Computer System Security Updates

Why patch?

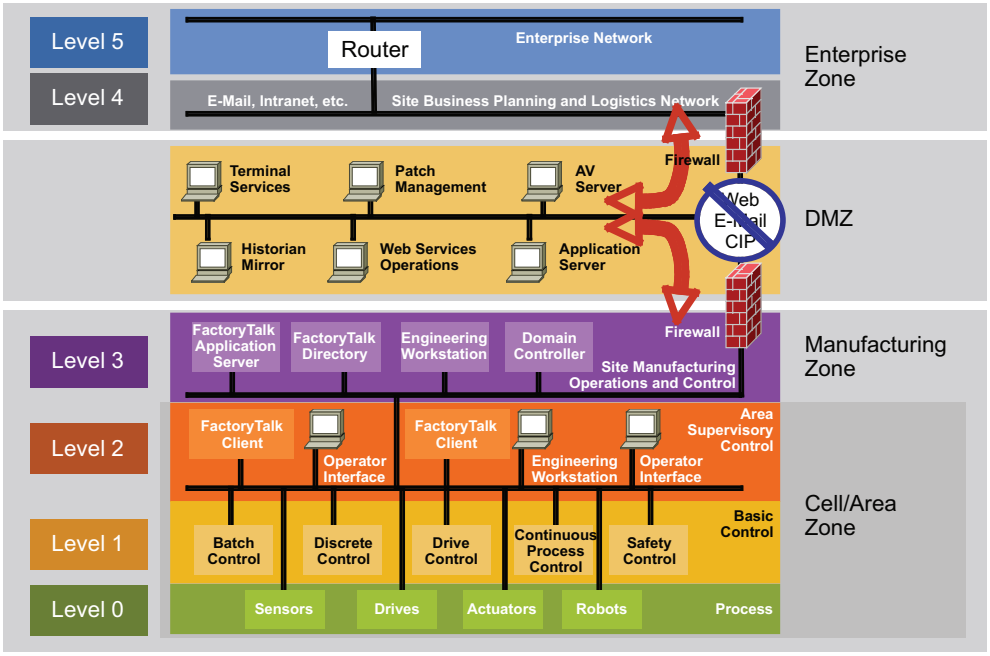
If you have already deployed a network architecture, such as the one recommended by Rockwell Automation and Cisco in the Converged Plantwide Ethernet Design and Implementation Guide (http://www.ab.com/networks/architectures.html), you have successfully provided a buffer zone between your enterprise and manufacturing zones.

Congratulations!

So why should you be concerned about applying security patches to the computers in your manufacturing zone? For the simple reason that no buffer zone, such as the demilitarized zone (DMZ) concept documented in the Converged Plantwide Ethernet Architecture (see Figure 1), provides a perfect security solution for your automation system. The reality is that in order to operate your plant, data and people still need to move between the enterprise and manufacturing zones. Along with that movement comes the possibility of the unintentional or intentional transport of viruses, worms or other undesirable payloads. These undesirables can impact the operation of your manufacturing systems. In a worst case scenario, they can "call home" to an attacker outside of the facility and provide that attacker with the ability to explore your enterprise or manufacturing zone.

