

SIEMENS



RUGGEDCOM Software

Network Management and Secure
Access Management Solutions

Brochure

10/2017

siemens.com/ruggedcom-software

Rugged communication equipment requires equally rugged software. The RUGGEDCOM product line offers first-rate solutions for network management, secure remote IED access, data conversion, configuration and visualization.

Contents

RUGGEDCOM Software	3
RUGGEDCOM CROSSBOW	4
RUGGEDCOM ELAN	10
RUGGEDCOM REFLEX	14
RUGGEDCOM NMS	17
RUGGEDCOM DIRECTOR	21
RUGGEDCOM EXPLORER	22
RUGGEDCOM PING	23

RUGGEDCOM Software

RUGGEDCOM Software has been developed with our harsh environment customers in mind to provide network management and tools, secure remote IED access, data conversion, configuration and visualization solutions.

RUGGEDCOM Software is widely used in both field and enterprise environments. RUGGEDCOM software has been developed and tested to ensure high levels of reliability as well as robustness.

For installation guides and documentation for all RUGGEDCOM Software, visit Siemens Industry Online Support site (SIOS).

<http://support.industry.siemens.com>

RUGGEDCOM CROSSBOW

Secure Access Manager and Station Access Controller – application overview

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

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 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

RUGGEDCOM 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. The RUGGEDCOM CROSSBOW 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). 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 CROSSBOW system provides an integrated, comprehensive solution with a seamless configuration environment, ensuring IED connectivity. Activity logging is maintained at the substation level, even if the connection to the central server is disabled.

In addition, RUGGEDCOM 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.

RUGGEDCOM 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.

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;



A unique solution for local or emergency substation access, the RUGGEDCOM 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

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

Secure Access Manager and Station Access Controller – system overview

RUGGEDCOM CROSSBOW Secure Access Manager (SAM)

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

After verification, the SAM allows the logged-in user to view all devices available to the user. When a device is selected for connection, the RUGGEDCOM 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 (SAC)

RUGGEDCOM CROSSBOW provides local and emergency connectivity through its optional Station Access Controller, which can be installed at the local or substation level. The RUGGEDCOM 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.

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.



Enterprise integration

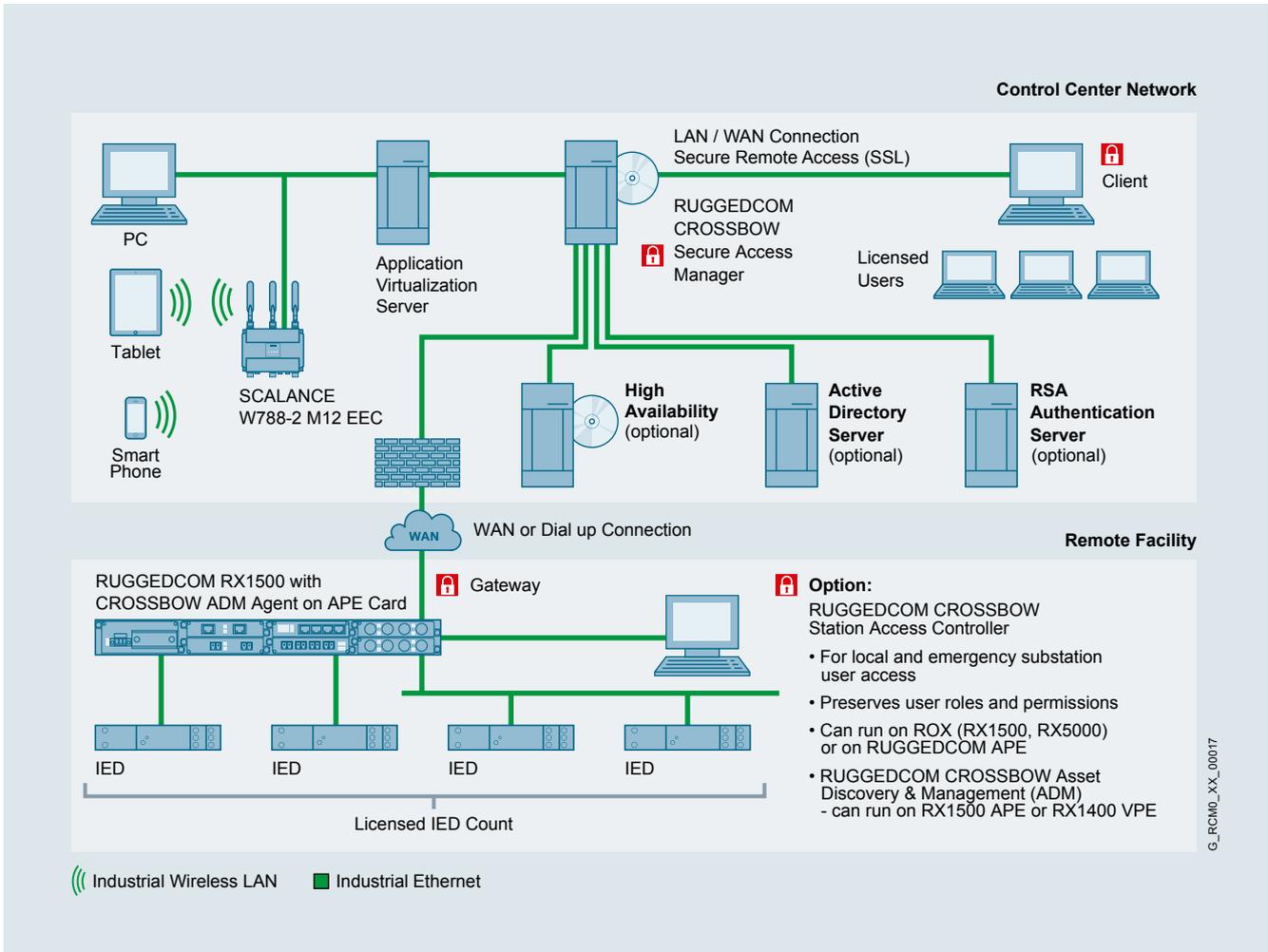
Most customers of RUGGEDCOM CROSSBOW will have their own enterprise security components such as Active Directory, RSA, or RADIUS, as well as SQL databases. RUGGEDCOM CROSSBOW can integrate and make use of these components for authentication.

System architecture

The diagram on the right illustrates a typical utility architecture using RUGGEDCOM CROSSBOW. The RUGGEDCOM 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. RUGGEDCOM CROSSBOW clients connect to the SAM via secure SSL connections to provide user access to remote IEDs.

