Recommended Practice for Patch Management of Control Systems

December 2008

Homeland Security

Control Systems Security Program

National Cyber Security Division

Recommended Practice for Patch Management of Control Systems

December 2008

DHS National Cyber Security Division
Control Systems Security Program

ACKNOWLEDGEMENT

This document was developed for the U.S. Department of Homeland Security (DHS) to provide guidance for creating a patch management program for a control systems environment. The author team consisted of Steven Tom, Dale Christiansen, and Dan Berrett from the Idaho National Laboratory.

For additional information or comments, please send inquires to the DHS Control Systems Security Program at cssp@dhs.gov

ABSTRACT

A key component in protecting a nation's critical infrastructure and key resources is the security of control systems. The term industrial control system refers to supervisory control and data acquisition, process control, distributed control, and any other systems that control, monitor, and manage the nation's critical infrastructure. Critical Infrastructure and Key Resources (CIKR) consists of electric power generators, transmission systems, transportation systems, dam and water systems, communication systems, chemical and petroleum systems, and other critical systems that cannot tolerate sudden interruptions in service. Simply stated, a control system gathers information and then performs a function based on its established parameters and the information it receives. The patch management of industrial control systems software used in CIKR is inconsistent at best and nonexistent at worst. Patches are important to resolve security vulnerabilities and functional issues. This report recommends patch management practices for consideration and deployment by industrial control systems asset owners.

CONTENTS

1. INTRODUCTION 1
1.1 Background 1

2. PATCH MANAGEMENT PROGRAM 2
2.1 Elements of a Good Patch Management Program 2
2.1.1 Configuration Management Program 2
2.1.2 Patch Management Plan 3
2.1.3 Backup/Archive Plan 3
2.1.4 Patch Testing 3
2.1.5 Incident Response Plan 4
2.1.6 Disaster Recovery Plan 4
2.1.7 Unit Patching Operations: 5
2.2 Specific Evaluation Issues 5

3. PATCHING ANALYSIS 6
3.1 Vulnerability Analysis 6
3.1.1 Deployment 8
3.1.2 Exposure 8
3.1.3 Impact 8
3.1.4 Simplicity 8
3.2 Patch Process 9

4. CONCLUSION 10

5. RECOMMENDED READING REFERENCES 10

6. WEBSITES LISTED 11

Appendix A—Issues 13

Appendix B—Unit Patch Process 18

Appendix C—Vulnerability Analysis 21

Appendix D—Acronyms & Definitions 22

Recommended Practice for Patch Management of Control Systems

1. INTRODUCTION

A single solution does not exist that adequately addresses the patch management processes of both traditional information technology (IT) data networks and industrial control systems (ICSs). While IT patching typically requires relatively frequent downtime to deploy critical patches, any sudden or unexpected downtime of ICSs can have serious operational consequences. As a result, there are more stringent requirements for patch validation prior to implementation in ICS networks. The Department of Homeland Security (DHS) Control Systems Security Program (CSSP) recognizes that control systems owners/operators should have an integrated plan that identifies a separate approach to patch management for ICS. This document specifically identifies issues and recommends practices for ICS patch management in order to strengthen overall ICS security.

1.1 Background

ICSs are deployed and used worldwide, spanning multiple industries and sectors. The advent, deployment, and maturity of universal communication protocols such as the Transmission Control Protocol/Internet Protocol (TCP/IP) allow previously isolated control systems to be easily and economically joined, thus creating large integrated systems. The rapid pace of this evolution has allowed existing IT cyber security issues to span into control systems, resulting in cross-sector issues that now affect all ICS users.

Patches for ICS, particularly legacy systems, are typically applied either late or not at all. Some legacy systems are not patched due to their service age, proprietary nature, perceived obsolescence or simply because the patches are unavailable. ICS patches have traditionally addressed functionality and stability issues within the original code rather than enhance security.

Isolated legacy systems have historically operated under the illusion of security through obscurity—if a system has not been exploited to date, why would it be targeted now? While awareness of vulnerabilities within these systems has increased, so has the interconnectivity between legacy and newer architectures. In the past, if a single ICS component on a segregated system failed, it could be easily traced, isolated, shutdown, and repaired. Today, with the advent of increased network communications, a single ICS component compromise could lead to a much larger cascading failure in adjacent networked systems by allowing unintended, exploitable access. Tracing and isolating the root cause of system failure in networked systems becomes much more difficult with failure leading to potentially far reaching consequences.

A few major issues between IT security and ICS security should to be addressed when developing a cohesive patch management plan, (see more details in Appendix A). They include:

- Network integration of ICS
- Slower patch evolution
- Differences in patch deployment
- Abandoned and unmaintained software and hardware
- Reliable patch information
- Disclosure of vulnerabilities

- Embedded commercial off-the-shelf packages.

Some industrial sectors require 99.999% or greater ICS uptime. This requirement relates to 5 minutes and 35 seconds or less allowable downtime per year for any reason, making unscheduled patching out of the question. Other industrial sectors may require patching activities at hundreds of sites, with a large number of units at each site, making a quick response difficult.

To meet these challenges, a cohesive patch management plan must be developed. This plan is most effectively created when personnel from IT, IT security, process engineering, operations, and senior management are actively involved.

2. PATCH MANAGEMENT PROGRAM

Management policies are codified as plans that direct company procedures. A good patch management program includes elements of the following plans: Configuration Management Plan, Patch Management Plan, Patch Testing, Backup/Archive Plan, Incident Response Plan, and Disaster Recovery Plan. Each of these plans requires input and approval from all affected organizations, with necessary direction and support from senior management.

2.1 Elements of a Good Patch Management Program

Several key practices or elements are recommended for any good patch management program. These elements are mentioned in the sections that follow.

2.1.1 Configuration Management Program

A configuration management program should consider the following elements:

- The asset owner should maintain a current, functional software code library containing the most recent, stable, deployed software versions used in the ICS (including configuration files for switches, routers, file servers, database servers, and printers). Controls should prevent unauthorized access or changes to operational code.
- A current hardware inventory of all control systems equipment should be maintained and made available to authorized personnel only. This inventory should be cross-referenced to the software code library.
- A current network schematic map locating wiring, junction boxes, and connections for data communications should be maintained.
- Configuration documentation including schematics and inventory lists should be controlled to prevent public or casual access. Access, including update capabilities, should be limited to authorized staff.
- An archive of at least one or more revisions of the older production code should be maintained in a separate and secure location.
- An archive of the software library, hardware inventory, current configuration, and schematics should be maintained on a separate server and in a separate physical location than the production system.
- The policies and procedures related to the configuration management plan are disseminated, reviewed, and updated on a periodic basis.
- It is recommended that a Configuration Control Board be used to monitor, authorize, and control changes to the control systems configuration.

To review additional references on the configuration management program see "Guide to Industrial Control Systems (ICS) Security," September 2008, National Institute of Standards and Technology (NIST), 800-82 Final Public Draft, Section 6.2.4, "Configuration Management." For greater detail see "Information Security," December 2007, National Institute of Standards and Technology (NIST), Special Publication 800-53, Revision 2, Appendix F-CM.

