The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

Using Advanced IT Technologies in an OT Environment Part 1 - Principles

The Difference between Information Technology (IT) and Operational Technology (OT)

For the purposes of this discussion, I'll say that IT is the set of computing resources that deals with information, finances, inventory management, human resources, business processes – almost anything to do with a business and how it is managed falls into this category. One of the main concerns within an IT environment is cost of ownership, which drives return on investment.

In contrast, OT is the set of computing resources and devices that monitor and control equipment. Sensors might monitor temperature, voltage, current, pressure, fluid levels or other parameters. Actuators can be used to control equipment from afar, without human presence. In the area of the NERC Reliability Standards, OT encompasses all Cyber Assets subject to the CIP Standards. The primary concerns of OT are reliability, resilience and security.

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.

Lew's Principles for Adopting IT Technologies in an OT Environment

This is the first in a series of articles where I will discuss adopting technologies developed for IT environments into your OT environment.

I'll start by suggesting some core principles to apply to the analysis of IT technologies that are new to an OT environment.

1. Clearly identify the IT technology to be implemented

In order to effectively assess a technology for implementation in an OT environment, you must clearly understand the technology you will be implementing. Each technology has its own vocabulary, core concepts and principles. You need to review vendor claims and determine the parts of the technology that will be useful. Your entity must have a subject matter expert (SME) who understands the technology and can apply that knowledge to your environment.

Cooper Harbor, MI – Photo: L Folkerth

As an example, let's say you plan to implement cloud computing in your Control Center. Rather than making such a broad statement, it might be better to say that you will implement a private cloud infrastructure to be contained wholly within the Electronic Security Perimeter. A private cloud is a type of cloud computing that does not carry all of the risks of a public cloud implementation. By using the more specific language, you have better defined the expectations of management and compliance staff.

2. Objectively assess the benefits

Any new IT technology will have obvious benefits in the IT environment, or you wouldn't be considering it for the OT environment. But take a close look at the technology from an OT perspective. Will the new technology improve reliability? Resilience? Security? If so, try to quantify your expectations. If not, why are you adding complexity for no operational benefit?

Continued on page 11

Continued from page 10

Be careful of vendor claims of benefits and performance. Remember that these vendors are generally selling into the IT market where reliability concerns are not as important. A 30-minute server outage in the IT environment is not usually a major concern, but a 30-minute SCADA outage is a reportable event. Once you've identified and quantified the potential benefits, make sure those benefits can be realistically achieved.

You might identify cost savings and reliability improvements from a private cloud implementation, for instance. Your staff will need full training on this technology prior to implementation. Also, don't neglect the ongoing skills maintenance needed to keep your staff fully effective in maintaining the new technology. Be sure to consider any actions needed to retain your now more-qualified staff. Factor these and other costs into the cost/benefit analysis. Providing the necessary training may erode the cost benefits, but if you don't train your staff, you will forfeit reliability benefits.

3. Objectively assess the risks

Any new technology will likely present new or heightened risks to your OT operations. You will need to identify and assess those risks and determine how to address them. Be sure you're assessing risks in the OT context – reliability, resilience and security. You should also include compliance risk in terms of the enforceable language of the NERC Reliability Standards and any other applicable standards. If the technology could increase the likelihood of a compliance violation, that should be factored into the decision. Also include in your assessment any side effects of implementing the technology, such as generating unit downtime.

In our private cloud example, be sure to contain the private cloud within an Electronic Security Perimeter if the cloud will be hosting high or medium impact BES Cyber Systems. If you are using or considering advanced technologies, such as a private cloud, you should be actively involved with the development efforts for the CIP Standards. See the NERC Reliability Standards under Development webpage for more information.

4. Perform a risk/benefit analysis in addition to a cost/benefit analysis

Most businesses require a cost/benefit analysis in order to make a procurement. In an OT environment you should also perform a risk/benefit analysis. In other words, do the benefits of the new technology justify the additional risk? Add the cost of mitigating the identified risks to the cost/benefit analysis. Make sure you include the cost of new and ongoing training and credential acquisition and maintenance for your staff. Factor retention of staff into both the risk/benefit and the cost/benefit analyses.

Review the risk/benefit analysis to ensure that the new technology improves the reliability, resilience and/or the security of the operation without impairing its compliance posture.

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.

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.