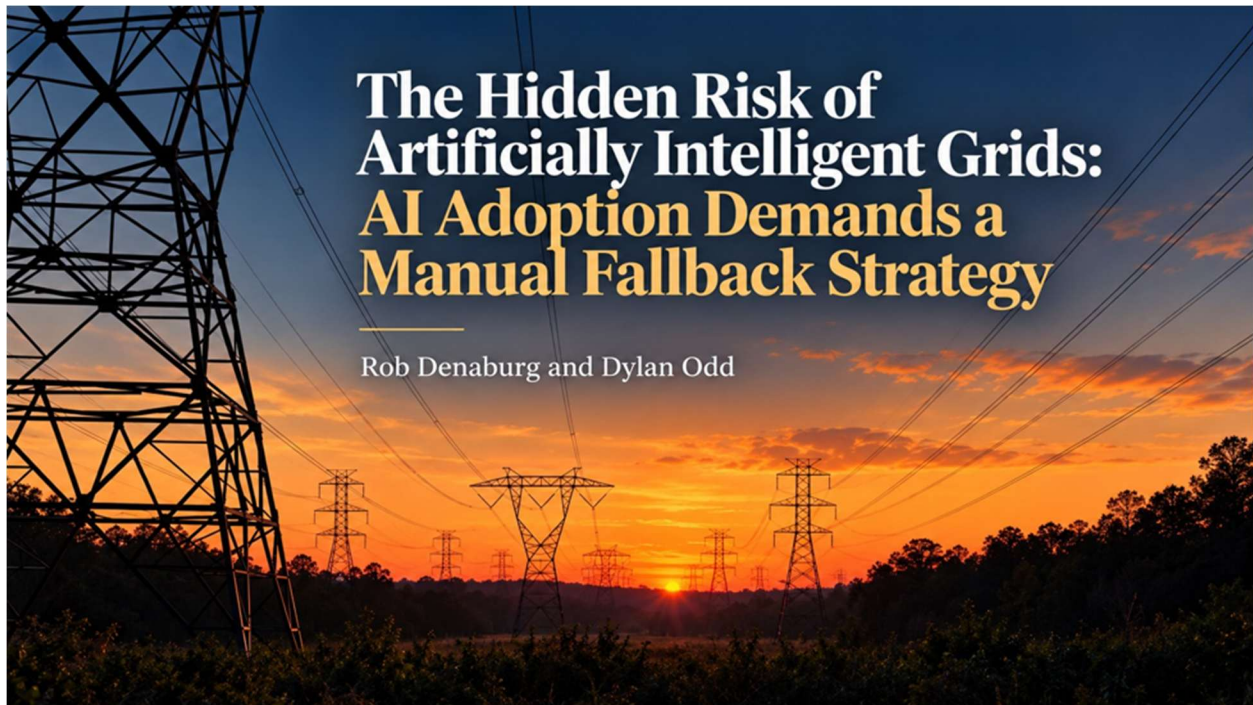




October 2026 | Rob Denaburg and Dylan Odd

As AI adoption increases the electricity sector's reliance on automation, grid operators must deliberately preserve the skills and expertise necessary to reliably maintain operations if AI systems are unavailable or cannot be trusted.

Artificial intelligence is already reshaping how utilities manage the grid and its supporting infrastructure.[1] The efficiency gains are real; so too are the pressures driving adoption. As rising electricity demand, integration of renewables, aging infrastructure, and transmission bottlenecks necessitate an evolution of electric systems, grid operators have no choice but to get “smarter” about how they manage power flows.

Increased integration of artificial intelligence for grid operations is one path to getting “smarter,” but it also poses emerging risks. One potential risk is the longstanding human-factors problem associated with increasing automation - in this case, operational dependency on AI.

Put simply: how can utilities ensure they will be prepared to manage their systems if the AI they rely on becomes unavailable?

While this is an important consideration for the electricity sector, it has implications for society more broadly. Given the electric grid's central role in supporting other critical infrastructure systems, power outages also create significant interdependency risk. A major disruption to electricity can cascade across sectors and interrupt the lifeline services Canadians rely on for public health and safety, economic activity, and national security.



AI and the Electric Grid

The modern electric grid is considered the most complex machine humanity has ever built and operated continuously.[2] At any given moment, generation (supply) and consumption (demand) must be balanced across thousands of nodes in real time, to fractions of a Hz in frequency. Even small imbalances propagate instantly and can cascade into widespread failures if not properly managed.

