The Lighthouse

By: Lew Folkerth, Principal Reliability Consultant

Cybersecurity and CIP for Small Entities

In this recurring column, I explore various CIP issues. I share with you my views and opinions, which are not binding, but rather are intended to provoke discussion within your entity and to be helpful to you as you and your entity 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 may also 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.

Q I'm at a small company and I've been tasked with creating a cybersecurity and CIP compliance program. Where do I start?

A There are a number of resources available to help you on your way. Since you are a small entity, I will assume for this article that you are in the CIP program at the low impact level, although most of my suggestions will be applicable to the high and medium impact levels as well.

I suggest you begin with a basic Information Technology (IT) program and then adapt it to your Operational Technology (OT) environment. As you build your program keep the CIP Standards in mind. I feel it will work best if you build the CIP Standards into your security program, as opposed to building a security program around the CIP Standards. In other words, a good cybersecurity program should go far beyond the minimum requirements of the CIP Standards, while maintaining compliance with all aspects of those Standards.

If you're new to cybersecurity, a good way to start is with a class on the fundamentals. If you need advice on choosing a class, send me an email at the address below.

Books

If your budget or your schedule won't accommodate a class, start with a basic book on IT security. One example of an introductory book I've found useful is "Defensive Security Handbook" (2017, O'Reilly Media Inc., ISBN 978-1-491-96038-7). This walks you through building a cybersecurity program from the ground up, although it does not deal with Industrial Control Systems (ICS).

St. Joseph, MI – Photo: L Folkerth

To build ICS capability into your cybersecurity system, a book like "Hacking Exposed – Industrial Control Systems" (2017, McGraw Hill Education, ISBN 978-1-25-958971-3) is one possible choice. In particular, the first chapter provides an excellent introduction to ICS security. RF will post a list of books and resources you may find useful in the upcoming CIP Knowledge Center on our website.

CIS "Top 20" Controls

As you are working through understanding your environment, a key facet of your cybersecurity program will be a set of security controls. You can start with a set such as the "Basic CIS Controls," available for free at

	CIS Control	CIP Standard
1	Inventory and Control of Hardware Assets	CIP-002-5.1 R1, BES Cyber System Categorization
12	Boundary Defense	CIP-003-7 R2 Att 1 Section 3, Electronic Access Controls
17	Implement a Security Awareness and Training Program	CIP-003-7 R2 Att 1 Section 1, Cyber Security Awareness
19	Incident Response and Management	CIP-003-7 R2 Att 1 Section 4, Cyber Security Incident Response

Continued on page 13

Continued from page 12

These controls, also known as the "Top 20," may be adapted as needed to your OT environment or adopted as a whole for your entire organization. Because the "Top 20" deal with IT environments, you should also read "Implementation Guide for Industrial Control Systems," available at here in order to adapt the Basic CIS Controls to your control systems environment.

At the low impact level, the CIS controls in Table 1 (on the previous page) have applicability to the CIP Standards.

US-CERT/ICS-CERT

While not required by the CIP Standards at the low impact level, your security program should include vulnerability management. This will enable you to address weaknesses in your security posture before these weaknesses are exploited by malicious actors. The U.S. Cyber Emergency Response Team (US-CERT) tracks and alerts on vulnerabilities in the IT environment while ICS-CERT does the same for control systems.

You can sign up for alerts here and here. ICS-CERT also has a good overview of ICS vulnerabilities here.

ICS-CERT goes beyond vulnerability alerts in offering free training. The available training ranges from introductory videos to instructor-led classes (also free, except that you must pay your own travel expenses), culminating in an advanced five-day hands-on class. More information on ICS-CERT training is available here.

CSET

As you get deeper into your cybersecurity program, you will want to conduct evaluations of the program. A valuable tool for our industry is the ICS Cyber Security Evaluation Tool (CSET) provided for free by the National Cybersecurity and Communications Integration Center (NCCIC), an organization within DHS. This tool helps you to perform a self-assessment of your control system security posture, and goes into detail about your control system networks and how they are protected. CSET is a Windows application that you will download and install on a local PC.

It includes a network diagramming tool so that you can easily describe your control systems network to the tool. CSET will ask you a series of questions regarding your security practices. The final result is a set of reports that will provide details about the results of the assessment (see Figure 1 for a sample page).

CSET has the ability to take the CIP Standards into account in its assessment. This capability could be used to give you a more accurate picture of your security and compliance posture. CSET does not directly support low impact at this time, but you can select standards for high and medium impact that will address the low impact requirements.

