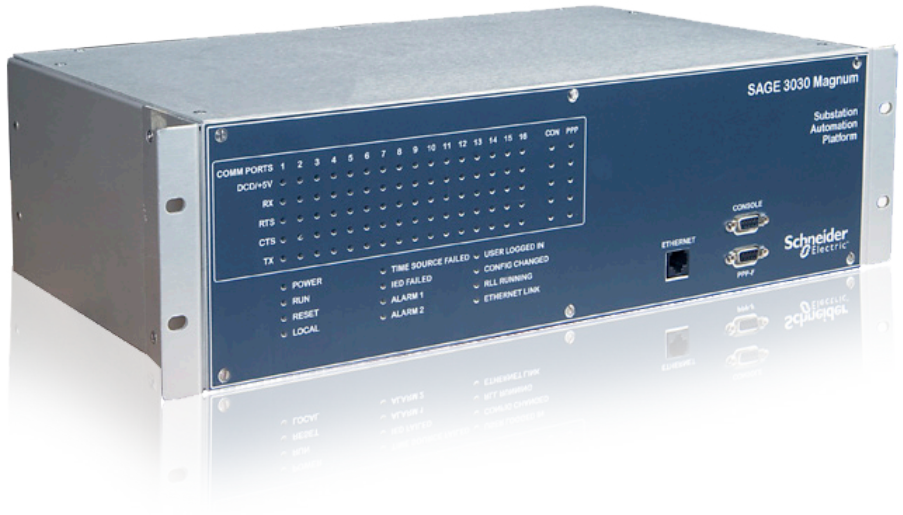
NERC CIP

Critical Infrastructure Protection

Compliance for SAGE Intelligent Terminal Units



Make the most of your energy℠

Schneider Electric™

NERC Critical Infrastructure Protection (CIP)

As security grows increasingly important, Schneider Electric continues its focus on helping system users be secure and comply with mandated security requirements.

This document outlines the NERC CIP guidelines, highlights specific capabilities and features integral to the SAGE product line, and how SAGE features and functions support a utility's compliance with CIP criteria.

CIP-003: Security management controls

Describes the development of a security policy and defines the controls to be used to manage various aspects of general security.

SAGE controls the addition and deletion of privileged users. Users can be assigned different levels of access, ranging from 'display only' to 'full admin' privileges. A downloadable User Log documents user activity and provides an audit trail for CIP compliance.

CIP-004: Personnel and training

Identifies the personnel training and awareness recommended for supporting security-related operations and procedures.

SAGE maintains a User List for monitoring users and user privileges for workforce management. The User List is designed to manage changes in workforce with tools that allow administrator level users to change privileges and/or delete privileges or terminate a user.

CIP-005: Electronic security perimeter(s)

Deals with identification and protection of 'Security Perimeters' that define physical and electronic access to equipment.

SAGE requires a valid password and user login for access. Privileges are defined on a per-user basis. Strong passwords are supported, and all passwords are hidden. Each time a user logs in, the SAGE generates an alarm indication that can initiate user access validation by SCADA or other means. Additionally, IP Tunnel capability eliminates dial-up access, and IP filter capability adds an additional layer of security.

CIP-006: Physical security of critical cyber assets

Discusses physical accessibility to equipment. In addition to being housed

in an enclosure with a locking door, SAGE can send access alarms, such as door and/or gate open indication, to SCADA. SAGE also can support video, key pads, and biometric validation indicators.

CIP-007: Systems security management

Deals with security patches and virus protection and reinforces CIP-005 concepts.

SAGE runs on a non-Windows®-based OS, making it inherently immune to typical virus and malware threats and less likely to be targeted by hackers or persons intent on causing harm. The downloadable User Log monitors login and change activity. Any access requires a user password.

Login generates an automatic alarm indication that can be sent to SCADA.

CIP-008: Incident reporting and response planning

Relates to the managing and handling of reports and logs.

The complete library of SAGE Logs can be downloaded and saved to provide documentation and audit trail for compliance. The Library includes: User Log, SOE log, System Log, and Control Log.

CIP Features Summary Table

Requirement	NERC CIP Standard	SAGE Solution
User access	CIP-004 CIP-005 CIP-007	• Individual user accounts/passwords • Privileges defined on a per-user basis • Strong passwords supported • Passwords hidden when entered
Access control	CIP-003 CIP-005 CIP-004	• Passwords can be managed from central location Multiple admin-type accounts can be configured • User Log , IP Filter list
Electronic security perimeter	CIP-005 CIP-003 CIP-007	• Elimination of dial-up access with use of IP tunnel • Appropriate banner usage • Electronic access logged; can be monitored and alarmed • Port data paths configurable • SSL/SSH LAN
Logging of Access and Usage	CIP-003 CIP-004 CIP-007 CIP-008	• Every access attempt logged • Resets logged • User changes logged • Time-tagged events logged
Workforce management	CIP-004 CIP-007	• User accounts revocable by administrator • User accounts 'downgradable' to lower level of authority
Security software management	CIP-007	• Non-Windows® based OS • All software upgrades available for real-time updates (Ever-Green)
Alerts and notifications	CIP-005 CIP-007 CIP-008	• Every access attempt logged • Access notification alarms available to SCADA

Schneider Electric Industries SAS

14400 Hollister, Suite 400
Houston, TX 77066
Phone: 713-920-6801
Fax: 713-920-6909
www.schneider-electric.com/us

October 2013