SIEMENS

RUGGEDCOM RNA

Developer Guide

12/2014
RC1000-EN-02

Disclaimer Of Liability

Siemens has verified the contents of this manual against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

ROX™, Rugged Operating System On Linux™, CrossBow™ and ELAN™ are trademarks of Siemens Canada Ltd.. ROS® is a registered trademark of Siemens Canada Ltd..

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Third Party Copyrights

Siemens recognizes the following third party copyrights:

- Copyright © 2004 GoAhead Software, Inc. All Rights Reserved.

Security Information

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

Warranty

Refer to the License Agreement for the applicable warranty terms and conditions, if any.

For warranty details, visit www.siemens.com/ruggedcom or contact a Siemens customer service representative.

Contacting Siemens

Address	Telephone	E-mail
Siemens Canada Ltd. Industry Sector 300 Applewood Crescent Concord, Ontario Canada, L4K 5C7	Toll-free: 1 888 264 0006 Tel: +1 905 856 5288 Fax: +1 905 856 1995	ruggedcom.info.i-ia@siemens.com **Web** www.siemens.com/ruggedcom

Table of Contents

Preface

This document describes RUGGEDCOM RNA modules, a family of compact network switches that incorporate the latest advances necessary for reliable high-speed networking. RNA modules are highly self-contained, and are designed to be integrated into OEM equipment such as IEDs.

About This Guide

This guide is meant to provide a reference for OEM equipment integrators seeking to incorporate a RUGGEDCOM RNA module into their equipment. Mechanical, electrical, command and network interfaces are specified.

This document also covers detail of the networking features of RUGGEDCOM RNA, to provide a reference for system and network designers considering the overall system in which RUGGEDCOM RNA will be deployed.

Alerts

The following types of alerts are used when necessary to highlight important information.

> **DANGER!**
> *DANGER alerts describe imminently hazardous situations that, if not avoided, will result in death or serious injury.*

> **WARNING!**
> *WARNING alerts describe hazardous situations that, if not avoided, may result in serious injury and/or equipment damage.*

> **CAUTION!**
> *CAUTION alerts describe hazardous situations that, if not avoided, may result in equipment damage.*

> **IMPORTANT!**
> *IMPORTANT alerts provide important information that should be known before performing a procedure or step, or using a feature.*

> **NOTE**
> *NOTE alerts provide additional information, such as facts, tips and details.*

Related Documents

Other documents that may be of interest include:

- *Rugged Operating System (ROS) User Guide for RS950G*

Accessing Documentation

The latest Hardware Installation Guides and Software User Guides for most RUGGEDCOM products are available online at www.siemens.com/ruggedcom.

For any questions about the documentation or for assistance finding a specific document, contact a Siemens sales representative.

Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit www.siemens.com/ruggedcom or contact a Siemens sales representative.

Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support through any of the following methods:

- **Online**

  Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.

- **Telephone**

  Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.

- **Mobile App**

  Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

  - Access Siemens' extensive library of support documentation, including FAQs, manuals, and much more
  - Submit SRs or check on the status of an existing SR
  - Find and contact a local contact person
  - Ask questions or share knowledge with fellow Siemens customers and the support community
  - And much more...

1 Product Overview

RUGGEDCOM RNA (Redundant Network Architecture) modules are a family of compact network switches that enable OEM devices with the latest advances in High-availability Seamless Redundancy (HSR - IEC 62439-3 Clause 5) and Parallel Redundancy Protocol (PRP - IEC 62439-3 Clause 4), offering the ultimate network reliability and zero fail-over time. RNA modules are available in 100 Mb or 1 Gb speeds with up to three ports providing tremendous flexibility to suit any host IED and application.

Based on the latest addition to the IEC 62439 standard for High Availability Ethernet, RNA can make any IED fully inter-operable with any High-availability Seamless Redundancy (HSR) or Parallel Redundancy Protocol (PRP) network providing redundancy down to the packet level.

These self-contained modules allow system designers to build all of these technologies into their designs that take advantage of them with a minimum of integration effort.