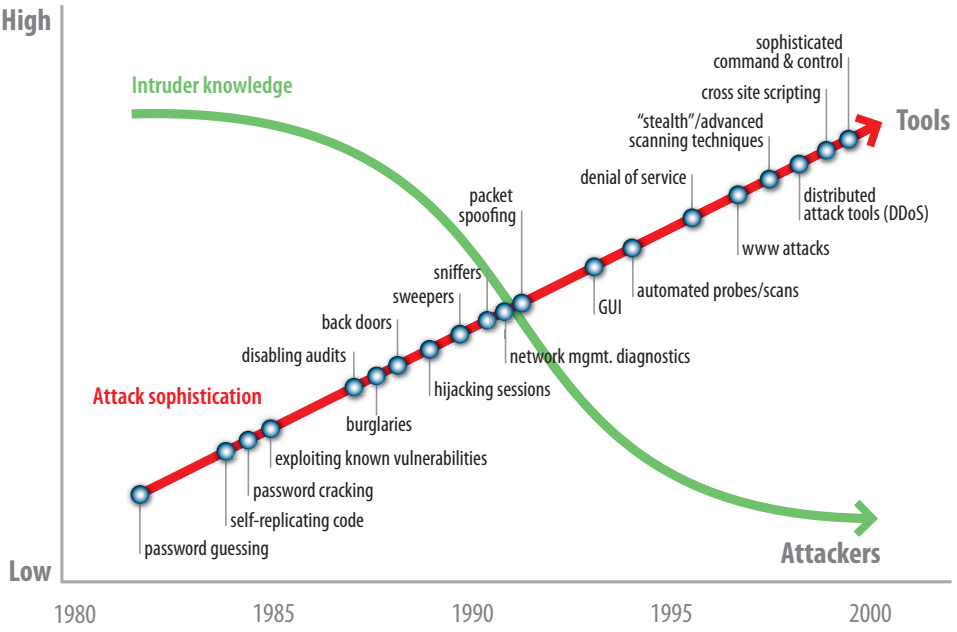
In order to lower the probability of such an event, you need to first understand how such an event might occur. The installation and configuration of the DMZ provides an excellent barrier to block direct attacks from the outside. By designing the DMZ to force all traffic to originate or terminate within it, you make it very difficult for an attacker to communicate directly with the manufacturing zone. The only other option, then, is for an attacker to take a more indirect route. One such route is for an attacker to first gain a solid foothold, or launching point, inside the enterprise (the Trojan horse scenario). This enables the attacker to discover resources inside the enterprise with one less layer of defense to slow him down. The most likely target for such a foothold is a computer on the enterprise network. Taking control of that computer allows the attacker to use tools already installed on that computer, or to install other tools, to help him explore the enterprise from within. Once there, the attacker may discover a resource that is communicating to a computer in the DMZ. With that knowledge, the next step is taking control of a computer inside the DMZ and so on until the attacker gains control of a computer inside the manufacturing zone.

Figure 1
Manufacturing Framework



Keeping a computer patched with both the latest operating system and application software security updates is the best defense against such an attack. Published security vulnerabilities can be easily turned into exploits with the availability of popular and easy-to-use freeware tools. As shown in Figure 2, these tools have become so advanced that sophisticated attacks can be carried out by intruders with limited knowledge and technical skills, resulting in an increased number of individuals with the ability to carry out an attack and shortening the time between publication of a vulnerability and the possibility of an exploit.

Figure 2



Exploitation of published vulnerabilities in a computer operating system or software application is the number one way in which attackers gain a foothold inside the enterprise. Most of the studies done in this area indicate that almost all successful exploits are perpetrated against known vulnerabilities and could have been prevented with already existing patches. In many cases, patches for the vulnerability existed more than six months before the attack occurred. A memorable example of this was the SQL Slammer in 2002. The patch for the exploited vulnerability was available more than 6 months before the Slammer wrecked havoc on enterprise networks worldwide. For this reason, keeping computers, in both the enterprise and manufacturing zone, up to date with the latest security patches is one of the simplest, most effective and lowest cost security mitigation strategies that you can undertake. However, patching computers in the manufacturing zone is not without its challenges. Some of those challenges include:

- The need to have production up and running 24/7/365
- Computer downtime that results in missing audit records and subsequent product loss
- Lack of skills needed to manage patching such systems
- Downtime associated with untested patches
- The need to test patches that results in delays in applying those patches

Patch Management Process

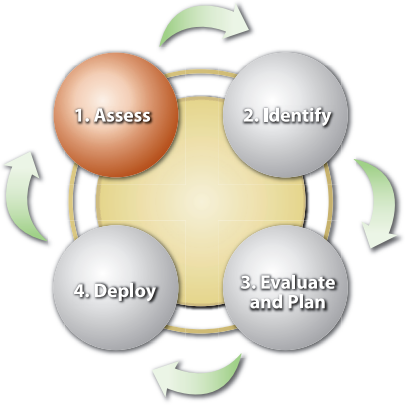
For these reasons (and many others), patching computers in the manufacturing zone requires the development of an elaborate and rigorous process for managing such patches.

Several studies have shown that more manufacturing downtime has resulted from poor or missing patch management processes than was caused by the exploitation of the vulnerability being patched. In this instance, the cure is worse than the disease. This is also the primary reason why disabling "automatic patch updates" is considered to be a recommended "best practice" in the manufacturing zone. In most of these cases, downtime would have been averted if a well designed patch management process had been followed.

Microsoft recommends that companies adopt a four step model for managing patches on enterprise IT systems (as shown in Figure 3). These steps include:

1: Assess 2: Identify 3: Evaluate 4: Deploy

Figure 3



Our challenge is to modify and enhance this process for the manufacturing zone. The following sections will provide an overview of each of these steps along with some recommended best practices for the application of this process to manufacturing.

