It is essential that software updates/patches be kept up to date throughout an automation-system lifecycle to prevent cyber attacks and maintain reliability.

Focus on Automation System Updates

Keeping software updates current is an oft-neglected activity, resulting in exposure to cyber attacks and reduced reliability.

AS COMPANIES FOCUS more energy and resources on protecting mechanical equipment, one key asset is often overlooked: the plant's automation system.

Because automation-system hardware components are typically very reliable out-of-the-box, it is easy to deprioritize monitoring and maintenance activities for the overall control system. Unfortunately, "set it and forget it" is not a good strategy with automation systems. To keep such a critical investment running reliably over its 30-to-40-yr. lifespan, organizations must focus on proactive maintenance and upgrades of their automation systems.

Proper automation-system maintenance means keeping critical hardware and software elements up to date. Leaving the system and its operating environment unpatched or out of date means exposing the plant to potential equipment failure and cyber attacks. In addition, it is essential to maintain the hardware and software backbone on which the automation system relies.

Behind the curve

A properly installed system should start with all software and hardware completely up to date. When a plant begins using its new, fully patched and updated system, it is easy to be lulled into a false sense of security and let it operate without further intervention.

Unfortunately, nowhere is it truer than in the technology field that "change is the only constant." Though an automation system may continue to run under its original configuration for a long time, the environment in which it operates is continually evolving.

Every month, Microsoft releases new security updates. These updates add or improve essential functionality and security in the operating system that supports the automation system.

Along with operating-system updates, automation-system manufacturers will also release regular updates, patches, and hotfixes for their products. Staying up to date with these improvements means protecting the organization from unexpected failures or unauthorized intrusions, while also adding opportunities to improve plant and operator performance.

Furthermore, at some point, the hardware and software on which the automation systems run will no longer be supported by the manufacturer. Organizations then must move beyond updates and look toward upgrading systems.

Often, an organization will wait 8 to 10 years before considering an upgrade to their automation-system hardware or software, as they don't see the urgency if they don't witness any active problems. Yet, there is a serious risk to operating in this manner.

System hardware has a lifespan. Eight years ago, Microsoft Windows 7 was released, meaning a 9-yr.-old system today is likely running Windows XP (retired) or Windows Vista (soon to be retired). Hardware failure on a Windows XP or Windows Vista machine will be tremendously difficult to remedy. Because these operating systems are either no longer supported, or soon to be retired, manufacturers have ceased producing computers or parts for these systems. At best, users will be able to find used replacement parts that are unreliable themselves, due to their age. At worst, they could be facing an outage until they can complete an emergency upgrade.

Moreover, the cyber-security risk of running an outdated operating system is significant. Since the April 2014 termination of support for Windows XP, several security flaws have been discovered in the retired software. These include CVE-2014-6332, which remains unpatched in Windows XP since its November 2014 discovery, allowing remote attackers to execute code on the machine, even to the point of remote control of the system. With such vulnerabilities not only in existence, but also widely published, running an outdated operating system leaves organizations open to a potential disaster scenario.

There is also a strong business case to be made for keeping automation systems updated and upgraded. Organizations that strive to improve reliability, automation, plant and operator performance, and cyber security will find themselves facing an uphill battle if they try to make these changes with an old, outdated automation system. Advancements made in the past five to eight years have enabled plants to realize vast improvements in intrusion prevention, alarm management, optimized work practices, process throughput, and paperless record keeping. All of these advancements can be implemented to give organizations better visibility to the health of their assets and the status of their processes.

Yet, even knowing the risks of falling behind in system health, many organizations let updates languish for a variety of speculative reasons. There are several understandable and resolvable concerns that can keep operations from performing the system monitoring and preventive maintenance that they need.

Automation-System Support

Guardian Support is a comprehensive, prognostic service designed to optimize reliability and performance of an organization's automation system. The program helps organizations minimize and simplify automation-system issues with comprehensive incident management. Users have access to 24x7x365 global factory support, and can speed issue resolution by collaborating with Emerson (emerson.com) experts to determine the fastest and most appropriate corrective actions.

To help ensure automation-system performance over its 40+-year lifespan, Guardian Support offers organizations lifecycle management. Users can simplify record keeping with system-specific inventory management. In addition, organizations can ensure the best cyber security and patch management with proactive lifecycle status notifications on their automation systems.

What if something breaks?

Users are sometimes concerned that, by updating their software or hardware, some features, or even the entire system, will stop working. In addition, companies often worry about the risk of updates having a negative workflow impact if employees need to be retrained because the interface changed.

The reality is that properly planned and executed system updates are successful. Updates, patches, and hotfixes released by the operating- or automation-system manufacturer undergo regular, rigorous testing for compatibility and are thoroughly documented on the manufacturer's support site.

In addition, though interface changes are a reality, such changes are designed with efficiency in mind. Changes to operator interfaces are generally implemented with the intention of increasing efficiency. Thus, any potential workflow upset will be offset, over time, by increased operator efficiency when users learn and leverage the new system updates.

We don't have time.

A plant's priority is to stay productive. As such, many organizations feel that they do not have the time to properly maintain their system health, even if they recognize that patches, updates, and upgrades are essential for improved performance and security.

However, the goal of a plant's control system is to help the plant stay productive. As such, keeping automation-system technology up to date can be a key to finding more time. Unexpected failures in automation-system servers and workstations can mean plant downtime until issues are resolved. If resolving the issue requires sourcing legacy parts, the outages can be lengthy.