RNA modules are programmed with industry leading Siemens ROS firmware for the ultimate Utility Grade reliability and performance. The RS950G Redbox host is available to provide designers with a reference to quickly design and prove the IED interface.s

The following are highlights of the RNA module features:

RNA Module Hardware Features

- 3 external ports at either Fast Ethernet or Gigabit speeds
- Latest generation FPGA parts for minimum power consumption
- 3.3VDC power inputs
- Compact size: 7.62cm x 5.08cm x 1.52cm
- Low profile: height when installed on a PCB is less than or equal to the height of an RJ45 connector
- CPU embedded within FPGA
- 512MBit SDRAM for the ROS firmware
- 128Mbit SPI Flash for FPGA and ROS binary images

RNA Packet Processor

- All ports operate at wire-speed; non-blocking
- Software configurable for HSR or PRP

Self-Contained, Managed System

- Independent CPU reduces IED CPU overhead from management protocols
- Greater reliability - IED sub-system failure should not impact network
- CSV file or SQL configuration compatible with Rugged Operating System (ROS)®

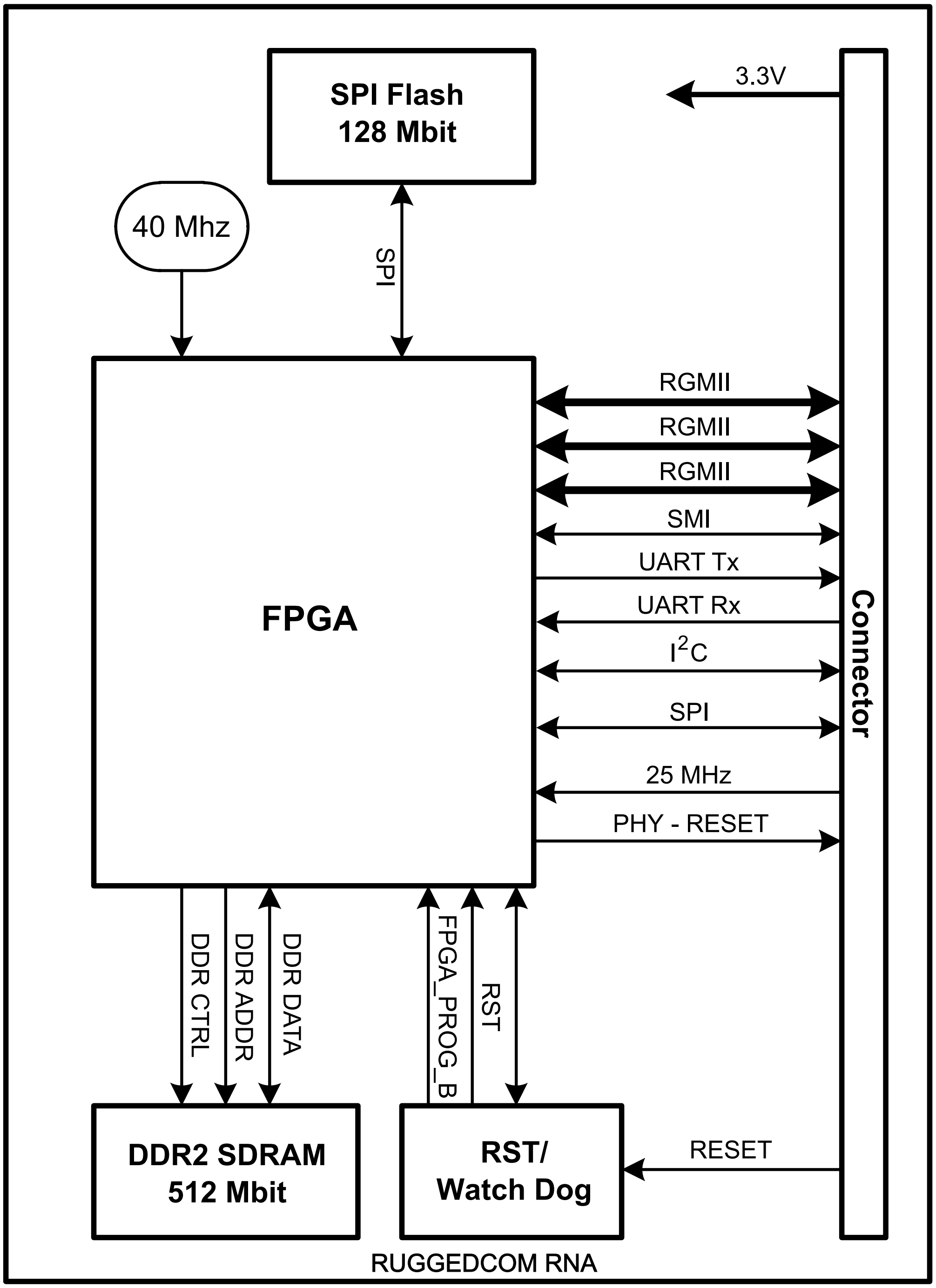

Figure 1: RNA Block Diagram

2 Featured Technologies

The following sections describe the technologies used in RUGGEDCOM RNA modules:

- Section 2.1, “Parallel Redundancy Protocol”
- Section 2.2, “High-Availability Seamless Redundancy”
- Section 2.3, “Modes”
- Section 2.4, “Reference Implementation (RS950G)”
- Section 2.5, “Precision Time Protocol (PTP) 1-Step Transparent Clock”

Section 2.1

Parallel Redundancy Protocol