Assess

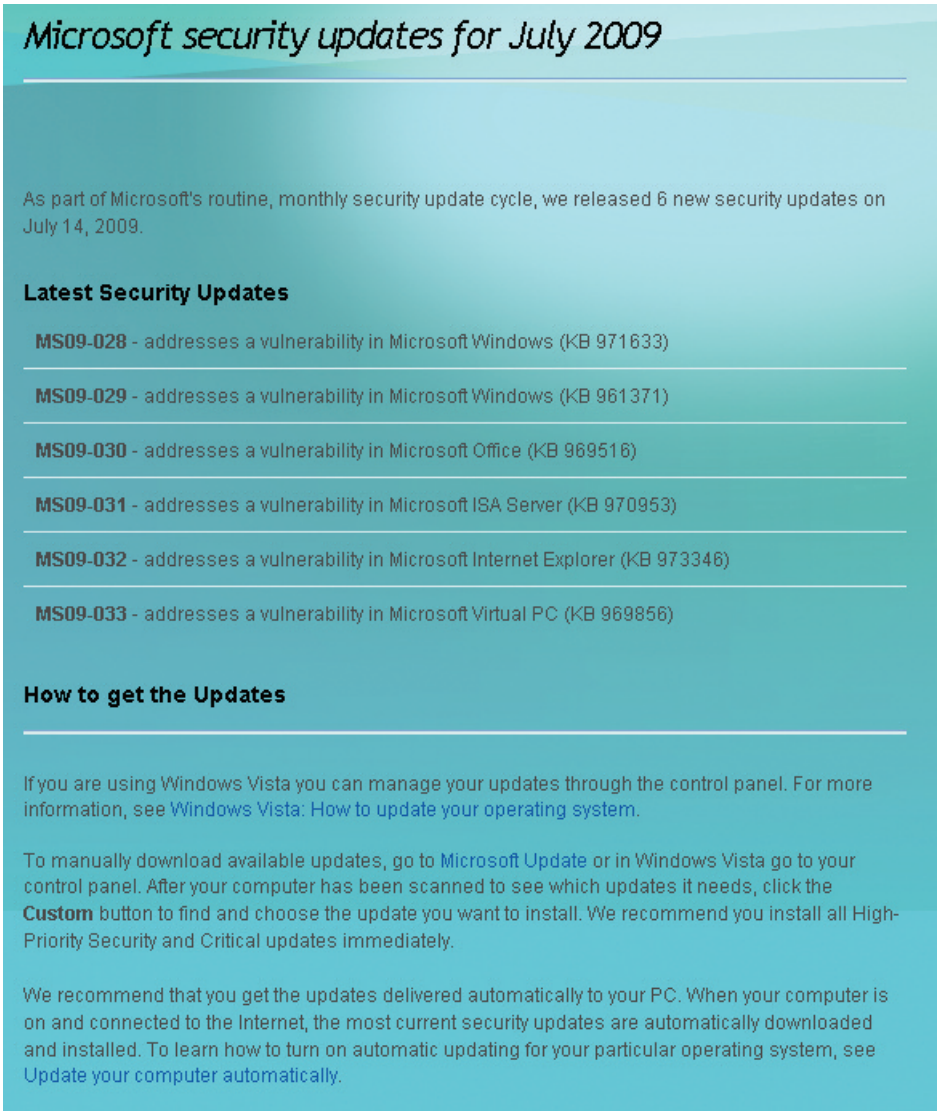
The first step begins with an assessment of all managed assets, such as networked computers installed in your enterprise and manufacturing zones. The focus of this step is on creating an inventory of the computer assets, software applications and operating systems currently deployed. There are a number of excellent tools available from Microsoft (http://www.microsoft.com/security/default.mspx) and others to help streamline this process. You also need to do an inventory of unmanaged assets such as stand-alone computers, firewalls, routers and other infrastructure items.

As part of this audit process, you need review your security policies and do a security assessment in order to develop a baseline of the existing security posture of the facility. This includes reviewing password policies, encryption standards, antivirus compliance, administration policies and the like.

You also need to include the function of each of these assets so that you can determine if they can or cannot be updated due to other constraints like third party validation, regulatory compliance, up- time requirements, etc. The most important part of this process is determining an acceptable schedule for applying security updates, in order to minimize the impact on production and other critical systems. In addition, you need to assume that something bad will happen during a security update. This means you need to have a backup image of all software loaded on all critical systems and a disaster recovery plan to back out any updates made in order to return the facility to an operational state quickly. As an alternative to this, a high availability solution can be used to reduce the risk significantly and make the patch management much less painful. With a high availability solution, you can switch over to the back-up system while patching the production system and then switch back to the production system after patches have been applied and confirmed.