2.1.2 Patch Management Plan

Consideration should be given to several elements in the patch management plan. For example:

- Vulnerability and exposure reviews should be conducted by personnel knowledgeable of the system and its usage in conjunction with those who are accountable for those systems. These reviews should be convened to examine vulnerability and exposure when an exploit is identified, or as a preventative action when cyber security weaknesses are discovered. These personnel must have the authority to decide on the urgency of patching activities. Note: Scheduling of the activity will be a business decision.[a]
- Urgency reviews should be conducted to evaluate the risk to operations and determine if immediate action is needed (i.e., patching or implementing a work-around) or if action can be delayed or deemed unnecessary at this time.
- Deployment of patches or other modifications to the system may nullify the ICS warranty, depending on the vendor and system. Arrangements should be made with vendors to address this issue before patch deployment.

2.1.3 Backup/Archive Plan

The asset owner should maintain a current and functional backup/archive. This archive should be created and/or updated prior to any patching activities and provides a last, "good" snapshot of the functional, production system. The plan should describe:

- The frequency of the backup
- The process and functional requirements of creating the archive
- The backup verification procedures
- The backup retention period
- The physical storage (location, duplication, etc.) requirements.

2.1.4 Patch Testing

As mentioned earlier, patch testing is of special importance in control systems because of the requirement for very high uptime. The following recommendations should be included in patch testing[b]:

- Test bed/simulation hardware should be dedicated for testing purposes.
- A testing environment should be created that closely simulates the operational environment and allows for software compatibility testing.

---

a. A discussion of patch management and patch testing was written by Jason Chan titled "Essentials of Patch Management Policy and Practice," January 31, 2004, and can be found on the PatchManagement.org website, hosted by Shavlik Technologies, LLC.

b. A white paper written by Nelson Ruest in 2004 for Wise Solutions titled "A Practical Guide for Patch Testing" provides additional insight into patch testing and the general information on patch management.

- Planned tests should be conducted that verify that the patch fixes the problem (or problems) identified by the supporting organization. (This may be difficult if details are not provided by the vendor.)
- Tests should be conducted to validate that the patch does not cause conflicts with coexisting applications on the system.
- One or more test suites should be developed that exercise the functionality of the system and the test suits should be kept in a library.
- Tests should be conducted, and procedures written, to verify that the installed patch can be removed without impacting operations. (Some patches may require immediate removal if testing has been inadequate. Backing out of installed patches can be quite difficult, and plans and procedures must be developed for critical systems recovery.)
- Tests should be conducted to verify that the patched application remains functional. This could be the System Operational acceptance test (SO test), which could be used to validate operations prior to a return to service (see Unit Operations).
- Checklists and procedures should be used for patching activities to ensure both initial accuracy and repeatability of patching activities and testing.
- Records of the patch, tests, and configuration changes should be logged and documented in the configuration management record.

2.1.5 Incident Response Plan

The actions defined in the incident response plan will often initiate the patching process. Where vendors are out-of-business or do not effectively publish vulnerabilities that might affect their systems, it is necessary to find and identify incidents applicable to the ICS. Within the context of patch management, several aspects of the incident response plan can be useful, including the following:

- Define a scheduled discovery process to identify new vulnerabilities and their impact to ICS
- Identify if patches and/or workarounds are available to mitigate the vulnerability
- Establish a procedure to alert the Configuration Control Board to review the discovered vulnerability and its impact to operations
- Develop procedures to either report an incident or provide feedback on any issues discovered in the patch process.

A number of incident response organizations provide guidance and information on exploits, patches, and how to develop an effective incident response plan.[c]

2.1.6 Disaster Recovery Plan

The disaster recovery plan[d] is critical if the patch impedes system functionality and cannot be successfully removed. (In the past, this plan was designed for physical disasters; however, it can be

---

c. The National Institute of Standards and Technology (NIST) developed a Computer Security Incident Handling Guide (SP 800-61), which provides guidance to security personnel in developing an incident response procedure.

US-CERT has extensive information and reporting capabilities available for any control system security incident. This report is located at http://www.us-cert.gov/control_systems (*Control Systems Cyber Security: Defense-in-Depth Strategies*, May 2006, INL/EXT-06-11478, p. 25). US-CERT also issued an official charter for companies creating an internal incident response plan. Details of how to build the plan and the related team within your company are available at Carnegie Mellon's security response site: www.cert.org/csirts/Creating-A-CSIRT.html (*Processor*, June 1, 2007, Vol 29, Issue 22, p. 13).

ISA has developed a draft version of guidelines addressing incident planning and response, among other subjects. See ISA-d99.02.01, "Security for Industrial Automation and Control Systems," Draft 4, Edit 5, September 2008, pp. 36–37.

effective in system recovery for severe cyber attack or patch recovery, and should include planning to encompass both physical and cyber requirements.) Recommendations for the disaster recovery plan include the following:

- A good practice is to have a test bed and simulator equipped with working hardware, located at an offsite location. In addition to supporting operational testing, this facility can have a secondary mission of being available as a disaster recovery facility. It is important that functional backup/archive restoration equipment and media be available for restoration.
- It is recommended that organizations track how long it takes to restore backups or archived images as some archives may take a day or more to restore. It is also important to verify that the backup data and image restoration functions work in real-world situations. This can be tested by using the last restoration point archive to create the test bed and simulation test environment.

2.1.7 Unit Patching Operations:

An ideal situation consists of multiple identical units in production, with one or more units in standby or backup mode. This scenario allows patching activities to be conducted with negligible impact on operations. Other types of scenarios exist, such as rolling patches, sequential patches, or situations where all units must be patched simultaneously. The mechanics of how to perform these different types of unit patches can be found in sector specific documentation.[e] Also, see Appendix B for more information on unit patching. The following should be considered for unit patching:

- SO tests can be conducted on this backup/standby unit. Most SO tests have identified specific functions that must be tested to validate the code prior to a return to operations, and these tests should be documented in the configuration management record and archived as documents supporting the decision to return to operations.
- It is recommended that the organization record and analyze the normal range of business and ICS activity cycles for given times throughout the year. This is useful when making decisions on when to implement patches with the least impact on operations.

When the resources of each plan are integrated and leveraged together, they support each other, thereby maximizing their effectiveness.

2.2 Specific Evaluation Issues

As identified earlier, priority and concerns of IT, IT security, process engineering, production operations, and senior management are not the same. When an exploit is identified, all these groups must coordinate requirements and constraints to determine the level of risk associated with the vulnerability and the organizations tolerance for that risk. An analysis method is discussed in the next section, but the following general issues should to be considered when developing a patch management program:

- How vulnerable is the ICS to this threat?
- What are the potential impacts?
- What is the urgency to deploy mitigation actions (patches or work-arounds)?
- What is the effect on operations from unscheduled downtime?

---

d. A general overview of disaster recovery and related planning can be found in Chapter 11, “Preparing for Contingencies and Disasters,” in the publication “An Introduction to Computer Security: The NIST Handbook,” National Institute of Standards and Technology (NIST), Special Publication 800-12.

e. Additional information can be found in “Security Guidelines for the Petroleum Industry,” Third Edition, April 2005, copyright 2005 – American Petroleum Institute.