While the electric industry has successfully managed this complexity for decades, the challenges associated with grid transformation will make it increasingly difficult for human operators using existing technology to maintain effective decision-making at scale.[3] Compounding this problem, growing demand for electricity and the roadblocks associated with adding capacity to the grid will create strong incentives to squeeze more capacity and performance out of the grid they already operate while waiting for new generation and transmission to come online.

AI is, in theory, ideally suited for managing this system and the electric sector is in the early stages of a significant adoption curve. Roughly three-quarters of energy companies worldwide are already implementing or exploring AI solutions. They are driven by the genuine complexity of operating a grid that must now integrate distributed renewables, respond to more extreme weather, and manage surging load. All this in the shadow of growing demand from the buildout of hyperscale data centres.[4]

Utilities tend to frame AI as augmenting their workers rather than replacing them, and in the early stages of adoption, this has proven true. But the economics of AI investment tell a different story over time. Tristan Harris, tech ethicist and co-founder of the Center for Humane Technology, has explicitly warned that hyperscalers view replacing human labor as a core financial objective for their increasingly sophisticated AI models.[5]

This concern is reflected in broader workforce planning. The World Economic Forum's Future of Jobs Report 2025 found that 41% of employers surveyed planned to reduce their workforce where AI could replicate human work.[6]

Anticipated productivity gains weaken the business case for large, distributed operating teams. Lean staffing, centralized operations, and greater integration of AI systems are the logical destination of efficiency-driven investment and growth.[3][7]

Implications for in Grid Systems

Among the concerns about the increase in society's reliance on AI and susceptibility to its malicious applications, overreliance on AI is generally underdiscussed. However, it is incumbent on energy providers and other critical infrastructure owners and operators to explore the unintended consequences of reliance - and potential overreliance - on AI.

This shift is already underway in Canada's electricity sector. Electricity Human Resources Canada (EHRC) reports that tasks including pattern recognition, fault detection and scheduling are moving from manual processes to intelligent systems.[7]



That reliance can become a problem in several ways. Sometimes the technology supporting this automation may simply become unavailable, whether because of a software defect, hardware failure, communications outage, cyber incident, disruption to the vendor's functions, a vendor suddenly going out of business and taking their service with them, or a foreign government preventing access to the model in Canada.[8] In other cases, the system may continue to operate while no longer being trustworthy, as corrupted data, model errors, unfamiliar operating conditions, or manipulated inputs call its outputs into question. A more foundational risk is the possibility that, over time, utilities lose some of the human expertise, staffing, and procedures required to operate effectively without it.

It is this last possibility that makes overreliance particularly difficult to remedy. A failed component can be replaced, but human expertise is not recovered so easily. If that capability is allowed to erode, it cannot simply be switched back on when it is needed - and it is precisely during rare, high-consequence events where manual operation would be most critical and its absence most catastrophic. You cannot spin up a generation of experienced operators on short notice.

Digital Analog: Ukraine 2015

On December 23, 2015, Russian-affiliated hackers remotely opened breakers at over 50 electrical substations across western Ukraine, cutting power to roughly 225,000 customers. The attack was sophisticated, but what saved Ukraine from even more widespread or longer lasting outages was that the operators still knew how to run the grid by hand.[9][10]

Crews physically travelled to substations to manually open and close breakers. The affected utilities were still operating breakers manually over two months after the attack. It was slow, exhausting, and imperfect, but it worked because the knowledge existed in people, not only in technology.

That capacity to manually sustain operations is not guaranteed to exist in the future. Even prior to AI adoption, automation has dulled grid operators' ability to run the grid manually if digital systems go offline. In the wake of the 2015 attack in Ukraine, U.S. officials raised concerns that many utilities - especially the most well-resourced ones with the largest customer base - would not have been able to revert to manual operations in a similar emergency due to a growing dependence on the automation already in place at that time.[10] AI will significantly amplify this challenge.[14]

The Ironies of Automation

There is a longstanding paradox here that predates ChatGPT and the ubiquity of large language models by several decades. In 1983, psychologist Lisanne Bainbridge described what she called the "ironies of automation." She argued that automation uses machines to increase reliability and efficiency, while transforming the human operator's role into one of oversight - ready to step in when the system stumbles or falls. The paradox, as Bainbridge recognized, is that the more advanced the control system becomes, the more crucial the contribution of the remaining human operators may be.[11]



The second, more insidious irony is that automation undermines the capabilities of the humans in the loop over time. Bainbridge observed that physical skills deteriorate when they are not used, just as operational knowledge is strengthened through use and feedback: “[b]y taking away the easy parts of his task, automation can make the difficult parts of the human operator's task more difficult.”[11]

In 1995, Mica Endsley and Esin Kiris examined this theory further, focusing on what they called the “out-of-the-loop performance problem.” In an experimental task using an expert system, they confirmed that automation reduced operators’ situational awareness and that operators were less effective at resuming control when the automated system failed.[12] Their results suggested that the shift from active involvement to passive monitoring was an important contributor to this decline.