RUGGEDCOM 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



RUGGEDCOM CROSSBOW system configuration

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 RUGGEDCOM 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 – the user is interacting directly with the device. Sophisticated password management functionality allows remote management of router, gateway, and IED passwords for supported devices.

Server requirements

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

Component	Specification
CPU	x86 Compatible, 4 core, 2 GHz or faster
RAM	4 Gigabytes or more, 8+ Gigabytes recommended
Disk	50 GB
Operating system	Windows Server 2012 (64-bit) Windows Server 2012 R2 (64-bit) Windows Server 2016 *RUGGEDCOM CROSSBOW server components can run on 64-bit versions of the above operating systems

Client requirements

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

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.



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, Syslog and e-mail. Priced per target system interface. (1-4 targets)

External Database Integration Service (EDIS)

The EDIS 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.



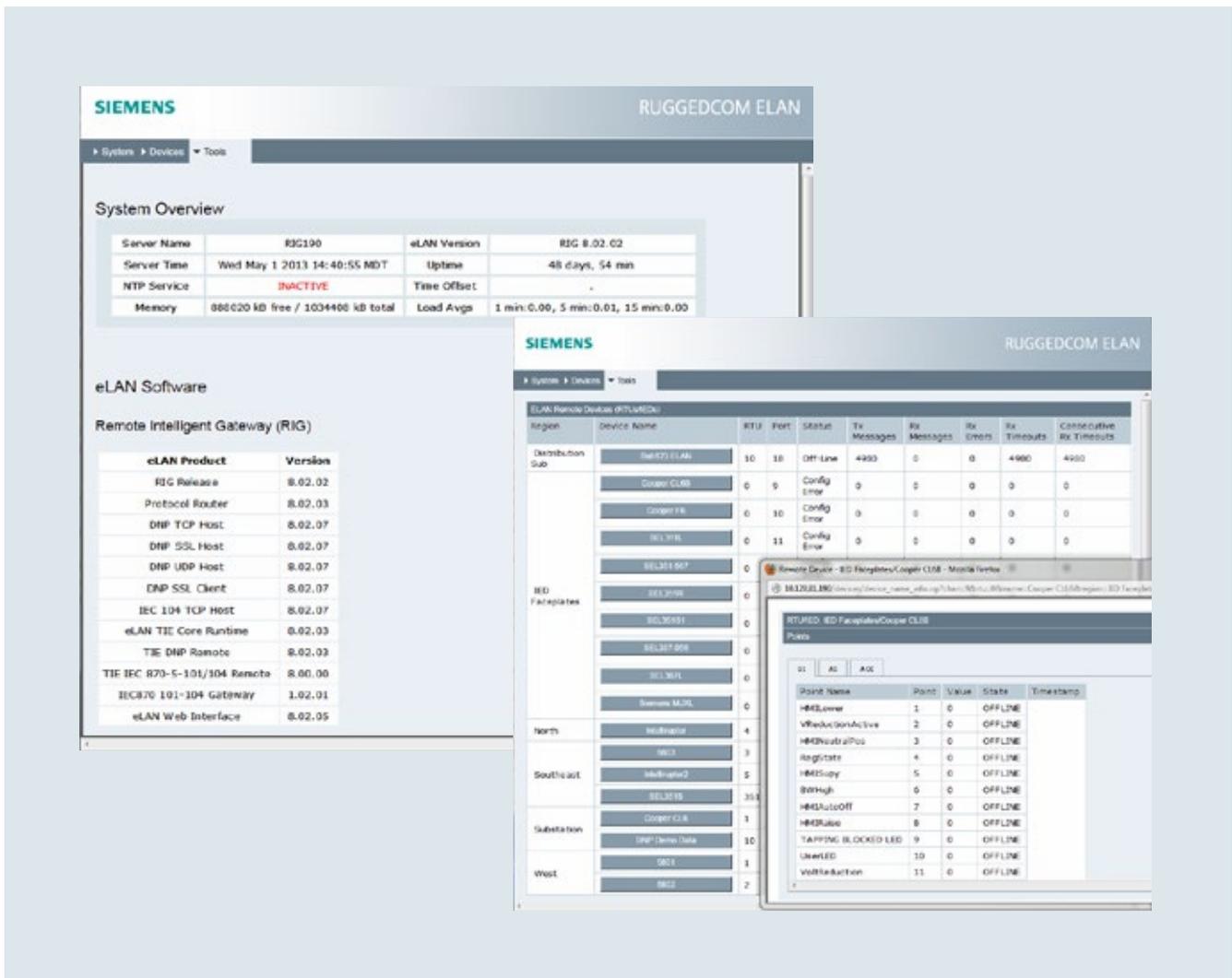
RUGGEDCOM ELAN

Data concentration and protocol conversion

RUGGEDCOM ELAN solves a wide range of communications and data integration issues, from the substation to the control center and into the enterprise.

The RUGGEDCOM ELAN family of products is based on the Linux operating system and includes the Substation Communications Server, Universal DNP Gateway, Remote Interface Gateway, and Front End Processor. Each product is focused on a specific application within the utility's communication infrastructure. The central benefit of using RUGGEDCOM ELAN solutions is that a broad range

of users within the utility are given secure access to the IED information that they require, made available in a format they understand, whenever they need it. When used with other RUGGEDCOM applications for secure remote access, data presentation and analysis, the user benefits from ease of integration and implementation.



Sample screenshots of RUGGEDCOM ELAN web interface



RUGGEDCOM ELAN is an off-the-shelf solution to a wide range of applications and system requirements, including:

- Protocol conversion
- Data concentration
- Serial to Ethernet (TCP/IP or UDP/IP) conversion
- Device proxy server
- Poll acceleration
- Multi-master support
- Protocol Routing
- Encryption, using TLS/SSL

RUGGEDCOM ELAN is based on the robust, flexible Linux architecture, and is available on a variety of diskless hardware platforms and I/O configurations, including integration with the RUGGEDCOM RX1400, the RUGGEDCOM RX15xx ROX II family of devices, and the RUGGEDCOM Application Processing Engine (APE). The Windows based RUGGEDCOM ELAN MAESTRO configuration tool allows rapid configuration and deployment of ELAN systems.