- What is the effect on operations from patch activities?
- What are the patch dependencies with other patches or operating system versions?
- Would no action be an acceptable action?
- Would an effective work-around provide better or more immediate temporary protection than a patch deployment?
- Can the ICS be easily and quickly segregated from the normal office data network? (These systems were originally designed to be isolated, so a return to a dedicated ICS isolated network may be acceptable in the short term.)
- Can the network be upgraded to provide better segregation of the ICS? For example, could hardware or software be upgraded to provide the needed functionality?
- Is it time to retire the old system and redesign or upgrade to a newer system?

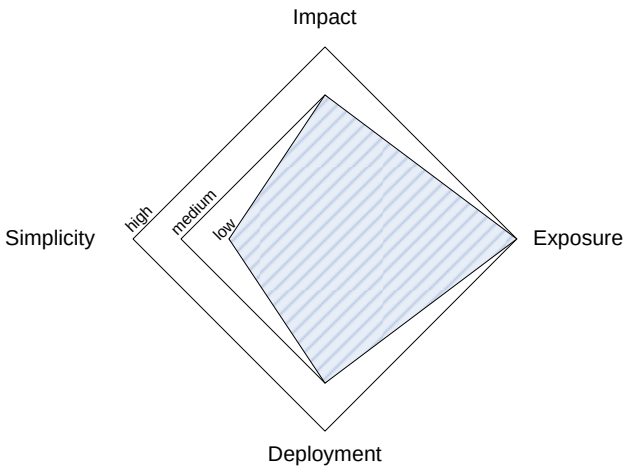
All necessary security and operational personnel should voice their issues and concerns to determine an acceptable unified method of response. The final result of this evaluation should be the recommendation to senior management to patch or not patch the ICS. This could be formally organized as a responsibility of the Configuration Control Board.

3. PATCHING ANALYSIS

3.1 Vulnerability Analysis

Vulnerability analysis, in relation to patch management, is the process of determining when and if a patch should be applied to the ICS. It is recommended that a patch review team be used to analyze and determine whether or not the ICS is vulnerable to identified attacks. A method used to determine if a control system is vulnerable to an identified attack is through the use of the “vulnerability footprint,” also known as the attack surface.

The vulnerability footprint consists of four subjective, primary elements (Impact, Exposure, Deployment, and Simplicity) that create a graphical representation of the vulnerability footprint in the shape of a diamond (see Figure 1). The larger the physical size of the footprint, the more vulnerable the ICS is to attack and the more urgent it becomes to mitigate that vulnerability. The relative shape of the diamond gives a graphical sense of key risk factors, where larger parts of the diamond correspond to a greater impact to risk. Figure 1 shows Medium Deployment, High Exposure, Medium Impact, and Low Simplicity. The highest vulnerability is Exposure from unauthenticated outside attacks.



This example is a heap-based protocol server overflow that allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted request for a WSDL file that causes a strncpy call. In this example, Deployment is Medium (other SCADA systems are vulnerable to attack from the first system), the Exposure is High (vulnerability from remote, unauthenticated attackers), the Impact is Medium (attacker can cause a denial-of-service attack), and Simplicity is Low (details of the exploit had not yet been published).

Figure 1. Example of a vulnerability footprint

US-CERT publishes a quarterly report of known vulnerabilities applicable to ICS configurations, including the vulnerability footprint. A published example of a vulnerability footprint shown in Figure 1 has typical information related to critical infrastructure control systems—in this case, a real-world recorded incident.

Asset owners can use the information provided in the Department of Homeland Security "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" as an analytical source, and apply their unique vulnerability assessment process to obtain an asset owner specific ICS vulnerability footprint. More detailed information on this analysis process and how it can be used by the asset owner is provided in Appendix C. This analytical approach is useful in understanding the vulnerability profile, and can provide a basis for prioritizing mitigation efforts.

The rest of this section describes how an asset owner can implement this process based on the following scenario:

> The asset owner has seven remote communications systems tied to industrial controls with only one of seven server systems using a vendor unique protocol. A web search for vulnerabilities relating to this protocol will list a number of sites, but references to US-CERT web pages listing Vulnerability Notes information or NIST National Vulnerability Database (NVD) Common Vulnerabilities and Exposures (CVE)-id information will provide the most reliable data. US-CERT Vulnerability Notes describe the issue, impacts, solutions, and the CVE number for that particular vulnerability. For this example we will use an actual CVE listing detailing the description, the impact to users, and the recommended solution.[f]

f. Additional US-CERT vulnerability information, which can be found in the NVD, are based on the CVE naming standard, and are organized according to severity determined by the Common Vulnerability Scoring System Version 2 (CVSSv2) standard. The division of high, medium, and low severities corresponds to the following scores:

- High—Vulnerabilities will be labeled "High" if they have a CVSS base score of 7.0–10.0
- Medium—Vulnerabilities will be labeled "Medium" if they have a CVSS base score of 4.0–6.9
- Low—Vulnerabilities will be labeled "Low" if they have a CVSS base score of 0.0–3.9.

3.1.1 Deployment

A review of the CVE-id among several informational websites reveals that users of a specific version of the protocol are vulnerable, while users of later versions are not. A quick inquiry of installed version of the protocol on the server would immediately determine whether further action is needed.

If the unaffected version is installed, all activity can stop because the vulnerability has been addressed. If an older version of the protocol is being used, it is vulnerable, and the next action is to determine the deployment risk. In this scenario, only one of the seven servers is using the vulnerable version of the protocol and a value of “Low” was assigned.

3.1.2 Exposure

Review of the US-CERT vulnerability footprint shows the Exposure value as “High” (based on unauthenticated access via the network). US-CERT data can be used to determine the ranking directly, or the asset owner can derive the ranking after reading the report. This vulnerability ranks high and requires immediate action as outside exposure means the ICS is wide open to external internet access.

3.1.3 Impact

Assuming that the ability to change general controls or set points does not exist on the system using the vulnerable protocol version, the Impact is “Medium.” Another concern with unauthenticated access is that all associated networked computer systems (for example, safety and production) are now vulnerable to cascading failure effects from this one system.

3.1.4 Simplicity

The final analysis will be to determine what skill level is needed to exploit this vulnerability. In our example, this exploit requires more advanced knowledge, so the ranking is marked as low. The vulnerability footprint for this particular asset owner configuration would now look like Figure 2, with Exposure being identified as the greatest risk factor. In this example, US-CERT would recommend that the asset owner immediately deploy an updated version of the protocol software. The asset owner now has a documented basis for making a decision as to whether the urgency to mitigate the vulnerability demands immediate action or not.

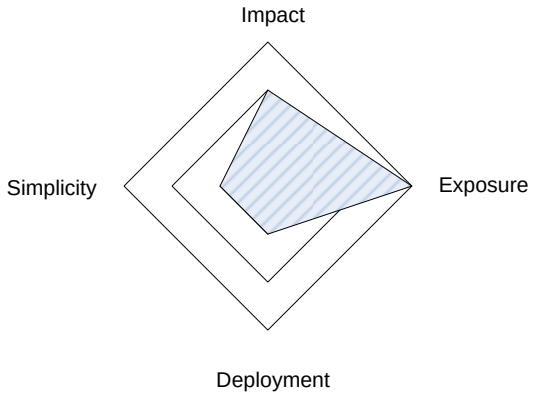


Figure 2. Specific asset owner vulnerability footprint.