Aviation provides a useful real-world analogue. As cockpit automation became increasingly capable, dependence on automated flight systems undermined pilots’ ability to respond when those systems failed. For example, the United Kingdom Civil Aviation Authority identified automation dependency and the erosion of manual flying skills through reduced practice as operational safety concerns.[13]

Artificial intelligence promises to extend automation into a narrower band of cognitive, human work: judgment calls operators make when conditions fall outside normal, automated parameters. As AI takes on more of that judgment, operators are likely to spend less time exercising the skills built from making those calls themselves, eroding the intuition that currently lets them safely intervene when conditions deviate from what existing automated systems are designed to handle.

Responsibility Without Capability

Beyond the erosion of operator skills, AI introduces another concern: growing dependence on external providers for critical operational functions. As utilities integrate AI into grid operations, they may find that some of the functions they once performed themselves, and the expertise required to perform them, increasingly reside with outside vendors. Yet responsibility for operating the grid remains with the utility. This creates a potentially serious vulnerability. If a vendor, supporting service, or even undergirding AI model becomes unavailable, the utility may find itself responsible for functions it no longer has the capacity to perform independently.

Earlier automation moved the operator away from direct control of the physical system and into supervision of the machines that controlled it. AI has the potential to move the operator another step back by taking on parts of that supervisory function itself. The operator may increasingly oversee an AI system that observes conditions, interprets information, and helps determine how the automated systems operating the grid should respond.[14][15]

The adoption of more complex AI tools are likely to deepen dependency on external vendors because of the cognitive and supervisory functions they are likely to play; functions that have traditionally remained within the utility.



The North American Electric Reliability Corporation has already identified vendor transparency around the assumptions, limitations, and capabilities of AI systems as important to their use in real-time grid operations, while Canadian critical infrastructure guidance specifically identifies cloud-hosted vendor services within the operational control loop as a dependency that operators must be prepared to function without.[15][16]

Where these systems are developed or maintained by outside vendors, utilities may also become dependent on those providers for the expertise necessary to understand, maintain and troubleshoot them. The resulting risks are not only hypothetical. EHRC found that 63% of organizations responding to its 2025 survey planned to use a combination of internal and external expertise to integrate AI into their operations.[7]

As a result, some of the knowledge necessary to understand how operational decisions are being produced may ultimately sit outside the organization, or even outside the country.[8][15][17]

Intentional Resilience in AI Adoption

None of this is an argument against adopting AI. It has already proven to be an effective tool, with the potential to deliver significant productivity benefits as grid complexity increases. But the reasonable push toward rapid adoption must be balanced by careful consideration of the new dependencies and risks it may create.

A basic principle in systems engineering is that resilience is easier and cheaper to build in from the start than to add later.[18] That should apply to the human side of grid operations as much as it does to cyber or physical security, and the long lifespan of electrical infrastructure makes this even more consequential. If grid operators overvalue efficiency, they risk creating systems that work very well under normal conditions but are poorly prepared for abnormal ones.

Utilities cannot treat operational AI systems as just another technology add-on.

Instead, they should decide in advance how AI and human operators will work together during normal operations, how humans can take over when AI systems are degraded or unavailable, what knowledge operators need to preserve, and what level of manual operating capability they must retain.

Utilities must also ensure that contracts with AI providers include explicit continuity of operations provisions (e.g., data portability, fallback access, and transition support) that can minimize disruptions if service is interrupted or the vendor relationship ends.

Those choices can become difficult to reverse. Grid operators should build decisions about how much authority is given to AI, what fallback capacity is kept, how knowledge is documented, and how staffing and procurement are structured into operating procedures, contracts, and workforce plans.