In addition to protocol conversion, RUGGEDCOM ELAN is also capable of protocol routing, which can be configured to provide the following functionality:

- Concurrent access: access to a single IED from multiple master stations
- Address masquerading: solves address contention issues
- Redundant host support: redundant hosts can eavesdrop traffic to/from the primary host

Built in redundancy

RUGGEDCOM ELAN supports two modes of redundancy:

1. Communications path redundancy: in this mode two RUGGEDCOM ELANs are used to communicate with an end device. There is typically a PRIMARY path to the end device as well as a

SECONDARY path. The RUGGEDCOM ELAN router can detect which route is active (connected or disconnected) and will forward messages from the master station to the end device via the appropriate channel. The two RUGGEDCOM ELAN servers communicate this pathing information to one another so each of them is aware of the available paths to the end device(s).

2. Substation/ELAN gateway redundancy: in this mode the full substation communications gateway is redundant with two RUGGEDCOM ELAN servers. In this mode the two RUGGEDCOM ELAN servers communicate with one another to determine which one of them is the PRIMARY and which one is the SECONDARY/STANDBY. If the PRIMARY goes down, it will be detected by the SECONDARY, and all traffic will be switched and routed by the SECONDARY until the PRIMARY recovers.

Universal data gateway

RUGGEDCOM ELAN UDG is the core of the ELAN application family created to address specific protocol conversion and translation issues related to RTUs, protection relays, PLCs, DFRs and other utility IEDs. Typical protocol support includes all of the following, along with lesser known formats:

- DNP3
- IEC-61850
- IEC 870-5-101
- IEC 870-5-104
- IEC 870-5-101 to 104 Gateway (Device level protocol conversion)
- Modbus

RUGGEDCOM ELAN UDG solves two common problems when deploying DNP 3.0:

1. Poll latency. Placing an ELAN UDG between masters and high latency RTUs and IEDs allows data to be readily available during the polling cycle. This results in lower overall latency and better network utilization.
2. Multi-host support. Multiple virtual instances of a given field device (a.k.a. Virtual RTU–VRTU) allow for multiple masters to independently communicate with them. The point map is preserved throughout to the master station. It is also possible to have multiple RTUs and IEDs mapped into a single VRTU, thus ELAN server acts as a data concentrator.

Substation Communications Server

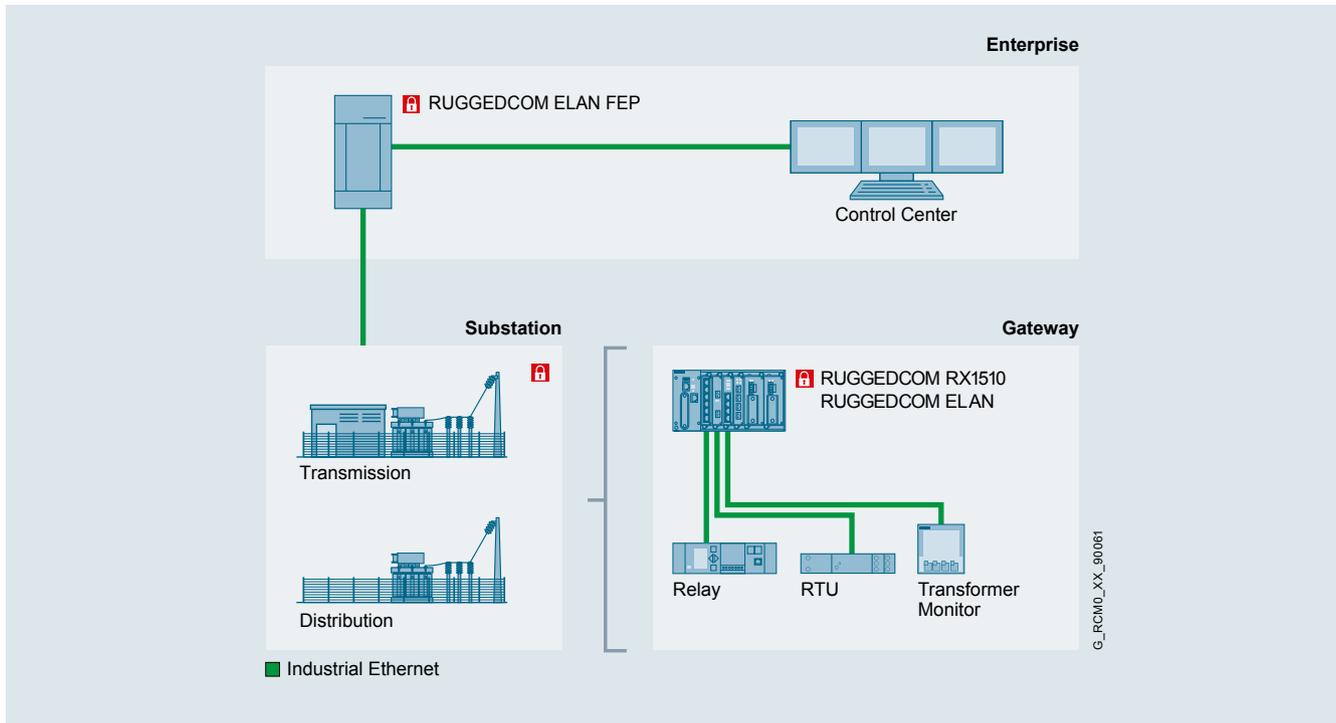
The RUGGEDCOM ELAN SCS typically resides in the substation and has direct connection to all IEDs. It provides a single point of access over a Wide Area Network (WAN), or modem connection (dial-up or leased line). The strength of the ELAN SCS lies in its ability to support multiple, concurrent host interfaces, each getting the specific data it needs.

For example, from a particular relay, SCADA data may be sent to the EMS using a SCADA protocol, a different subset of data may go to a historian, and fault files may be automatically extracted and distributed to interested users.

Front-End Processor

The RUGGEDCOM ELAN Front-End Processor is packaged to address the need to manage communications from remote sites, over a range of communications media. The RUGGEDCOM ELAN FEP provides protocol mediation capability in a vendor-neutral configuration, allowing users of a wide range of EMS systems to offload many of the tasks of managing communications with their field devices. RUGGEDCOM ELAN FEPs are frequently deployed to provide capabilities not available in native front ends, such as IP network support, security, or simply as a cost effective way to add additional ports.

The RUGGEDCOM ELAN FEP is based on the field-proven TIE (Telemetry Integration Environment) module, which was originally developed as the telemetry front end for a major EMS vendor and is currently installed in over 50 utilities worldwide.



