The Five Deadly Sins of SCADA/PCS Cybersecurity

by Bob Reilly

This article is the third and final installment in our series on the Five Deadly Sins of SCADA and Process Control Systems Cybersecurity (Communicator 2016, Issue 1 and 2017, Issue 1). We've already addressed deadly sins two and three: allowing web browsing to the internet from SCADA/PCS and allowing direct access to the internet from SCADA/PCS. In this article we examine deadly sins one, four, and five, and recommend strategies and alternatives to mitigate their risks without impeding productivity. The remaining sins are:

Sin 1: Do you allow direct external access into your SCADA/PCS?

Direct access to your SCADA/PCS usually means there is no separation between your business network and your SCADA/PCS network. Although not uncommon in the water sector, this is a major security vulnerability. The risks associated with this kind of design are many of the things that you may hear about on the news such as ransomware, phishing, bitlockers, or, even worse, the ability of an attacker to control your network without your knowledge. This is because the business network and the SCADA/PCS reside on the same physical network with no separation. Any kind of successful attack on the business network can easily affect the SCADA/PCS network.

Figure 1 below represents a simple network where there is no separation between the two networks.

How do you know if you are safe from direct external access to your SCADA/PCS? If employees have unfettered access from your business network or remotely to the SCADA/PCS network, you are in violation of this rule and your network is at risk. A vulnerability scan of all your systems will tell you if this is a current problem on either network.

The first step in running a vulnerability scan is to talk with your information technology department, system integrator, or your technology contractor. Determine all the different access points into your SCADA network, including contractors, wired, wireless, and remote. Any