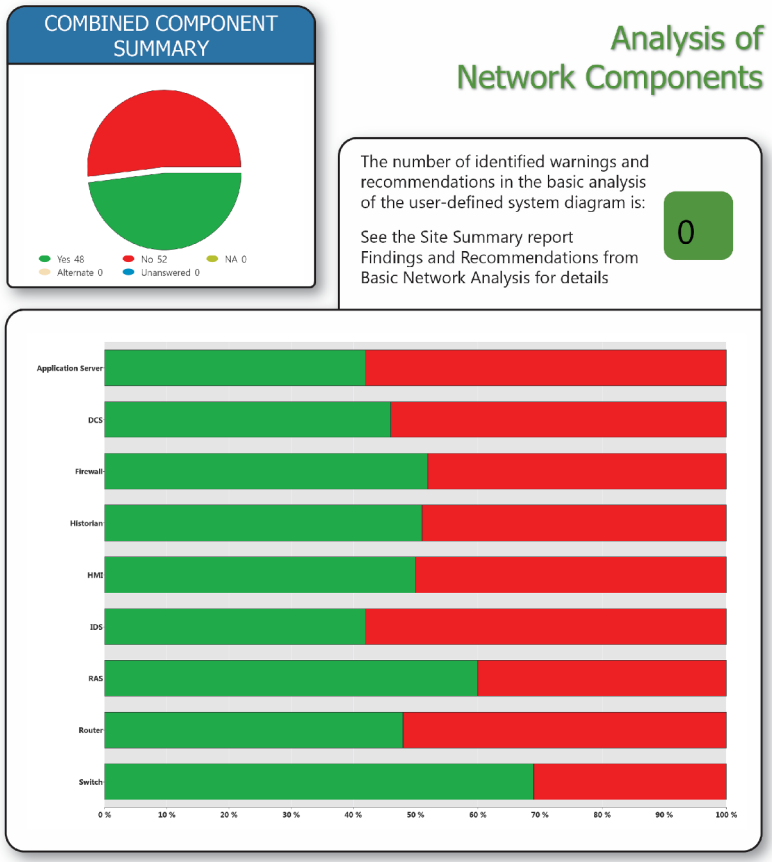

Figure 1

NIST CSRC

The National Institute of Standards and Technology (NIST) operates a Computer Security Resource Center (CSRC). The CSRC has many publications (read here) which are useful for our cybersecurity efforts. One of the most popular CSRC publications is Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. This 462 page document contains an exhaustive set of controls for implementing IT

Continued on page 14

Continued from page 13

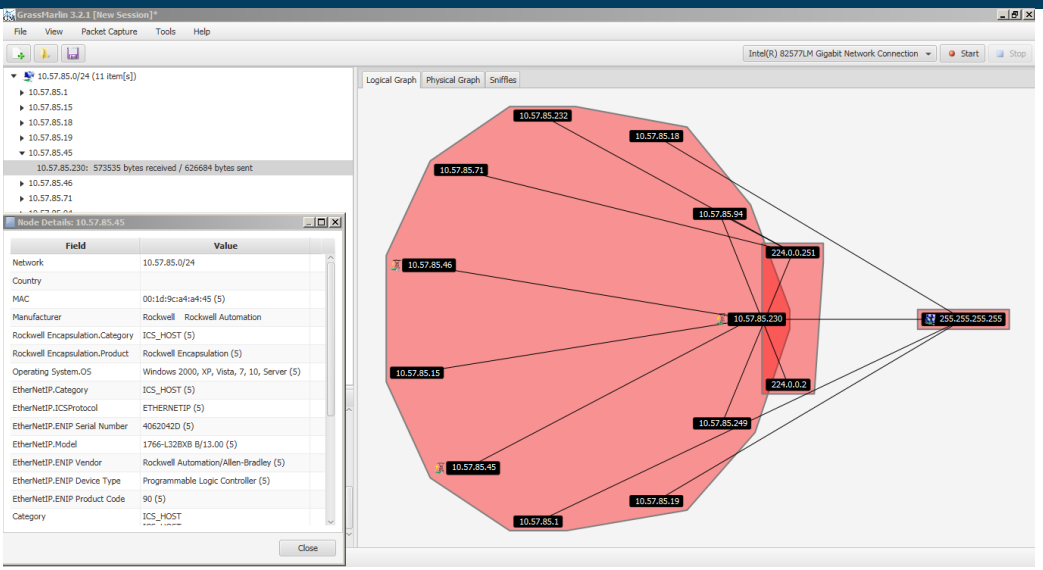

Figure 2 - Grassmarlin

security and is used, among other things, to implement security controls in the US Government.

I recommend that you download a copy of SP800-82, *Guide to Industrial Control Systems (ICS) Security*. SP800-82 contains an excellent comparison of IT and OT security in Section 2.4. Chapter 4 discusses development of an OT security program, and Chapter 5 provides an in-depth look at designing a security architecture for OT systems.

Security Onion

Security Onion is a special-purpose version of the Linux operating system that performs monitoring and recording of network traffic using standard PCs. CIS Control 12, Boundary Defense, contains sub-control 12.5 which calls for configuration of monitoring systems to record network packets. Monitoring and recording network traffic is also an element of incident response, required by CIP-008-5 for high and medium impact BES Cyber Systems and by CIP-003-7 R2 Attachment 1 Section 4 for low impact BES Cyber Systems.

There are some very good commercial products available to do this, but those products can also be expensive. Security Onion is available for free here.