RUGGEDCOM ELAN substation automation and integration

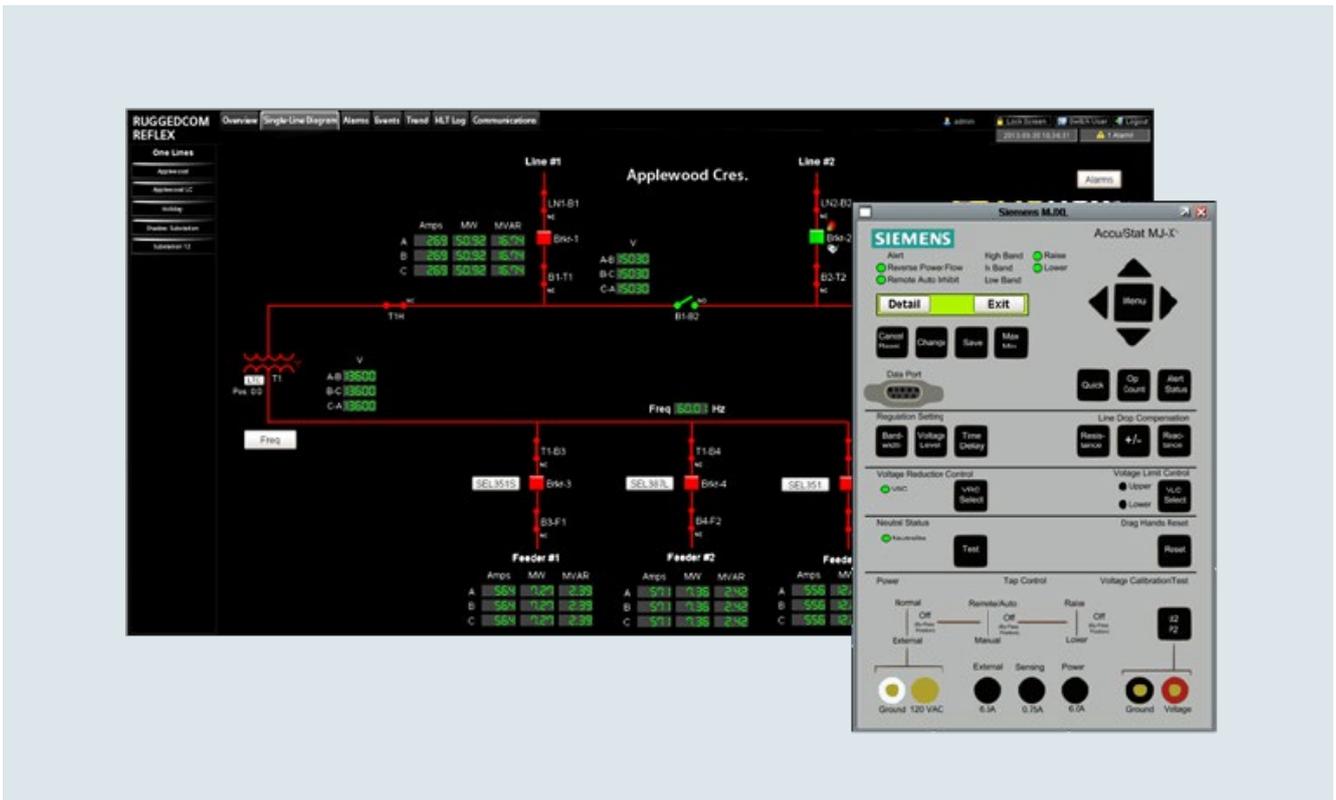
RUGGEDCOM REFLEX

Substation HMI, monitoring and control for distribution systems

RUGGEDCOM REFLEX substation HMI is a purpose built solution for local and remote monitoring and controlling all aspects of substation operations.

Whether you need support for users locally or remotely, RUGGEDCOM REFLEX makes information available through the following ready-to-deploy features:

- Single line diagram with rich graphics editor
- Multiple protocol support
- Faceplate emulation of many IEDs
- Alarm acknowledgement and summary
- Sequence of events summary
- Graphical trending of values
- Extensive reporting facility
- Historian option to record years of information



RUGGEDCOM REFLEX HMI and visualization

Custom screens and applications can also be quickly developed using the RUGGEDCOM REFLEX advanced scripting language. The RUGGEDCOM REFLEX device interface library is large, with more than 50 protocol interfaces that allow you to get to data from decades old RTUs as well as the latest 61850-based IEDs. RUGGEDCOM REFLEX can also be combined with the RUGGEDCOM ELAN Substation Communications Server to extend data visualization to include non-operational data and enhance reliability by partitioning the data acquisition and visualization functions.



Network view

In order to see the state of a substation network at a glance, RUGGEDCOM REFLEX provides a highly customizable view that can be panned and zoomed quickly. Drill down into device faceplate emulations or detailed data summaries, while keeping a view of the network in the background.

Hot line tagging

RUGGEDCOM REFLEX allows a user to select any system point or device and tag it with information or inhibit controls to devices, such as a breakers or reclosers. A visual indicator on the single line diagram shows the operator at a glance which devices have hot line tags applied and will ensure that close commands cannot be given.

Historical data logging

On occasion, real-time information isn't enough. For this reason, RUGGEDCOM REFLEX has an integrated historian feature using our open source database that allows users to tag data points for capture simply by checking a box. For most substation HMI applications this historian will grant rapid access to months and years of information.

Rapid deployment

RUGGEDCOM REFLEX web and database-centric architecture allows for ultimate flexibility in getting projects developed quickly and cost effectively. Electric utility specific templates and graphic elements allow for rapid design and deployment. Many device types, such as commonly used relays, recloser controls, remote terminal units and power quality meters are supported out-of-the-box and are quickly configurable.

Powerful graphics editor

Users can go beyond the standard graphic elements, such as breakers, buses, transformers and faceplates to create their own customized view of the world. Drag and drop graphic elements and shapes as well as custom drawing tools are provided to allow for unlimited flexibility in tailoring the visibility.

Scalability

RUGGEDCOM REFLEX is based on modern software architecture and systems: Java, web servers, databases and protocols. Combined with advanced features like load-balancing clustering and client re-targeting, its scalability is exceptional. From a single user HMI application to enterprise wide SCADA that spans service territories via corporate WANs to provide the base for a future Distribution Management System, REFLEX is designed to expand to virtually any requirements.

Security

RUGGEDCOM REFLEX was built with security in mind from the ground up. Communication channels are encrypted using SSL technology. SCADA projects use advanced role-based authentication, and can integrate seamlessly with corporate network security using Microsoft Active Directory®.

