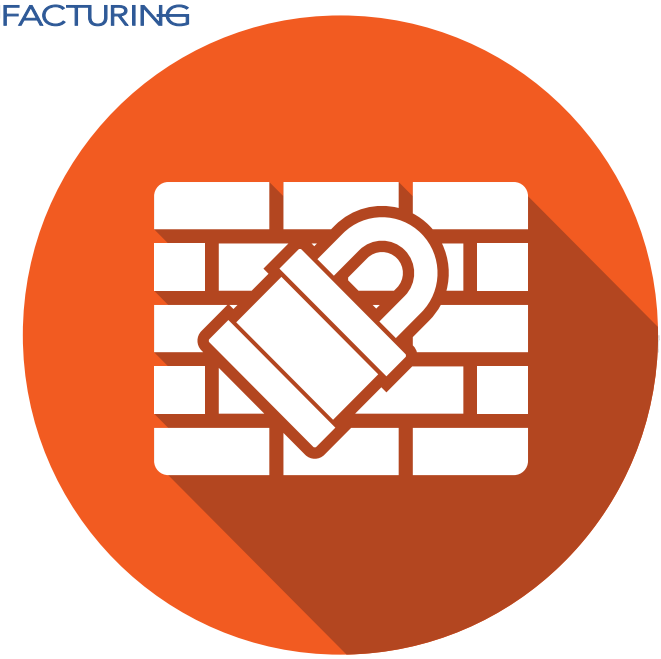
Pharmaceutical MANUFACTURING



Automating
Distributed Control System Patching

How Eli Lilly's Indianapolis facility reduced the time needed to gather information, and deliver and install plant-wide system updates

By Kurt Russell, Consultant Engineer–Automation, Eli Lilly and Company

AS INDUSTRIAL control systems have moved from proprietary hardware and software to commercial off-the-shelf (COTS) equipment, they have become exponentially more vulnerable to cyber threats. New threats appear in rapid succession. For this reason, security patches developed by Microsoft, antivirus updates by security companies such as Symantec, and hotfixes by industrial control equipment companies are distributed on a regular basis. This can present a considerable problem for those in charge of keeping everything up to date.

Which patches should be implemented? Not all are relevant to all users. When should updates be installed? While some can be installed while the control system operates, others require a reboot of the various portions of the system, which can lead to downtime if not properly coordinated. Also, which patches go with which systems? Putting a patch in the wrong place can have serious consequences.

Eli Lilly and Company in Indianapolis faced exactly

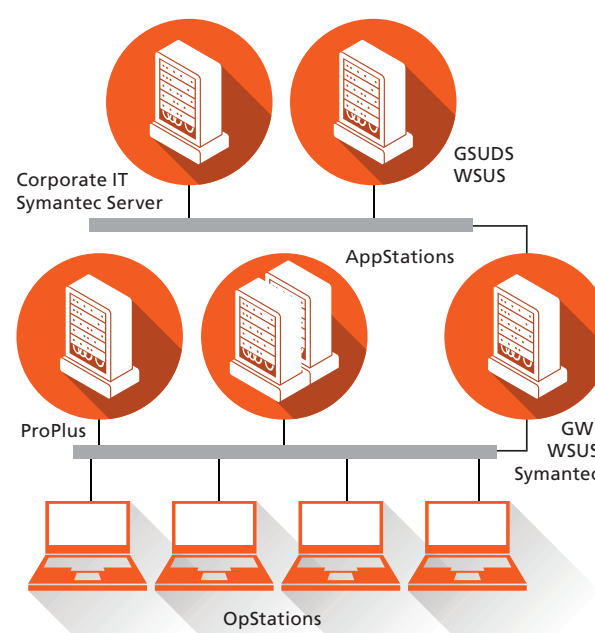


Figure 1. The systems at Lilly's Indianapolis facility consist of one upstream server and a number of downstream servers in a one-to-many arrangement. The upstream server has Internet access and hosts Microsoft Windows Sever Update Services (WSUS) and Emerson's Guardian Software Update Delivery Service (GSUDS).