GRASSMARLIN

GRASSMARLIN is another free tool used for network monitoring, but GRASSMARLIN differs from Security Onion in that it is designed to passively monitor ICS networks and identify ICS systems and traffic patterns on those networks. Passive monitoring is important in ICS environments due to the sensitivity of some ICS systems to any change in the network environment. GRASSMARLIN can be used to monitor for unexpected or unwanted patterns of traffic, and can also be used as a discovery tool for ICS devices.

This can be useful in CIP-002 to ensure you have inventoried all of the systems that can have a 15-minute impact on the BES. GRASSMARLIN can identify ICS devices by network traffic analysis.

Figure 2 shows the result of a GRASSMARLIN monitoring session on a small test network. Note the control system icon next to three of the devices on the network. This denotes a device that is communicating with one or more ICS protocols, making it a subject of interest in the identification and protection of control systems.

GRASSMARLIN was developed by the NSA and is available for free here. This web page also has links to the User Guide and to a brief slide deck on the capabilities of GRASSMARLIN.

Security Testing Environment

You should not implement any of these tools directly into your control system environment. First, you should first familiarize yourself with the operation of each tool. You should understand the possible impact of each tool on your production environment.

If you don't already have one, I strongly suggest that you set up a security testing environment to try out and evaluate any tool you plan to incorporate into your security program.

It is possible to set up your own security testing environment without expending a lot of resources. A couple of ICS devices and a small PC can provide a lot of benefit if your company can't afford a full test environment. Figure 3 (on the next page) shows my personal testing environment as it was used to test GRASSMARLIN. The used PLCs were obtained from eBay, the Ethernet hub from a garage sale, and other components from commercial sources. The wood backboard and legs (actually shelf brackets) were obtained

Continued on page 15

Continued from page 14

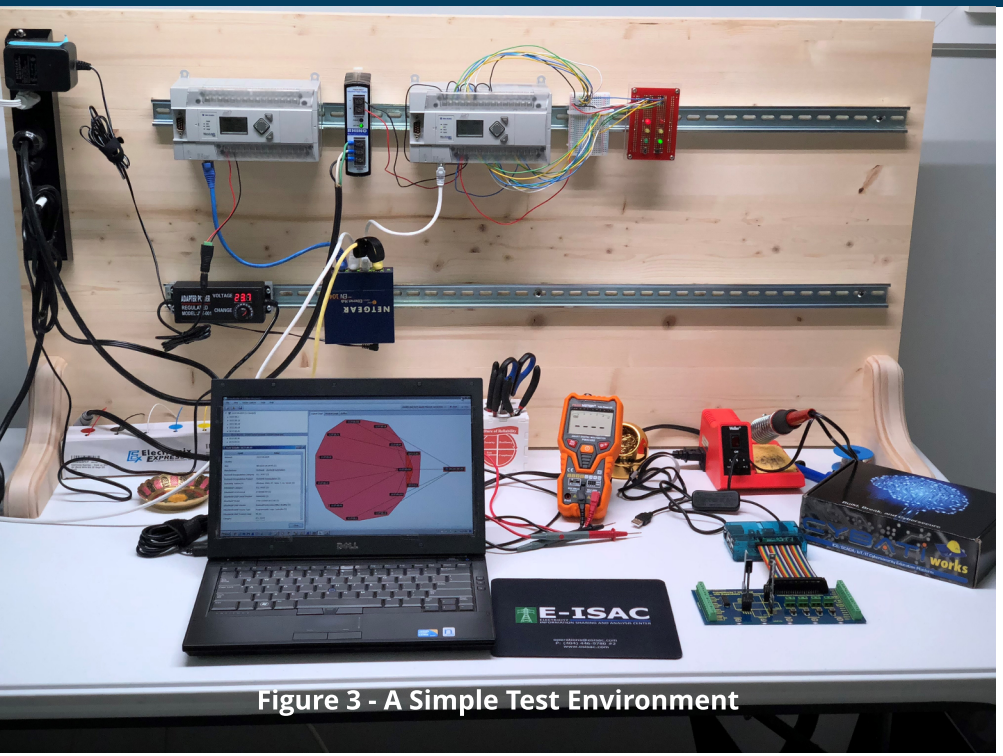

Figure 3 - A Simple Test Environment

from my local Lowe's. Except for the PC, which is an older repurposed laptop, the entire setup cost less than $500.

RF Knowledge Center – CIP

There are many resources available in addition to those I describe above. In recognition of this, RF is establishing a CIP area within the Knowledge Center on the RF website. We will update the CIP Knowledge Center with resources and links to resources for CIP compliance and ICS cybersecurity that we believe may help our entities. An expanded version of this article will be posted there as well.

Requests for Assistance

If you are an entity registered within RF 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 rfirst.org web site here.

Newsletter Correction

In our previous issue, an error was discovered in the Lighthouse article regarding the initial implementation date for low impact Cyber Security Incident response plans.

We promptly identified and corrected the pdf, but if you downloaded the original version of the May/June newsletter, please be aware of the correction to avoid any confusion.

Feedback

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

I may be reached here.