Doubly Attached Node, PRP-aware (DANP) provides network redundancy by connecting to two independent LANs (e.g. LAN A and LAN B) operating in parallel. The two LANs can have different topology and performance. In order to achieve true redundancy, the two LANs must be failure-independent (the failure of either network must not affect the operation of the other).

Periodic PRP supervision frames are sent out by DANP in order to assist nodes on the network in monitoring the integrity of the network and presence of nodes. These supervision frames help other nodes to figure out which devices are on the network, the type of the device (e.g. DANP, SANA, SANB), MAC addresses of the device and operating mode (e.g. duplicate accept vs. duplicate remove).

Section 2.2

High-Availability Seamless Redundancy

HSR was officially integrated into the IEC 62439-3 standard in February 2010. A ring network, or a ring of rings, implementing HSR technology supports zero switchover time in the case of a single link failure. Compared to PRP (Section 2.1, “Parallel Redundancy Protocol”), HSR only demands about half of the network infrastructure. However, network bandwidth on an HSR ring is roughly halved compared with a network ring based on RSTP, MRP or DRP technology. All of the network nodes inside an HSR ring must be HSR-capable (i.e. DANH or Doubly-Attached HSR Node). HSR-unaware nodes can be attached to the HSR ring through the use of a *RedBox* (Redundancy Box).

Unlike STP (Spanning Tree Protocol), which requires the reconfiguration of an active network topology over redundant physical links, HSR provides *hitless* network recovery in a ring topology. In other words, HSR network convergence time from single link failure is zero. The basic principle behind HSR is the replication of frames over both sides of the HSR ring as shown in Figure 2.

