Cyber security for industrial control systems

New threats for Industrial Control Systems

The threat landscape is changing. Industrial Control Systems are being actively targeted by many bad actors, each with its own motivation. Threats such as ransomware, state sponsored espionage, and activist vandalism, unheard of until recently, pose an increased cyber risk to your plant operations. Did you know:

1 It is important to have a documented cyber security program that can be maintained even when leadership of the program changes. One example of a process that needs to be documented is the steps necessary if the person in charge leaves the company or changes responsibilities within the company.

2 A terminology widely used in cyber security is reducing “attack surface”. That means such actions as changing default passwords, eliminating unneeded accounts, removing software that is not required for the core mission, and closing network ports that are not required. This reduces the likelihood of vulnerabilities in the system and simplifies the requirement for software patching. This is one of the most critical steps with the biggest payoff according to the Department of Homeland Security.

3 Even when the only software on a machine is what is required for its primary mission, flaws may be discovered in that software over time that provide an opening for malware or intentional compromise. Patches are released on a very regular basis for almost all software, but if the patches are not installed, the machines remain vulnerable. The majority of cyber security incidents are related to unpatched flaws for which patches were available already. DHS rates this step as one of the top couple of steps to be taken to secure a system. For this reason, timely patching is required by most standards and regulations.

4 Software backup is a critical part of a cyber security program. Ransomware is only one example of a threat where this may be a salvation in a crisis. It is very important to do this right because finding out your backups are no good when you need them is going to be a very bad thing. Backups must be tested, and the tested backup must be secure from compromise in case of assault on the system.

5 Many system owners think an “air gap” between the control system and the outside world is a completely effective security measure. However, that just forces individuals maintaining the system to walk around the air gap with removable media. Most compromises ABB Field Service encounter on customer systems come from accidental infection by individuals with the best of intentions. It is very important to have limitations on use, but also a well thought out plan for use of this media as required.

6 Almost always, the stories in the news about major compromises of systems where a great deal of confidential information is stolen or systems are damaged, involve attackers having plenty of time after penetration of perimeter defenses to look around in the system undetected. They can take time to learn the system and choose targets. Only later when the damage is done do those who are investigating see these tracks. This is because the monitoring programs are lacking. If no one is paying attention to what is normal and what is not, the system is extremely vulnerable.

7 In order to have an organized consistent approach to cyber security, it is important to have focused attention on the tasks involved. At least one person should be designated as the leader of the program to provide this focus. A second person is a plus to provide continuity during absences of the primary person or if that person leaves the role.

Complete the Plant Cyber Security Survey on the next page to see how well your system is protected.

Plant Cyber Security Survey

1. Does your organization have a policy to describe the plant cyber security program?
   - ☐ Yes
   - ☐ No or don't know
   - ☐ Can you share a copy with ABB?

2. Has your organization verified the ABB DCS meets the minimum cyber security requirements documented within the ABB DCS Secure Deployment Guide?
   - ☐ Yes
   - ☐ No or don't know

3. Does your organization have a program of regularly updating computers with important security related software patches?
   - ☐ Yes
   - ☐ No or don't know
   - – Most recent update (Month/Year) _____

4. Does your organization have a program for performing regular software backups?
   - ☐ Yes
   - ☐ No or don't know
   - – How many times per year is this done? ____ /yr
   - – ☐ Do you test backups?
   - – ☐ Do you have off-line copies?

5. Does your organization have a policy for removable media use, limiting who can use it and how it is secured before use?
   - ☐ Yes
   - ☐ No or don't know

6. Does your organization have a method of monitoring for abnormal activity?
   - ☐ Yes
   - ☐ No or don't know

7. Does your organization have a designated person in charge of plant cyber security?
   - ☐ Yes
   - ☐ No or don't know

– Contact information

Customer name: _____

FSE Name: _____

Customer email: _____

Customer telephone: _____

20170119