Logical data creation

Users can manipulate actual data points to generate pseudo and logical data points using RUGGEDCOM REFLEX integrated logic engine functionality. Beyond data generation, users can implement automation schemes using the built in logic engine.

Alarm view

The purpose built alarm view gives users an immediate snapshot of all alarm states, with the ability to acknowledge and clear on a selected basis.

Alarms can be configured based on the following criteria:

- Binary change of state with the ability to customize alarm descriptions
- Analog dead bands with five severity levels
- Optionally send an e-mail or SMS text to a person or distribution list

Event view

The built-in sequence of events view uses a powerful data interface engine to generate a tabular, chronological view of event history regardless of device type. Binary state changes as well as logical data points moving out of range can be triggered to be included in either event or alarm views.

Trending

Virtually any point can be displayed in the trend view with the ability to quickly alter the view based on:

- Data source assignment
- Multiple pen colors
- Slide bar display for date and time ranges
- Pan and zoom
- Real-time or historical trending modes

E-mail notification

To enhance user awareness of critical system events, RUGGEDCOM REFLEX provides an easy to configure notification facility. E-mails or text messages can be generated to notify individual users or user groups of events of interest, including relevant data files if necessary.

Cost effective client access

With a web-launched client architecture customers don't have to choose only a select few to have the system on their computer. Any desktop, laptop or tablet capable of running Java or a web browser can have access to information.

Mobility without boundaries

RUGGEDCOM REFLEX web-launched architecture also makes it easier than ever to support field personnel who need to securely monitor and control devices. Our Java engine insures cross platform support (Windows, Linux, iOS, Android) and visibility on virtually every laptop, tablet or smart phone. No client software installation is required, just connect to the RUGGEDCOM REFLEX server like any other user.

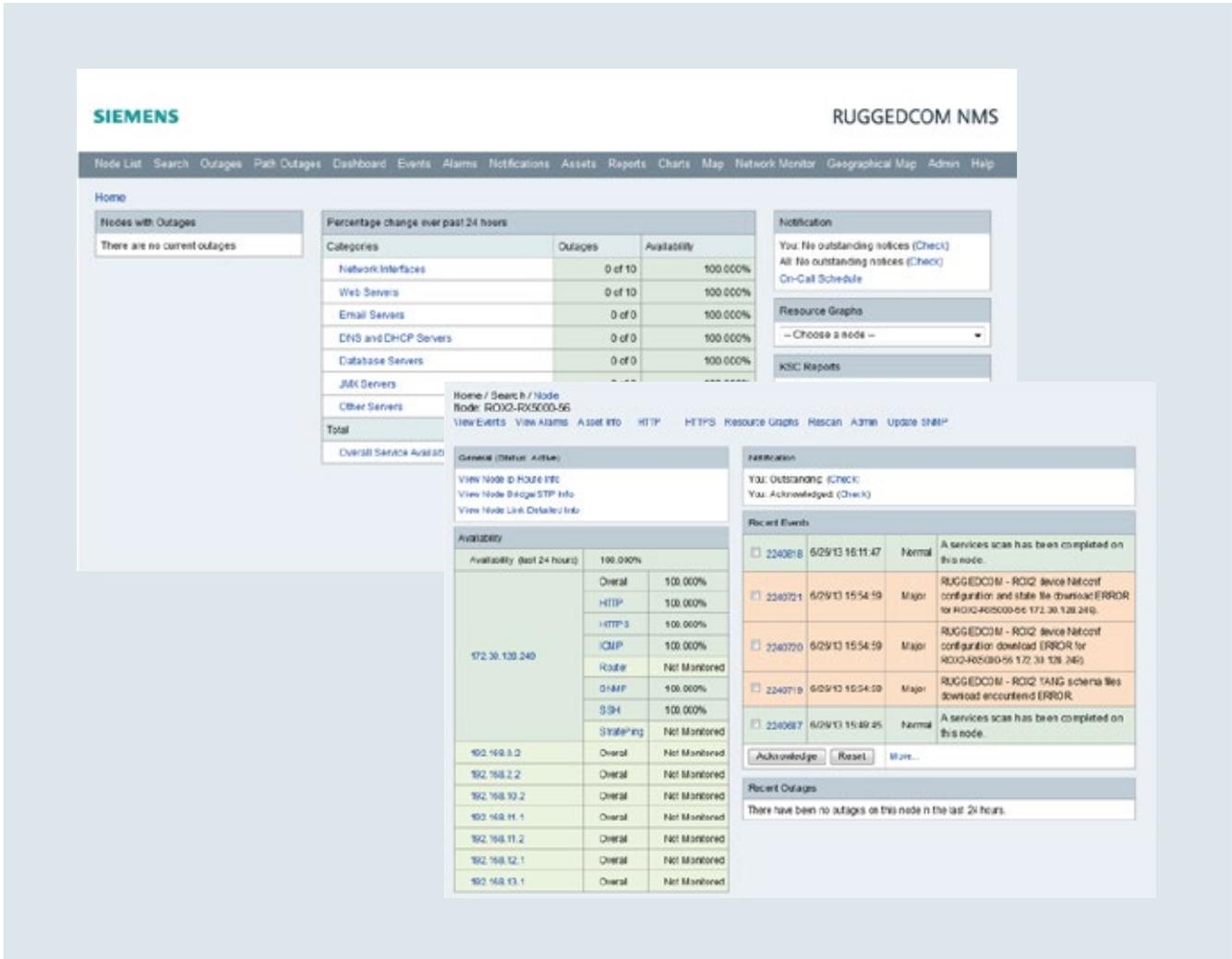
User friendly

RUGGEDCOM REFLEX is based entirely on modern, cross-platform technology, such as web (HTTP+SSL), SQL databases, and Java. This insures that the investment is not boxed in to a specific database or operating system.

RUGGEDCOM NMS

Network Management software





The home page (top) shows the availability of all the nodes under management by RUGGEDCOM NMS. Managed node information screen (bottom) shows the node status, including services availability.

RUGGEDCOM NMS is scalable, fully-featured, enterprise grade software for monitoring, configuring and maintaining RUGGEDCOM mission-critical networks. It improves operational efficiency, speeds up system provisioning, and preserves data validity, while allowing focus on the key events in the network.

