SIEMENS

Ingenuity for life

RUGGEDCOM CROSSBOW

Secure Access Management Solution

Brochure 05/2018

usa.siemens.com/ruggedcom

RUGGEDCOM CROSSBOW is a proven Secure Access Management solution designed to provide cyber security compliance including NERC CIP access to Intelligent Electronic Devices.

Contents

Product overview

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

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

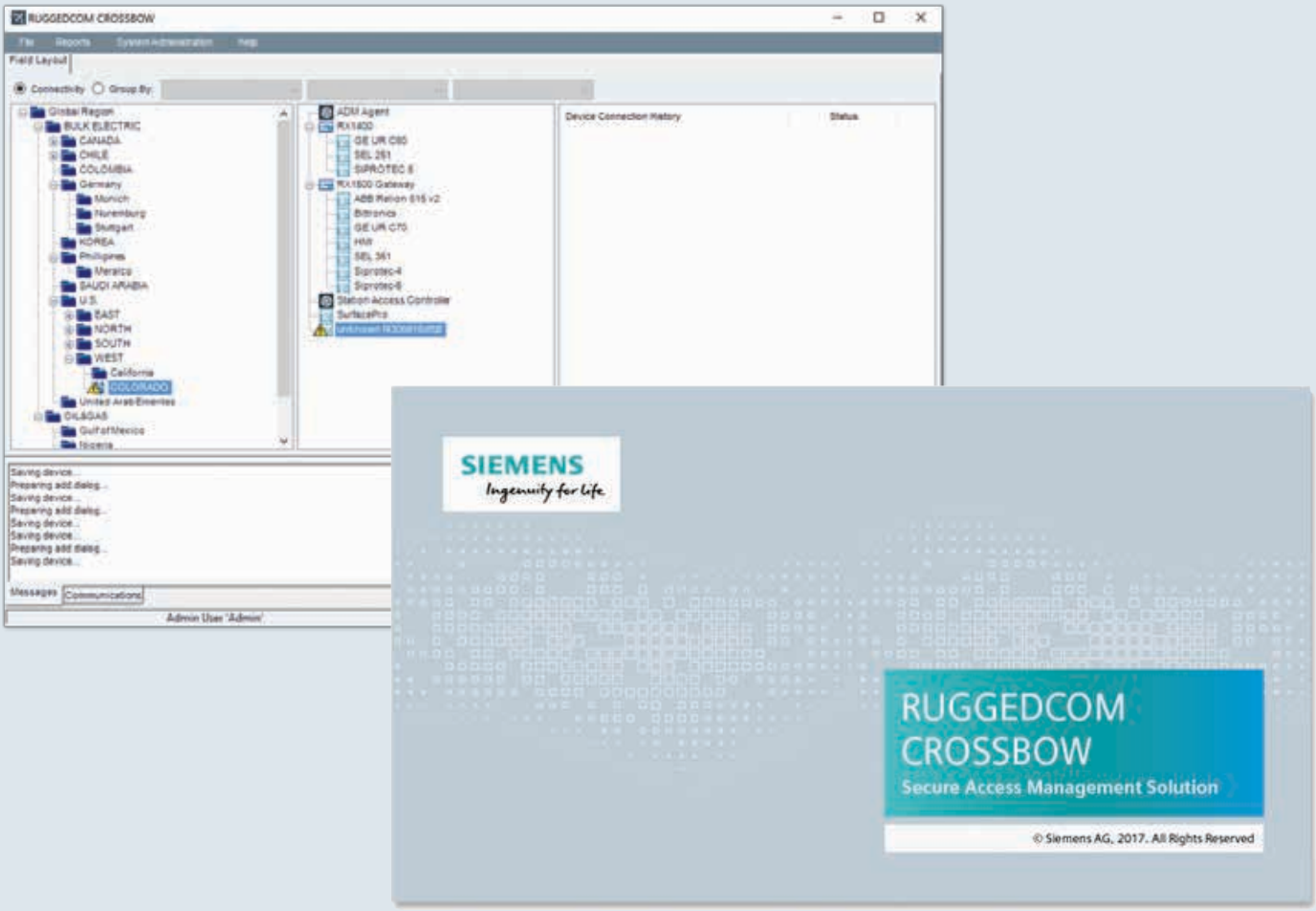
CROSSBOW allows an Intelligent Electronic Device (IED) maintenance application to remotely communicate with its associated IEDs as if the users were directly connected to the device. CROSSBOW's client-server architecture is designed to allow a large utility to easily manage remote connectivity to its 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 also provides a mechanism to discover previously unknown or transient devices connected to the IP network, providing an additional tool to enhance network security and maintainability.

