Decrease your HMI/SCADA risk

Key steps to minimize unplanned downtime and protect your organization.

Are you running your plant operations with serious risk? Most industrial applications lack recommended updates and security patches, which make them a target for hackers. Outdated architectures, backups and spares can also create problems. With the number of attacks on industrial applications rising and the critical need for plant system availability, take simple steps now to minimize risk. You can decrease unplanned downtime while helping to protect your organization. Here’s how…

Check the expiration date
Software doesn’t usually come with an expiration date. But, the expiration date on your operating system might have already passed. If you’re using Windows 7, that “expiration date” is January 14, 2020 - the date that Microsoft stops supporting Windows 7. Don’t use software that is no longer supported by the manufacturer; you could be running with serious risk every day. In addition to your OS, make sure your other software packages are still supported. Were any of the vendors acquired? Do the new companies still support those software packages?

Our business environment today is constantly changing – make sure your software is keeping up.
Schedule HMI/SCADA risk assessments and reviews

Minimizing risk isn’t a one-time or once-a-year activity. With serious threats on the rise, you need to incorporate risk assessments and reviews into your schedule.

The frequency of your risk assessments depends on your particular business, industry and plant applications. Start with a conservative, high-frequency schedule – and you can always increase the time between assessments, as needed.

Assign a champion to minimize risk in your plant operations to drive leadership and consistency to the program.

Sample questions for each review

- Are you using obsolete software (Windows 7 or other)?
- Are you running your application with non-default / non-Administrator accounts with low privileges? Have you removed ADMIN and GUEST default accounts, using a separate administrator account?
- Where are the points of entry/failure?
- Are you properly isolating (DMZ) servers from untrusted network access?
- Is your system missing any security patches? Are you using the most up-to-date version of your software?
- Are you managing Bring Your Own Device (BYOD) securely?
- Do you have spare parts, and when were they last tested?
- Have you put additional controls in place to protect the HMI/SCADA security files from unauthorized change?
- Have you changed the default password for Trusted Network Computing?
- Do you have an up-to-date backup plan in place?
Upgrade, the right way

If you do have outdated software in your plant operations, make a plan now to upgrade the right way. Rethink your HMI/SCADA strategy – securely. Some HMI/SCADA users haven’t updated their systems in 10 years or more. Don’t just upgrade. Review your system with experts and use an upgrade as an opportunity to assess and modernize.

4 steps to include in your upgrade plan

1) Check and limit users’ rights
2) Update / install the latest anti-virus software
3) Create a controlled zone around your machines – place them behind a firewall
4) Make sure you have installed all of the latest service packs

Consider technologies that will make the life of your Plant & IT personnel easier. For example:

- Can existing Windows 7 machines be converted into thin clients or virtualized?
- Can critical applications be migrated to a server-based machine?
- Time to rethink your app strategy. How many applications are you running that could be consolidated?
- What applications can you leverage to turn your installation into a web-enabled one? Have you looked into Proficy Operations Hub or Webspace?
- What applications are available now that can extend the functionality of your HMI/SCADA? Consider new levels of efficiency by adding simple analytics, task management, alarm response management, and more.
- How are you storing and analyzing your data to improve operations? It might be time to look into a plant-wide historian, such as Proficy Historian.

Don’t wait for unplanned downtime or a disaster. Take action now.
Put rigor around security

The priority for plant systems has historically been availability. Plant operations simply must keep running in order to achieve organizational success. However, plant operations teams need to include cyber security as a high priority and implement best practices to minimize vulnerabilities.

Security is the process of maintaining the confidentiality, integrity, and availability of a system:

- **Confidentiality**: Ensure only the people you want to see information can see it.
- **Integrity**: Ensure the data is what it is supposed to be.
- **Availability**: Ensure the system or data is available for use.

General IT goals and industrial control systems goals have historically differed. Make sure you review your goals and adjust as necessary, with consideration for the increase in industrial security threats and requirements for data protection and privacy.

Source: Cyber Security Assessments of Industrial Control Systems CNPI / US Homeland Security
Assess your current HMI/SCADA system, preferably with an outside expert, and develop a plan to reduce risk. You can identify common vulnerabilities and take action before a disaster.
Leverage standards and best practices

A wealth of current information exists about how to reduce risk in HMI/SCADA systems.

Your software vendors have the best information regarding your particular applications. Reach out to them for their advice and best practices. Read your software manuals and follow the instructions, especially concerning networks/connectivity and user accounts/privileges. For example, if a manual recommends that you disable or remove a certain account after installing an I/O driver, then don’t forget to do it.

Also, tap into the many industry associations. Learn about new standards and implement the parts that fit your situation. Not every standard—or even all sections of a standard—will work for you, but you can use the standards as a framework and add to them.

Check into ISA, OPC Foundation, MTConnect, MESA and other plant systems organizations for more information and learning opportunities during the year. Government agencies, such as the U.S. Department of Homeland Security, National Institute of Standards and Technology (NIST), and U.S. Department of Energy, have valuable information—which applies to almost every SCADA user.