The flowchart in Figure 3 shows the basic decision process in determining the urgency to patch the ICS. A documented process should be in place to monitor new exploits and vulnerabilities. When a

vulnerability and patch has been identified, the asset owner should determine if it affects any ICS in the operation. If it does affect one or more systems, then a work around or alternative action should be considered. If a work around is found, then the patch should be evaluated and scheduled as part of the regular patch cycle. If there are no work-arounds, then the patch review team will have to analyze the risk associated with the patch. Factors that are considered in the analysis include the key elements of the vulnerability footprint measured against the potential impact to the business operations. If the risk is high, then an immediate patch may be required. Conversely, if there are strong business constraints or operational concerns related to implementing the patch at a specific time, then it may be necessary to hold off on patching the system until the scheduled maintenance window. Once the patch has been implemented all applicable documentation and patch records should be updated.

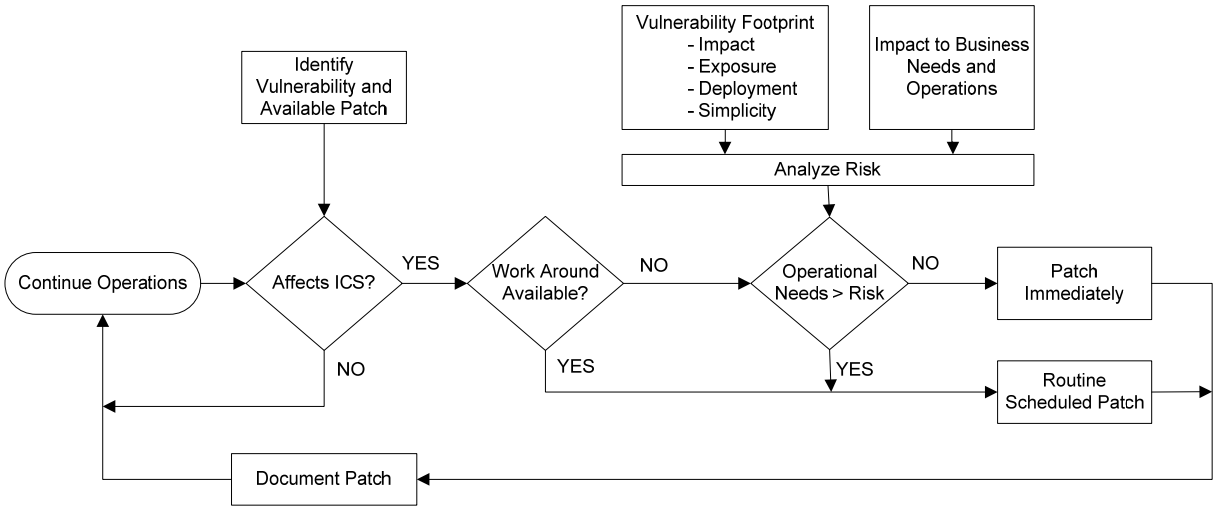


Figure 3. Patch urgency decision tree.

3.2 Patch Process

If the urgency determination requires immediate action and a work-around solution is either not available or not the best option, then the following actions should to be taken:

1. Where possible, create a backup/archive and verify its integrity by deploying it on a standby system.
2. Create a checklist/procedure for patch activities and deploy the patch on the standby system.
3. Test the patched standby system for operational functionality and compatibility with other resident applications.
4. Swap the patched standby system into production and keep the previous unpatched production system as a standby for emergency patch regression.
5. Closely monitor the patched production system for any issues not identified during testing.
6. Patch the standby system (old production) after confidence is established with the production unit.
7. Update software configuration management plan and related records.

Even though it is recommended that a standby system be in place, some sectors may not have a requirement for this system. In these cases, at a minimum, there should be a backup and archive performed that has been verified for restore capability.

If the urgency determination (risk) does not require immediate action, patching may be delayed until a more mature and tested service level patch is deployed or an alternative work around is developed. The final patch decision may be to wait until the next maintenance cycle outage occurs to update the system. Some issues to consider when making the final patch determination are:

- Can the patch be deployed at a later date within a routine maintenance window?
- Is there a work-around option that would provide adequate protection without patching?
- Does the exploit allow an intruder access into other sensitive systems?
- What is the impact if the entire system had to be reloaded using disaster recovery backup procedures?
- Does the affected system have to remain in continuous operation?
- Is this a critical system that supports life, health, or commerce?
- Are other operational modes (e.g., manual) available?

If the internal staff lacks training, experience, and expertise in evaluating and deploying patches, using the services of a managed software service provider may be a more cost effective approach. There are several managed software service providers who, as contractors, conduct the tasks of patching, configuring, deploying, and restoring systems. The issues of cost and availability of internal versus external staffing and security requirements may drive this issue.

A detailed explanation of the patch process is provided in Appendix B.

4. CONCLUSION

The issue of timely ICS security patching is a serious cross-sector issue. There are no simple solutions when applying or assessing patches on an ICS. The first critical step in resolving these issues is to initiate open communications between IT, IT security, process engineering, production, and senior management. Only then will major stakeholders be aware of all concerns confronting cyber security issues allowing a coherent path forward to be created. This document has identified resources that provide additional information on cyber threats, vulnerabilities, self-assessment tools and recommended practices that may be used to incorporate ICS patch management processes into existing IT security plans.

5. RECOMMENDED READING REFERENCES

1. "Security Guidelines for the Petroleum Industry," Third Edition, April 2005, copyright 2005, American Petroleum Institute.
2. "Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition," American Petroleum Institute/National Petrochemical and Refiners Association, October 2004.
3. J. Stamp, P. Campbell, J. DePoy, J. Dillinger, and W. Young, "Sustainable Security for Infrastructure SCADA," White Paper, Sandia National Laboratory, viewed November 12, 2008 at http://www.tswg.gov/subgroups/ps/infrastructure-protection/documents/SustainableSecurity.pdf.
4. "IT Governance—Practical Case using CobiT QuickStart," *Greet Volders*, Journal On-Line, copyright 2005 by Information Systems Audit and Control Association Inc. ISCA Information System Control Association.
5. "Utility Customer Concerns," proprietary information—not for public dissemination.
7. "Recommend Practice Case Study: Cross-Site Scripting," February 2007, Homeland Security, National Cyber Security Division, Control Systems Security Program.

8. William Rush and Aakash Shah, “Impact of Information Security Systems On Real-Time Process Control,” NIST Project SB1341-02-C-0081, Gas Technology Institute, GTI Project numbers 61160 and 15335.1.01 and FERC Project Numbers 30802-05 and 15063.1.01.

9. Prepared by Energetics Incorporated, “Roadmap to Secure Control Systems in the Energy Sector,” U.S. Department of Energy and U.S. Department of Homeland Security, January 2006.

10. “Roadmap to Secure Control Systems in the Energy Sector,” Energy Sector Control Systems Working Group, *ieRoadmap Workshop*, May 2008.

11. Troy Nash, “Backdoors and Holes in Network Perimeters—A Case Study for Improving Your Control System Security, Vol 1.1,” August 2005, Vulnerability and Risk Assessment Program, Lawrence Livermore National Laboratory, UCRL-MI-215398.

12. “DHS Bulletin: Securing Control Systems,” Cyber Security Research Department, February 11, 2005.

13. Jason Chan, “Essentials of Patch Management Policy and Practice,” January 31, 2004, on PatchManagement.org website, hosted by Shavlik Technologies, LLC.

