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 Outdated architectures, backups and spares can also create problems.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 XP®, that “expiration date” was April 8, 2014 – the date that Microsoft stopped supporting XP. 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.

10 sample questions for each review

1. Are you using obsolete software (Windows XP or other)?
2. 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?
3. Where are the points of entry/failure?
4. Are you properly isolating (DMZ) servers from untrusted network access?
5. Is your system missing any security patches? Are you using the most up-to-date version of your software?
6. Are you managing Bring Your Own Device (BYOD) securely?
7. Do you have spare parts, and when were they last tested?
8. Have you put additional controls in place to protect the HMI/SCADA security files from unauthorized change?
9. Have you changed the default password for Trusted Network Computing?
10. 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.

Consider technologies that will make the life of your Plant & IT personnel easier. For example:
- Can existing XP 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 GE Webspace and GE Cimplicity?
- 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.

4 steps to include in your upgrade plan
- Check and limit users’ rights
- Update / install the latest anti-virus software
- Create a controlled zone around your machines – place them behind a firewall
- Make sure you have installed all of the latest service packs

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**
- Confidentiality
- Integrity
- Availability

**Industrial Control System**
- Availability
- Integrity
- Confidentiality

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.

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, 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.
### HMI/SCADA Security - Best practices example

| Patch management | → Define a risk-based patching policy & procedure  
|                 | → Apply the latest Microsoft security patches  
|                 | → Ensure coverage for all layers and assets (OS, DB, etc.)  |
| System hardening | → Disable unnecessary ports, services, accounts & shares  
|                 | → Define secure configuration standards for all asset types  
|                 | → Consider restricting the use of untrusted USB media  |
| Host-based protection | → Install anti-virus software on control systems PCs  
|                 | → Keep anti-virus definitions up-to-date  
|                 | → Consider HIPS/HIDS or application white-listing solutions  |
| HMI/SCADA configuration | → Deploy in a DMZ architecture configuration  
|                 | → Install application using a least-privileged user account  
|                 | → Disable or remove default accounts  
|                 | → Configure applications to require user authentication  
|                 | → Configure applications to use SSL or encrypted communication  
|                 | → Limit access to functions at all levels:  
|                 |   - By role: only give to the users access to what they really need  
|                 |   - By server  
|                 |   - By runtime/development  
|                 |   - By asset/device  
|                 | → Implement e-signature for complete regulatory and procedural compliance  |
Smart with secure-by-design innovation

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’s Agent provides an encrypted and authenticated channel to forward monitoring and diagnostic data from remote agents to a central repository over an intranet or the internet, replacing the need for dedicated VPN connections.

This secure-by-design technology also delivers functionality to send files and/or create RDP sessions from the GE Agent Enterprise Server to GE Agents over the established connection.

External/Remote Data Sources
GE Agent can be used to create trusted encrypted remote connections over the internet using standard ports.

Internal Data Sources
GE Agent can be used to create trusted connections between networks internally to build a layered defense solution.
Minimizing risk is, and always will be, a top priority for GE Intelligent Platforms – 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.
Useful links

GE
www.ge.com/digital
www.ge.com/digital

Microsoft
enterprise/endofsupport.aspx
http://windows.microsoft.com/eos

Associations / Government Agencies
ISA
MESA
U.S. Department of Homeland Security
National Institute of Standards & Technology
U.S. Department of Energy
North American Electric Reliability Corp
EU CSS
European Union Network and Information Security Agency

Need help with minimizing HMI/SCADA risk?
Contact GE for complimentary risk assessment tools and information.
www.ge.com/digital