



## How Wonderware Software Helps with NERC Critical Infrastructure Protection Standards

Eduardo Ballina,  
Wonderware Geo-SCADA Industry Manager

With the approaching milestone dates to meet regulatory compliance, significant attention in the Electrical Industry is being focused on the Critical Infrastructure Protection (CIP) standards introduced by **NERC**, the **North American Electric Reliability Corporation**. This Whitepaper will explain how Wonderware software helps to enforce CIP standards to create compliant end-user applications.

NERC's mission is to ensure the reliability of the bulk power system in North America. It oversees eight regional reliability entities and encompasses all of the interconnected power systems of the contiguous United States and Canada. It also has influence over Mexican systems in the Baja California area connected to the Western Interconnect, although it is not considered the "Electric Reliability Organization (ERO)" for Mexico. In the USA, NERC is subject to oversight by the U.S. Federal Energy Regulatory Commission. In Canada it is subject to the oversight of the corresponding Canadian governmental authorities.

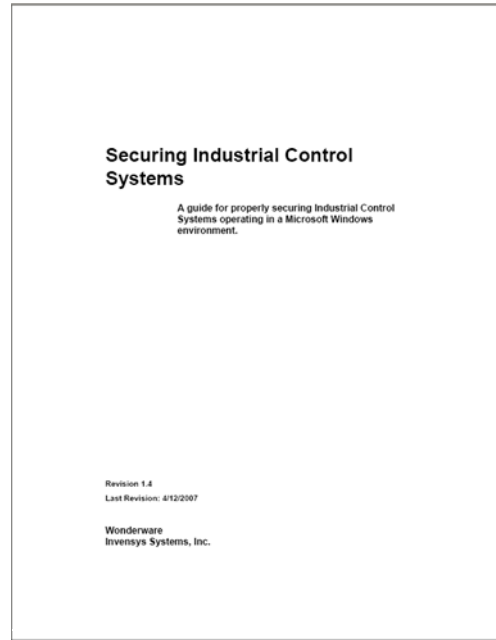
NERC CIP standards apply to bulk power systems in the North American Electric Industry only. These standards apply to critical cyber assets in every phase of a power system including generation, transmission and distribution. It is important to note that these standards are not limited to the SCADA portions of these systems but rather apply to critical infrastructure and related policies, procedures and practices through the entire operation.

### **Is Wonderware Software NERC CIP Compliant?**

While Wonderware software and tools provide features and functionality intended to help in achieving compliance with NERC CIP-002 through CIP-009, it is the resulting application and the entire system which must be CIP compliant rather than the base software itself.

That said, Wonderware software offers features and functionality that may assist in creating applications that can comply with the sections relevant to SCADA/HMI software in the NERC CIP-002 through CIP-009 standards.

Additionally, Wonderware has a security guidelines document entitled "Securing Industrial Control Systems" available for download from our Wonderware Security Central website which provides advice on the use of Wonderware software in critical infrastructure environments requiring cyber security consistent with NERC CIP and other cyber security standards.



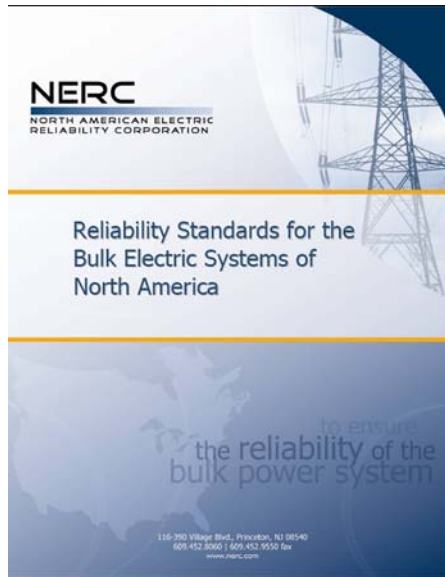
## **Do All Aspects of the CIP-002 Through CIP-009 Apply to a Wonderware-based Application?**

NERC CIP standards cover different security related aspects which are complementary and must be observed by *the responsible entity* as a set. In this sense, text in the standards requires that each one of them be read as part of a group of standards numbered CIP-002 through CIP-009.

In many areas, compliance with NERC CIP standards goes well beyond SCADA software and covers aspects such as personnel and training, physical security, incident reporting, incident response plans, etc. that the responsible entity must ensure are implemented and enforced. Only certain sections of the standards apply directly to the actual software implementation of Wonderware based systems. Full compliance of the NERC-CIP 002 through 009 standards requires not only proper engineering and implementation of the software solution but any additional measures required to meet the complete set of standards.