14. Ian Green, “DNS Spoofing by The Man In The Middle—GSEC Practical Assignment (Version 1.4c - option 1),” January 10, 2005, SANS Institute 2005, Exposing how the Windows XP DNS resolver vulnerabilities can be exploited, and how to harden network protocols.

15. “Web Servers, Application and OPC-UA - A Study in Control Systems and Cyber Security,” Michael Clark, June 2007, INL Control Systems Security Center - Cyber Security Division.

16. “A Strategic Approach to Protecting SCADA and Process Control Systems,” IBM Global Services, July 2007, IBM Internet Security Systems, Inc.

17. “Good Practice Guide—Process Control and SCADA Security,” National Infrastructure Security Coordination Centre, PA Consulting Group.

18. Larry Seltzer, “Beware Fake Malware Cleaner Programs,” *PC Magazine*, Security Watch, Sunday July 27, 2008.

19. *Processor magazine* (June 1, 2007, Vol 29, Issue 22, page 13) used in incident response plan.

20. “Information Security,” December 2007, National Institute of Standards and Technology (NIST), Special Publication 800-53, Revision 2

21. Nelson Ruest, “A Practical Guide for Patch Testing,” “A Report by Wise Solutions,” 2004.

22. “An Introduction to Computer Security: The NIST Handbook,” National Institute of Standards and Technology (NIST), Special Publication 800-12

6. WEBSITES LISTED

http://www.kb.cert.org/vuls/. US-CERT vulnerability Notes Database; current data on exploits, vulnerabilities, and resolutions.

http://nvd.nist.gov/home.cfm. National Vulnerability Database is the U.S. Government repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g., Federal Information Security Management Act).

http://www.cert.org/other_sources/viruses.html. Computer virus resources hosted by Software Engineering Institute and Carnegie Mellon for US-CERT.

http://www.us-cert.gov/cas/tips/ST04-009.html. US-CERT website National Cyber Alert System (Cyber Security Tip ST04-009) Identifying Hoaxes and Urban Legends, this site also lists recommended websites specializing in validating information on hoaxes and urban legends.

http://www.us-cert.gov/control_systems/index.html. US-CERT CSSP homepage, containing information on cyber threats, vulnerabilities, self-assessment tools, and recommended practices.

http://csrp.inl.gov/Introduction.html. US-CERT recommended practices web page.

http://www.ciac.org/ciac/index.html. Computer Incident Advisory Capability (CIAC) has been providing the U.S. Department of Energy with incident response, reporting, and tracking, along with other computer security support since 1989. CIAC is a founding member of Government FIRST and FIRST an international incident response and security organization.

http://vil.mcafee.com/hoax.asp. Security firm McAfee lists information on viruses, fixes, and patches. This particular site lists a number of computer hoaxes in circulation. McAfee cautions that while some issues originate as hoaxes, they can be repackaged to deploy exploits.

http://www.snopes.com/computer/virus/virus.htm. Urban legends and some virus information.

http://cve.mitre.org/about/index.html. CVE Website.

http://csrc.nist.gov/groups/SMA/fisma/index.html. National Institute of Standards and Technology, Computer Security Division, and Computer Security Resource Center homepage.

http://nvd.nist.gov/cvss.cfm?version=2. CVSSv2 website.

http://www.cert.org/csirts/Creating-A-CSIRT.html. CERT Computer Security Incident Response Team process.

http://www.sgi.com/support/security/. FIRST member that tracks and identifies vulnerabilities, patches, and other incident response teams.

http://technet.microsoft.com/en-us/security/bb977553.aspx. Microsoft website that contains a number of security and compliance guides. Covers client, server, network and general security planning and guidance for recommended cyber security.

http://www.microsoft.com/technet/security/current.aspx. Microsoft security bulletin search page. Find general and technical information about released Microsoft patches relating to vulnerability, update, detection, deployment tools and guidance as well as CVE references.

Appendix A—Issues

The cyber security and operational issues that should be considered in developing a cohesive patch management plan include: network integration of industrial control systems, slower patch evolution, differences between information technology (IT) and industrial control system (ICS) patch deployment cycles, abandoned and unmaintained software and hardware, impact to system operations, impact to support mechanisms, impact to vendor warranties and support, reliability of patch/vulnerability information, and the disclosure of vulnerabilities.

The organization most frequently tasked with patching activities is the IT department, which provides ICS cyber security support. It typically delegates ICS patching responsibilities to process engineering departments. Many IT and control systems departments identify funding and resources as limiting factors to maintaining a dedicated ICS test bed/simulator facility. As an alternative to in-house simulators, ICS vendors are now offering test bed simulations as part of the services they provide.

Because maintenance windows are small and approval to patch is difficult to get, the need for testing patches and verifying stability on a test bed/simulator before installation is significant. As a result of these issues, ICS patches tend to be applied late or not at all for fear of causing unscheduled downtime.

The lack of communications between IT, IT security, process engineering, and senior management, concerning ICS security, can contribute to lack of understanding and awareness of the patch management process leading to slow ICS patch implementation. Asset owners with excellent intradepartmental communications tend to have more proactive patching programs in place and see patching activities as preventative maintenance to their manufacturing process.

IT departments tend to focus primarily on data and defense-in-depth from unauthorized intruders from outside the outer protection perimeter. Traditional IT defenses consist of firewalls, intrusion detection systems/intrusion protection systems, routing access control lists, workstation and server policies, antivirus and other host based protection technologies, limited user privileges, and robust patch management programs. The primary focus is to keep unauthorized individuals from accessing corporate cyber systems, stealing or corrupting data and resources, and causing malicious system behavior. However, some ICS operations utilize additional communication channels (modems/WAN access), or other protective equipment that IT departments may not be aware of or may not have configured or deployed correctly. Traditional IT security priorities are based on Confidentiality (authorized access), Integrity (accuracy of data), and Availability (system uptime), which does not necessarily translate to the priorities of ICS.

ICS operations are discovering that standard IT security patching and upgrade activities are frequently incompatible with operational concerns. For example, standard IT security activities may require reboot cycles that can cause ICS failure. Many ICS operations demand 99.999% or greater operation/availability uptime. This requirement implies that downtime due to scheduled or unscheduled patching/upgrades activities becomes unacceptable. Security priorities for ICSs are typically Availability, Integrity, then Confidentiality, which is the inverse of traditional IT priorities.

Network Integration of Industrial Control Systems

Most existing legacy ICS were designed as proprietary, robust, stand-alone systems, with the highest priority being reliability and longevity. Most were not designed with integrated network access control and security capabilities. These legacy systems met, or are now meeting, their original design considerations of reliability and longevity (20–30 years in some cases) and will continue to function until reaching end-of-life failure (mechanical, technical, or economic). Improvements and advances in data

communications and interoperability have allowed isolated systems to be integrated into large control systems, thus increasing the life of stand-alone legacy systems far beyond their original design. The main drivers of this effort have been reduced cost and increased efficiency through automation. Due to this increased longevity, ICS configurations continue to operate, often using old, unsupported software.