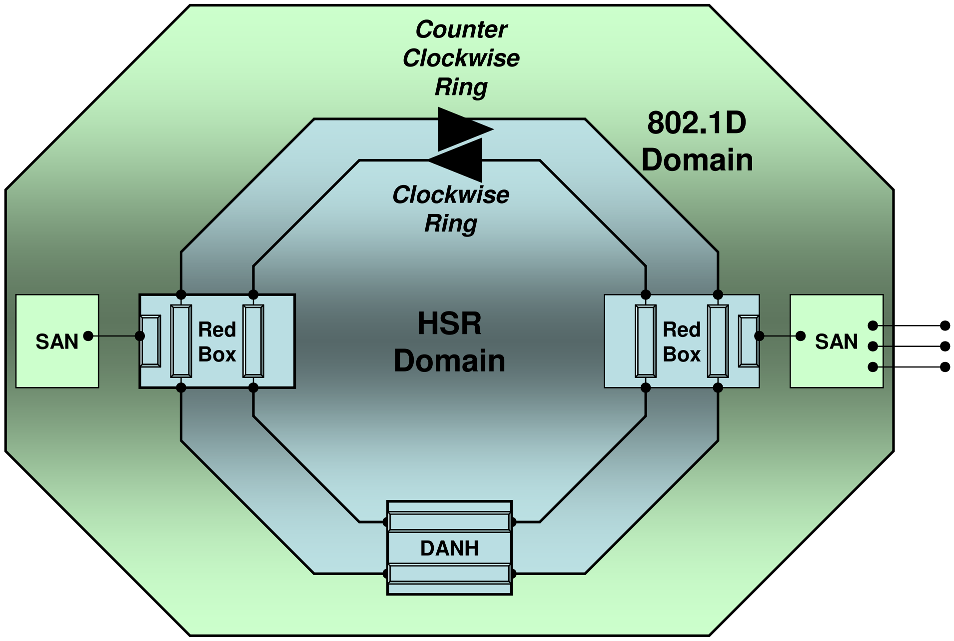

Figure 2: Encapsulation of HSR Ring In IEEE 802.1D domain

Nodes within the ring are restricted to be HSR-capable switching nodes. General-purpose nodes (HSR unaware nodes or SAN - Singly Attach Node) cannot be attached directly to the HSR ring, but require a RedBox. A RedBox is a device with at least three ports, two of them being ring ports for the HSR protocol, the third port being connect to an interlink.

HSR treats two physical Ethernet ports as a single aggregate port. An HSR node uses a single MAC address on both HSR ports. This makes redundancy transparent to layers above MAC. HSR therefore provides layer 2 redundancy according to the OSI networking model.

RUGGEDCOM RNA supports full HSR RedBox functionality as described in IEC62439-3, including generation of HSR supervision frames on behalf of SANs.

When a network link fails inside an HSR ring, one of the two frames sent out from source DANH will never reach the destination DANH. The destination DANH may report the missing duplicate, but even so, the communication path between source and destination DANH remains fully operational.

NOTE
Current HSR implementation limits link utilization at 74% when using multicast traffic.

Section 2.3

Modes

The RNA Module supports two modes of operation which leads to different possible use cases. The first mode of operation is called DANH Mode (Doubly Attached Node HSR Mode) and the other mode of operation is called DANP Mode (Doubly Attached Node PRP Mode). These two operation modes and their corresponding use cases will be described in the following sections:

The following sections describe the available modes in further detail:

- Section 2.3.1, "DANH Mode"
- Section 2.3.2, "DANP Mode"

Section 2.3.1

DANH Mode

Under this mode, the RNA Module is integrated into a 3rd party system (i.e. Host System). One example of such system would be an IED which requires direct connection to an HSR ring. As depicted in the following diagram, the RNA Module acts as a bridge between Host System network traffic and HSR ring traffic. The RNA Module will take care duplicating Host System traffic onto both ring ports as well as removing duplication in the received HSR ring traffic. HSR supervision frames will be transmitted and processed by the RNA Module on behalf of the Host System and as a result, from the perspective of other nodes on the HSR ring, the Host System is simply a DANH node.