Product overview

- Centralized web based management of the RUGGEDCOM and IP-network
- Auto-discovery of device links and services and representation on a network map
- Real-time monitoring and notification of events, alarms and thresholds

- Continuous collection of traffic statistics for analysis and reporting
- Deployment of firmware/software upgrades across RUGGEDCOM devices
- Automatic backup of RUGGEDCOM device configuration data
- Creation of templates and propagation of configuration changes across ROX II devices
- Monitors Rugged Operating System (ROS) and ROX II configurations and reports changes that exceed the authorized user-defined boundaries
- Bulk password changes of ROS, ROX I based RUGGEDCOM devices, as well as RUGGEDCOM WIN products

Automated network discovery and data polling

RUGGEDCOM NMS has a configurable versatile polling engine. Devices are discovered using ICMP pings and upon RUGGEDCOM NMS receiving traps or logs from a device. Services are detected for devices supporting LLDP and a topology map is created. All discovered devices have their performance data regularly collected by the NMS polling system.

Alarms and event management

RUGGEDCOM NMS continuously monitors the network and reports any changes or errors it detects. Events can originate outside RUGGEDCOM NMS, such as SNMP traps or syslog messages generated by devices under management. NMS can also generate events internally, such as upon the detection of a new device or when forcing a service scan of a device. Alarms are events that have been selected as being representative of the current health of the network.

Many alarms can be cleared by the system without operator intervention. For example, when an alarm posted for a broken network link subsequently receives an event indicating the network link has been reestablished, the alarm condition is then removed from the alarm List. RUGGEDCOM NMS users can quickly and intuitively create and manipulate complex filtering criteria for the list of events and alarms to display. It is also possible for events and logs received by RUGGEDCOM NMS to be forwarded to one or multiple destinations.

Network performance monitoring and reporting

RUGGEDCOM NMS continuously collects traffic statistics for analysis and reporting. Reports allow a network operator to assess the current and historical health of the network. These reports provide the tools needed to pro-actively detect issues and correct them before an outage or unacceptable network latency occurs.

Through the Network Monitor feature, RUGGEDCOM NMS learns the traffic characteristics of all devices supporting RMON 2 on a network.

- Monitors network traffic for abnormal behavior such as a rapid rise or fall in throughput
- Triggers RUGGEDCOM NMS events and notifications on discovery of abnormal traffic conditions
- Automatically adjusts the monitoring baseline over time to account for natural increases in network traffic and allows users to define their own customized threshold rules

Network mapping

RUGGEDCOM NMS provides powerful, flexible, browser-based mapping of network entities under NMS management. It can automatically map and lay out a selected set of devices, save and restore custom map views, perform live map updates, display map updates in real-time, and more.

- Icons specific to each device type
- Hierarchical and organic views
- Grouping of multiple objects under a single icon
- Color coded representation of each node and link status
- Graphical representation of the bandwidth used between ports
- Network monitor usage Gauge (for overall usage of network bandwidth)
- Drill down capability by clicking on desired devices icon and getting detailed information
- A geographical map is also available for display of RUGGEDCOM WIN base stations

Management of RUGGEDCOM devices

RUGGEDCOM NMS is the perfect tool to perform the configuration management and maintenance of RUGGEDCOM devices running ROX, ROX II, ROS and WIN firmware. From a centralized platform, it is possible to perform a bulk update of device firmware. Configuration data is automatically backed up on the NMS server. NMS can also automatically change the password used on ROS and ROX I based RUGGEDCOM products, as well as RUGGEDCOM WIN products.

Dynamic configuration

RUGGEDCOM NMS minimizes the time required when configuring ROX II based devices with the use of templates dynamically created from the data of an existing device. The dynamic configuration feature allows viewing, manipulating and comparing configuration data and distributing changes across multiple devices easily and efficiently.

Firewall management

RUGGEDCOM NMS simplifies the deployment of firewall policies for RUGGEDCOM ROX II devices with an interface enabling to view policies configured and to efficiently deploy changes across multiple devices.

RUGGEDCOM DIRECTOR

Serial port redirector software

RUGGEDCOM DIRECTOR is a serial port redirection application that is designed to extend the life and reach of applications written for serial communications.

With RUGGEDCOM DIRECTOR, serial port communications are no longer limited by serial protocol cable length requirements or physical port counts that restrict the design and flexibility of networks and the ability to manage them.

Using RUGGEDCOM DIRECTOR, the application communications destined for host serial ports are mapped to the host LAN ports for transport across a TCP/IP network to RUGGEDCOM serial servers. This allows the host to be located centrally for easier management and maintenance and provides access to many more serial devices. The redirection is done seamlessly and with no modification required to the host application.

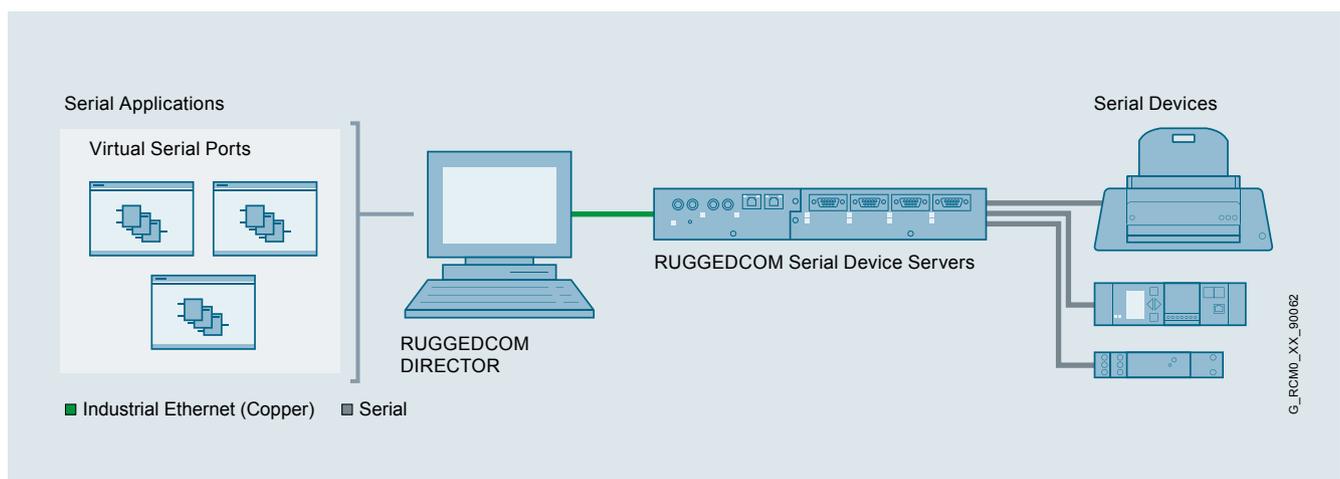
Getting up and running quickly is easy with the Windows based graphical user interface. Simply provide the port parameters on the application host and the RUGGEDCOM serial server and RUGGEDCOM DIRECTOR automatically generate the required connections.