The next part of this step is to determine if an update source is available for all installed software. An example of this type of data is the Microsoft Security Bulletins (http://technet.microsoft.com/en-us/security/default.aspx) shown in Figure 4.

Figure 4



Microsoft security updates for July 2009

As part of Microsoft's routine, monthly security update cycle, we released 6 new security updates on July 14, 2009.

Latest Security Updates

MS09-028 - addresses a vulnerability in Microsoft Windows (KB 971633)

MS09-029 - addresses a vulnerability in Microsoft Windows (KB 961371)

MS09-030 - addresses a vulnerability in Microsoft Office (KB 969516)

MS09-031 - addresses a vulnerability in Microsoft ISA Server (KB 970953)

MS09-032 - addresses a vulnerability in Microsoft Internet Explorer (KB 973346)

MS09-033 - addresses a vulnerability in Microsoft Virtual PC (KB 969856)

How to get the Updates

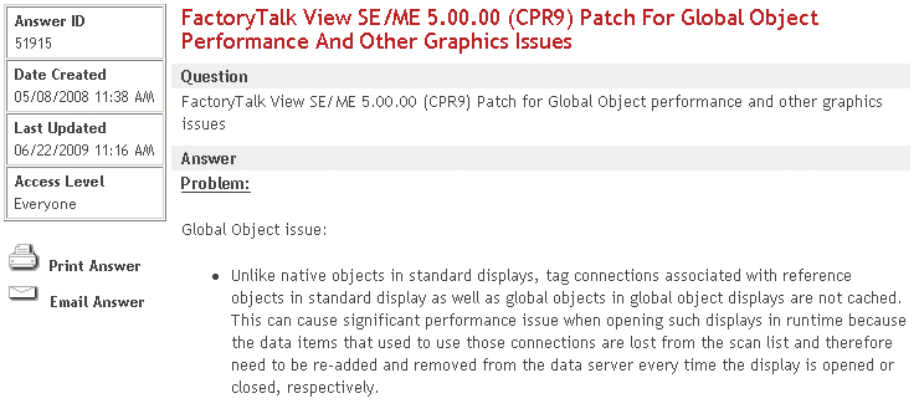
If you are using Windows Vista you can manage your updates through the control panel. For more information, see Windows Vista: How to update your operating system.

To manually download available updates, go to Microsoft Update or in Windows Vista go to your control panel. After your computer has been scanned to see which updates it needs, click the **Custom** button to find and choose the update you want to install. We recommend you install all High-Priority Security and Critical updates immediately.

We recommend that you get the updates delivered automatically to your PC. When your computer is on and connected to the Internet, the most current security updates are automatically downloaded and installed. To learn how to turn on automatic updating for your particular operating system, see Update your computer automatically.

Rockwell Automation provides downloadable updates for all software at Knowledgebase (http://www.rockwellautomation.com/knowledgebase). Figure 5 is an example of a software update for the FactoryTalk View SE® 5.00.0 software application.

Figure 5



Answer ID
51915

Date Created
05/08/2008 11:38 AM

Last Updated
06/22/2009 11:16 AM

Access Level
Everyone

Print Answer

Email Answer

FactoryTalk View SE/ME 5.00.00 (CPR9) Patch For Global Object Performance And Other Graphics Issues

Question

FactoryTalk View SE/ME 5.00.00 (CPR9) Patch for Global Object performance and other graphics issues

Answer

Problem:

Global Object issue:

- Unlike native objects in standard displays, tag connections associated with reference objects in standard display as well as global objects in global object displays are not cached. This can cause significant performance issue when opening such displays in runtime because the data items that used to use those connections are lost from the scan list and therefore need to be re-added and removed from the data server every time the display is opened or closed, respectively.

This Knowledgebase document includes the problem, cause, solution, installation instructions and the software update binary for a specific issue.

The final part of step one is to make sure your personnel have the assigned roles, responsibilities, tools and training required to perform software updates.

Identify

The focus of step two is to identify whether updates are available for any of your installed application software or operation systems. Most software vendors employ some type of proactive update notification system. Microsoft provides the Windows Server Update Service (WSUS) and Microsoft Systems Center Configuration Manager (MSCCM) to assist in the identification and notification process. Rockwell Automation provides an email subscription service using the Knowledgebase (discussed above) that allows you to be notified about updates that pertain to a specific software application.