For a summarized list of the NERC CIP standards, see 'Appendix A' in this document. For more detailed information, see the document entitled "*Reliability Standards for the Bulk Electric Systems of North America*" by NERC:

[http://www.nerc.com/files/Reliability\\_Standards\\_Complete\\_Set\\_2009Feb25.pdf](http://www.nerc.com/files/Reliability_Standards_Complete_Set_2009Feb25.pdf) <sup>1</sup>



---

<sup>1</sup> Look for the latest version at [www.nerc.com](http://www.nerc.com). The actual name of the file may change, since this document is updated from time to time.

## Who is Responsible for Compliance?

The CIP standards indicate that the ultimate responsibility to achieve and maintain compliance with the CIP-002 through CIP-009 lies on the power utilities and associated organizations. Specifically, the text of CIP-002 through CIP-009 lists some or all of the entities below as a “*Responsible Entity*”, depending on the specific CIP standard:

- Reliability Coordinator,
- Balancing Authority,
- Interchange Authority,
- Transmission Service Provider,
- Transmission Owner,
- Transmission Operator,
- Generator Owner,
- Generator Operator,
- Load Serving Entity,
- NERC,
- Regional Reliability Organizations.

This being said, a responsible entity may choose to request a vendor (i.e. Engineering Firm, System Integrator, OEM, VAR) to provide certain functionality in a finished system or may choose to do so themselves. For example, they may choose to have the implementer install anti-virus in a bundled system prior to delivery or may choose for the company’s own IT department to install it. Either way, the responsible entity must ensure that this takes place one way or the other in order to assure compliance.

The standards also provide some room for decision making to accommodate the reality of a business environment: “*The standards Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.*”

### CIP-002 through CIP-009 Requirements

The following section summarizes general aspects of CIP-002 through CIP-009 and expands on a number of requirements most relevant to SCADA applications such as Wonderware-based systems. It also describes a number of related features and functions in Wonderware software that can be used in the design and

implementation of related applications. The complete text of NERC's Critical Infrastructure Protection standards is available online from the NERC website:

<http://www.nerc.com/page.php?cid=2%7C20>

### **CIP-002 Cyber Security — Critical Cyber Asset Identification**

Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

This activity is led by the responsible entity with or without the assistance of a consulting firm.

### **CIP-003 Cyber Security — Security Management Controls**

Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

Compliance with this standard involves primarily the responsible entity creating, maintaining and documenting a security policy which includes –amongst other things- identifying information to be protected (topology, disaster recovery plans, equipment layouts, etc.), a leadership team, access control to this information, etc.

A section relevant to Wonderware-based applications is requirement **R6 - Change Control and Configuration Management**: *“The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.”*

The Wonderware Integrated Development Environment (IDE) includes functionality to enable managed access control for modifications to the application as well as a log that enables tracking of changes to the application.

The Wonderware IDE can not only be used with Wonderware System Platform-based systems but also with Wonderware InTouch® HMI-based systems in order to leverage application management and change control.

Another option for InTouch-based systems (versions 9.0 and prior) is the use of third-party source management tools, such as the product called AutoSave from MDT Software.

[http://www.mdtsoft.com/products/autosave/pdfs/wonderware\\_in\\_touch.pdf](http://www.mdtsoft.com/products/autosave/pdfs/wonderware_in_touch.pdf)

The Wonderware security guidelines document addresses these topics (change control, configuration management) in a number of sections throughout the document including section “*Configuration Management Policy*” and “*Operational Controls*” amongst others.

#### **CIP-004      Cyber Security — Personnel & Training**

Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training and security awareness.

This set of activities is led primarily by the responsible entity. If an external firm was involved in the development of a Wonderware-based system, it may be involved in providing training on the access and use of the application.

While training on access and proper use of cyber assets which may include a Wonderware-based system is covered under this standard (Requirement R2.2), full compliance goes beyond the scope of a Wonderware-based application and includes aspects such as personnel risk assessment (R3).

Another requirement related to a Wonderware-based system is the ability to revoke access rights (R4.2), for terminated employees as well as employees which no longer require them.

Wonderware software provides the functionality to control secured application access management.