The main interface window shows the connected ports, status and the number of packets sent and received providing real-time information on the health of system.

Troubleshooting is simplified with the logging feature of RUGGEDCOM DIRECTOR; the data flow on a selected port can be monitored in the detail dialogue window and directed to a file for further analysis. RUGGEDCOM DIRECTOR saves time and cost allowing legacy serial devices and applications to communicate over LAN connections without modification to hardware or software. RUGGEDCOM DIRECTOR is a complimentary software package designed to work with RUGGEDCOM serial device servers.

System requirements

Component	Specification
Operating system	Windows 7 (32 and 64 bit) Windows 7 Embedded (32 bit, running on an APE card) Windows 8 (32 and 64 bit) Windows 10 (32 and 64 bit) Windows Server 2012 (64 bit)



RUGGEDCOM DIRECTOR

RUGGEDCOM EXPLORER

RUGGEDCOM ROS device discovery and configuration software

RUGGEDCOM EXPLORER is a powerful tool to easily provision and configure new ROS based devices. Its built-in file transfer capabilities allow users to easily upload and download files and firmware from one convenient console.

Features

- Discover and configure new and existing RUGGEDCOM ROS devices on a LAN
- Intuitive GUI interface displays all ROS devices and visually identifies duplicate IP addresses
- Auto configuration capabilities on groups of devices
- Bulk firmware upgrade and file backup

Commissioning of new devices

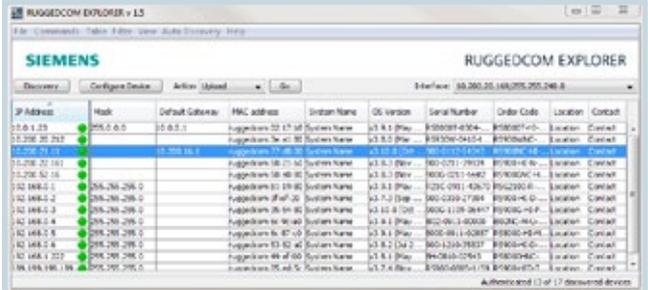
Allows a network of ROS devices to be commissioned in place on the network with no prior configuration necessary. Capable of discovering and configuring ROS devices that have been taken directly from the factory and connected to the network.

Bulk configuration or reconfiguration

Modifies the network and identification configuration parameters of one or multiple ROS devices, either one at a time, or using a template-based auto-incrementing tool.

Asset reporting

Generate a report of ROS based network device assets on a network segment. If RCDP is supported on all devices, RUGGEDCOM EXPLORER need not have any prior knowledge of IP addressing used by ROS devices.



The screenshot shows the RUGGEDCOM EXPLORER v1.5 interface. The main window displays a table of discovered devices with columns for IP Address, Host, Default Gateway, MAC address, System Name, OS version, Serial Number, Order Code, Location, and Contact. The table lists several devices, including Ruggedcom 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100. The interface also includes a menu bar (File, Commands, Table, Filter, View, Auto Discovery, Help) and a toolbar with buttons for Discovery, Configure Device, Action, Upload, and Go. The status bar at the bottom indicates 'Authenticated 13 of 17 discovered devices'.