Additionally, some industries such as water and power have entities such as the North American Electric Reliability Corp. (NERC), which provide information on HMI/SCADA risk reduction and security.

<table>
<thead>
<tr>
<th>Patch Management</th>
<th>• Define a risk-based patching policy &amp; procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Apply the latest Microsoft security patches</td>
</tr>
<tr>
<td></td>
<td>• Ensure coverage for all layers and assets (OS, DB, etc.)</td>
</tr>
<tr>
<td>System Hardening</td>
<td>• Disable unnecessary ports, services, accounts &amp; shares</td>
</tr>
<tr>
<td></td>
<td>• Define secure configuration standards for all asset types</td>
</tr>
<tr>
<td></td>
<td>• Consider restricting the use of untrusted USB media</td>
</tr>
<tr>
<td>Host-based Protection</td>
<td>• Install anti-virus software on control systems PCs</td>
</tr>
<tr>
<td></td>
<td>• Keep anti-virus definitions up-to-date</td>
</tr>
<tr>
<td></td>
<td>• Consider application white-listing solutions</td>
</tr>
<tr>
<td>HMI/SCADA Configuration</td>
<td>• Deploy in a DMZ architecture configuration</td>
</tr>
<tr>
<td></td>
<td>• Install application using a least-privileged user account</td>
</tr>
<tr>
<td></td>
<td>• Disable or remove default accounts</td>
</tr>
<tr>
<td></td>
<td>• Configure applications to require user authentication</td>
</tr>
<tr>
<td></td>
<td>• Configure applications to use SSL or encrypted communication</td>
</tr>
<tr>
<td></td>
<td>• Limit access to functions at all levels:</td>
</tr>
<tr>
<td></td>
<td>• By role: only give to the users access to what they really need</td>
</tr>
<tr>
<td></td>
<td>• By server</td>
</tr>
<tr>
<td></td>
<td>• By runtime/development</td>
</tr>
<tr>
<td></td>
<td>• By asset/device</td>
</tr>
<tr>
<td></td>
<td>• Implement e-signature for complete regulatory and procedural compliance</td>
</tr>
</tbody>
</table>
The good news is that HMI/SCADA software designs can inherently minimize some vulnerability to risk. Fundamental engineering principles mandate safe and reliable systems. Additionally, new secure-by-design innovation takes traditional practices to a higher level.

As an example, GE Digital offers a Secure Deployment Guide to HMI/SCADA customers. Coming in both iFIX and CIMPLICITY versions, the Secure Deployment Guide describes the optimal security architecture and configuration for the HMI/SCADA nodes, communication between the nodes, and integration with other GE Digital solutions. Some security guidance is applicable to all HMI/SCADA installations and other security recommendations should be evaluated based on the size, complexity, and criticality of the process being monitored and controlled.

Throughout the Secure Deployment Guide, readers will encounter helpful “Want to Learn More?” sections, directing users to specific Getting Started, Help, or other documentation.

In addition to design guidance, make use of the latest secure-by-design technologies. GE Digital is a leader in leveraging OPC UA, as an example. OPC UA solutions are secure-by-design and use certificate-based communication.

Our Global Discovery Server allows you to track and catalog the variety of OPC UA servers and acts as a certificate authority for your system.

Lastly, make sure your HMI/SCADA provider has security as a top priority. Our Achilles Practice Certification, which is part of an IEC standard, indicates that we follow good practices when it comes to security. In addition to providing guidance to our customers through our Secure Deployment Guide, GE Digital does code analysis, using several different tools. We perform vulnerability analysis using teams that attack systems to find vulnerabilities.

Even more importantly, with all of these practices put together, we have a response mechanism if something does happen. If there is a vulnerability found in the field, there is a process to respond to it. At GE Digital, security is part of our philosophy as we build software.
Minimizing risk is, and always will be, a top priority for GE Digital – and should be a top priority for every HMI/SCADA user. Take advantage of standards, best practices and information sharing. GE works with customers, industry working groups and standards bodies, government agencies, and the security research community to continually improve industrial automation and control systems and global infrastructures. Plan a risk assessment program for your organization – and stick with it. Simple steps, such as upgrading unsupported software and limiting user rights, can make a big difference. There are many ways to reduce risk, but it is important to take the steps now – before unplanned downtime or a disaster occur.

Summary
About GE

GE (NYSE: GE) is the world’s Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive and predictive. GE is organized around a global exchange of knowledge, the “GE Store,” through which each business shares and accesses the same technology, markets, structure and intellect. Each invention further fuels innovation and application across our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry.

Contact Information

Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

GE HMI SCADA

© 2019 General Electric. All rights reserved. *Trademark of General Electric. All other brands or names are property of their respective holders. Specifications are subject to change without notice. 10 2019