The Wonderware security guidelines document addresses these topics (training, awareness and personnel risk assessment) in a number of sections throughout the document including section *“Providing training and security awareness, “Institute Periodic Employee Security Awareness Training”* and *“Personnel Security”* amongst others.

## **CIP-005      Cyber Security — Electronic Security Perimeter(s)**

Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.

Recommendations for establishing an Electronic Secured Perimeter (Requirement R1) for Wonderware-based applications are included in the Wonderware security guidelines document Chapter 5 *“ICS Security recommendations”* and Chapter 6 *“Configuring IPSec and domain isolation for the ICS environment”*.

Another requirement to note under this standard:

*R2.2. “At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.”*

The installation of Wonderware software enables only those services and ports required by the specific Wonderware component in case. This information is documented in our document entitled *“Security Settings for Wonderware products”* available from [wdn.wonderware.com](http://wdn.wonderware.com).

**Requirement R3 - Monitoring Electronic Access** — *“The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.”*

The Wonderware System Platform enables logging of successful logons to the Wonderware-based system for audit tracking purposes.

Wonderware software also provides the functionality for InTouch-based systems to leverage OS security as well as to implement a logon audit trail.

When using OS security in combination with Wonderware software, the capability to configure Windows® security to disable a user's account after consecutive failed logons can be leveraged.

### **CIP-006 Cyber Security — Physical Security of Critical Cyber Assets**

Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

Wonderware software provides functionality that enables implementation of a Wonderware-based application that can be used to monitor access to a Physical Secured Perimeter (Requirement **R3**), to detect intrusions and alert accordingly.

The Wonderware security guidelines document addresses this topic in the section *“Protecting the physical environment”*.

### **CIP-007 Cyber Security — Systems Security Management**

Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).

#### **Requirement R2 - Ports and Services**

*“The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.”*

The installation of Wonderware software enables only those services and ports required by the specific Wonderware software component. This information is contained in the document entitled *“Security Settings for Wonderware products”* available from [wdn.wonderware.com](http://wdn.wonderware.com).

### **Requirement R3 – Security Patch Management.**

In order to assist our customers with Security Patch Management, Wonderware tests Microsoft® updates with our software, and publishes results of this testing on the Wonderware Security Central website.

The Wonderware security guidelines document addresses these topics (security patch management and malicious software prevention) in Chapter 4 “*Managing Security Patches and Virus Protection*” and the section “*policies and procedures*”.

### **Requirement R4 - Malicious Software Prevention**

*“The Responsible Entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).”*

Wonderware has tested our software, working side-by-side with a number of anti-virus packages. Wonderware Tech Article “*Antivirus and malware removal in the FactorySuite A2 - ArcestrA® environment. Security considerations*” provides recommendations for proper configuration of anti-virus programs for use with Wonderware-based systems.

<http://wdnresource.wonderware.com/support/kbcd/html/1/t002098.htm>

The Wonderware security guidelines document addresses these topics in the section entitled “*Incident Response*”.

**Requirement R5.2.** *“The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.”*

**R5.2.1.** *“The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.”*

Wonderware software requires an “ArcestrA account” for use by certain key services. The name and password of this account is selected upon installation of the software. This account name and/or password can be changed using the Wonderware “Change Network Account” utility. This ArcestrA account needs the same user name and password on all computers that are participating in the

solution. Changes to this account must be performed in a planned fashion in order to prevent disruptions.

**Requirement R5.3.** “At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and special characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.”

Wonderware software enables the use of OS Security which in turn enables the use of password management policies required by NERC.

The password for the “ArchestrA account” can be changed using the Wonderware “Change Network Account” utility as a planned scheduled activity.

InTouch software applications can make use of a password script function library in order to implement password management functionality. This script library is available from the Wonderware Developer Network (WDN) website.

### **CIP-008-1 Cyber Security — Incident Reporting and Response Planning**

Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

This activity is led by the *responsible entity*.

The Wonderware security guidelines document addresses these topics in the section named “*Incident Response*”.

### **CIP-009 Cyber Security — Recovery Plans for Critical Cyber Assets**

Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Wonderware software enables a number of choices to address Disaster Recovery requirements.

The Wonderware security guidelines document addresses this topic in the section “*Planning for Disaster Recovery*”.

## **Compliance Assessment**

Compliance with NERC CIP-002 through CIP-009 standards is a system-wide effort covering diverse aspects where a Wonderware-based system is only a component of the entire process. Full compliance by a responsible entity requires security assessments, gap analysis, etc. Customers may chose to contract with a consulting firm to assess compliance of their system or chose to use a self assessment tool.