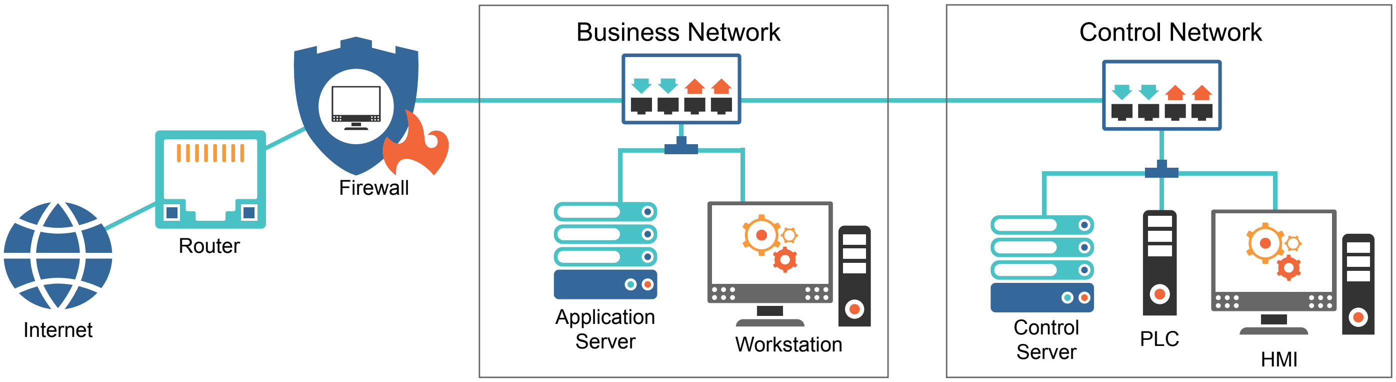


Figure 1: Direct external access

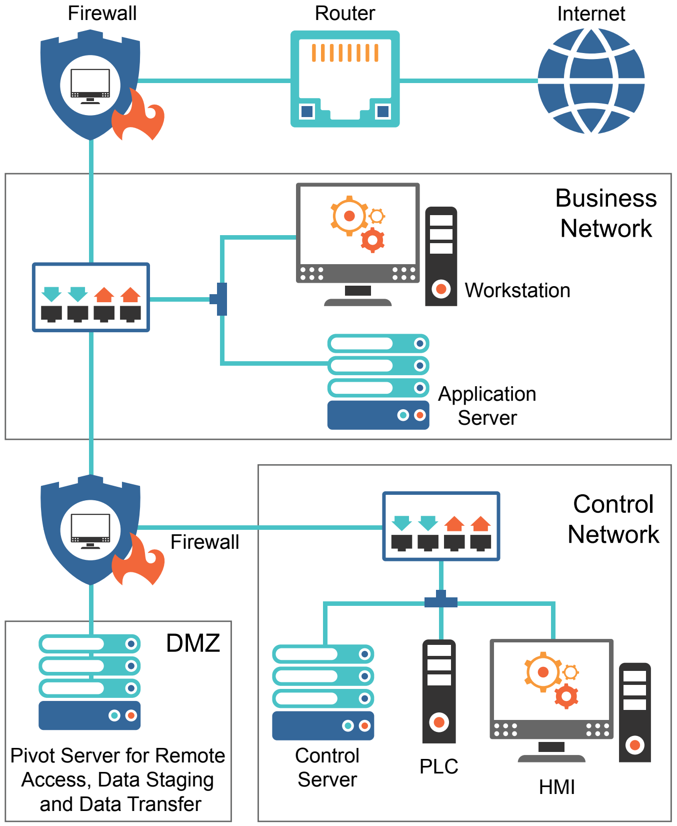


Figure 2: No direct external access

access point is a potential vulnerability and should be treated as path for potential attackers.

Ensure you have a **stateful packet inspection firewall** between your business and SCADA networks. Stateful packet inspection firewalls perform a deeper inspection of traffic as it passes through to ensure packets are compliant with policies and don't contain malware. If you already have one in place, make sure all access ports between the two networks are closed. You can check this via a penetration test against your firewall. This may require bringing in outside expertise. If your information technology department or contractors says you are secure, don't take them at their word; have them prove it to you. To do this, at a minimum you should run vulnerability scans and firewall penetration tests. Make sure proper precautions are in place on both the business network and the SCADA/PCS network. Creating a firewall between the two networks is a must. If this is something that a utility cannot do or is unwilling to do, then the two networks should be "air gapped," or physically separated.

Figure 2 shows what a secure, or potentially secure, network looks like. The firewall between the business network and the SCADA/PCS network blocks all traffic between them. Staging servers and pivot servers, located in the demilitarized zone (DMZ), control access to the SCADA/PCS network and its data. You should control any data access needs between the SCADA/PCS and the business network through a pivot server. A pivot server is a physical system located in the DMZ that acts as a secure traffic cop between the two networks. Any kind of remote access or data exchange should be limited to this location. A pivot server can be locked down to limit access to allow specific functionality only to users that have properly authenticated and have the appropriate rights. See Sin 4 for more information.