The next part of this step is to determine if these updates are relevant to your production systems. Many of them have little or no impact on your security posture or system reliability and can be dismissed immediately.

Evaluate

The evaluation step is the most critical part of the process and the most overlooked. You need to evaluate each software update against a well defined process to determine the value to the business. It is important that each update is evaluated individually based on the benefit it brings the business versus the risk of deployment. The benefits to the business can include lowering the risk associated with a known security threat, increasing productivity, increasing reliability, better product quality, etc. The risks to the business can include deployment cost, downtime, system stability, loss of functionality, etc.

During this step, you also need to determine the level of urgency associated with each of the available updates. In some cases, the risk associated with the identified vulnerability is so low that the update can be deployed at some time in the future when it is most convenient. In other cases, the risk is so high that the update needs to be deployed immediately. This process can be quite subjective so it needs to be done carefully and consistently by trained personnel who consider all of the available facts before making a decision. Keep in mind that very few security vulnerabilities have been exploited so quickly that it justifies bypassing the evaluation and planning process. This is especially true if you have properly deployed the Converged Plantwide Ethernet Architectures.

The last part of the evaluation process is to test each update to make sure it does not negatively impact the operation of the computer or software application. Rockwell Automation assists customers in this area by qualifying all Microsoft security updates against the most popular set of Rockwell Automation software applications. This qualification service provides a report covering all Microsoft updates that could have an impact on software products. These reports are typically posted to the Knowledgebase 7-14 days following the release of the security update. Figure 6 is an example of a report showing updates released from Microsoft in July 2009.

Figure 6

Answer ID
35530
Date Created
09/26/2006 08:47 AM
Last Updated
07/30/2009 03:14 PM
Access Level
TechConnect

Microsoft (MS) Patch Qualification For 2007-2009 (Year-To-Date)

Question

Where can I get Microsoft™ (MS) patch qualification information?

Answer

In order to get the full view of the latest Microsoft Patch Qualification Results please click on the following link:

July 2009 Results w/ CPR9 SR1

Summary: What's New this Month

Last Updated: 7/30/2009

MS KnowledgeBase	MS Security Bulletin	Date Released	Qualification Status	Recommendation	CPR	Date Published	Details	OS
KB973825	None	7/28/2009	Published	Partially Qualified See Details	7	7/30/2009	PQUAL00023953	2003R2SP2
KB972260	MS09-034	7/28/2009	Published	Partially Qualified See Details	9	7/30/2009	PQUAL00023950	XPSP2, 2003R2SP2
KB972260	MS09-034	7/28/2009	Published	Partially Qualified See Details	7	7/30/2009	PQUAL00023951	2KProSP4, XPSP2, 2003R2SP2
KB972260	MS09-034	7/28/2009	Published	Partially Qualified See Details	6	7/30/2009	PQUAL00023952	2KAdvSP4, XPSP2
KB973825	None	7/28/2009	Published	Partially Qualified See Details	9	7/30/2009	PQUAL00023954	2003R2SP2
KB971633	MS09-028	7/14/2009	Published	Fully Qualified	9	7/22/2009	PQUAL00023587	XPSP2, 2003R2SP2

It is strongly recommended that Microsoft updates are not applied to the manufacturing zone until they have been fully qualified by Rockwell Automation. Fully qualified means that Rockwell Automation has tested the Microsoft updates with the primary functional areas of the relevant installed software. This includes qualification of updates for the Microsoft operating system, Microsoft Office products, Internet Explorer and Microsoft SQL Server.

In addition to the Rockwell Automation qualification, it is our recommendation that all software updates be tested first in a non-production environment, or when the facility is not active, to ensure there are no unexpected results or side effects. This will help to identify any other interactions between the automation software application and other installed software prior to deployment.

Deploy

The goal for this step is to successfully deploy the verified software update onto the computers in the manufacturing zone. The first part of this step is to communicate to users and administrators in advance about the pending update, allowing everyone to be prepared in the event of an unexpected consequence resulting from the installation. It should include a detailed schedule and process for deployment including any production downtime or off-line time that might be required.

The second part of this step is the distribution of the updates to the impacted computers. This involves moving the updates onto the individual computers (but not installing them) and then notifying the users of its availability. There are a number of automated tools available, like Microsoft Windows Server Update Service (WSUS) and Microsoft Systems Center Configuration Manager (SCCM) that can help to automate the distribution process.