IP Address	Host	Default Gateway	MAC address	System Name	OS version	Serial Number	Order Code	Location	Contact
192.168.1.23	192.168.1.23	192.168.1.1	88:88:88:88:88:88	Ruggedcom 32 17 18	3.2.1 (P)	R32001-4304-	R32001-4304-	Location	Contact
192.168.1.24	192.168.1.24	192.168.1.1	88:88:88:88:88:88	Ruggedcom 34 17 18	3.2.1 (P)	R34001-4304-	R34001-4304-	Location	Contact
192.168.1.25	192.168.1.25	192.168.1.1	88:88:88:88:88:88	Ruggedcom 36 17 18	3.2.1 (P)	R36001-4304-	R36001-4304-	Location	Contact
192.168.1.26	192.168.1.26	192.168.1.1	88:88:88:88:88:88	Ruggedcom 38 17 18	3.2.1 (P)	R38001-4304-	R38001-4304-	Location	Contact
192.168.1.27	192.168.1.27	192.168.1.1	88:88:88:88:88:88	Ruggedcom 40 17 18	3.2.1 (P)	R40001-4304-	R40001-4304-	Location	Contact
192.168.1.28	192.168.1.28	192.168.1.1	88:88:88:88:88:88	Ruggedcom 42 17 18	3.2.1 (P)	R42001-4304-	R42001-4304-	Location	Contact
192.168.1.29	192.168.1.29	192.168.1.1	88:88:88:88:88:88	Ruggedcom 44 17 18	3.2.1 (P)	R44001-4304-	R44001-4304-	Location	Contact
192.168.1.30	192.168.1.30	192.168.1.1	88:88:88:88:88:88	Ruggedcom 46 17 18	3.2.1 (P)	R46001-4304-	R46001-4304-	Location	Contact
192.168.1.31	192.168.1.31	192.168.1.1	88:88:88:88:88:88	Ruggedcom 48 17 18	3.2.1 (P)	R48001-4304-	R48001-4304-	Location	Contact
192.168.1.32	192.168.1.32	192.168.1.1	88:88:88:88:88:88	Ruggedcom 50 17 18	3.2.1 (P)	R50001-4304-	R50001-4304-	Location	Contact
192.168.1.33	192.168.1.33	192.168.1.1	88:88:88:88:88:88	Ruggedcom 52 17 18	3.2.1 (P)	R52001-4304-	R52001-4304-	Location	Contact
192.168.1.34	192.168.1.34	192.168.1.1	88:88:88:88:88:88	Ruggedcom 54 17 18	3.2.1 (P)	R54001-4304-	R54001-4304-	Location	Contact
192.168.1.35	192.168.1.35	192.168.1.1	88:88:88:88:88:88	Ruggedcom 56 17 18	3.2.1 (P)	R56001-4304-	R56001-4304-	Location	Contact
192.168.1.36	192.168.1.36	192.168.1.1	88:88:88:88:88:88	Ruggedcom 58 17 18	3.2.1 (P)	R58001-4304-	R58001-4304-	Location	Contact
192.168.1.37	192.168.1.37	192.168.1.1	88:88:88:88:88:88	Ruggedcom 60 17 18	3.2.1 (P)	R60001-4304-	R60001-4304-	Location	Contact
192.168.1.38	192.168.1.38	192.168.1.1	88:88:88:88:88:88	Ruggedcom 62 17 18	3.2.1 (P)	R62001-4304-	R62001-4304-	Location	Contact
192.168.1.39	192.168.1.39	192.168.1.1	88:88:88:88:88:88	Ruggedcom 64 17 18	3.2.1 (P)	R64001-4304-	R64001-4304-	Location	Contact
192.168.1.40	192.168.1.40	192.168.1.1	88:88:88:88:88:88	Ruggedcom 66 17 18	3.2.1 (P)	R66001-4304-	R66001-4304-	Location	Contact
192.168.1.41	192.168.1.41	192.168.1.1	88:88:88:88:88:88	Ruggedcom 68 17 18	3.2.1 (P)	R68001-4304-	R68001-4304-	Location	Contact
192.168.1.42	192.168.1.42	192.168.1.1	88:88:88:88:88:88	Ruggedcom 70 17 18	3.2.1 (P)	R70001-4304-	R70001-4304-	Location	Contact
192.168.1.43	192.168.1.43	192.168.1.1	88:88:88:88:88:88	Ruggedcom 72 17 18	3.2.1 (P)	R72001-4304-	R72001-4304-	Location	Contact
192.168.1.44	192.168.1.44	192.168.1.1	88:88:88:88:88:88	Ruggedcom 74 17 18	3.2.1 (P)	R74001-4304-	R74001-4304-	Location	Contact
192.168.1.45	192.168.1.45	192.168.1.1	88:88:88:88:88:88	Ruggedcom 76 17 18	3.2.1 (P)	R76001-4304-	R76001-4304-	Location	Contact
192.168.1.46	192.168.1.46	192.168.1.1	88:88:88:88:88:88	Ruggedcom 78 17 18	3.2.1 (P)	R78001-4304-	R78001-4304-	Location	Contact
192.168.1.47	192.168.1.47	192.168.1.1	88:88:88:88:88:88	Ruggedcom 80 17 18	3.2.1 (P)	R80001-4304-	R80001-4304-	Location	Contact
192.168.1.48	192.168.1.48	192.168.1.1	88:88:88:88:88:88	Ruggedcom 82 17 18	3.2.1 (P)	R82001-4304-	R82001-4304-	Location	Contact
192.168.1.49	192.168.1.49	192.168.1.1	88:88:88:88:88:88	Ruggedcom 84 17 18	3.2.1 (P)	R84001-4304-	R84001-4304-	Location	Contact
192.168.1.50	192.168.1.50	192.168.1.1	88:88:88:88:88:88	Ruggedcom 86 17 18	3.2.1 (P)	R86001-4304-	R86001-4304-	Location	Contact
192.168.1.51	192.168.1.51	192.168.1.1	88:88:88:88:88:88	Ruggedcom 88 17 18	3.2.1 (P)	R88001-4304-	R88001-4304-	Location	Contact
192.168.1.52	192.168.1.52	192.168.1.1	88:88:88:88:88:88	Ruggedcom 90 17 18	3.2.1 (P)	R90001-4304-	R90001-4304-	Location	Contact
192.168.1.53	192.168.1.53	192.168.1.1	88:88:88:88:88:88	Ruggedcom 92 17 18	3.2.1 (P)	R92001-4304-	R92001-4304-	Location	Contact
192.168.1.54	192.168.1.54	192.168.1.1	88:88:88:88:88:88	Ruggedcom 94 17 18	3.2.1 (P)	R94001-4304-	R94001-4304-	Location	Contact
192.168.1.55	192.168.1.55	192.168.1.1	88:88:88:88:88:88	Ruggedcom 96 17 18	3.2.1 (P)	R96001-4304-	R96001-4304-	Location	Contact
192.168.1.56	192.168.1.56	192.168.1.1	88:88:88:88:88:88	Ruggedcom 98 17 18	3.2.1 (P)	R98001-4304-	R98001-4304-	Location	Contact
192.168.1.57	192.168.1.57	192.168.1.1	88:88:88:88:88:88	Ruggedcom 100 17 18	3.2.1 (P)	R100001-4304-	R100001-4304-	Location	Contact

RUGGEDCOM EXPLORER

Network debugging

Reports the occurrence of duplicate IP addresses, or inconsistencies in IP address allocation among ROS devices.

Bulk firmware upgrade

Upgrades the firmware of one or multiple devices at once.

System backup

Archives in one single step the configuration, firmware, log, and other ancillary files of one or multiple devices.

Diagnostic data retrieval

Retrieves and archives diagnostic data (system logs and alarms) from one or multiple devices in a single step.

RUGGEDCOM PING

High accuracy graphical ping utility

RUGGEDCOM PING is a high accuracy graphical ping tool useful for monitoring a list of devices in order to measure in detail the performance and behavior of the self-healing mechanisms of fault-tolerant networks.

Fault-tolerant networks are typically designed with some inactive, or standby, redundant connections. When an active connection is interrupted, the network works to converge on a solution that results in it regaining full connectivity. RUGGEDCOM PING is designed to measure the time it takes from the moment the network is damaged to the time it regains full connectivity.

RUGGEDCOM PING only requires the tested devices to support the ubiquitous 'Internet Control Message Protocol' (ICMP - Internet RFC-792) better known as 'ping' that is implemented by the vast majority of IP devices. RUGGEDCOM PING can send ICMP echo messages and process incoming responses with a granularity of 1ms.

Features

- Flexible and configurable network auto-discovery mechanism
- Millisecond resolution of events both initiated and detected by the system
- Testing, monitoring and measurement of up to 256 IP devices concurrently
- Real-time display of test progress
- Generation of test reports in HTML format
- Option to save discovered nodes for later retrieval and use

System requirements

Component	Specification
Operating system	Microsoft Windows XP SP2 Windows 7 Windows 8



For more information, please visit:
[siemens.com/ruggedcom-software](https://www.siemens.com/ruggedcom-software)

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany

Siemens Canada Limited
300 Applewood Crescent
Concord, Ontario, L4K 5C7
Canada

© Siemens AG 2017
Subject to change without prior notice
Article No. 6ZB5531-OAC02-OBA1
W-FPN7Z-RG-PD204 / Dispo 26000
BR 1017 2. ROT 24 En
Printed in Germany

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](https://www.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](https://www.siemens.com/industrialsecurity)

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.

Scan this
QR code
for more
information