WHO SHOULD CONSIDER PATCH MANAGEMENT?

Candidates for automatic patching:

1. Users with a large distributed control system or multiple systems where high-value labor is consumed in scheduling and deploying updates to a large number of workstations and servers.
2. Users with requirements to keep their systems up to date with security and/or anti-virus updates and in audit compliance.
3. Users with an IT infrastructure and organization capable of sustaining an automated update program.

TYPICAL ARCHITECTURES

Figure 2 shows how deployment is done manually using a connection to a secondary network. This manual solution uses off-the-shelf products from Microsoft WSUS and Symantec Endpoint Protection managers to obtain the files from their website(s). They are then periodically put on a secure thumb drive and taken to the appropriate systems for installation.

In the semi-automatic architecture shown in Figure 3, once the provider(s) have sent down their files, they are received at the Patch Management Update server. The green line shows the files' path from the Symantec and Microsoft "cloud" to the Patch Management server. The five-step software update process previously discussed must be followed in order that the correct files are readied for transfer down to the correct DeltaV stations and servers for installation and commissioning. Once there, it is now possible to "manually" extract those files and distribute them on to each workstation or server within the system through an external drive, CD or thumb drive storage transfer device.

As shown in Figure 4, automated patch management picks up where GSUDS stops. The deployment piece automates the distribution of DeltaV hotfixes, Emerson-approved Microsoft security updates and Symantec antivirus updates. It also provides these updates to all the appropriate system nodes, with subsequent installation determined by user-specific policies that govern the timing and approval of installation. As mentioned, this solution utilizes off-the-shelf products from Microsoft WSUS and Symantec Endpoint Protection managers and automates the delivery of all of these downloaded updates to the individual workstations in the control network. In addition to Microsoft WSUS and Symantec Endpoint Protection Manager, the Guardian WSUS Interface (GWI) makes sure that only Emerson-approved updates get deployed.