Slower Patch Evolution

The exposure and impact of ICS security exploits have raised awareness to the extent that newer ICS vendors are mitigating vulnerabilities by increasing the frequency, testing, and deployment of patches, thus securing the ICS against new exploits. However, patches for ICS legacy components, which have traditionally focused on resolving operational issues rather than security issues, are being developed at a much slower rate than new ICS. Some factors that contribute to the lack of legacy ICS patching are as follows:

- ICS-specific vulnerabilities are not fully understood or widely known
- Original equipment manufacturers (OEMs) no longer support some legacy systems
- Asset owners may not have renewed service level agreements with OEM on legacy systems
- Asset owners and vendors may not be aware of embedded ICS vulnerabilities
- OEM and asset owners may lack the experience or knowledge to create and test security patches
- ICS patches require extensive operational testing prior to deployment to verify functional operation and compatibility with coexisting applications
- Funds and resources may not be available to resolve known vulnerabilities
- Some patches may have problems because of configuration and compatibility issues with obsolete unsupported operating systems
- Operational demands impact the allowable maintenance window for patch deployment.

Differences in Patch Deployment

ICS patching is different from desktop IT systems in several ways. Typically, ICS cannot support unscheduled service interruptions, and when they are scheduled for maintenance and patching, these interruptions are often short and may occur only once over a multiyear cycle. ICS patches must therefore have extensive operational testing before being deployed and have an approved maintenance window before being granted approval to proceed with the actual patching evolution. In some sectors, vendors have provided extensive testing assistance to asset owners; in other cases, patching a system may jeopardize contractual agreements.

Many companies incorrectly assign all computer patch management responsibilities to the IT department with the expectation that all cyber security related operational issues will be addressed. For the reasons stated above, this may not be a good practice because IT, IT Security, process engineers, and production operations have different priorities as well as different functional requirements. It is important that IT departments share cyber security responsibilities with other stakeholders. Some reasons include:

- Standard office IT policies frequently automate nightly patch/software upgrade deployment on desktop systems, requiring frequent rebooting, which may not be consistent with ICS operational requirements.
- Urgent, IT office-type, patches sometimes require immediate unscheduled shutdown and deployment.

- IT patches may or may not be tested for functionality and compatibility with legacy systems deployed in the ICS environment or with collocated applications. For example severe ICS disruptions occurred when Microsoft Windows XP, Service Pack 2 was deployed.

There are many incident organizations, such as United States Computer Emergency Readiness Team (US-CERT), Army CERT (ACERT), Air Force CERT (AFCERT), and Forum of Incident Response and Security Teams (FIRST), which are becoming aware of the differences ICS presents to cyber security. However, regulations and these support organizations specializing in IT security are not uniformly addressing cyber issues and resolutions on ICS security. US-CERT supports and documents recommended practices for ICS security (http://csrp.inl.gov/Introduction.html), which are located on the US-CERT Control Systems Security Program (CSSP) website (http://www.us-cert.gov/control_systems/index.html).

Abandoned and Unmaintained Software and Hardware

Legacy systems also have issues when OEM ICS component companies cease to exist and support for these systems becomes problematic. Over time, older systems are frequently removed from software and hardware maintenance, thereby removing legal access to software and hardware upgrades and patches. Return-to-service fees can be expensive, if available, and both IT and the process engineers may not have the expertise to maintain legacy systems.

A common misconception is to inherently trust patches from the OEM without verification. If the OEM is not known or unavailable, or the ICS component contains hidden features or functions, the responsibility for timely patches and issue resolution is unclear. As new vulnerabilities on these unsupported systems are identified, creating, testing, and issuing patches and acquiring financial and legal responsibilities associated with third party patches can be problematic, if available.

Third party vendors provide valuable patching services and expertise, but new issues of unscrupulous entities packaging malware with legitimate patches is emerging. Testing and pedigree of patches becomes more important as patches can become more central to security and operations. In some cases it may be more economical to remove the existing system from service and upgrade or replace it than to obtain, test, verify, and deploy third party patches.

Reliable Patch Information

Understanding and knowing the components within the production ICS is important when assessing system vulnerability and exposure. The issue is to understand and recognize the need for a patch and then formulate the proper response.

IT administrators frequently use a number of websites in addition to OEM notices to verify if virus/patch alerts are legitimate:

- http://www.us-cert.gov/cas/tips/ST04-009.html,
- http://www.ciac.org/ciac/index.html
- http://vil.mcafee.com/hoax.asp
- http://www.snopes.com/computer/virus/virus.htm.

ICS asset owners can use similar sources of currently known vulnerabilities and mitigation resolutions published and maintained in US-CERT's Vulnerability Notes. These sites contain reliable information about known exploits, validated and recommended resolutions, and/or patch locations. In particular, CVE Control System information is available in the National Vulnerability Database (NVD).

The ICS websites are as follows:

- http://www.kb.cert.org/vuls/
- http://www.cert.org/other_sources/viruses.html
- http://nvd.nist.gov/home.cfm

Disclosure of Vulnerabilities

In an ideal situation, security researchers or ICS users would, upon discovering a security vulnerability, contact and disclose it to the vendor. The vendor would then act immediately to resolve the vulnerability by creating and thoroughly testing a patch, and then disseminate the patch to the vendor's customers. In actual practice, some vendors are not responsive and vulnerabilities may remain in the ICS indefinitely. As a result, security researcher may publish the exploit in an attempt to cause the vendors to address the vulnerability.

The timely public disclosure of vulnerabilities constitutes a double-edged sword. While public alerts of vulnerabilities in exposed systems motivate asset owners and vendors to address these issues, these alerts also flag potential attackers that system vulnerabilities exist. This allows attackers a window of opportunity to act immediately, while the asset owners need time to evaluate the vulnerability, resolve the issue, and test the patch.

This dilemma can be addressed as asset owners demand action from vendors to resolve issues as soon as they are disclosed. As the vendors do so, there will be no need for public disclosure resulting in increased security provided by timely patches and a lack of public awareness of the vulnerability.[g]

Embedded Commercial Off-the-Shelf Software

Asset owners rarely know exactly what embedded components and services exist inside their control systems. The current business trend is to use commercial off-the-shelf (COTS) products and standard operating systems whenever possible to simplify maintenance, operations, and procurement costs. Newer COTS product components are frequently delivered with unknown and undocumented services, such as FTP and web-based maintenance, which can provide unknown access points for an exploit. In some older systems, a common password was included in the device that cannot be changed. In some newer systems, asset owners do not change default passwords even though the ability exists.

Most ICS components use real-time operating systems (RTOS), which are small, simple computer systems intended for real-time applications. The use of these simple components is widespread, and they are in common use in control system architectures. A few examples include: pressure control valves, voltage regulator, programmable thermostats, appliance controllers, industrial controls and scientific research equipment (legacy oscilloscopes). The complexity of components with these embedded systems range from simple single-processor chips to very high numbers of integrated units within a single component.

A correctly configured component should only run necessary tasks specified by the operation, but older legacy systems may have any number of active unused services that may not be disabled or blocked. These active unused services and communications ports within the ICS component present a cyber security issue. Most ICS devices that can communicate or allow upgrade of its firmware code must contain an embedded RTOS. It is impossible to patch and secure ICS components if embedded

---

g. US-CERT does provide guidance on ICS vulnerabilities located at http://www.us-cert.gov/control_systems/csvuls.html.

capabilities are not known or understood by the cyber security team. In addition, embedded capabilities of ICS components are not typically addressed in an asset owner's operational configuration security review.