### *Consulting*

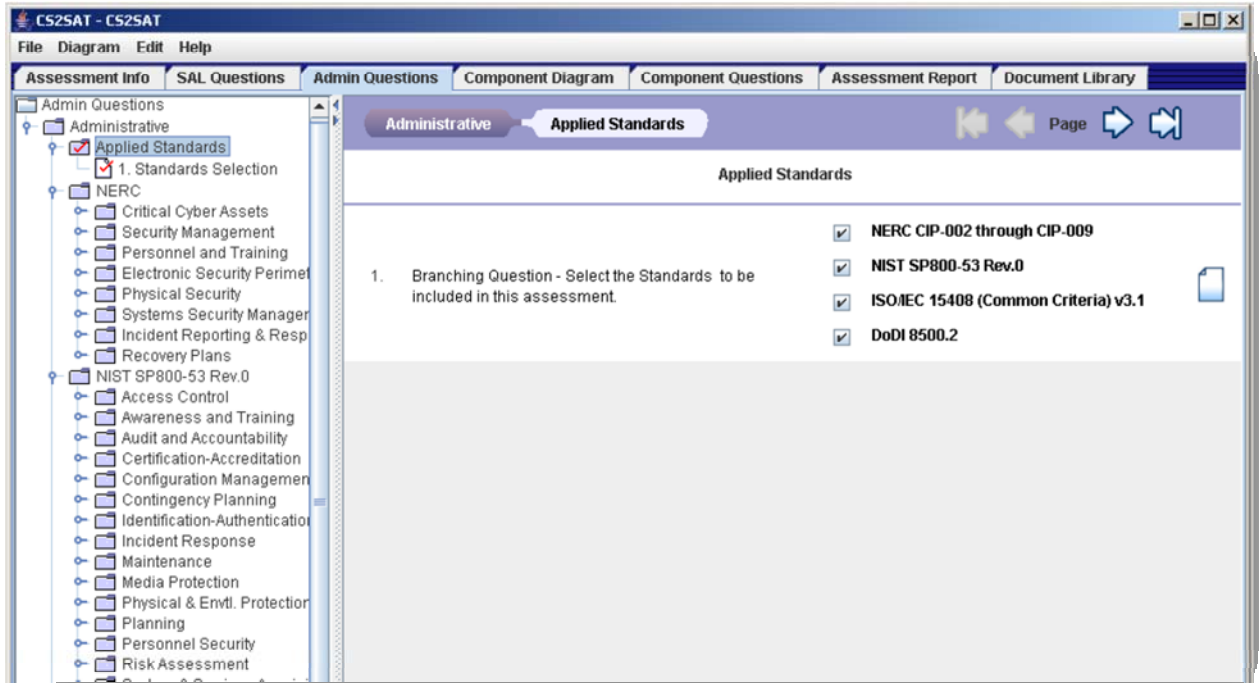
**Invensys IPS** provides consulting services to assist utilities meet compliance with the NERC CIP standards. For more information, see:

[www.ips.invensys.com/en/consulting/consulting/Documents/IPS\\_CIP\\_CyberSecurity\\_0209.pdf](http://www.ips.invensys.com/en/consulting/consulting/Documents/IPS_CIP_CyberSecurity_0209.pdf)

### *Assessment tools*

One of the options to evaluate NERC CIP-002 through CIP-009 compliance is the use of the CS2SAT tool.

The Department of Homeland Security National Cyber Security Division has developed a software application called “Control System Cyber Security Self-Assessment Tool (CS2SAT)” which can be used to perform a repeatable assessment of a system’s compliance to certain cyber-security standards, including NERC CIP-002 through CIP-009.



For more information on the CS2SAT “Control System Cyber Security Self-Assessment” Tool and how to obtain a copy, visit:

<http://www.isa.org/CS2SAT/>

## CONCLUSIONS

Wonderware software offers features and functionality that may assist in the implementation of NERC CIP compliant solutions. Wonderware provides additional information - such as guidelines, security patch test results, technical articles and more – that can be leveraged in the development and implementation of Wonderware-based applications for use in critical infrastructure systems. Options to perform compliance assessment are available including consulting services and specialized tools.