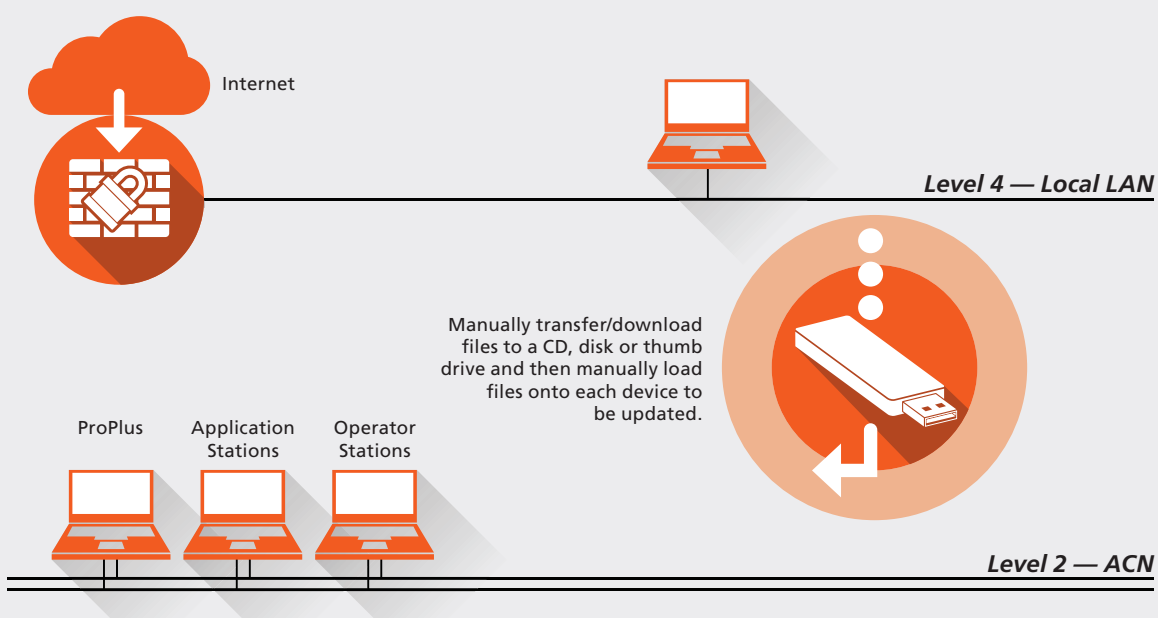


Figure 2. Manual patching using a connection to a secondary network. This manual solution uses off-the-shelf products from Microsoft WSUS and Symantec Endpoint Protection managers to obtain the files from their website(s). They are then periodically put on a secure thumb drive and taken to the appropriate systems for installation.

this problem. For the facility's 15 DeltaV distributed control systems (DCS) — both offline and online running multiple batch operations — keeping track of everything in regard to administration and system maintenance took up a great deal of time and cost a substantial amount of money.

Eli Lilly began to experiment with ways to automate the patching process when Emerson Process Management introduced its Guardian Software Update Delivery Service (GSUDS) and Automated Patch Management Service. Lilly became early adopters and worked with Emerson on refinement of this Lifecycle Services offering.

The systems at Lilly's Indianapolis facility (Figure 1) consist of one upstream server and a number of downstream servers (in what Emerson calls a one-to-many arrangement). The upstream server has Internet access and hosts Microsoft Windows Server Update Services (WSUS) and GSUDS.

The multiple downstream dedicated non-DeltaV server machines (one for each DeltaV system) host Microsoft WSUS, Guardian WSUS Interface (GWI) and Symantec Live Update Server – Distribution Center (LUS-DC). Each downstream server can also talk to other DeltaV servers via plant LAN connections where available.

The GSUDS client solicits system hot fixes and approval information for Microsoft security updates from Emerson via the Internet. GWI is

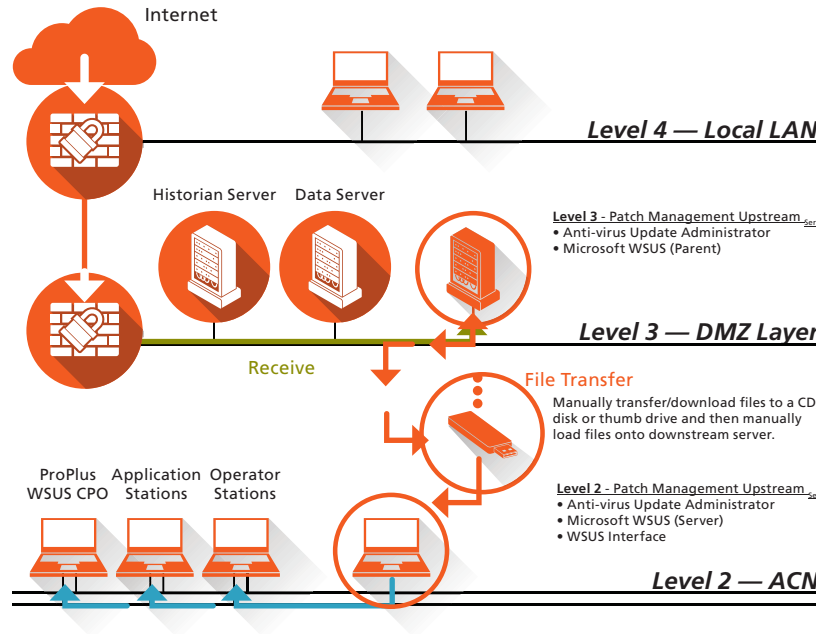


Figure 3. In the semi-automatic architecture, once the provider(s) have sent down their files, they are received at the Patch Management Update server. The green line shows the files' path from the Symantec and Microsoft cloud to the Patch Management server. The files are then extracted and loaded onto the system through an external drive, CD or thumb drive storage transfer device.

