges of intermittency and drive performance across the entire fleet. Providers can use real-time data to prioritize assets based on conditions and determine true capacity, while analyzing historical data gathered from the IoT network to help anticipate intermittency and adjust capacity accordingly. As P&U companies look to add solar, wind, geothermal, and other renewable energy sources, IoT sensors can help manage natural intermittency and battery technology limitations. And, as energy production further decentralizes to incorporate more customer-owned renewable generation, IoT also will help P&U control and track the ebb and flow of production and distribution between home or business and the power plant.

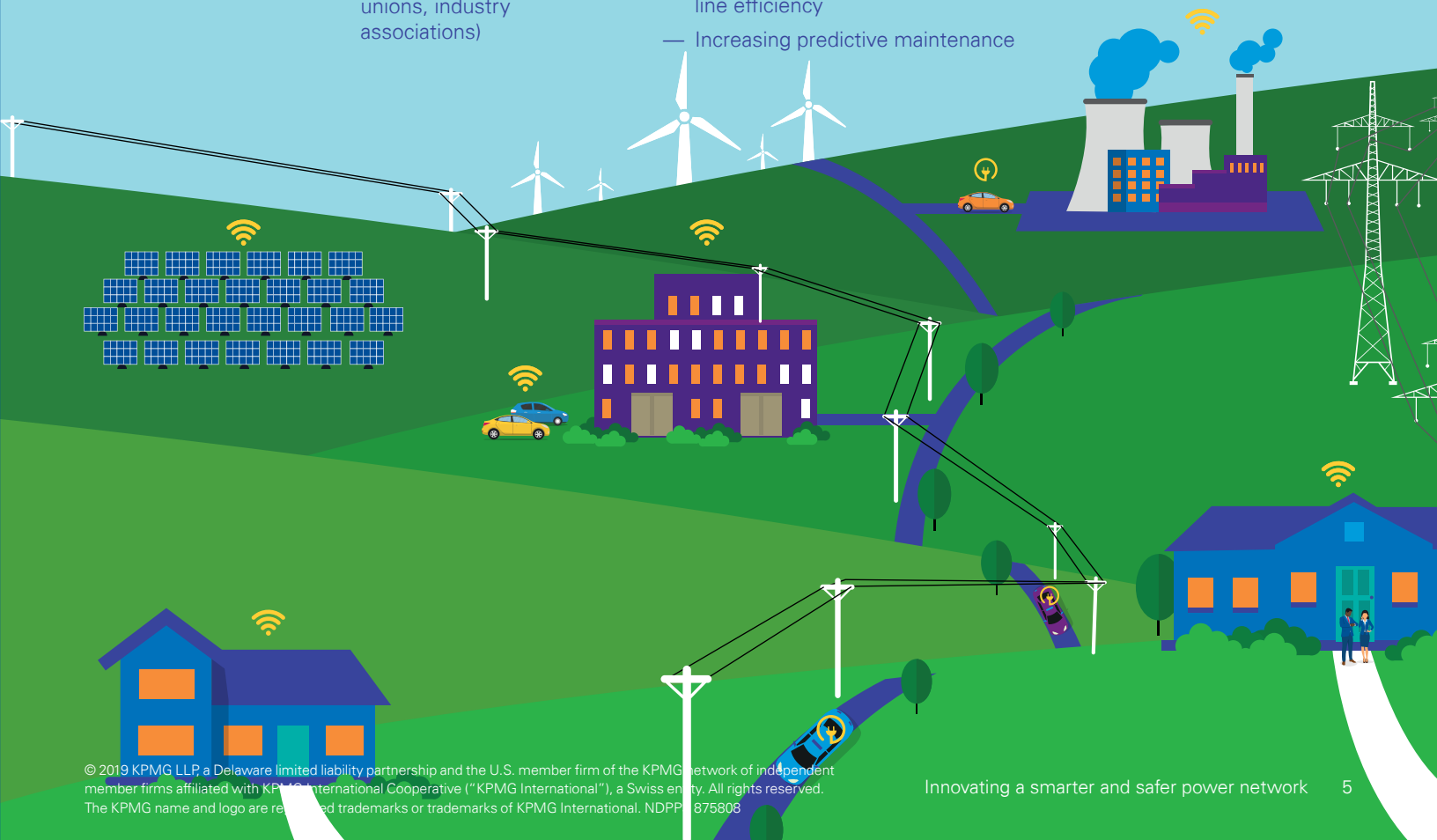


As power and utility companies explore the benefits of introducing IoT-driven advances across their operations, more are incorporating risk management as part of the process—rather than simply an afterthought. Ultimately, the industry seeks to add innovation and address risk *simultaneously*.