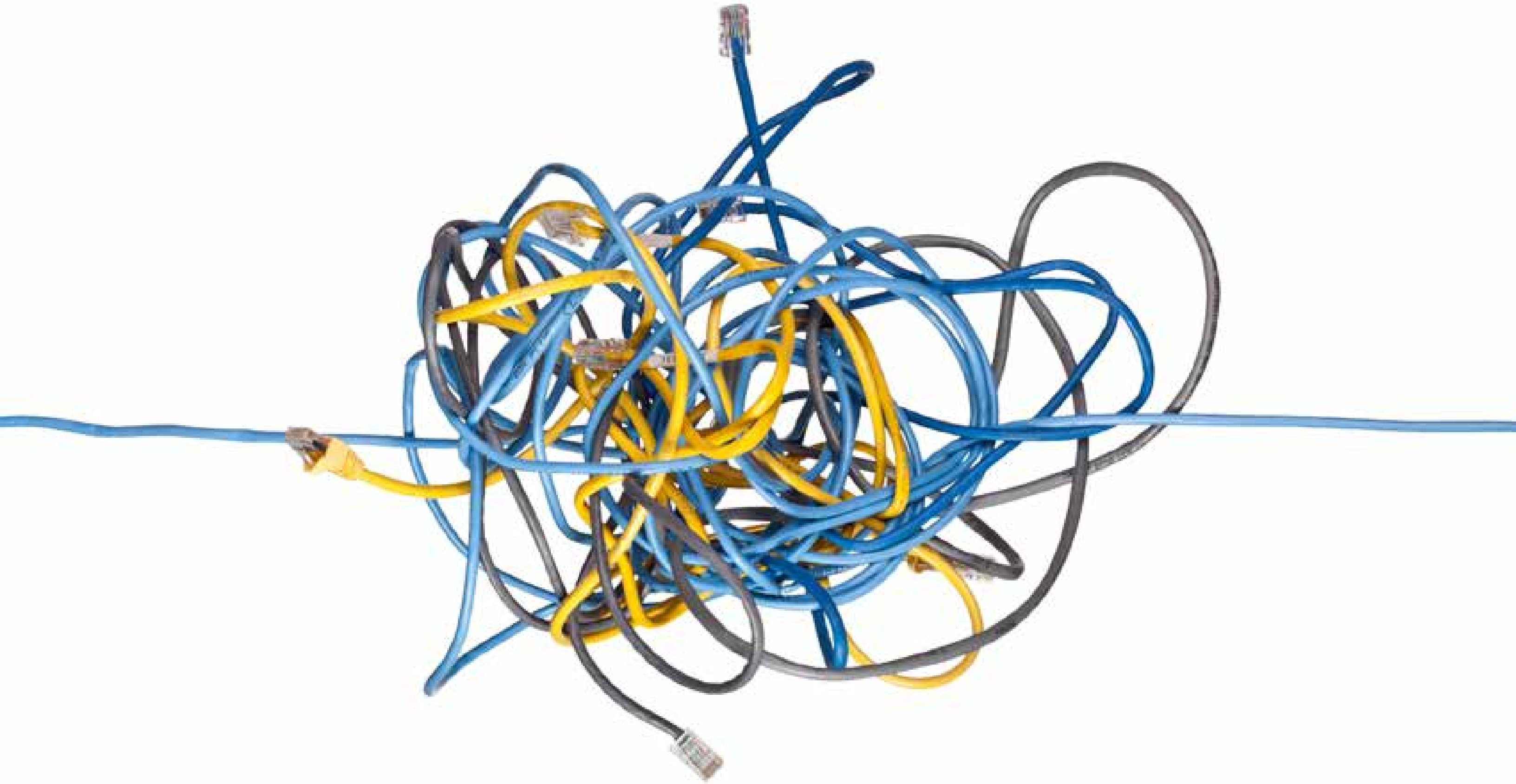
Sin 4: Do you allow SCADA/PCS laptops to be used outside of SCADA/PCS?

Many SCADA/PCS networks allow access by multiple portable devices, either for remote access or programming of programmable logic controllers (PLCs), remote terminal units (RTUs), or other equipment. These can be laptops, tablets, or even mobile smartphones. This sin manifests itself through usage of these devices outside of their intended purpose, whether on other networks or even for personal use. If you find you are using SCADA/PCS devices outside of the SCADA/PCS network, you are creating an unnecessary vulnerability.

Laptops or any mobile device set up to use on the SCADA/PCS network should be purpose-built for that task as well as **hardened** and physically controlled. Hardening is a process of securing devices to perform a certain task and locking them down from performing other tasks. Hardened devices will typically have unnecessary ports, such as FTP and HTTP, closed.

You should use multiple methods including MAC (media access control) filtering, two-factor authentication, and mobile device management to control access from remote devices to the SCADA/PCS network.

- Filtering by MAC address is not a foolproof access control method, but it can be used along with other methods to secure systems. MAC filtering is a security method to allow only specific device addresses access to the network.
- Two-factor authentication for remote access devices is an authentication method whereby users must utilize at least two of the following three methods for access:
  - Something you know – usually a password, PIN, or a passphrase



  - Something you have – usually a physical token or a text message
  - Something you are – usually a biometric such as a fingerprint
- Mobile device management (MDM) is a third-party application that is installed on mobile devices where granular policies can be set to update, monitor, and control the devices.

These are all strategies that can be incorporated into a security program to increase the overall security posture of the organization. Any one of these methods, used alone, will lower the risk of attack. Incorporating multiple methods will reduce your exposure even further.