The last part of this step is the application and installation of the software update. This should be handled as a manual process, not automatic. Automatic application of updates should be disabled on manufacturing assets. Some updates require computers to be rebooted and all updates can result in downtime and lost production. The installation should be scheduled for a time when the potential for lost production is minimal, and it should always be done by personnel who are trained on the equipment and process so that recovery from a failure can be handled as quickly as possible. This will also ensure that the equipment is in a safe operating state before the installation begins.

Conclusion

The convergence of manufacturing and enterprise networks has provided greater access to manufacturing data, leading to greater agility in making business decisions for manufacturers. This business agility has provided a competitive edge to manufacturers who have embraced the convergence trend.

However, network convergence also has exposed manufacturing assets to the security threats that were traditionally found in the enterprise. In the past, computers used in the manufacturing zone were not routinely patched because of their isolation from the enterprise and Internet. The increased exposure resulting from this convergence means that now, more than ever before, computers used in manufacturing need to be treated with the same level of security update rigor as those used in the enterprise.

The Rockwell Automation Security Position

Rockwell Automation recognizes the importance of maintaining security with industrial control systems. We listen to the concerns of our customers. We collaborate with appropriate government agencies. We are active in standards bodies and emerging global standards. We provide security solutions and services and we address security concerns as they relate to our solutions. First and foremost, we strive to work with our customers as a partners and help enable our customers protect their people, property and proprietary information.

Rockwell Automation's consulting team of security specialists called the Rockwell Automation Network and Security Services (NSS) team conducts security risk assessments and makes recommendations to customers for how to mitigate existing vulnerabilities and help avert potentially new ones. Information on the NSS team can be found online at http://www.rockwellautomation.com/services/security .

Rockwell Automation provides key information about control system validated designs and security best-practices to complement our recommendations for use of layered security models and defense-in-depth measures within a control system. Converged Plantwide Ethernet Architectures, a set of manufacturing focused reference architectures, provides resources, comprised of the Rockwell Automation Integrated Architecture and Cisco's Ethernet to the Factory, providing users with the foundation for success to deploy the latest technology by addressing topics relevant to both Engineering and IT professionals. Converged Plantwide Ethernet Architectures provides education, design guidance,

recommendations and best practices to help establish a robust and secure network infrastructure for manufacturing assets. These architectures can be found online at http://www.ab.com/networks/architectures.html.

Rockwell Automation also provides specific technologies, including FactoryTalk® Security and products enabled with specific security-focused capabilities as an added measure of increasing system-level security within a control system. More information can be found online at http://www.rockwellautomation.com/solutions/security/technology.html.

To Rockwell Automation, industrial security is just another important aspect of a control system's design– an aspect to be addressed with our customers as we partner to deliver an overall control system solution.

Additional Automation Security Resources

1 **Rockwell Automation Network and Security Services**
http://www.rockwellautomation.com/solutions/security/

2 **Cisco and Rockwell Automation Design & Implementation Guide (DIG)**
http://literature.rockwellautomation.com/idc/groups/literature/documents/so/enet-so001_-en-e.pdf

3 **Ethernet Design Considerations for Control System Networks**
http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

4 **Reference Architectures for Manufacturing Website**
http://www.ab.com/networks/architectures.html

5 **FactoryTalk Website**
http://www.rockwellautomation.com/rockwellsoftware/factorytalk/

6 **Reference Architectures for Manufacturing Whitepaper**
http://literature.rockwellautomation.com/idc/groups/literature/documents/wp/enet-wp004_-en-e.pdf

7 **Stratix 8000 Hardware User Manual**
http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um002_-en-e.pdf

8 **Stratix 8000 Software User Manual**
http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1783-um003_-en-e.pdf

9 **FactoryTalk Security Quick Start Guide**
http://literature.rockwellautomation.com/idc/groups/literature/documents/qs/ftsec-qs001_-en-p.pdf

10 **Rockwell Automation Knowledgebase**
http://www.rockwellautomation.com/knowledgebase/

Other Links

12 **ISA99, Industrial Automation and Control System Security**
http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

13 **Microsoft Security Updates**
http://www.microsoft.com/technet/security/current.aspx

14 **Network Infrastructure for EtherNet/IP: Introduction and Considerations**
http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00035R0_Infrastructure_Guide.pdf

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation, Vorstlaan/Boulevard du Souverain 36, 1170 Brussels, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication SECUR-WP002A-EN-E – October 2009