The Lighthouse

By Lew Folkerth, Principal Reliability Consultant

CIP in the Cloud

This article is based on a presentation I gave at the 2022 NAES NERC Conference and the September Technical Talk with RF. It included additional background information about cloud services that you can read by viewing the presentation here.

In contacts with some of RF's Registered Entities, I'm seeing a movement of some operational functions to cloud-based technologies. A prime example is workflow management, where the software providers are well along in a Software as a Service (SaaS) delivery model. Some of these providers use methods that do not fit well with even the latest CIP Standards. Note that I am not necessarily promoting the use of cloud systems in the Operational Technology (OT) space, but I believe some cloud adoption is inevitable and we should get ahead of the adoption curve.

Potential Cloud Drivers for OT

Why move OT systems to the cloud? Unlike the move of IT systems into the cloud, moving OT systems should not be about cost. The only good reason to move OT systems to a cloud environment will be to improve reliability, resilience or 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, resiliency 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.

Reliability consists of not letting problems happen. This is normally accomplished in OT systems by redundancy. Cloud environments can provide a large amount of redundancy, as this is their strength. Making use of a multi-cloud environment using more than one cloud service provider (CSP) in a failover situation may also help to achieve a highly reliable OT architecture.

Resilience means recovering swiftly and smoothly if problems do occur. Improved resilience might be achieved by leveraging some of the features of cloud computing such as geographic diversity. This can prevent a widespread event (hurricane, wildfire, flooding, etc.) from affecting all of your OT resources. Another cloud benefit is elasticity, where resources available to a service can dynamically expand when needed.

Grand Haven, MI – Photo: Lew Folkerth

Security includes assuring availability, integrity and confidentiality. Moving to a cloud environment can improve security in some areas, but can also pose challenges in other areas. The CSP provides security for the physical facilities, servers and networks. Depending on the service model (see background information referenced above), the CSP may also provide security for the operating system and the application software.

Elasticity is a property of cloud computing that permits dynamically expanding the resources available to a process or service. When computationally intense processes are used in real-time or near-real-time environments, these processes may be able to benefit from the effectively unlimited computational resources available in the cloud.

Operational Challenges for OT Cloud Services

In counterbalance to the benefits above, any move of OT services to cloud providers will present significant operational challenges. I've listed some of those challenges below.

Availability is a measure of the "uptime" of a system, usually measured as a percentage. Major CSPs quote various levels of availability depending on services, some levels as high as 99.99% (four nines, or 52 minutes of downtime per year) availability. However, SCADA systems target a higher availability, usually 99.999% (five nines, or five minutes of downtime per year). In addition to

Continued on page 9

Continued from page 8

system availability, network and storage availability will also be critical factors.

Latency is a measure of the delay from data generation to data consumption. Major CSPs use the public Internet for communications, so there is the possibility of delay and dropped communications between the data endpoints.

Mobile access is the ability to easily access cloud services from any device anywhere in the world. While this feature can be a huge benefit for IT systems, it can present serious problems for OT. We do not want anyone, anywhere, to be able to control the breakers in a substation or the feed pump in a steam generator.

Financial challenges include not just the cost of cloud services, but the type of money used. For some utilities, on-premises computer systems are capitalized and can be added to the utility's rate base. Cloud services will use operational dollars.

Cyber security tools and processes will be different in a cloud environment. Entities using cloud services for operational systems will need to train personnel and adapt processes and tools to the new environment.

Compliance Challenges for OT Cloud Services

The use of cloud services will not be possible under the present CIP Standards except in the most limited case, such as some forms of BES Cyber System Information (BCSI) in the cloud. New Reliability Standards will be required, and those Standards will need to be risk-based. There are too many variables in cloud environments to be able to write prescriptive Standards for these cases.

Compliance processes will need to be very mature and integrated with operational processes and procedures. Internal controls will become even more important.

Auditing processes will need to be adapted to cloud environments to determine the type, quality and quantity of evidence that will be needed to provide reasonable assurance of compliance.

Path Forward

To adequately prepare for the adoption of cloud services, I believe we need to develop use cases for this technology. We can then address the operational, security and compliance challenges for each use case. We should begin with known needs, such as cloud-based service providers (such as work management systems) that store BCSI in the cloud. After we take these initial steps, we can evaluate additional use cases.

We will need an environment in which we can test these concepts without incurring compliance risk to the Responsible Entities involved in this forward-looking work. There is precedent for this in the CIP version 5 Transition Advisory Group (v5TAG). The v5TAG provided a forum where transition from the version 3 CIP Standards to version 5 could be tested and modified as needed without incurring compliance risk. I suggest that a Cloud Technology Advisory Group (CTAG) be formed to experiment with and monitor the transition to cloud technologies.

If a CTAG is formed, it should be a partnership with ERO Enterprise staff and a small group of Responsible Entities that are interested in pioneering cloud technologies. Cloud services can be tested, and operational and security issues addressed. Potential revisions or additions to Reliability Standards can be outlined and compliance processes and evidence tested for effectiveness. In this way, cloud transitions can be performed in a small, controlled environment before right-sizing the use of cloud services.

Conclusions

I am not advocating the migration of OT systems and services to the cloud, but I believe some movement in this direction is inevitable.

Reduced cost, the primary driver of early cloud adoption, should not be a significant driver for real-time cloud migration. Rather, the leveraging of cloud technologies for improved reliability, resilience and security should be the drivers, but the associated risks must be effectively managed.

The CIP Standards will need to be modified or new Standards developed to address cloud risks. These Standards will need to be explicitly risk-based to effectively adapt to the wide range of cloud service provider options and features.

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.

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.