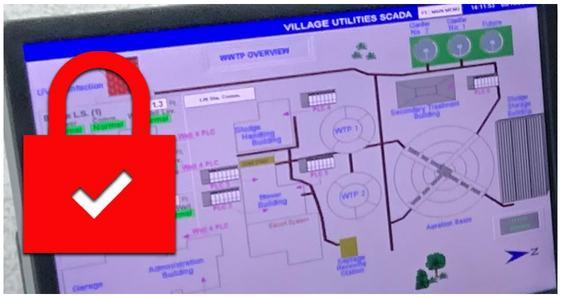
3 Easy Ways To Improve HMI/SCADA Security



Many of you might have seen the recent breach of a SCADA system in Florida in the news. Unfortunately, in the connected age, this is and will continue to be a concern. Anything short of simply disconnecting from the internet and all outside connectivity, there will always be a risk. It is not dire, however. There are easy ways that you can maintain a level of SCADA security:

Change Passwords Regularly, Don't Share Them!

There is no way around this, you must use passwords. They should be strong (use a generator), every person should have their own, and they should not be shared. Passwords should be changed on a regular basis – every 3 – 6 months.

Do not use the same password across multiple accounts – your login is typically your email address, so if you are using the same login and password across multiple sites, you make it quite easy for hackers to access all your accounts once your password has been compromised. If you have multiple users on your network or HMI – make sure you are enforcing these password rules. Do not leave a post-it with the password taped to your machine. If an employee leaves, make sure to disable or delete their account access.

Use 2 factor Authentication

Two factor authentication allows the web site to contact you on a mobile or other device to ensure that it is in fact you logging in. It is an added step, and possibly a hassle, but a small inconvenience in comparison to staying safe. There are many versions available from Microsoft, Google and others. Find one and use it.

Optionally you can also use a hardware key which looks like a USB drive – you plug it into your computer and it is used to authenticate you when you log into your accounts from that PC. Remove the key and even if someone has your credentials, they would be unable to access your account.

Keep OS and HMI/SCADA Software Updated

Software is not perfect. The more people that use something the more often people are targeting the weaknesses and finding vulnerabilities. Make sure you are keeping your operating system (OS) up to date – in most cases setting it to update automatically will be fine. There are some instances where you do need to be cognizant of major upgrades/patches that might interfere with other software on your machine.

In these cases it may take a couple weeks for the software to patch for the OS upgrade. Make sure you are keeping your HMI/SCADA and other software up to date and running most current versions possible. Most programs will alert you to updates but it does not hurt to periodically check for updates manually just to be sure. Make sure that your OS and software is still supported. Windows 7 for example has been unsupported for well over a year but some figures have Windows 7 running on over 10% of all Windows installations.

SCADA Security Diligence

In today's day and age constant connectivity and remote access is almost a human right. You can of course disconnect entirely but this opens up other implications and quality of life issues. I am suggesting that we can remain connected but need to know what this means and the risks associated with it. If you are diligent in meeting all the suggestions above you are ahead of the game. However, anything less than this and you are setting yourself up for needless risks.

Energenecs is a professional control system integrator serving water and wastewater utilities primarily in Wisconsin, Illinois, and UP Michigan. Energenecs provides professionally programmed comprehensive Supervisory Control & Data Acquisition (SCADA) systems from the smallest rural water community to a large city water or wastewater treatment facility.