# Complex and conflicted

Stakeholder	Example	Business focus	Risk focus
<b>Creators</b> who design and manufacture IoT products	<ul style="list-style-type: none"> <li>Connected product and platform manufacturers (smart sensors, gauges and meters, analytics platforms, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>Enabling product and platform functionality</li> <li>Collecting and analyzing data</li> <li>Increasing product and platform adoption</li> </ul>	<ul style="list-style-type: none"> <li>Improving user experience</li> <li>Enabling availability and connectivity</li> <li>Enabling data integrity, security, and privacy</li> </ul>
<b>Enablers</b> who support IoT technology functionality	<ul style="list-style-type: none"> <li>Software developers</li> <li>Network and connectivity hardware manufacturers</li> <li>Cloud-hosting providers</li> </ul>	<ul style="list-style-type: none"> <li>Delivering platform interoperability</li> <li>Enabling availability and connectivity</li> <li>Expanding feature set and functionality</li> <li>Maintaining cost margins</li> <li>Optimizing IoT performance</li> </ul>	<ul style="list-style-type: none"> <li>Enabling availability and connectivity</li> <li>Enabling hardware and software reliability</li> <li>Compliance with corporate, federal, or industry requirements</li> </ul>
<b>Consumers</b> , the end users of IoT products	<ul style="list-style-type: none"> <li>P&amp;U companies (producers, distributors, cooperatives, retailers, and trade counterparties)</li> <li>Third-party companies (regulators, maintenance and equipment suppliers, unions, industry associations)</li> </ul>	<ul style="list-style-type: none"> <li>Increase operational efficiency</li> <li>Improve data, analytics, and insights</li> <li>Improve user experience</li> <li>Improving safety and compliance</li> <li>Manage plant, generation, and line efficiency</li> <li>Increasing predictive maintenance</li> </ul>	<ul style="list-style-type: none"> <li>Enabling return on investment</li> <li>Enabling product reliability and interoperability</li> <li>Enabling data integrity, security, and privacy</li> </ul>



# How KPMG helps govern power & utility IoT risk

So how can power and utility companies use IoT solutions in a responsible manner, tapping into anticipated current and future opportunities? A robust, agile, and responsive IoT governance function is absolutely essential.

An IoT governance function is typically led by representatives from technology, both operations and corporate, structured in a way that works best for each company, asset team, or line of business. The function standardizes the initial development, ongoing operation, and tuning of connected solutions, and it establishes guardrails to mitigate risk along the way, applying lessons learned to scale deployment across the organization.

Most power and utility companies have a wide variety of connected solutions already in place and recognize the need for governance, but they may not have formalized or effective integrated governance practices working in concert with other technology programs and activities.

**KPMG's Emerging Technology Risk and Cyber practices** are made up of highly experienced industry, technology, and risk management specialists. By bringing the latest knowledge and skills to the challenge of IoT risk management, we help P&U companies establish successful IoT governance functions that:

- **Are strategic**, with a core focus on aligning IoT investments with the needs of the business
- **Empower collaboration** between stakeholders
- **Drive consistency** through process standardization
- **Provide guidance** through leading practice sharing
- **Mitigate risk** through controls, metrics, and monitoring
- **Accelerate innovation and change** through timely and risk-informed decision making.

Our flexible, scalable and customizable approach governs risks across the strategy, delivery, and operations of an IoT program, helping power and utility companies and the wider ecosystem innovate and operate reliable and secure IoT solutions.



## Enabling the power and utilities industry through risk-informed digital solutions

IoT solutions help P&U companies manage risk, improve operations, and protect employees, customers, and communities. As an integrated digital solution, IoT along with automation, artificial intelligence, unmanned drones and vehicles, large-scale data science platforms, and other innovations provide the potential for significant business improvement—and are potential sources of significant risk.

P&U companies operating in the new age need relevant risk management programs to help ensure innovation progress is not hindered by threats and mistakes. KPMG can help.

**Digital-oriented strategies:** We help develop integrated digital strategies to drive operations improvement for generators, transmission and distribution entities, and retail and service companies as they tackle reliability challenges, manage regulatory change, and meet cost objectives.

**Performance-oriented outcomes:** We work with utilities to establish and enable performance management programs that leverage IoT to monitor and improve asset availability, diagnose equipment, plan and execute maintenance, and reduce unplanned downtime.

**Risk-informed solutions:** We assist P&U companies as they digitally enable processes to better manage the risks associated with technology, operations, and value across the enterprise. Further, we help utilities develop strategies to reduce risk from cyber attack on key assets and equipment, industrial control systems, and network infrastructure.



# Contact us

## **Joshua Galvan**

### **Principal**

#### **Emerging Technology Risk**

**T:** 713-319-2082

**E:** jgalvan@kpmg.com

## **Michael Krajecki**

### **Director**

#### **Emerging Technology Risk**

**T:** 312-665-2919

**E:** mkrajecki@kpmg.com

## **The KPMG Global Energy Institute (GEI)**

Launched in 2007, the KPMG GEI is a worldwide knowledge-sharing forum on current and emerging industry issues. This vehicle for accessing thought leadership, events, webcasts, and surveys about key industry topics and trends provides a way for you to share your perspectives on the challenges and opportunities facing the energy industry. For information about becoming a member of the GEI, please visit our [website](#).

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

## **[kpmg.com/socialmedia](https://kpmg.com/socialmedia)**



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 875808