Embedded COTS applications that exist within custom solutions present an additional level of complexity. They may require patches that are incompatible with the custom application, causing the component to fail. This requires a greater degree of awareness, testing, and planning in the patch management process.

Vendor Involvement

In many cases, patching or modifying of ICS components without notifying and/or involving the vendor can nullify the system warranty. In the process of patch planning, the issues of warranty, vendor responsibilities, and liabilities must be considered. Ideally, a "trusted" relationship with the vendor should be established to address both anticipated and unanticipated patching issues.

Appendix B—Unit Patch Process

A vulnerability must be reviewed by information technology (IT), IT security, process engineering, operations, and senior management (Configuration Control Board or CCB) to determine if there is an immediate need to patch the industrial control system (ICS). If the decision is made not to patch at this time, patch planning/testing documentation should be maintained to support future patch planning.

The information that follows provides an example of the steps to take in an ideal situation. There are other approaches available, depending on the sector requirements, ICS architecture, operational needs, and type of patching (other types include rolling, sequential, and simultaneous).

System Patching

If the CCB approves the maintenance window for this activity, proceed with the patch. If an asset owner has a redundant ICS with units in cold or hot standby status, it is always recommended to patch the cold standby units first.

- ***Backup or Standby Units.*** A good practice would be to have one or more completely identical systems located at separate locations cycling between operational, standby, and backup status. If redundant standby units are not available, the next best option is to have a working, stable software backup or archive and a representative test bed available for patch testing. If a test bed is not available, it becomes absolutely essential to have a working backup or archive system in place before any patch activities take place. This archive is the last chance to create a known recovery point of the stable operational environment. In the event that none of the recommended options are available, the alternative is to patch on the operational system, which may be an acceptable risk-based approach to mitigate the vulnerability. The criticality of the system being patched and its downtime tolerance must be carefully considered before patching directly on the production system.
- ***Backup Patch.*** In the event of multiple redundant systems, an approved and tested patch should be applied first to the units not in production. For organizations that have multiple production units, the recommended patch management process is to patch the backup units prior to patching the production or hot standby units. The normal risk management process is to minimize the risk prior to implementation on the production unit.
- ***Operational Stability.*** Organizations should establish criteria for benchmarking stability. Based upon this established criteria, the newly patched system must be monitored and evaluated for stable operations. The previous unpatched operational unit should not be patched at this time, serving as an emergency standby unit.
- ***Production.*** After the operational criterion is achieved in establishing production stability on the backup system, the organization is now ready to implement the patch on the production unit. The original production unit should then be patched and tested, now becoming the backup to the operational production system (see Figure C-1). The final step is to document and update the configuration management plan to include system modifications and the deployed patch update information.

A sample flow chart identifying patching operations is presented in Figure C-1.

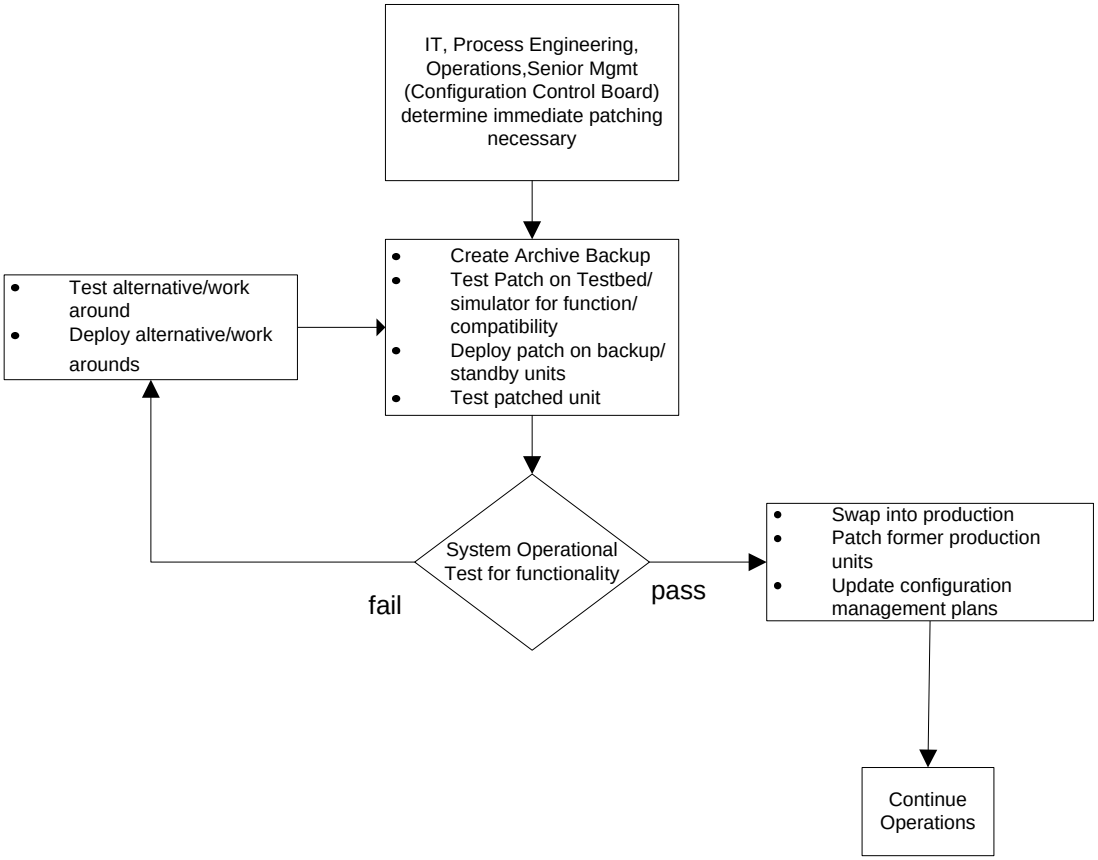


Figure C-1. Flow chart of patching operations.

Issues to Consider

The following issues should be considered when creating the patch management plan and the processes and policies related to it:

- ***Testing***. It is always recommended that organizations duplicate the operations environment with absolute functional fidelity, but issues associated with component cost and test space may limit the ability of the organization to have a fully functional test unit. For some scenarios it is adequate to simulate application functions without absolute system replication fidelity. For example, testing nuclear reactor safety systems or flight control systems demands more fidelity than simulating facility heating, ventilation, air conditioning systems or simpler ICS applications. The primary function of a test bed/simulator is to mitigate risk prior to implementing changes to the operational environment. An additional benefit from a test bed/simulator is to allow operator training on new configurations, develop checklists, and evaluate procedures prior to deployment on production systems.
- ***Archiving.*** An archive image or data backup of the existing stable operating system should be captured before production patching is conducted to create a valid restoration point. It is recommended that the organization backup the operational system and restore it on the test bed/simulator system. This activity helps validate that the restore point is usable for disaster recovery. Backup/archiving is frequently done in operations, but the attempt to restore this backup to a working stable environment is frequently only done when needed in a disaster.
- ***Rollback***. Depending upon the patch, a contingency plan should be developed in the event the patching process corrupts the existing stable environment. On legacy systems and new ICS patch

failure or incomplete patching activities can cause expensive physical damage to equipment. A recommended contingency practice is to create a recovery point by archiving/imaging the current stable system as part of a backup/disaster recovery plan. The organization would then develop and test uninstall activities and have hardware spares identified and available (such as power supplies, system motherboards, hard drives, communication switch boards, etc.) depending on the criticality of the system.