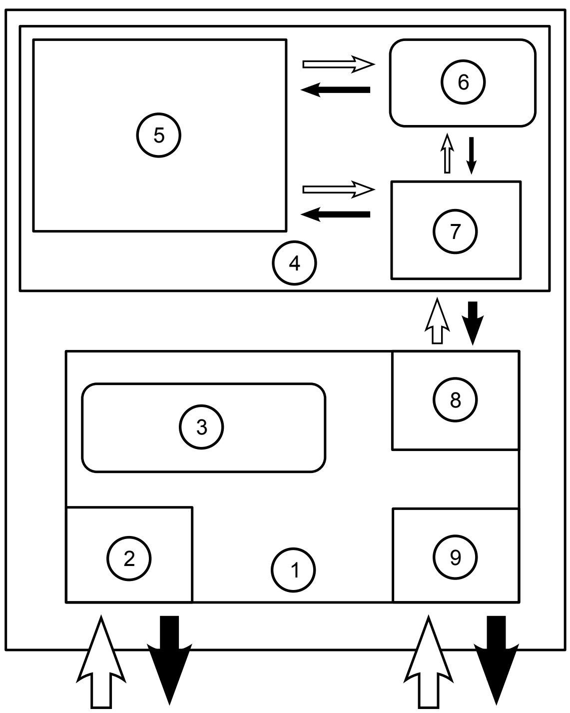

Figure 3: Internals of a DANH Node powered by the RNA

1. RNA Module **2.** Port A **3.** Embedded CPU **4.** Host System **5.** Data Generation and Processing **6.** Host CPU **7.** Ethernet Port **8.** Local **9.** Port B

The most common network topologies involving DANH nodes are:

- Ring Topology
  DANHs are connected directly to each other to form an HSR ring. Zero switchover time is supported in the case of a single point link failure. However, available network bandwidth in the ring is roughly halved due to the nature of duplicate transmission of HSR protocol.
- Separate Network Topology
  PRP network uses this topology to achieve redundancy. The advantage of such topology with HSR is that the network can still support zero switchover time for multiple link failures as long as those link failures all occur

inside one of the networks. The downside of this topology is that it requires higher setup costs for the extra network infrastructure.

The following diagram shows an example implementation of an HSR ring featuring several IEDs (with RNA Module integrated) connect directly to the HSR ring. These IEDs are made HSR-aware by the RNA Module. RS950G performs as an HSR RedBox allowing Non-HSR device connect to the same HSR ring indirectly.

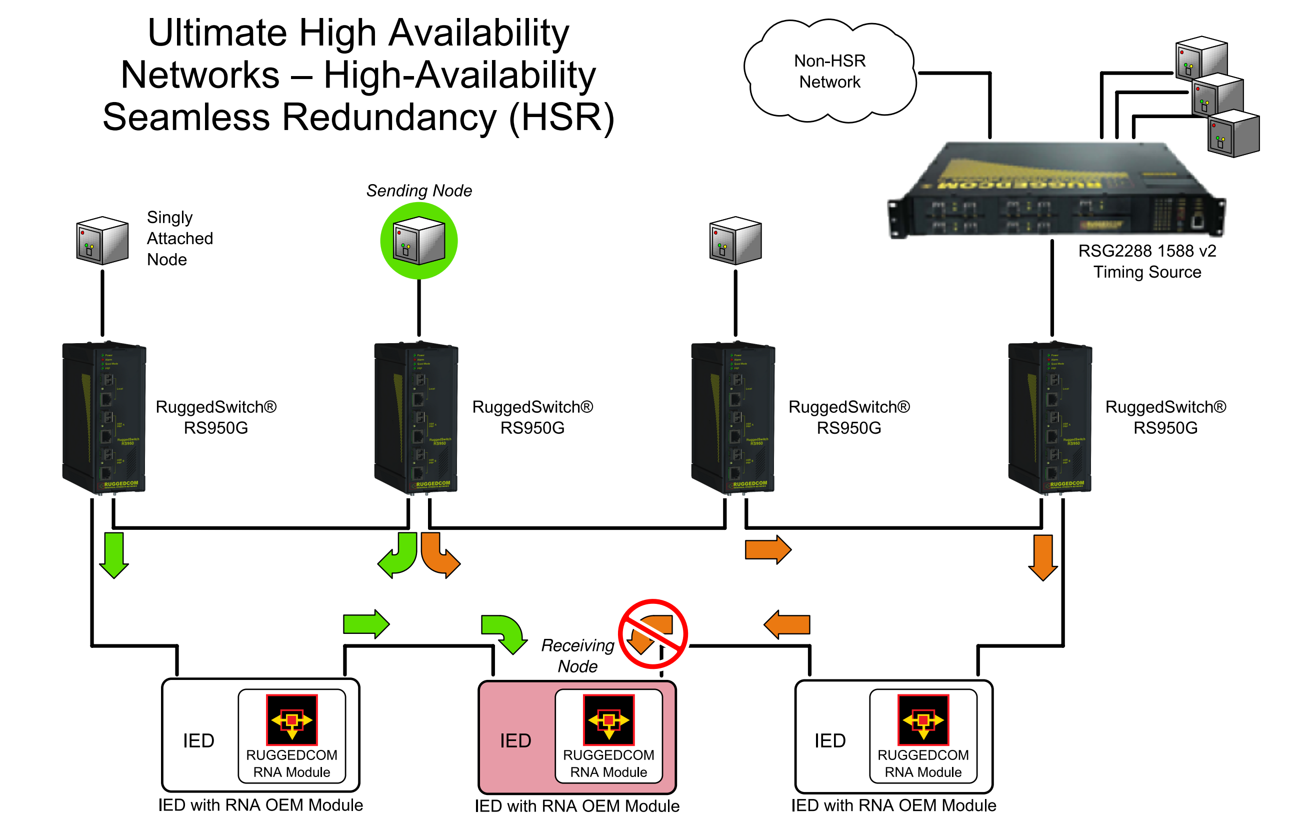

Figure 4: DANH Implementation Example

Section 2.3.2
DANP Mode

In DANP mode, the RUGGEDCOM RNA Module is integrated into a 3rd party host system. One example of such a system is an IED which requires a direct connection to a PRP network. The RNA Module running in DANP Mode acts as a bridge between host system network traffic and PRP network traffic. The RNA Module will handle duplication of host system traffic onto both sides of a PRP network as well as removal of duplicates upon receiving traffic from the PRP network. PRP supervision frames are transmitted and processed by the RNA Module on behalf of the host system. As a result, from the perspective of network nodes on the PRP network, the host system is simply a DANP node.

The most common network topologies involving DANP nodes are:

- Bus/Ring Topology
  A very simple topology where each DANP is connected to two LANs to provide the network redundancy. Each of the LAN can be a ring on its own.

- Separate Network Topology
  The two LANs in a PRP network do not have to be identical in terms of topology or performance. With the Separate Network Topology, you can have a ring network on one side and a tree network on the other side of the PRP infrastructure. The advantage of this topology is that the network can still support zero switchover time for multiple link failures as long as those link failures all occur inside the same LAN. The downside, in general for a PRP network, is that it requires higher setup costs for the extra network infrastructure.

Section 2.4

Reference Implementation (RS950G)