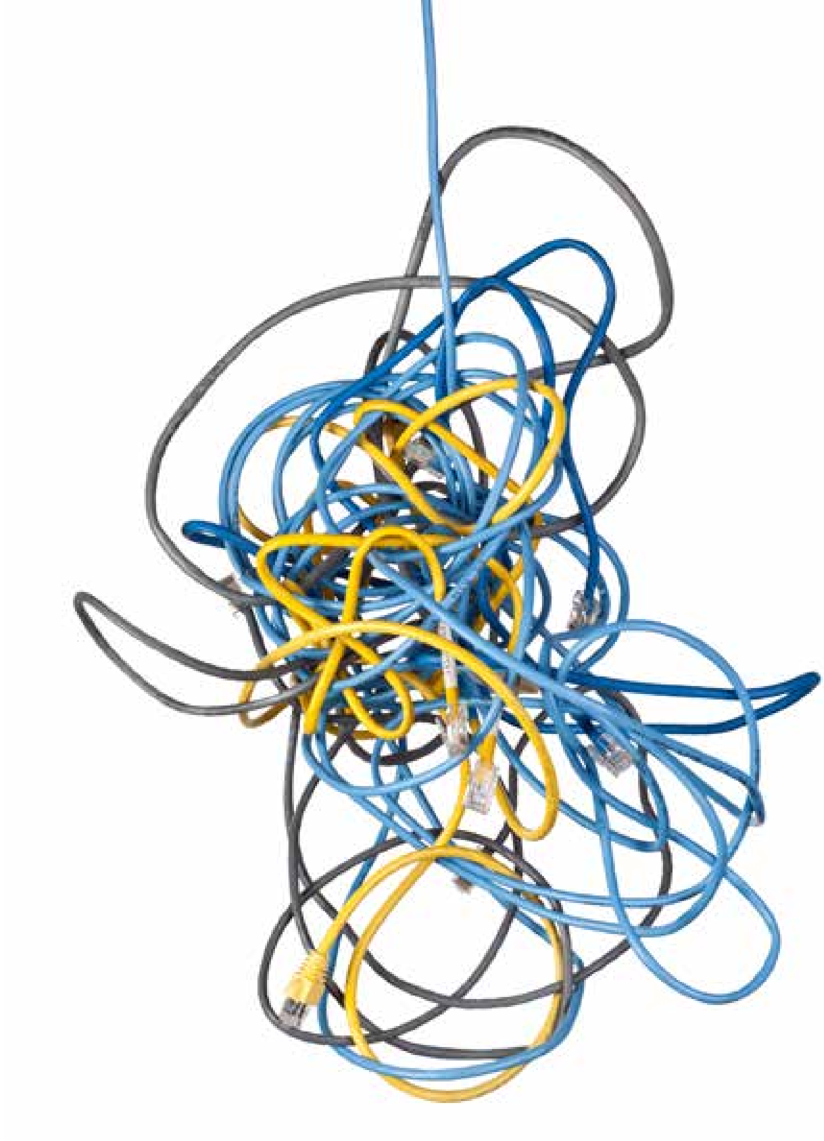
A pivot server, as shown in Figure 2, can be used for remote access from the business network or a remote location. Pivot servers should be set up to provide virtual desktop access to the SCADA/PCS network, meaning devices are never actually connected to the control network. There are many types of virtual connections that work well for this type of connection, including VMware Horizon, Microsoft Remote Desktop Services, and Citrix Xen. These systems can be controlled at many levels including at the user, application, and even at the port level.

Prior to allowing remote access, organizations should have a security program in place that includes proper log management and monitoring, intrusion prevention, and even ensuring that their policies are in place and up to date. The National Institute of Standards and Technology (NIST) recommends that critical infrastructure organizations have continuous monitoring of logs. A utility must also monitor intrusion prevention and detection at the SCADA/PCS gateway. Many utility organizations either incorporate on-site log monitoring systems that can parse log data known as a SIEM (Security Incident and Event Management), or utilize off-site log monitoring companies, known as a managed service security provider or MSSP.

Policies for the security around a SCADA/PCS are critical pieces of the overall puzzle. The latest AWWA Cyber Security Evaluation Tool lists 21 policies and plans that organizations should have in place to manage their security and their security program. Utilities cannot stop at creating this program; they must monitor and maintain it as well. In order to maintain a state of constant preparedness for the newest threats, utilities must have defined periodic reviews of this program.