A facility that doesn't have the time or staff to dedicate to system monitoring and preventive maintenance and upgrades can and should find a solution to keep its automation system up to date. Investing in a key partner in automation-system reliability and maintenance can pay significant dividends.

Expensive systems should work.

Automation systems can be a huge capital expenditure. A high-quality, well-designed automation system will work well for a long time. However, as with any intricate, high-quality system or device, a large capital investment does not preclude maintenance and upgrades.

Maintenance and upgrades become more capital intensive based on how

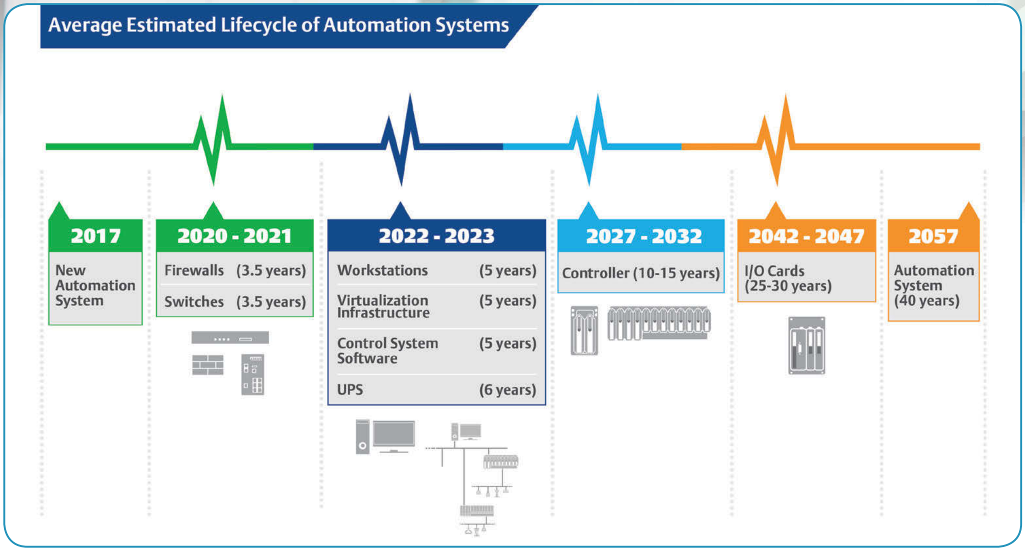

Fig. 1: Over the course of an automation system's lifecycle, individual system and infrastructure components will have their own lifecycles that need to be managed.

long it has been since either was last performed. Ignoring the automation system for 8 to 10 years will mean that making changes will be a more complicated and more expensive project. Smaller steps are often more manageable, take less time, allow organizations to take advantage of new features and functions more quickly, and prove less complicated with a smaller risk of major hardware and software overhaul.

Where do we start?

Implementing a best-practice automation-system maintenance and upgrade strategy begins with lifecycle planning. Organizations that want to keep their systems up to date need to understand and document the lifecycles of each control-system component. These vendor-specific guidelines will be available in product documentation for all automation-system components, as well as in vendor-support services such as Emerson's (Round Rock, TX, emerson.com) Guardian Support (see sidebar).

Following is a general trend for component lifecycles, though length will vary among specific vendors:

- control-system software: 5 to 7 yrs.
  workstations: 4 to 6 yrs.
- controllers: 10 to 15 yrs.
- I/O cards: 25 to 30 yrs.

In addition to automation-system-specific component lifecycles, organizations must consider devices that aren't system-specific but have an impact on performance:

- switches
- firewalls
- virtualization infrastructure
- universal power supplies.

All of these components will have an expected lifecycle that affects the organization's plan. Figure 1 above shows a typical automation-system lifecycle.

In combination with component lifecycle data, organizations should take advantage of a site evaluation available from automation-system vendors. Effective site evaluations look at component firmware, lifecycles, cyber-security issues, plant performance and Key Performance Indicators, and value-add opportunities. This information is used in conjunction with a return on investment (ROI) calculator to determine tangible benefits that will come from adding individual features during an upgrade. Armed with lifecycle information, a site-evaluation report, and ROI data, organizations can find a lifecycle plan that will keep systems up to date without financial risk.

Maintaining momentum

Whether organizations want to implement their lifecycle-planning programs themselves or work with vendors to do so, many offerings and/or programs are available to help the process. For example, to avoid the shock of a single capital expenditure for the project, many vendors offer flexible payment schedules, allowing organizations to spread the payments out over several years.

Many organizations are also looking to hardware virtualization to simplify the update and upgrade process. By moving from standard computer hardware to virtualized systems, organizations can, to some extent, decouple some hardware and software requirements, allowing them to quickly move machines between different hosts and easily create test environments to ensure that updates and upgrades will be successful, before they are applied.

The process of keeping automation systems up to date is never finished. Effective, sustainable, and measurable programs for maintaining and improving automation-system reliability and performance are always evolving. By staying on top of the update process and developing and sticking to thorough equipment lifecycle plans, organizations can leverage the newest features, the best cyber-security protection, and the most stable equipment platforms to help drive plant reliability and performance every day. **MT**

Information for this article was provided by Yoga Gorur, program manager in Emerson's PSS Lifecycle Services organization, Round Rock, TX. He manages global service offerings to DeltaV customers, and the DeltaV Upgrade Service, Scheduled System Maintenance, and Site Evaluation Service. He has a degree in Instrumentation Engineering, an MBA, and PMP certification.