**APENDIX A**  
**SUMMARY OF NERC CIP STANDARDS AND REQUIREMENTS**

(Please refer to [www.nerc.com](http://www.nerc.com) for the complete latest version of the standards as information may change)

STANDARD	TITLE	COMMENTS ON REQUIREMENTS	
CIP-002-1	Critical Cyber Asset Identification	<ul style="list-style-type: none"> <li>• R1. Critical Asset Identification Method</li> <li>• R2. Critical Asset Identification</li> <li>• R3. Critical Cyber Asset Identification</li> <li>• R4. Annual approval</li> </ul>	Requires system wide assessment, making a list of critical assets, a list of critical cyber assets, maintaining and updating these lists and a yearly review of them.
CIP-003-1	Security Management Controls	<ul style="list-style-type: none"> <li>• R1. Cyber Security Policy</li> <li>• R2. Leadership</li> <li>• R3. Exceptions</li> <li>• R4. Information Protection</li> <li>• R5. Access Control</li> <li>• R6. Change Control and Configuration Management</li> </ul>	
CIP-004-1	Personnel and Training	<ul style="list-style-type: none"> <li>• R1. Awareness</li> <li>• R2. Training</li> <li>• R3. Personnel Risk Assessment</li> </ul>	See page 78 of WW “Securing Industrial Controls”.

STANDARD	TITLE	COMMENTS ON REQUIREMENTS	
		<ul style="list-style-type: none"> <li>• R4. Access</li> </ul>	
CIP-005-1	Electronic Security Perimeter(s)	<ul style="list-style-type: none"> <li>• R1. Electronic Security Perimeter</li> <li>• R2. Electronic Access Controls</li> <li>• R3. Monitoring Electronic Access</li> <li>• R4. Cyber Vulnerability Assessment</li> <li>• R5. Documentation Review and Maintenance</li> </ul>	Architecture centric. ISA SP99 layered architecture and WW recommended architectures apply to this standard.
CIP-006-1	Physical Security	<ul style="list-style-type: none"> <li>• Physical security plan</li> <li>• Physical Access Controls</li> <li>• Monitoring Physical Access</li> <li>• Logging Physical Access</li> <li>• Access log Retention</li> <li>• Maintenance and Testing</li> </ul>	Physical security of Critical Assets. Locks, card keys, CCTV, security personnel fit in this category.
CIP-006-1a	Cyber Security – Physical	<ul style="list-style-type: none"> <li>• Physical security plan</li> <li>• Physical Access Controls</li> <li>• Monitoring Physical Access</li> <li>• Logging Physical Access</li> </ul>	Physical security of cyber assets.

STANDARD	TITLE	COMMENTS ON REQUIREMENTS	
		<ul style="list-style-type: none"> <li>• Access log Retention</li> <li>• Maintenance and Testing</li> </ul>	
CIP-007-1	Systems Security Management	<ul style="list-style-type: none"> <li>• R1. Test procedures</li> <li>• R2. Ports and services</li> <li>• R3. Security Patch Management</li> <li>• R4. Malicious software prevention</li> <li>• R4. Account management</li> <li>• R5. Security status monitoring</li> <li>• R6. Disposal or redeployment</li> <li>• R7. Cyber vulnerability assessment</li> <li>• R8. Documentation review and maintenance</li> </ul>	
CIP-008-1	Incident Reporting and Response	<ul style="list-style-type: none"> <li>• R1. Cyber Security Incident Response Plan</li> <li>• R2. Cyber Security</li> </ul>	

STANDARD	TITLE	COMMENTS ON REQUIREMENTS	
		Incident Documentation	
CIP-009-1	Recovery Plan for Critical Cyber Assets	<ul style="list-style-type: none"> <li>• R1. Recovery Plans</li> <li>• R2. Exercises</li> </ul>	



Contact Wonderware or your local Wonderware Distributor for more information on Wonderware software solutions.

Wonderware • 26561 Rancho Parkway South, Lake Forest, CA 92630 • Tel: (949) 727-3200 • Fax: (949) 727-3270 • [www.wonderware.com](http://www.wonderware.com)

© 2009 Invensys Systems, Inc. All rights reserved. No part of the material protected by this copyright may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, broadcasting, or by any information storage and retrieval system, without permission in writing from Invensys Systems, Inc.

Invensys, Wonderware, ArcheStrA, InTouch, ActiveFactory, InBatch, InControl, SCADAAlarm, Factelligence and IntelaTrac are trademarks and registered trademarks of Invensys plc, its subsidiaries and affiliated companies. All other brands and product names may be the trademarks or service marks of their respective owners.

Part No. 15-0258 05/09