Sin 5: Do you allow contractor or other outside laptops into SCADA/PCS?

If you are letting contractors bring in outside laptops or devices, or allowing them unmonitored remote access, you are guilty of Sin 5. Contractors will often bring in their own devices, connect to PLCs, and even move data between systems using a USB device.



Are you monitoring this access, either remotely or when they are on-site? Are you allowing devices not owned by the utility local access to your SCADA/PCS network?

The utility, not the contractor, should control contractor access, and all on-site and remote access should be monitored. Prior to any contractor connection to a utility SCADA/PCS network, the utility should have a defined change management plan. All production changes should be tested in a test environment and have a backout plan. A backout plan is a documented list of the steps needed to restore a system to its original state. This change management plan would be required as part of the vendor access policy. This policy will define these requirements and access will not be allowed without a signed agreement.

Utilities should control contractor remote access similarly to remote access for employees, except with even more restrictions. This access should be activated by the utility and staff should monitor the access to ensure that the contractor follows the approved change. Many of the remote access systems defined in Sin 4 allow monitoring and some have built in recording of sessions as well. This is a good idea in case any issues arise from a change.

Remote access by contractor devices should be controlled at the gateway or firewall through several methods. As discussed in Sin 4, all devices that access or can potentially access the SCADA/PCS network should first perform a two-factor authentication. Since the contractors' laptops are not owned or controlled by the utility, outside contractor devices should be placed in a quarantine where they can undergo a suitability screening. These screenings can be automated and controlled based on the potential vulnerabilities the device may introduce. The utility may choose to quarantine access to a limited access area based on the results or deny access altogether. These decisions should be documented in a policy and reviewed on a regular basis.

On-site access by contractors should be monitored as well. Staff knowledgeable of the SCADA/PCS network should escort and monitor contractors' access. If the changes are previously documented, tested, and approved by the utility, there should be little chance of a major disruption in operations.

Many contractors will use USB drives to move programs or data to and from systems. In order to avoid contractors' use of personal USB drives, the utility should have secure, encrypted USB drives that can be used when this is the only option available. Utility staff should manage and control the use of these USB devices to avoid unknowns being introduced onto the production network.

Don't stop what you're doing now, but make sure your cybersecurity improvements address these issues as priorities.

Utilities should work to create or improve their current security posture as well as their security program. A documented security program with hard deadlines for areas such as policy review, vulnerability scans, and even periodic cybersecurity assessments is a step in the right direction.

This program should incorporate all your policies and plans including incident management and disaster recovery. Not only should you have a set periodic review of all policies, but you should have a set schedule for auditing and testing of both your incident management and your disaster recovery plan. These tests should be performed, documented, and improved on a regular basis.

The bad practices mentioned in this article are not impossible to do securely, but a layered security model using the concept of defense in-depth is the best practice approach. Bring increased attention to cybersecurity. Allowing these practices presents very real and immediate threats to your system.

Recap and Next Steps

We've reviewed the five deadly sins of SCADA and Process Control Systems cybersecurity:

1. Allowing direct external access into your SCADA/PCS
2. Allowing web browsing to the internet from SCADA/PCS
3. Allowing direct access to the internet from SCADA/PCS
4. Allowing SCADA/PCS laptops to be used outside of SCADA/PCS
5. Allowing outside laptops into SCADA/PCS

Consider the five sins an opportunity for a defense in-depth approach. The more layers of defense, the better chance of having the proper countermeasure in place to thwart an attack. If you are just starting down this road, come up with a plan of measures that will need to be in place and begin a process of prioritization. The defenses that create the best bang for your buck should be implemented first. Policies and plans will help to guide some of these decisions based on the risk that an organization is willing to accept. A cybersecurity plan is really a roadmap to continually lower current risks while actively planning for future risks.

For more information, visit the NIST website to review special publication 800-82 Rev 2 and/or try using the AWWA Cybersecurity Guidance and tool to quickly assess your current security posture.

csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx