The Lighthouse

Public

By Lew Folkerth, Principal Reliability Consultant, External Affairs

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your entity. It may also help you and your entity as you strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resilience and sustainability of your CIP compliance programs. There are times that I also may discuss areas of the Standards that other entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes-stormy waters of CIP compliance.

Artificial Intelligence and CIP

Tipping point

On March 14, 2023, the OpenAI companies released ChatGPT version 4. ChatGPT 4 appears to have been a tipping point in the capability and use of Artificial Intelligence (AI) for consumer applications. This has generated massive public and media attention and has raised concerns about the use of AI in operational technology (OT) systems, such as the systems we use to operate the electric grid.

What is AI?

AI is a knowledge domain of computer science that has many sub-domains, such as:

- Natural language processing (NLP) processes and generates language that humans can use to communicate with computers. If you use personal voice assistants such as Siri or Alexa, you’re already using a form of NLP.

Saugatuck, Michigan – Photo: Lew Folkerth

- Machine learning (ML) takes information and "trains" a computer to perform certain tasks. The facial recognition in your smartphone is one example of how ML is changing the way we live. Self-driving cars show how far ML can be taken today.

- Generative AI extends the functions of NLP and ML to simulate the generation of knowledge.

ChatGPT, Google Bard are examples of text-based generative AI. See the sidebar on the next page for Google Bard’s description of generative AI.

Other types of AI can be used to generate images from a text prompt, such as the image of a lighthouse weathering a storm by DALL-E, on the next page.

How might AI benefit reliability, resilience, or security?

There are many areas where appropriate use of AI could benefit electric operations. Here are a few examples:

- ML might be used to improve dynamic response to rapidly changing generator outputs such as solar farms on a party cloudy day.

- Generating valid alerts from massive amounts of data from devices such as such as synchrophasors or dynamic line sensors could be facilitated by using ML.

Continued on page 8

Continued from page 7

- Internal Network Security Monitoring could use ML and NLP techniques to improve the accuracy of alerts and reduce false positives.

What will be needed for AI use in OT?

A key issue in using any third-party software for OT purposes is confidentiality. The most reliable way to achieve this is to keep all processing and information on locally controlled systems. Software, both free and commercial is available and public versions of some training models might be available for private use.

Any use of AI for OT should be on a computer that is trusted and secured. As a good practice, any AI should be able to show how its output is derived from its input, so that you can see and document how answers are generated. Any BES Cyber System Information (BCSI) used as input to the AI processes must be identified to ensure that confidentiality is not compromised.

Precautions for today

While efforts are under way to enable use of third-party services (e.g., cloud services) within the CIP Standards, those changes are not ready yet. For now, you must keep tight control of all BCSI.

To ensure this continued control, look at modifying your cybersecurity policies and your information protection plan to address the use of AI.

External AI services should not be accessible from control networks. This should already be the case for CIP-005 compliance. I also recommend that access to external AI systems be blocked for business systems within a control environment such as a generating plant or Control Center. This may help prevent data leakage through inadvertent use of AI systems by operating personnel.

You should keep abreast of developments in this area. The use of AI has the potential to transform every area of human endeavor but must be used with extra caution in any area where safety, reliability, resilience or security is an issue.

Requests for assistance

If you are an entity registered within the RF Region and believe you need assistance in sorting your way through this or any compliance-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the RF website here.

Back issues of The Lighthouse, expanded articles and supporting documents are available in the RF CIP Knowledge Center.

Lew to Bard: Describe generative AI

Bard Response [edited for brevity]: Generative AI is a type of artificial intelligence (AI) that can create new content, such as text, images, or music. It is powered by machine learning algorithms that are trained on large data sets of existing content.

The algorithms learn to identify patterns in the data and then use those patterns to generate new content that is similar to the original data.

Generative AI is a powerful tool that has the potential to revolutionize many industries. However, it is important to be aware of the potential risks of using generative AI, such as the creation of fake news and deepfakes.

It is also important to use generative AI in a responsible way that respects the privacy and safety of others.

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

Lew Folkerth, Principal Reliability Consultant, can be reached here.