Meeting NERC CIP requirements with Cooper Power Systems IED Integration and Automation Solutions

This document describes the security features of **Cooper Power Systems SMP Gateway** and **Yukon IED Manager Suite** applications. It also describes how utilities can use these solutions to develop a secure, NERC CIP-compliant, solution to integrate their substation devices.

In this document

Quebec City
730 Commercial Street
Suite 200
Saint-Jean-Chrysostome, Quebec
Canada G6Z 2C5
Phone: +1.418.834.0009
Fax: +1.514.227.5256

Montreal
1290 St. Denis Street
Suite 300
Montreal, Quebec
Canada H2X 3J7
Phone: +1.514.845.6195
Fax: +1.514.227.5256

www.cooperpowereas.com

B1100-09021 • January 2013

Introduction

Cooper Power Systems IED Integration and Automation Solutions provide utilities with the tools necessary to access substation devices for data retrieval and remote maintenance. Cooper Power Systems solutions help utilities put their substation data to use while meeting NERC CIP requirements, both at the substation and enterprise level.

The key component at the substation level is the **SMP Gateway**. This third generation data concentrator provides access to real-time data while meeting all the security requirements of a NERC CIP-compliant electronic perimeter. It provides a secure single point of access to all substation devices. Its advanced security features allow it to integrate legacy IEDs, with little or no security, in a modern IED integration system.

At the enterprise level, **Yukon IED Manager Suite** (IMS) provides secure enterprise-level access to field devices. Besides secure communications, it provides the automated tools to help utilities manage IEDs while meeting NERC CIP security requirements.

SMP Gateway security features

SMP Gateway retrieves data from substation devices and makes it available to SCADA and to enterprise level applications. It also provides remote maintenance access to connected IEDs using its secure **Passthrough** function. The SMP Gateway supports both modern and legacy devices, using standard and proprietary protocols. It provides a secure single point of access to all substation devices, acting as NERC CIP-compliant electronic perimeter that protects connected devices, including those with little or no security.

The **SMP Gateway** implements the following security features that ensure that all connected devices can be accessed in a NERC CIP-compliant manner –

- **Authentication and authorization** — SMP Gateway includes a built-in security server that authenticates users via a user name and a password. Strong passwords, individual user accounts, user groups, and detailed group permissions are used to protect critical system functions from unauthorized access. All access attempts are logged, and accounts are locked out in the event of multiple failed access attempts. Alternatively, it can be used with the **IMS Security Server** to implement centrally managed authentication and authorization and simplify management of multiple users and SMP Gateways.
- **Network security** — SMP Gateway is protected by a built-in firewall. All TCP/IP ports are blocked by default, except those required for control center communication and SMP Gateway status monitoring and management. All communication between the SMP Gateway and the SMP Tools is secured through the use of the Transport Layer Security (TLS) protocol (successor to "Secure Sockets Layer" or SSL).
- **Secure remote maintenance access** — The SMP Gateway Passthrough function provides remote users with the capability to securely use a terminal emulator application or native vendor tool as if they were connected directly to the IEDs maintenance port.

- **Monitoring and locking of remote connections** — Control centers can control and monitor usage of the modem and remote maintenance access (Passthrough) services; access is restricted to authorized users only; all successful and unsuccessful access attempts are logged locally, or to a standard Syslog server.
- **Integrity checking** — All SMP Gateway software and firmware components are digitally signed in order to ensure their authenticity and integrity. The integrity of executable files is continuously monitored to prevent execution of unauthorized code.

Authentication and authorization

SMP Gateway authentication and authorization functions are used to control maintenance access to the gateway and to connected devices.

SMP Gateway provides the following authentication and authorization functions —

- Support for distributed and centralized authentication. The default security model is distributed authentication, where each gateway has its own security server that performs authentication and authorization of users based on an internal user database. Alternatively, the **Security Server**, part of **Yukon IED Manager Suite**, can be used to maintain a global list of users and permissions and offer centralized authorization. This security model is described further on.
- Authentication by user name and a strong password. The maximum user name length is 20 characters and the maximum password length is 64 characters. Password complexity can be enabled, requiring a combination of letters, numbers and special characters, as required by NERC CIP.
- Account lockout can be enabled to prevent password cracking and unauthorized access. Account will automatically be locked after a predetermined number of failed login attempts. Locked accounts can be unlocked by the administrator, or automatically after a configurable delay. Internal data points can be used to report failed login attempts and account lockout to SCADA, and can be used to trigger an intrusion detection function.
- Comprehensive role-based access control mechanism based on user groups and privileges –
  - Predefined user groups have been provided for the most common usage scenarios. System administrators can add new groups, and rename or delete default groups to suit specific requirements.
  - Users can be assigned to one or more user groups.
  - Each group defines which privileges are assigned to users. A privilege consists of a number of activities, and each activity is authorized individually. The predefined privileges include:
    - Security Management — Update security database: users, groups, and privileges; unlock user accounts; access to Security and Firewall logs.
    - System Management — Update firmware, software, license and components; configure redundancy, RAS, and SNMP; console access.
    - Configuration — Read or update SMP Gateway configuration file.
    - Diagnostic — Use SMP Gateway diagnostics tools: SMP Log, SMP Trace and SMP Stats.
    - Device Maintenance — Use SMP Gateway to remotely connect to an IED via Passthrough connections.

  - Monitoring — Access SMP Gateway internal real-time database through the internal web server.
  - Operation — Perform control operations, inhibit data points, and force operations on data points using the web-based commissioning tool.
  - Remote Access — Connect to an IED remotely, via dialup or the network.

- All access attempts, whether accepted or refused, and all user activities are recorded in the security log. If technically possible, information about the PC connecting to the SMP Gateway is also recorded: IP address, Windows login user name, and machine name. All events can also be published to a Syslog server.
- User accounts, groups, and privileges are edited centrally, using the **SMP Manager** tool.
- The SMP Gateway security database is encrypted using AES 128-bit encryption. Security information is never directly visible in clear form.
- Access to the security and firewall logs requires the Security Management permission.

Network security

SMP Gateway ensures network security via a built-in firewall and the use of the SSL/TLS protocol.

Firewall

- By default, all network ports are blocked, except for the management port (TCP 6650), the HTTPS web server port (TCP 443), and the legacy status server port (UDP 23). Firewall rules can be defined to restrict access through these ports.
- Ports are opened dynamically for the SNTP, SNMP, and redundancy functions. Access can be limited to specific IP addresses or subnets.
- TCP/IP ports used by slave protocols for SCADA, EMS or control centers, are automatically unblocked by the configuration tool. Access can be limited to specific IP addresses or subnets.
- Simplified one-click management of CoDeSys Soft PLC Workbench, Visual T&D, SNMP and ICMP PING.
- All blocked accesses are recorded in the firewall log.

Transport Layer Security (TLS)

To prevent identity spoofing, data tampering and information disclosure, the SMP Tools use the Transport Layer Security (TLS) protocol (successor to "Secure Sockets Layer" or SSL).

The built-in web server uses the Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) protocol.

Secure remote maintenance access

The SMP Gateway **Passthrough** function provides remote users with the capability to securely use a terminal application or native vendor tool as if they were connected directly to the IED maintenance port.

The **SMP Connect** application runs on the user PC and acts as port redirector. It captures all data from the application and forwards it to the SMP Gateway over a secure TLS channel. The SMP Gateway then forwards the data to the target device.

The Passthrough function can be used with serial and TCP/IP devices. Usage is limited to authenticated users with the correct permissions. Access is logged and can be monitored and controlled by SCADA.

The Passthrough function acts as a secure proxy or intermediate device and does not bridge traffic from the substation network to the enterprise network. Network devices cannot establish outgoing connections through the SMP Gateway. Only preconfigured Passthrough connections can be activated.

Monitoring and locking remote connections

SMP Gateway can monitor and lock connections to the internal modem. It can also monitor and lock Passthrough connections.

Modem connections

- Modem accesses can be monitored by a control center, through a logical binary input data point.
- Modem accesses can be locked by a control center, through a logical binary output data point or through a RAS Manager command.
- Control centers can interrupt active modem connections.
- Lock settings are preserved between SMP Gateway restarts.

Passthrough connections

- Passthrough connections can be monitored and locked individually by a control center, through a logical binary input data point or by the **IMS Passthrough Client** in Supervisor mode.
- An active passthrough connection can be interrupted by a control center.
- The startup lock settings can be specified via the configuration tool.

Malware protection and integrity checking

Standard virus detection software is not designed to be used on devices running embedded software such as SMP Gateway. Virus detection only works with known threats and needs to be updated regularly, which is challenging in a substation setting.

SMP Gateway thus provides the following integrity checking functions to protect against viruses and other forms of malware:

- All SMP Gateway executable files (firmware and software) are signed by Cooper Power Systems. Only signed executable files can be loaded onto the SMP Gateway.
- The integrity of all executable files on the SMP Gateway is continuously monitored in the background. This feature automatically detects any change resulting from hardware or software failure, or tampering.
- If an invalid executable file is detected, the SMP Gateway records the name of the file in the security log, and puts itself into a safe mode in which it interrupts all communication with devices and control centers. Maintenance access remains possible to diagnose problems and restore functionality.

Yukon IED Manager Suite

Yukon IED Manager Suite is a family of software applications that bridge the gap between the substation and the enterprise. They provide users with a single, enterprise-level, point of access to substation data and substation devices.

SMP Gateway and **Yukon IED Manager Suite** work in tandem, providing utilities with a comprehensive communications infrastructure and a powerful set of tools to manage their IEDs, simplifying the implementation of NERC CIP management procedures.

The following applications provide are part of Yukon IED Manager Suite (IMS):

- **IMS Security Server** provides centralized authentication and authorization services.
- **IMS Passthrough Manager** provides corporate users with a single point of access to substation devices, for maintenance and engineering purposes.
- **IMS Event Manager** automatically retrieves event files from protection relays, notifies the appropriate users by email or pager, and provides access to event data through a web-based interface.
- **IMS Configuration Manager** provides centralized configuration management services for SMP Gateways and connected devices.
- **IMS Password Manager** provides centralized management of all device passwords.

Security Server

The **IMS Security Server** provides centralized authentication and authorization services for all IMS applications. It also offers a centralized security model where access to SMP Gateways and IEDs can be managed globally instead of individually.

In the default SMP Gateway security model, each gateway implements its own security server and performs its own authentication. System administrators use the **SMP Manager** application to define users, groups and permissions. Administrators then load the encrypted security database on each individual SMP Gateway.

When the centralized security model is implemented, user credentials are validated by the **Security Server** instead of being validated by individual SMP Gateways.

- The Security Server manages a database of users that need to access IMS applications, SMP Gateway, and IEDs.
- The Security Server can authenticate users from its own list of accounts, or it can tie into the existing Microsoft Active Directory infrastructure.
- The Security Server ties in natively to Active Directory through the Microsoft Security Support Provider Interface (SSPI), providing seamless access to user accounts and Active Directory groups.
- Active Directory integration ensures that access to IMS, SMP Gateway and IEDs is subject to the same security policies as all other enterprise applications: single user account and password for all applications, password complexity, two-factor authentication, password aging, etc.

- IMS system administrators define groups that specify permissions and devices. Administrators then assign users to these groups. Permissions can be assigned to individual users, IMS groups, or Active Directory groups.
- SMP Tools and IMS applications validate the user's Windows credentials with the Security Server to determine access permissions.
- For valid users, the Security Server issues an encrypted and signed message that contains the user name and permissions. Client applications and tools forward this message to the IMS module or SMP Gateway which decrypts the message and enables the appropriate functions.
- The authenticity of the messages exchanged between the Security Server and SMP Gateway is ensured by a shared private key. The physically secure central server uses the shared key to encrypt messages. The SMP Gateway uses the key to decrypt the message. The SMP Tools cannot decrypt these messages.

Once an SMP Gateway is configured for centralized security, the internal security server and authentication database is no longer used, except in emergency situations. Local "rescue" accounts provide access if contact with the Security Server is lost.