Application overview



Client server architecture
The CROSSBOW client-server architecture is designed to scale to the needs of small, medium and large utilities while maintaining peak performance 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 Multi-Service Platforms based on ROX (Rugged Operating System), so no additional substation computers are required.

Benefits

- Meets NERC standards for cyber security
- 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
- Blocking and logging of specified IED commands
- Optional encryption between server and remote facility

Enterprise integration

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

NERC CIP compliance
As the first commercially available application for helping customers with achieving NERC CIP compliance, RUGGEDCOM CROSSBOW has maintained a leadership role in the field. 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

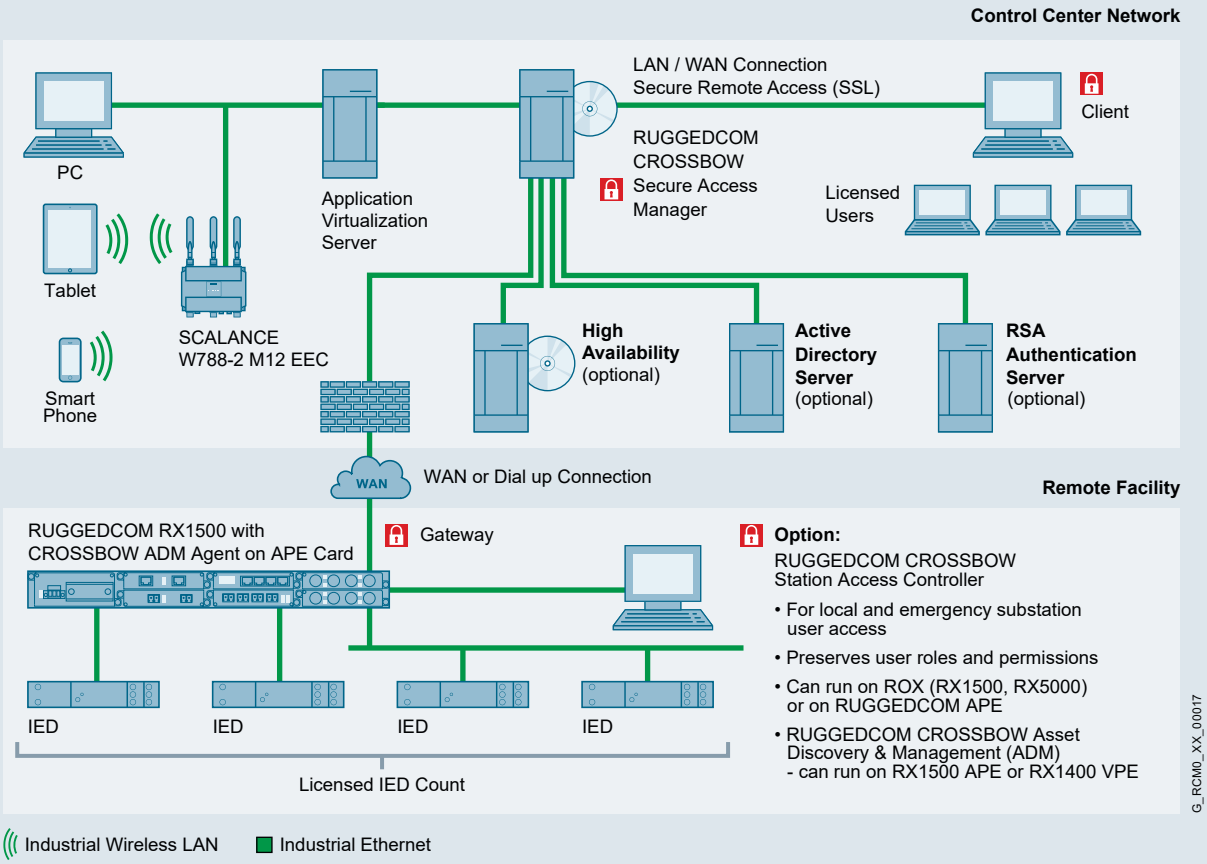
Flexible architecture

- 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
- SEL
- GE
- ABB
- Novatech
- Cooper
- RFL
- Industrial Defender
- Micom
- 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.