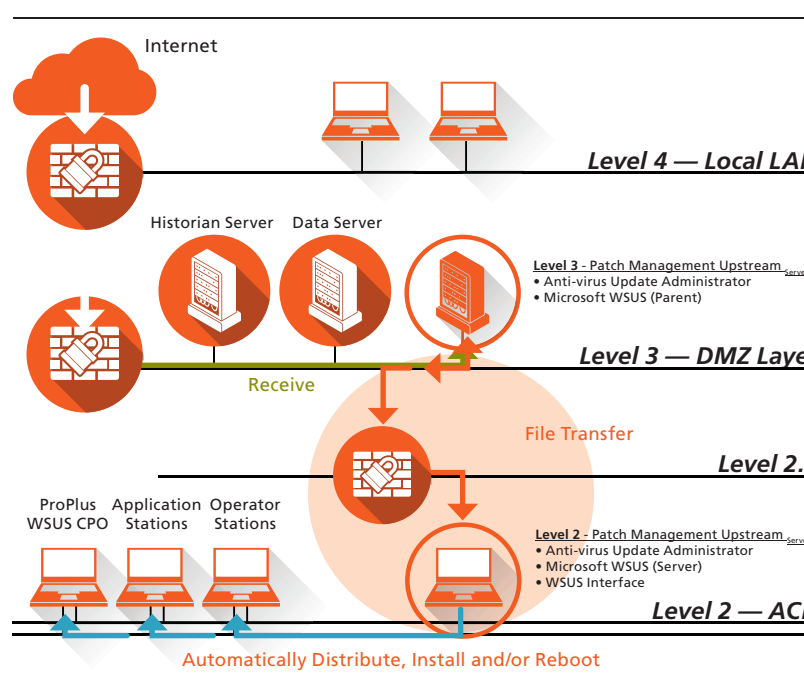


Figure 4. Automated patch management picks up where GSUDS stops. The deployment piece automates the distribution of DeltaV hotfixes, Emerson-approved Microsoft security updates and Symantec antivirus updates. It also provides these updates to all the appropriate system nodes, with subsequent installation determined by user-specific policies that govern the timing and approval of installation.

a software application that periodically checks with the GSUDS Client for new DeltaV hot fixes and the latest approval information for Microsoft security updates. It then programmatically injects them into WSUS.

Depending on the particular system, the downstream servers also support other needs, including Emerson's Backup and Recovery Services and Mimic (simulation software from MYNAH Technologies). The potential also exists for the downstream servers to be virtualized. Configuration for WSUS is handled through a separate Group Policy Object (GPO).

ENTERPRISE PATCHING APPROVALS

All Microsoft security patches are automatically approved at the upstream server and synchronized to each downstream server. DeltaV hotfixes are approved at the downstream server level, with each system administrator handling approvals for his/her own system. The advantage here is that it saves time as the patches and updates are automatically placed on the computers where they are required. Patches and hotfixes are installed through Windows Update on each computer. DeltaV hotfixes do involve some manual interaction during the installation process.

It's worth noting that it is still necessary to follow all release notes prior to installation, and all hot fix prerequisites must still be performed. Oversight of the patching process is strongly encouraged to verify distribution.

There are often significant differences among the multiple systems in a plant, which means that the set of patches must be customized for each. The automated system delivers the right patches to the right machines via the network. For those patches that require a reboot, it gives the option to automatically reboot, automatically install or just automatically download. In Lilly's case, automated patching saves several days of effort for each patching event. It reduces the time needed to gather information, delivers updates to systems all over the plant site, makes sure the right updates are in the right places, and installs the updates.

In Eli Lilly's experience, automatic patching saves anywhere from a few hours to a few days for each Emerson Process Management DeltaV system. With 15 systems in place, that can add up to a significant amount of time and money saved, while minimizing human error associated with patching.

ABOUT THE AUTHOR

Kurt Russell is a Consultant Engineer at Eli Lilly and Company in Indianapolis, IN, working in the Biotechnology & Life Sciences manufacturing area. Kurt has worked in automation and control system engineering with multiple platforms over the past 20 years. His current work involves managing multiple DeltaV DCS implementations from an operational, system administrative and project delivery perspective.