Siemens RUGGEDCOM CROSSBOW Secure Access Manager and Station Access Controller

Siemens RUGGEDCOM CROSSBOW is a proven Secure Access Management solution designed to provide NERC CIP compliant access to Intelligent Electronic Devices.

Introduction

Siemens RUGGEDCOM CROSSBOW is a scalable solution tailored to the ever increasing industrial and utility asset owners needs. It provides cyber-secure local and remote user access to and management of all Intelligent Electronic Devices and their associated files. It is an enterprise class solution in compliance with the comprehensive and evolving US NERC CIP standard.

RUGGEDCOM CROSSBOW is a unique cyber security system designed to be simple, economical and intuitive enough to be operated by large numbers of personnel according to, and without inhibiting their normal duties. Users of the system could be from a diverse group of staff associated with:

- Asset condition monitoring
- Event response and investigation
- Maintenance (including vendors)
- Control, protection and telecommunications engineering

CROSSBOW allows an Intelligent Electronic Device (IED) maintenance application to remotely communicate with its associated IEDs as if the users were directly connected to the device.

CROSSBOW’s client-server architecture is designed to allow a large utility to easily manage remote connectivity to its entire population of field IEDs. User access is role based, and the user is not provided with any device password or network topology detail. User access is governed by the appropriate authentication model (e.g. Active Directory, RSA SecurID) and all user activity is logged and reported per the NERC CIP specification.

When used in combination with the RUGGEDCOM CROSSBOW Station Access Controller for local substation access, the RUGGEDCOM CROSSBOW system provides an integrated, comprehensive solution with a seamless configuration environment, ensuring IED connectivity and activity logging is maintained at the substation level, even if the connection to the central server is disabled.

In addition, CROSSBOW allows extensive automation of common device management tasks, such as password changes, file retrieval, and configuration management. CROSSBOW functionality may be extended through scripts and plug-ins, allowing users to develop automated solutions to their unique requirements.
CROSSBOW’s client-server architecture is designed to allow a large utility to easily manage remote connectivity to its entire population of field IEDs. Key features include:

- Vendor agnostic design that works with all common substation gateways and IEDs, allowing deployment without adding or upgrading substation devices;
- An intuitive, complete product solution for ease of use and configuration:
  - Competitive solutions rely more heavily on integrating multiple 3rd party technologies together, making deployment and maintenance more complicated;
- A scalable, extendable platform, including:
  - Password management of relays and gateway devices;
  - Firmware management of relays and gateway devices;
  - Device configuration management (e.g. relay settings);
  - Event file (e.g. fault oscillography) retrieval, either on demand or automatically scheduled.
- Integrated file management facility allows utility staff to control and retrieve device related files:
  - Includes version control, check-in/check-out, access control, and reporting;
  - Includes management of files associated with electromechanical and non-communicating devices, which may otherwise have no means of file management.

A unique solution for local or emergency substation access, the CROSSBOW Station Access Controller provides the same level of security at the substation by pushing CROSSBOW database updates out to the field. This unique offering runs natively on the RUGGEDCOM ROX operating system, so no additional substation computers are required.

**Benefits**

- Meets NERC standards for cybersecurity
- Strong (2-factor) authentication
- Individual user accounts and privileges
- Audit log of activity
- WAN or dial-up access to remote devices

**Security**

Integration with Active Directory, RSA SecurID and other enterprise authentication solutions

- Individual user accounts with highly configurable permissions
- Audit log/reports of all activity
- Ability to block commands on a per device type/per user basis
- Role based user access control
- Local substation access control through Station Access Controller

**Enterprise integration**

- Reporting interface into event management systems (Industrial Defender, TDi, OSIsoft)
- Microsoft SQL server-based

**NERC CIP compliance**

CROSSBOW has maintained a leadership position in the market and continues to evolve with the evolution of the standard as the first commercially available application for addressing NERC CIP compliance. When combined with RUGGEDCOM routers and multi-service platforms, CROSSBOW offers one of the only completely integrated solutions for the substation:

- One-click compliance reports
- Following the CIP requirements set out for access control and change management
- User activity (key stroke) logging

**Ease of administration**

- Administration interface allows management of thousands of IEDs and hundreds of users
- Structured view of IEDs (region/substation/gateway)
- Grouping of devices and users
- Configurable sub-admins

**Flexible architecture**

- Client-server or “clientless” architecture using virtual desktops
- Available redundancy
- Dial-up or WAN access

**Broad device support**

Preserves investment in legacy gateway devices and communication infrastructure

- Siemens RUGGEDCOM routers and switches
- Siemens SIPROTEC
- Garrettcom
- GE
- ABB
- Novatech
- Cooper
- RFL
- Industrial Defender
- Many other IEDs
System overview

System architecture

The diagram on the left illustrates a typical utility architecture using RUGGEDCOM CROSSBOW. The CROSSBOW Secure Access Manager (SAM) is the central enterprise server through which all remote connections are made, and is the only trusted client source for the IEDs. This is the heart of the system, providing user role-based access control, site and IED access management.

CROSSBOW clients connect to the SAM via secure SSL connections to provide user access to remote IEDs. The SAM is connected over a secure WAN to substation gateway devices, such as RUGGEDCOM RX1500, or other supported device. The gateway connects to IEDs either directly or through downstream RTUs.

CROSSBOW SAM also connects through to IEDs with their own direct modem access such as for pole top applications, meters or process control, condition monitoring IEDs, and other host computer/servers. This ability of CROSSBOW to provide secure RBAC remote access to any IED makes it an essential tool for any IED based application for:

- Utilities (electricity, water, gas)
- Transport control systems
- Industrial and mining applications
- Building/site management systems

Typical workflow

RUGGEDCOM CROSSBOW is specifically designed to be intuitive and enhance users’ normal activity. After logging in to the central SAM server, the user will be presented with a simple directory structure, displaying regions, substations and devices, to which that user has been granted access to by the administrator.

From there, the user simply clicks on a chosen device to display a list of applications associated with the device. Selecting a program will instruct CROSSBOW to launch the application and initiate a connection to the device – no need to negotiate connections, boot applications, or remember passwords. In most cases – just one click - and the user is interacting directly with the device. Sophisticated password management functionality allows remote management of all router, gateway, and IED passwords.
RUGGEDCOM CROSSBOW Secure Access Manager

The CROSSBOW Secure Access Manager (SAM) runs on an enterprise grade Windows server platform, either on dedicated hardware or a virtual machine. When a CROSSBOW client initiates a connection from its maintenance application to a remote device's maintenance interface, it contacts the CROSSBOW server.

The SAM server verifies the authenticity of the user, either through a personal user name and password login (basic security), or through interaction with a corporate security system (strong authentication), in order to establish the Role Based Access Control permissions. After verification, the SAM server establishes a communication path to the device, either directly or through one or more remote gateways. The RBAC is configured during the system (strong authentication), in order to establish the security), or through interaction with a corporate security system. The RBAC may be installed at the local or substation level. The CROSSBOW SAC provides the same level of command control and logging when a user is physically present in the station, even when there is a loss of communication path between the central SAM and the remote site. The CROSSBOW SAC is completely synchronized with the CROSSBOW SAM server. The SAC may run directly on ROX (e.g. on a RUGGEDCOM RX1100/1500/1500D), or on the RUGGEDCOM RX1500 APE module.

Enterprise integration

Typically, most customers of RUGGEDCOM CROSSBOW will have their own enterprise security components such as Active Directory, RSA, or RADIUS, as well as SQL databases. CROSSBOW can integrate and make use of these components for authentication. The use of an SQL server is required by the CROSSBOW server to store its database. It is recommended that the utility makes use of its enterprise SQL servers to hold this database, as often the enterprise will have its own backup and redundancy systems in place.

CROSSBOW high availability

The CROSSBOW server can be licensed to make use of multiple servers configured as a cluster. This allows multiple servers to exist as a single entity, allowing more users to utilize the system at once, and for faster processing of automated tasks, such as fault record retrieval.

The user configures a CROSSBOW cluster via server side configuration. When a client connects to a server, the cluster information is sent to the client and stored locally. For example, CROSSBOW servers A and B are configured in a cluster. A user connects to A via the CROSSBOW client and is informed of the cluster configuration. On subsequent connections, the user will be prompted to connect to the cluster and the client will attempt to connect to server A. If this fails it will automatically attempt to connect to server B.

The SQL server(s) may also be configured in a cluster for high availability. The primary DB ships data to the mirror in real time. A typical cluster may contain 3 SQL instances: the primary DB, the mirror DB and a witness server (optional). In this configuration the witness monitors the status of the primary DB. The witness is an optional instance of SQL server that enables the mirror server in a high-safety mode session to recognize whether to initiate an automatic failover. Unlike the two partners (primary and mirror DBs), the witness does not serve the database. Supporting automatic failover is the only role of the witness; for this reason the CROSSBOW server doesn't require knowledge of the witness. If there is no witness instance, then the failover may be done manually.

CROSSBOW Application Modules

CROSSBOW Application Modules (CAMs) are separately licensed “plug ins” which may be added to any CROSSBOW server, version 4.1 or later. CAMs are run by the CROSSBOW scheduler, and may run at the following times:

- On demand, when invoked by a user with rights to do so
- On a periodic, scheduled basis
- Following special “trigger events,”

It is important to understand that CAMs are initiated and run from the CROSSBOW server, not from the client. Each CROSSBOW server may be configured to run multiple CAM operations in parallel, and in a redundant server, each member of a CROSSBOW cluster will process tasks in the scheduler queue.

Configuration management CAM

The configuration management CAM connects to managed devices, reads their settings, and compares this to their latest approved baseline. The configuration compare CAM may be used for a wide range of devices, such as protection relays, where it monitors all protection, logic, and communications setting, and routers, where it monitors firewall rules and other communications settings. Any variation from baseline results in an alert being generated. The current state of all devices may be viewed via CROSSBOW's reports.

Firmware version CAM

The firmware version CAM connects to managed devices, reads the firmware version, and compares the devices' current value to the values expected for that device. Any variation from baseline results in an alert being generated. The current state of all devices may be viewed via CROSSBOW's reports.

IED data retrieval CAM

Fault and event data collection is performed by the IED data retrieval CAM. CROSSBOW can gather the following data from IEDs:

- Target status
- Sequence of Events (SOE) data
- Fault reports
- Oscillography files

This data is gathered on a scheduled, polled basis, and also on demand. This command may be invoked by an authorized user, and also by an external system (e.g. energy management system) with an additional interface. A data poll may be directed at a device, a line, a substation, or other grouping of devices. All gathered data is stored in the CROSSBOW database, along with the time and date it was last updated.

RUGGEDCOM CROSSBOW Station Access Controller

CROSSBOW provides local and emergency connectivity through its optional Station Access Controller (SAC), which can be installed at the local or substation level. The CROSSBOW SAC provides the same level of command control and logging when a user is physically present in the station, even when there is loss of communication path between the central SAM and the remote site. The CROSSBOW SAC is completely synchronized with the CROSSBOW SAM server. The SAC may run directly on ROX (e.g. on a RUGGEDCOM RX1100/1500/1500D), or on the RUGGEDCOM RX1500 APE module.

Enterprise integration

Typically, most customers of RUGGEDCOM CROSSBOW will have their own enterprise security components such as Active Directory, RSA, or RADIUS, as well as SQL databases. CROSSBOW can integrate and make use of these components for authentication. The use of an SQL server is required by the CROSSBOW server to store its database. It is recommended that the utility makes use of its enterprise SQL servers to hold this database, as often the enterprise will have its own backup and redundancy systems in place.

CROSSBOW high availability

The CROSSBOW server can be licensed to make use of multiple servers configured as a cluster. This allows multiple servers to exist as a single entity, allowing more users to utilize the system at once, and for faster processing of automated tasks, such as fault record retrieval.

The user configures a CROSSBOW cluster via server side configuration. When a client connects to a server, the cluster information is sent to the client and stored locally. For example, CROSSBOW servers A and B are configured in a cluster. A user connects to A via the CROSSBOW client and is informed of the cluster configuration. On subsequent connections, the user will be prompted to connect to the cluster and the client will attempt to connect to server A. If this fails it will automatically attempt to connect to server B.

The SQL server(s) may also be configured in a cluster for high availability. The primary DB ships data to the mirror in real time. A typical cluster may contain 3 SQL instances: the primary DB, the mirror DB and a witness server (optional). In this configuration the witness monitors the status of the primary DB. The witness is an optional instance of SQL server that enables the mirror server in a high-safety mode session to recognize whether to initiate an automatic failover. Unlike the two partners (primary and mirror DBs), the witness does not serve the database. Supporting automatic failover is the only role of the witness; for this reason the CROSSBOW server doesn't require knowledge of the witness. If there is no witness instance, then the failover may be done manually.

CROSSBOW Application Modules

CROSSBOW Application Modules (CAMs) are separately licensed “plug ins” which may be added to any CROSSBOW server, version 4.1 or later. CAMs are run by the CROSSBOW scheduler, and may run at the following times:

- On demand, when invoked by a user with rights to do so
- On a periodic, scheduled basis
- Following special “trigger events,”

It is important to understand that CAMs are initiated and run from the CROSSBOW server, not from the client. Each CROSSBOW server may be configured to run multiple CAM operations in parallel, and in a redundant server, each member of a CROSSBOW cluster will process tasks in the scheduler queue.

Configuration management CAM

The configuration management CAM connects to managed devices, reads their settings, and compares this to their latest approved baseline. The configuration compare CAM may be used for a wide range of devices, such as protection relays, where it monitors all protection, logic, and communications setting, and routers, where it monitors firewall rules and other communications settings. Any variation from baseline results in an alert being generated. The current state of all devices may be viewed via CROSSBOW's reports.

Firmware version CAM

The firmware version CAM connects to managed devices, reads the firmware version, and compares the devices' current value to the values expected for that device. Any variation from baseline results in an alert being generated. The current state of all devices may be viewed via CROSSBOW's reports.

IED data retrieval CAM

Fault and event data collection is performed by the IED data retrieval CAM. CROSSBOW can gather the following data from IEDs:

- Target status
- Sequence of Events (SOE) data
- Fault reports
- Oscillography files

This data is gathered on a scheduled, polled basis, and also on demand. This command may be invoked by an authorized user, and also by an external system (e.g. energy management system) with an additional interface. A data poll may be directed at a device, a line, a substation, or other grouping of devices. All gathered data is stored in the CROSSBOW database, along with the time and date it was last updated.
Server requirements

CROSSBOW server can run natively or in a virtual machine environment that meets the following requirements:

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>X86 compatible, 2GHz or faster</td>
</tr>
<tr>
<td>RAM</td>
<td>minimum 2 GB, 4 GB recommended</td>
</tr>
<tr>
<td>Disk</td>
<td>50 GB</td>
</tr>
<tr>
<td>Operating system</td>
<td>Windows 2008 server</td>
</tr>
</tbody>
</table>

CROSSBOW clients may also run in a CITRIX Xen App Server environment. This provides additional flexibility and security for remote access to the CROSSBOW system. The CROSSBOW client application is centrally hosted, and can be accessed by any device. Additionally, client application management cost and complexity are reduced.

System licensing

The CROSSBOW system is designed from the ground up to be scalable from small initial deployments to larger systems in the future. This is supported in the licensing model. The capabilities of the CROSSBOW system are controlled by a license file installed on the central SAM server. Core features of the product are included as standard, such as:

- Device and user access control
- Password management
- Reporting for NERC CIP compliance and device access

Other features previously mentioned in this document are optionally available as part of the licensing components.

IED definition

Within the licensing component there is an option to select the number of IEDs that may be configured within the system. From the point of view of the SAM server, an IED is any device that is to be configured in the CROSSBOW system which a user might want to connect to. This includes networking devices, serial device servers, HMI screens, PCs and data concentrators.

System support

Enhanced software maintenance is available that provides:

- Software upgrades, both minor bug fix releases as well as major feature releases
- New features and functionality delivered in a software release
- Device Support Packages (DSPs). These packages are periodically released as support for new devices becomes available. DSPs are rolled into the next software release
- Automatic notification of updates, patches, and fixes to the existing version of the customer’s product

Ongoing maintenance support is charged as a percentage of the system license price per annum.

Optional components

Strong authentication user licensing

Allows users in the CROSSBOW system to authenticate using strong methods e.g.: Active Directory, RSA, RADIUS, etc.

- 5 strong authentication user interfaces (minimum)
- 10 strong authentication user interfaces
- 25 strong authentication user interfaces
- 50 strong authentication user interfaces
- 100 strong authentication user interfaces
- Unlimited strong authentication user interfaces

CROSSBOW Application Modules (CAMs)

Govern which CAMs may be active on the system, and also how many IEDs the CAM may be active for. Each CAM is available in instance quantities equal to the IED licensing quantities:

- Firmware version CAM
- Configuration management CAM
- IED data retrieval CAM
- Station Access Controller (SAC)

Governs the maximum number of Station Access Controllers that may be configured in the CROSSBOW system:

- Licensed equal to exact number of SACs required in system
- Price per SAC lowers dependant on quantity of total SACs in system

User licensing

Governs the maximum number of users that can be configured in the CROSSBOW system:

- 5 user license (minimum)
- 10 user license
- 25 user license
- 50 user license
- 100 user license
- Unlimited user license

Event Log Distribution Service (ELDS)

The CROSSBOW Event Log Distribution Service distributes event information gathered by CROSSBOW to other external event tracking systems. This service checks for events on a user-defined schedule, and sends the events to a specified target. Supported targets for this service include the Windows event log (which can therefore support any third-party system that can monitor the Windows event log), Syslog and e-mail.

- Priced per target system interface (1-4 targets)

Unattended Application Client (UAC)

The Unattended Application Client (UAC) is designed to act as an intermediary between the CROSSBOW server and certain unattended applications, such as SEL 5040. The UAC emulates a modem to provide the application with its expected communication interface, but operations initiated by the application are routed through the UAC to the CROSSBOW server, so that they can be logged to assist with NERC compliance.

- Priced per client (1-4 clients)
Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens’ products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

The information provided in this brochure contains descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.