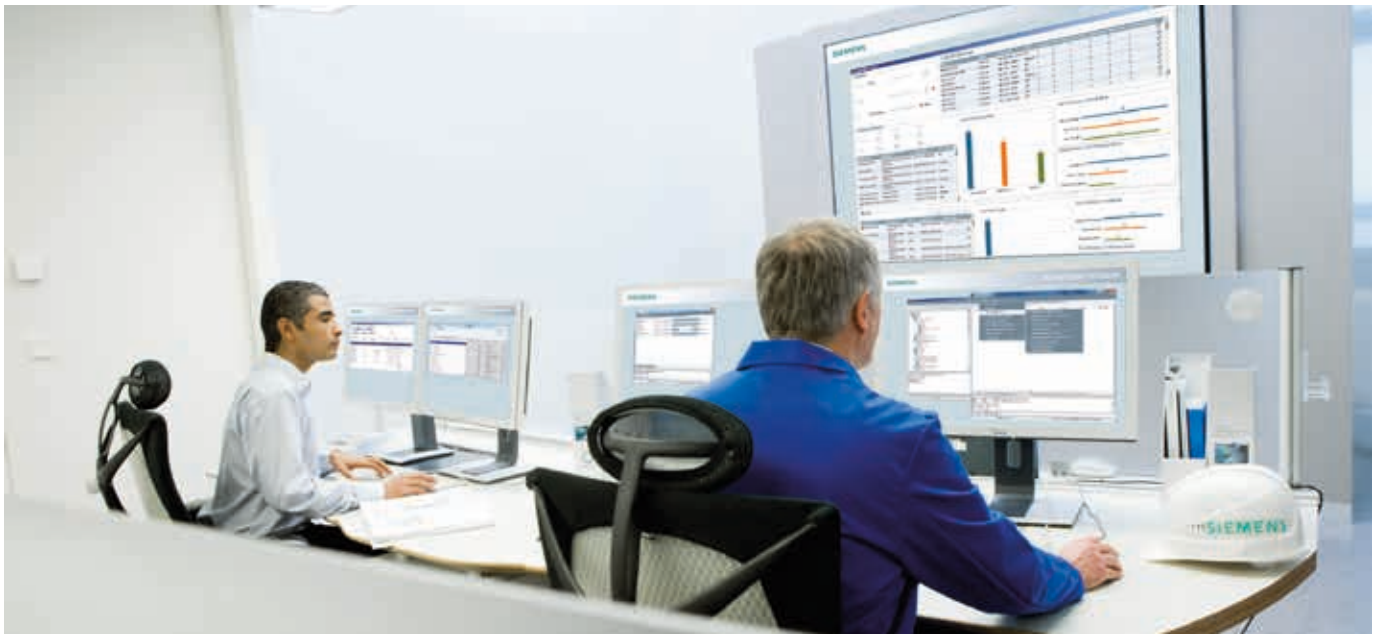
CROSSBOW SAM also connects through to IEDs with their own direct modem access such as for pole top applications, meters or process control, condition monitoring IEDs, and other host computer/servers. This ability of CROSSBOW to provide secure RBAC remote access to any IED makes it an essential tool for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

Secure Access Manager and Station Access Controller



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 allows the logged-in user to view all available devices. When a device is selected for connection, the CROSSBOW SAM server establishes a communication path to the device, either directly or through one or more remote gateways. The RBAC is configured during installation to control individual users and user groups to have varying arrangements of read/write access to IEDs, which can be controlled by region/facility/IED or even command level. The strong authentication option allows for integration of the user identification and permissions to be linked to the corporate system such as Active Directory, RSA SecurID or a RADIUS server.

RUGGEDCOM CROSSBOW Station Access Controller
CROSSSBOW offers 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 RX1500/RX5000), or on the RUGGEDCOM APE module.

Enterprise integration
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 SQL server is required by CROSSBOW SAM to store its database. It is recommended that the utility makes use of its enterprise SQL servers to hold this database, as 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).

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. Any variation from baseline results in an alert being generated.

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.

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

All gathered data is stored in the CROSSBOW database, along with the time and date it was last updated.

Connectivity CAM
The Connectivity CAM is designed to automate the monitoring of connectivity (i.e. CROSSBOW's ability to connect) to the devices in its database. The intent to ensure that any given end device remains available for other CROSSBOW communications (e.g. end user connections, other CAMs, etc.) and to alert an administrator when it is not.

Asset Discovery and Management
CROSSBOW Asset Discovery and Management (ADM) ensures that the operator has visibility to all network devices connected to monitored subnets. The key components are the ADM agents that reside on a RUGGEDCOM RX1500 APE module or RX1400 VPE virtual machine. The ADM agents are fully integrated into the CROSSBOW SAM, and passively monitor the subnet, and uses MAC and IP addresses to detect any network based device that is not contained in the CROSSBOW database. Upon detection of a previously unknown device an alert will be raised and a new "unknown" device will show up in the proper location on the CROSSBOW device tree view. CROSSBOW ADM will provide details of the unknown device, such as MAC / IP address and traffic type. If the device is legitimate it can be added and configured into the CROSSBOW database with a few mouse clicks.

