Deloitte.

5x5 series: Insights and actions

Advanced metering infrastructure (AMI): Embedding edge intelligence in smart meters

Edge intelligence devices are grid sensors that provide unprecedented insight and control through edge computing capabilities. They allow a greater ability to sample, process, store, and deliver data to the desired places in real time, benefiting both the utility and its customers. These capabilities have come together through the advancement of technologies enabled by a network of smart devices at the edge (meters with much greater computing power), advanced cybersecurity, and artificial intelligence/machine learning (AI/ML) technologies. The platform can make it easier for utilities to turn data into insights that help better serve the customers while improving operational and financial performance. The outcomes include improved situational awareness, careful analysis, and advanced event detection. Delivering information effectively could improve grid efficiency, reliability, and safety, transform customer service, and decrease operational costs. Insight, innovation, enablement, and trust will be the pillars for utilities to achieve in navigating the new business models.

***5** insights you should know*		***5** actions to take now*
Next-generation smart meters are Internet-of-Things (IoT) grid-sensing electric meters that support edge computing. They provide unprecedented insight and control through waveform data technology and offer edge computing capabilities to sample, process, store, and deliver data in real time.	1	**Monitoring and incident response:** Establish broad monitoring capabilities to detect anomalies or suspicious activity and develop effective incident response plans to promptly contain and mitigate security incidents.
A pillar to an AMI solution requires an **Edge Intelligence platform**. The evolution of the meter from a single-focus device to a device with an embedded operating system has created a robust endpoint enabling the meter to—perform analysis at the edge, make decisions to drive a positive outcome, and function as a real-time network monitoring and control device.	2	**Security by design:** AMI devices should be designed to be foundationally secure, with an end-to-end architecture. This provides security at many stages of product creation and deployment.
Adversaries continue to change their approach: AMI systems are vulnerable to cyber-attacks that can lead to theft of data and power, localized and widespread denial of power, and disruption of the grid. Cybersecurity threats to AMI systems include confidentiality, integrity, availability, and accountability of communication systems.	3	**Adapt existing cybersecurity programs:** Put in place organizational change management, governance, cyber goals and outcomes, strategy, architecture, innovation, and training programs for transformation and advanced detection of unknown threats.
Increasing threat complexity and frequency: Humans need to catch up with increasingly complex and frequent cyber threats. Organizations' security teams do not have full visibility of the ever-expanding threat landscape with relevant context and external data sources.	4	**Use AI/ML:** Artificial intelligence can be leveraged to defeat malware, protect assets, drive behavior analytics, improve cyber resiliency, increase cyber operations maturity, and develop a broad, collaborative, and scalable detection and response. Future attacks can also be predicted and prevented by learning and adapting from internal and external intelligence.
A smart grid microprocessor embedded in ubiquitous utility assets (the smart meter) enables wider adoption and commercialization of technology and redefines the role of edge computing. Using powerful microprocessors in meters creates the capability for high-frequency sampling and additional processing power to run local/edge analytics.	5	**Compute segmentation:** The Edge intelligence platform is based on the Linux operating system, containerized and separate from the core processor. Separation of metrology from the edge intelligence platform helps meter functions remain uninterrupted during various software routines.

Want to see this live? Visit us at the Cyber IoT Studio or The Smart Factory at Wichita State University!

Connect with us:

Wendy Frank
Principal | Cyber IOT Practice Leader
Deloitte & Touche LLP
wfrank@deloitte.com

Dave Nowak
Principal | Cyber IOT Practice Leader
Deloitte & Touche LLP
danowak@deloitte.com

Bakhshi Malhotra
Senior Manager | Cyber IOT Practice
Deloitte & Touche LLP
bmalhotra@deloitte.com

Anne Robbins
Senior Manager | Cyber IoT
Deloitte & Touche LLP
anrobbins@deloitte.com

Ted Justice
Specialist Master | Cyber IOT Practice
Deloitte & Touche LLP
tejustice@deloitte.com