IMS Security Server provides centralized authentication and access management for SMP Gateways and IEDs, without the complexity of setting up LDAP or RADIUS at the individual device level.

Passthrough Manager

IMS Passthrough Manager is an enterprise-level application that provides corporate users with secure remote access to substation devices. With Passthrough Manager, users can remotely perform configuration and maintenance operations on substation IEDs, using a terminal emulator program or native vendor tool.

Passthrough Manager is a client/server application. The **Passthrough Client** application can be installed on individual desktops or on a shared application server. Passthrough Client acts as a port redirector, capturing all data sent to a virtual serial or TCP/IP port and forwarding it from the native vendor tool to the **Passthrough Server** using a secure TLS connection. The Passthrough Server then forwards the data to the remote device directly, or through an SMP Gateway, SEL gateway, or NovaTech Orion gateway.

Passthrough Manager offers the following security features:

- Isolate client applications from the substation devices. Only the Passthrough Server needs access to the substation devices, it can be installed in a DMZ.
- Secure all data exchanges between the Passthrough Client, Passthrough Server and SMP Gateway using TLS.
- Set access permissions by device, by user or by group.
- Show users only the devices to which they have access.
- Maintain a log of all accesses.
- Maintain a detailed log of all operations performed on a device, down to the keystroke level.
- Automatically perform device login and hide device passwords from users, for supported devices. Users no longer need to know device passwords, reducing the number of shared accounts.

- Filter commands to prevent users from performing unauthorized functions such as changing device passwords, when technically feasible.
- Provide centralized remote session management using Supervisor commands: lock/unlock device, terminate remote session, and display current users and sessions.

Event Manager

IMS Event Manager is an enterprise-level application that automatically retrieves event data from protective relays and notifies the appropriate users by email. Emails contain all event data providing users with the capability to analyze fault data and eventually restore service more rapidly.

With Event Manager, protection engineers no longer need to connect to critical substation devices to analyze fault data. Event data is available by email, or through a web browser.

Event Manager offers the following features:

- Retrieve event data from devices directly, or through one or more cascaded gateways, using serial or TCP/IP connections.
- Retrieve events on demand or on a scheduled basis.
- When used with an SMP Gateway, events can be collected at the substation level, reducing bandwidth usage and providing faster event processing. Events are "pushed up" and retrieved immediately instead of waiting for the scheduled poll or a manual poll.
- Event notifications are sent automatically to the appropriate users by email.
- Event data is stored in an industry-standard SQL Server database.
- Web-based event viewer provides comprehensive event filtering and handling capability, including conversion to COMTRADE format.
- Event Viewer implements IMS security model and users only see data for the devices to which they have been granted access.

Configuration Manager

IMS Configuration Manager is an enterprise-level application that manages a database of configuration files for all SMP Gateways and supported substation-level devices. On demand, or on a scheduled basis, Configuration Manager retrieves the current configuration of registered devices, compares it to the baseline version, and notifies the system administrator of any change.

Configuration Manager provides the following features to assist utilities in meeting NERC CIP requirements:

- Automatically retrieve and store device configuration settings and files, detect changes, and notify appropriate personnel when changes are detected.
- Web-based client application provides access to device settings and configuration.
- Users no longer need to connect to critical substation devices to view and analyze settings.

- Track change history, software versions, settings, patches and service packs for all managed SMP Gateways and devices.
- Simplify change management with side-by-side display of configuration settings with changes highlighted.
- Retrieve last-known-good device configuration from the database for simplified system recovery.

Password Manager

IMS Password Manager is an enterprise-level application that manages user accounts and passwords for all supported devices. Password Manager helps utilities meet NERC CIP requirements by providing all the tools required to implement a password management process.

Password Manager provides the following features:

- Define accounts, default passwords, password length, complexity, and character set for each device type.
- Store current passwords for all device accounts.
- Web-based management interface allows authorized users to view device accounts and passwords, request password changes, and view reports.
- Provide IED passwords to field personnel on a need-to-know basis.
- Request a password change when work is done.
- Print Current Passwords report for emergency use if communications fail.
- Print Password Age report to plan and schedule password updates.
- Use Password Usage and Password Change History reports to demonstrate compliance during audits.