Server and client requirements

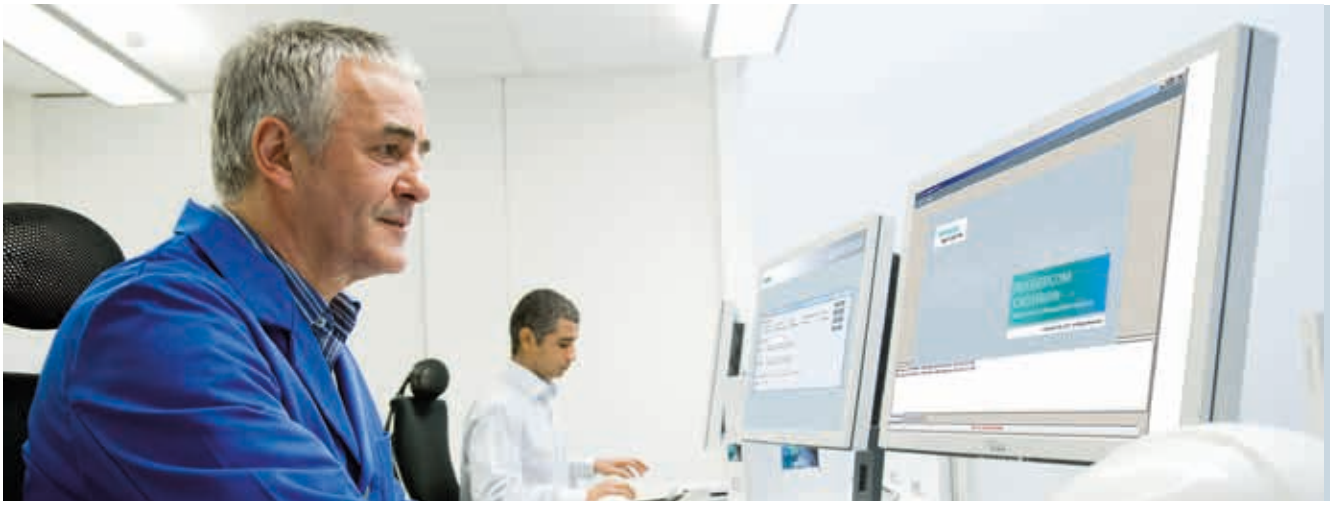
Server requirements

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

Component	Specification
CPU	x86 compatible, 2 GHz or faster
RAM	minimum 2 GB, 4+ GB recommended
Disk	50 GB
Operating system	Windows 2012 Server Windows 2012 R2 Server Windows 2016 Server *RUGGEDCOM CROSSBOW server components can run on 64-bit versions of the above operating systems

Client requirements

Component	Specification
CPU	x86 compatible, 1 GHz or faster 2 GHz or faster recommended
RAM	minimum 1 GB
Disk	1 GB
Operating system	Windows 7 Windows 8 Windows 10 Windows 2012 Server Windows 2012 R2 Server Windows 2016 Server *RUGGEDCOM CROSSBOW client components can run on 64-bit versions of the above operating systems



Component options

Optional components

RUGGEDCOM CROSSBOW Application Modules (CAMs)
Governs 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
- Connectivity CAM
- IED data retrieval CAM
- Station Access Controller (SAC)

Station Access Controller
Governs the maximum number of Station Access Controllers that may be configured in the RUGGEDCOM CROSSBOW system. Licensed equal to number of SACs required in system.

Asset Discovery & Management (ADM)
Governs the number of ADM Agents in the system. Licensed equivalent to the number of ADM Agents required in the system.

Event Log Distribution Service (ELDS)
The RUGGEDCOM 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)

External Database Integration Service (EDIS)
The External Database Integration Service provides a convenient way for CROSSBOW to integrate with other enterprise systems via an intermediate SQL database. This integration can be used to add/change devices in the CROSSBOW database, as well as share IED passwords with external password management systems. Priced on a per target system basis

Core component options

SAM server license

- RUGGEDCOM CROSSBOW SAM server software license
- RUGGEDCOM CROSSBOW SAM Quality Assurance (QA) testing server software license
- RUGGEDCOM CROSSBOW SAM high availability server software license

IED licensing
Governs the maximum number of IEDs that can be configured in the RUGGEDCOM CROSSBOW system. Licensed in blocks of 100 IEDs

User licensing
Governs the maximum number of users that can be configured in the RUGGEDCOM CROSSBOW system. Users can be configured with either CROSSBOW basic authentication, or strong authentication (Active Directory, RSA, or RADIUS). Licensed in blocks of 5 users

For more information, please visit:
usa.siemens.com/ruggedcom

Published by
Siemens Industry, Inc. 2018

Process Industries and Drives
100 Technology Dr.
Alpharetta, GA 30005

Subject to change without prior notice
Order No. RCBR-OAK02-0518
Article No. 6ZB5531-0AK02-0BA2

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit:
siemens.com/industrialsecurity

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under:
siemens.com/industrialsecurity

Scan this QR code for more information