Much of the knowledge necessary to operate Canada's electricity grid still resides with experienced operators. However, an aging workforce compounds future risk. According to Employment and Social Development Canada, 32% of power engineers and power systems operators were aged 50 or older in 2023.[19] Yet a 2023 survey by EHRC found that only 58% of electricity-sector employers had succession policies, almost exclusively focused on management positions.[20] EHRC has



since warned that the retirement of experienced workers without deliberate documentation, mentorship and knowledge transfer threatens institutional knowledge.[7]

To prevent AI adoption from eroding the human capability necessary when those systems fail, utilities need to identify which operational functions require a human fallback and deliberately preserve the knowledge required to perform them. That means more than redundant technology. Operators need opportunities to maintain those skills through exercises, simulations, and hands-on operation.

Regulators can play a role in ensuring this happens. Risk management frameworks should treat human operating capability as part of grid resilience, alongside cybersecurity, redundancy, and business continuity. As utilities become more dependent on AI, they should be required to demonstrate that critical operations can continue when those systems are unavailable or cannot be trusted. These requirements can be incorporated into existing reliability, emergency preparedness, and operator training frameworks rather than treated as a separate problem of AI governance.

The grid is getting smarter. To ensure that it remains resilient, the grid also needs to remain operable when that intelligence is unavailable.

Bibliography

[1] IBM Institute for Business Value, Utilities in the AI Era: Powering Ahead to a Smarter Future (IBM, 2025).

[2] Darren Orf, “The Power Grid Is the Largest Machine in the World, and Our Nation’s Greatest Engineering Achievement,” *Popular Mechanics*, June 8, 2023.

[3] International Energy Agency, *Electricity 2025* (Paris: IEA, 2025); International Energy Agency, *Energy and AI* (Paris: IEA, 2025).

[4] IBM, “New IBM Study Data Reveals 74% of Energy & Utility Companies Surveyed Embracing AI,” February 26, 2024.

[5] Fast Company, “Stop AI Doomscrolling and Start Organizing,” *Adventures in AI*, video podcast featuring Daniel Kwan and Tristan Harris, June 15, 2026.

[6] World Economic Forum, *Future of Jobs Report 2025* (Geneva: World Economic Forum, 2025).

[7] Electricity Human Resources Canada, *Powering Intelligence: AI-Driven Change in Canada’s Electricity Workforce* (Ottawa: Electricity Human Resources Canada, November 2025).

[8] Joe Castaldo, “Lost Access to Anthropic’s AI Models Highlights Risk of Relying on U.S. Tech, Canadian Experts Say,” *The Globe and Mail*, June 13, 2026.



- [9] SANS Institute, “Confirmation of a Coordinated Attack on the Ukrainian Power Grid,” SANS Blog, January 6, 2016.
- [10] Holly Williams, “Russian Hacks into Ukraine Power Grids a Sign of Things to Come for U.S.?” CBS News, December 21, 2016.
- [11] Lisanne Bainbridge, “Ironies of Automation,” *Automatica* 19, no. 6 (1983).
- [12] Mica R. Endsley and Esin O. Kiris, “The Out-of-the-Loop Performance Problem and Level of Control in Automation,” *Human Factors* 37, no. 2 (1995).
- [13] United Kingdom Civil Aviation Authority, *Flight Crew Human Factors Handbook, CAP 737, Chapter 13, “Automation and Manual Flying”* (2023).
- [14] Mica R. Endsley, “Ironies of Artificial Intelligence,” *Ergonomics* 66, no. 11 (2023).
- [15] North American Electric Reliability Corporation, *Artificial Intelligence and Machine Learning in Real-Time System Operations: White Paper – Revision 1* (Atlanta: NERC, 2024).
- [16] Canadian Centre for Cyber Security, *Critical Infrastructure Resilience and Escalated Threat Navigation Initiative* (Ottawa: Communications Security Establishment Canada, 2026).
- [17] Canadian Centre for Cyber Security, *Security and Privacy Controls and Assurance Activities Catalogue, ITSP.10.033* (Ottawa: Communications Security Establishment Canada, 2026).
- [18] Christoph Kern, with Brian Gustafson, Paul Blankinship, and Felix Gröbert, “Design Tradeoffs,” in *Building Secure and Reliable Systems*, ed. Heather Adkins et al. (Sebastopol, CA: O’Reilly Media, 2020).
- [19] Employment and Social Development Canada, *Canadian Occupational Projection System, occupational profile for Power Engineers and Power Systems Operators, 2023 workforce data*.
- [20] Electricity Human Resources Canada, *Electricity in Demand: Labour Market Insights 2023–2028* (Ottawa: Electricity Human Resources Canada, 2023).