Conformity to NERC CIP requirements

The following table summarizes how **SMP Gateway** and **Yukon IED Manager Suite** help utilities meet NERC CIP requirements.

NERC CIP Requirement	SMP Gateway and IED Manager Suite Feature
CIP-002 Critical Cyber Asset Identification	
R3. Critical Cyber Asset Identification *The Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset.*	**IED Manager Suite** manages the inventory of all devices and produce reports.
CIP–003 Security Management Controls	
R4. Information Protection *The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.*	**IED Manager Suite** is a key component in an information protection program. It supports strong passwords, individual user accounts, user groups, and detailed group permissions in order to protect critical information from unauthorized access. Database contents can be encrypted to protect information assets.
R5. Access Control *The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.*	**IED Manager Suite** system administrators can grant access to individual users, or groups of users. Users only see devices to which they have access. With Auto-Login, users do not need to know device passwords. Command filtering prevents unauthorized users from operating remote devices or changing device settings. Detailed reports identify accessible devices and permissions for each user.
R6. Change Control and Configuration Management *The Responsible Entity shall establish and document a process of change control and configuration management* […]	The **IMS Configuration Manager** module maintains a database of all configuration files and tracks all configuration changes for each managed SMP Gateway and IED. IMS Configuration Manager polls devices on a scheduled basis, automatically detects configuration changes, and notifies system administrators.

CIP–004 Personnel and Training	
R4. Access *The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.* *R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause* […]	**IED Manager Suite** provides centralized access control for applications, SMP Gateways and managed IEDs. System administrators can easily define access permissions and produce reports. When the **Security Server** module is tied-in to the corporate Active Directory, administrators can revoke a user's access to all applications and devices with a single operation. The **Security Management Console** application provides system administrators with the capability to easily update the local accounts of each individual SMP Gateway. The **Password Manager** module provides system administrators with the capability to change all IED and SMP Gateway passwords on demand.
CIP–005 Electronic Security Perimeter(s)	
R1. Electronic Security Perimeter *The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter.*	**SMP Gateway** performs all the functions required for an electronic perimeter and is a key component in a defense in depth approach.
R2. Electronic Access Controls R2.1. […] *shall use an access control model that denies access by default, such that explicit access permissions must be specified.*	**IMS Passthrough Manager** provides an enterprise-level single point of access to IEDs. Authenticated users can only see the devices to which they have been granted access, and can only perform authorized operations. The **SMP Gateway** provides an additional level of access control. Only authorized users can access the SMP Gateway or the devices behind it. Used together, **IMS Passthrough Manager** and **SMP Gateway** ensure that only authorized users can access remote devices.

R2.2. […] *shall enable only ports and services required for operations and for monitoring…*	By default, the **SMP Gateway**'s built-in firewall blocks all network ports, except for the management port (TCP 6650), the HTTPS web server port (TCP 443), and the legacy status server port (UDP 23). A firewall rule can be defined to restrict access through these ports to specific computers. The configuration tool unblocks only those ports required to connect to control centers, and to implement services such as SNMP and SNTP, when they are used. Access can be limited to specific computers. All serial ports are disabled unless configured to communicate with IEDs or control centers. All USB ports are disabled, unless configured to be used by the annunciator option to connect a mouse and keyboard.
R2.3. […] *shall maintain and implement a procedure for securing dial-up access to the Electronic Security Perimeter(s).*	By default, the **SMP Gateway** internal modem is disabled. Usage of the modem must be configured, and can be controlled by a SCADA interlock.
R2.4. […] *shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party* […]	The **IMS Security Server** ties in to Active Directory and benefits from any available two-factor authentication solution to provide strong access control.
R2.6. *Appropriate Use Banner* — […] *electronic access control devices shall display an appropriate use banner upon interactive access attempts…*	All **SMP Tools** and **IED Manager Suite** tools display a user-configurable appropriate use banner when they are launched.
R3. Monitoring Electronic Access R3.1. *For dial-up accessible Critical Cyber Assets* […] *shall implement and document monitoring process(es) …*	The **SMP Gateway** implements internal data points that SCADA can monitor to detect modem and passthrough usage. All accesses are logged in the internal security log.
R3.2. […] *shall detect and alert for attempts at or actual unauthorized accesses* […]	**IED Manager Suite** and **SMP Gateway** log all access attempts, whether successful or not, and generate security events. Logs and events are published through Syslog to be processed by a third party SIEM. The **SMP Gateway** security automatically locks out user accounts after a preset number of failed access attempts. **SMP Gateway** internal data points can be used to report failed login attempts and the locked-out state of an account.
R5. Documentation Review and Maintenance R5.1. […] *shall ensure that all documentation … reflect current configurations and processes* […]	**IMS Configuration Manager** tracks all version and change information for each device.