- ***Contingency***. Organizations should consider the worst case scenario in developing contingencies. Assuming a worst-case scenario where patch installation does not restore the system to a stable condition or patch installation and/or removal activity affects other applications, determine if the disaster recovery point restores the system to a stable configuration. An organization should establish criteria based upon the systems functionality over a specific duration that incorporates timing considerations. It is recommended that organizations know if a patch can be safely and quickly removed and how long this evolution takes as a contingency measure.

A final system operational test plan should be developed to exercise, validate, and document all important identified operational and functional testing points of all primary applications running in the same environment. This is to ensure stable functional system operations prior to a return to service.

Appendix C—Vulnerability Analysis

The following elements define the vulnerability footprint and can be used by industrial control system (ICS) asset owners in determining the vulnerability of their specific ICS configurations:

- ***Deployment***. This element rating gives the relative proportion of control systems installations having critical infrastructure and key resources thought to contain vulnerable configurations at one site. A high rating would indicate all, or at least a high number, of deployed ICS at the asset owner's site are affected. A low rating indicates that only a few minor systems are exposed. This rating is important in that the answer provides an immediate yes or no determination of whether patching should be done—does this vulnerability affect the asset owner's ICS or not?
- ***Exposure***. This element rating ranks available layers of defense such as defense-in-depth and existing adequate barriers (the exploit affects the asset owner's ICS and is readily available to attackers). A high exposure rating indicates that an attacker can gain unauthenticated access to the ICS from another less-secure network within the control systems perimeter. A medium rating indicates that an attacker can gain unauthenticated remote access. A low rating indicates that an attacker can only gain authenticated physical machine/network access. Exposure of the ICS to unauthorized access presents significant risk.
- ***Impact***. A high impact element rating indicates that an exploit is successfully deployed into the wild and an attacker can gain full system control. A medium rating indicates that an attacker can obtain limited access or gain enough information to launch a denial-of-service attack. A low rating indicates that an attacker gains enough information for a preliminary reconnaissance effort on a target system's architecture. Part of the impact assessment must consider cascade effects on safety and protection devices. The initial penetration may not be immediately significant, but safety and production components could be disabled in the same system due to cascade effects from exhaustion of computer resources.
- ***Simplicity***. This rating applies to relative ease of the technical exploit. A high rating indicates an exploit that is written, available, and only requires average or basic computer skills to use (e.g., a public script is available to implement the exploit). A medium rating indicates that a vulnerability exists, but original work needs to be done to use the exploit. A low rating indicates that the exploit requires a high level of computer skill and subject matter knowledge.

The "Quarterly Report on Cyber Vulnerabilities of Potential Risk to Control Systems" is prepared by Idaho National Laboratory for the Department of Homeland Security Control Systems Security Program. This report provides detailed information, such as identification, vulnerability footprint, description, analysis of known exploits and recommended remediation information. The abstract of this report gives a summary of the numbers of known vulnerabilities published. For instance, the second quarter of 2007, US-CERT[h] report reported publishing information on 1,498 computer security vulnerabilities. Eighty-six of these were significant to the Critical Infrastructure and Key Resources sector, based on the types of software applications used in these environments. Thirteen were of high significance based upon the fact that these vulnerabilities represented substantial opportunities for attack against applications commonly used in the sector. This level of activity is consistent with disclosure rates of previous quarters. This report can be obtained through the Control Systems US-CERT Secure Portal or by specific email requests to cssp@dhs.gov.

h. http://www.us-cert.gov/cas/bulletins/SB08-203.html—Cyber Security Bulletin SB08-203, July 14, 2008

Appendix D—Acronyms & Definitions

ACRONYMS

ACERT	Army Computer Emergency Readiness Team
AFCERT	Air Force Computer Emergency Readiness Team
AIC	availability, integrity, and confidentiality
CERT	Computer Emergency Readiness Team
CIA	confidentiality, integrity, and availability
CIAC	Computer Incident Advisory Capability
CI/KR	Critical Infrastructure/Key Resources
COTS	commercial off-the-shelf
CSSP	Control System Security Program
CVE	Common Vulnerabilities and Exposures
CVSSv2	Common Vulnerability Scoring System Version 2
DCS	distributed control system
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DNS	domain name services
DOE	Department of Energy
FIRST	Forum of Incident Response and Security Teams
FTP	File Transfer Protocol
IAC	integrity, availability, and confidentiality
ICCP	Inter-Control Center Communications Protocol—IEC 60870-6/TASE.2
ICS	industrial control system
INL	Idaho National Laboratory
IRP	Incident Response Plan
IT	information technology
NVD	National Vulnerability Database
OEM	original equipment manufacturer
RTOS	real-time operating system
SCADA	Supervisory Control and Data Acquisition
SO	system operation
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
US-CERT	United States Computer Emergency Readiness Team

GLOSSARY

Availability, Integrity and Confidentiality (AIC). AIC represents the typical priorities of ICS operations, where system availability and uptime has the highest priority at the expense of data integrity and confidentiality.

Asset Owner. The owner and operator of industrial control systems.

Confidentiality, integrity, and availability (CIA)/ availability, integrity, and confidentiality (AIC). Traditional IT priorities where data confidentiality has the highest priority. Systems will be shutdown immediately to maintain data confidentiality at the expense of system integrity and availability.

Common vulnerabilities and exposures. A diction of common names for publicly known information security vulnerabilities, while its common configuration enumeration provides identifiers for security configuration issues and exposures.

Common Vulnerability Scoring System Version 2 (CVSSv2). An open framework for communicating the characteristics and impacts of IT vulnerabilities.

Deployment. Refers to whether a vulnerable characteristic has been identified, readily available and can affect any part of the asset owners industrial control system.

Exposure. Refers to what access is needed to attack the process control system; high exposure indicates the system is very easy to attack and low exposure indicates physical access would be required to attack the system.

Hacker. A computer user who specializes in exploiting vulnerabilities in computer systems to obtain unauthorized access.

Impact. The determination of what the impact is if an attacker is successful; high impact indicates the attacker gains full control; low impact indicates attacker gains limited rights (enough to cause a denial-of-service type attack).

Inter-Control Center Communications Protocol (ICCP) Network. The ICCP network is being specified by utility organizations throughout the world to provide data exchange over Wide Area Networks between utility control centers, utilities, power pools, regional control centers, and nonutility generators. ICCP is also an international standard known as IEC 60870-6/TASE.2.

National Vulnerability Database (NVD). The U.S. Government repository of standards-based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g., Federal Information Security Management Act).

RTOS (Real Time Operating System). Multitasking operating system intended for real-time applications such as programmable thermostats, robots, instrumentation controllers and scientific research systems (oscilloscopes). Typical designs have three states: running, ready, blocked.

Simplicity. The relative ease of technical exploitation. Readily available written scripts that utilize exploits that can be used by any computer user are considered a high risk. Exploits requiring significant technical skills by sophisticated users are rated a low risk.

Threat. An identified person with the means, intent, and motivation to cause damage to a cyber system.