R5.3. […] *shall retain electronic access logs for at least ninety calendar days.*	The **SMP Gateway** maintains a log of all accesses and can be configured to publish the information to a Syslog server. System administrators can use the **SMP Log** application to manually retrieve and store the log contents. **IMS Passthrough Manager** logs all accesses to IEDs and can be configured to publish the information to a Syslog server. Passthrough Manager also logs all data exchanged between the user and the IED, to the keystroke level.
CIP–007 Systems Security Management	
R2. Ports and Services […] *shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.*	By default, the **SMP Gateway**'s built-in firewall block all network ports, except those required for operation. All serial and USB ports are disabled by default, unless configured for use.
R3. Security Patch Management […] *shall establish and document a security patch management program* […]	**IMS Configuration Manager** tracks software versions, settings, patches and service packs for all managed devices.
R4. Malicious Software Prevention […] *shall use anti-virus software and other malicious software ("malware") prevention tools* […]	**IED Manager Suite** is compatible with all industry-standard antivirus solutions. The **SMP Gateway** uses a white-listing approach to protect it from malicious software. Only files signed by Cooper Power Systems can be loaded on the **SMP Gateway**. The **SMP Gateway** integrity checking function continuously scans all executable files and shuts down the gateway if file contents are modified by hardware or software failure, or by tampering.
R5. Account Management R5.1.2. […] *shall establish methods, processes, and procedures that generate logs … of individual user account access activity* […]	**IED Manager Suite** and **SMP Gateway** maintain detailed logs of all accesses, and can publish this information to a Syslog server.
R5.2. […] *shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges* […]	**IED Manager Suite** and **SMP Gateway** implement individual user accounts, user groups, and detailed group permissions. **IMS Passthrough Manager** performs Auto-Login for supported devices and hides device passwords from users.

R5.2.3. […] *an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes* […]	**IMS Password Manager** provides the capability to automatically change device passwords. **IED Manager Suite** stores all passwords in its database and can provide them to authorized users on demand. It can produce a report identifying users that have requested passwords.
R5.3. […] *shall require and use passwords, subject to* […] *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.*	**IMS Security Server** provides centralized account management and it can tie-in to the existing corporate Active Directory. It extends corporate security policies to substation devices, without the complexity of implementing domain-based security at the substation level. The **SMP Gateway** local security accounts support user names of up to 20 characters, and password length of up to 64 characters. Password complexity can be enabled, requiring a combination of letters, number and special characters. **IMS Password Manager** automates the process of changing SMP Gateway and IED passwords.
R6. Security Status Monitoring […] *shall ensure that all Cyber Assets … implement automated tools or organizational process controls to monitor system events that are related to cyber security* […]	**IED Manager Suite** and **SMP Gateway** log all access attempts, whether successful or not, and generate security events. Logs and events are published through Syslog to be processed by a third party SIEM. **SMP Gateway** internal data points can be used to report failed login attempts, the locked-out state of an account, remote maintenance connections and dialup access.
CIP–009 Recovery Plans for Critical Cyber Assets	
R4. Backup and Restore […] *shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets* […]	**IMS Configuration Manager** stores all the configuration files required to restore all **SMP Gateways** and managed devices.