With reference to the *Rugged Operating System (ROS) User Guide for RS950G*

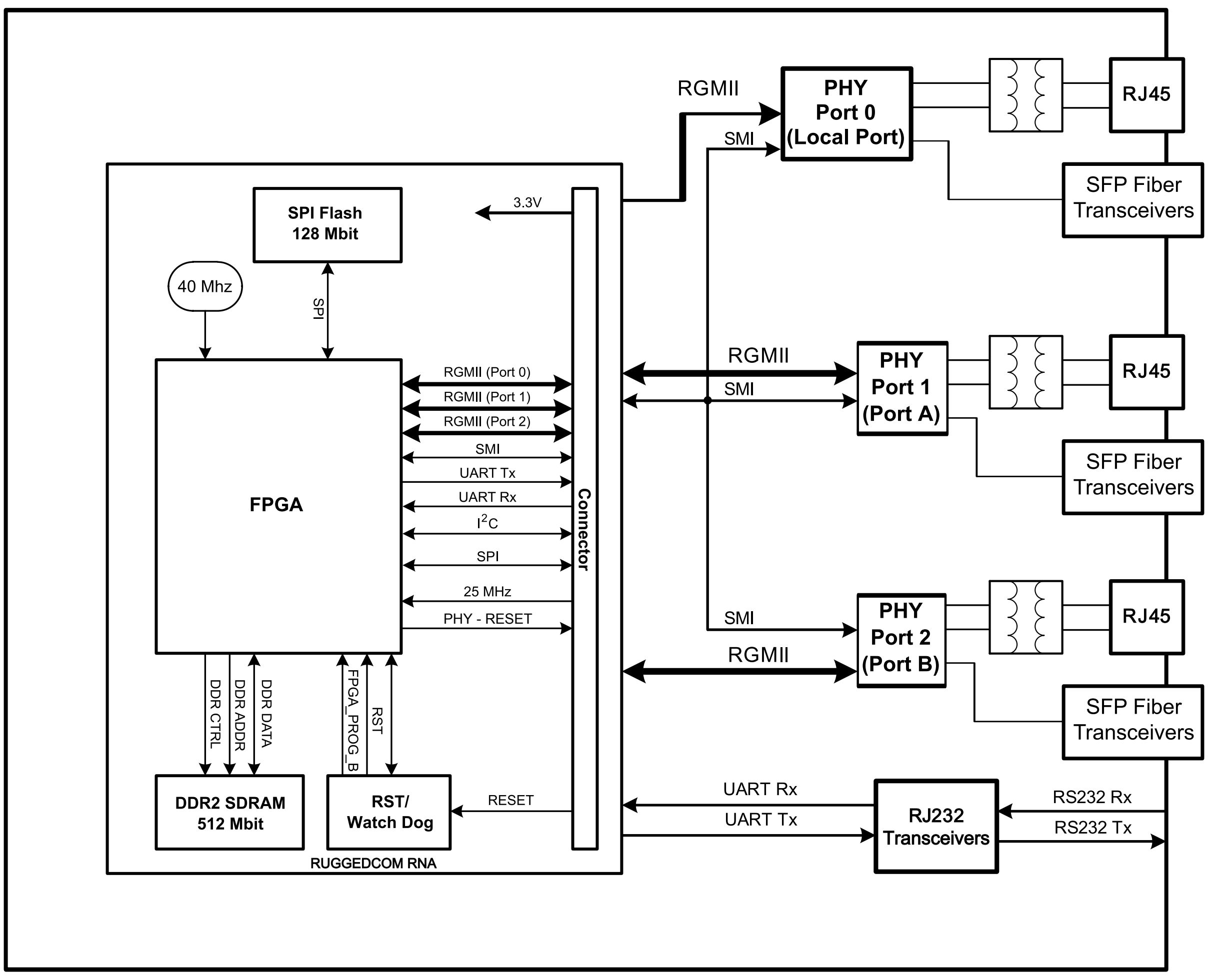

Figure 5: RS950G Block Diagram

Section 2.5

Precision Time Protocol (PTP) 1-Step Transparent Clock

PTP is a standard method of synchronizing network clocks over Ethernet. RNA supports 1-step Peer-to-Peer (P2P) Transparent Clock, which is defined by the IEEE 1588 working group in the IEEE 1588-2008 standard.

3 Operation

This chapter describes the operation of the RUGGEDCOM RNA module. It describes the following topics:

- Section 3.1, “Host System Frame Transmission and Reception”
- Section 3.2, “HSR/PRP Supervision Frame Transmission and Reception”
- Section 3.3, “Supported Network Services”

Section 3.1
Host System Frame Transmission and Reception

The RNA Module supports exchange of standard Ethernet frames with the Host system. Insertion and removal of HSR/PRP tag, frame duplication and duplicate removal are completely transparent from the host system.

Section 3.2
HSR/PRP Supervision Frame Transmission and Reception

The RNA Module will send and receive HSR/PRP Supervision frames on behalf of the Host System since the Host System will not generate or process the HSR/PRP Supervision frames. Host System MAC address will be transmitted as part of the HSR/PRP Supervision frame in order for other HSR/PRP nodes to detect Host System presence on the ring. Upon receiving HSR/PRP Supervision frames from the HSR/PRP ports, the RNA Module will only forward the frames to the embedded CPU for processing. Host System will not receive any HSR/PRP Supervision frames.

The RNA Module can detect the presence and network path integrity to and from other HSR/PRP nodes on the HSR/PRP network.

Section 3.3
Supported Network Services

The RNA Module supports a variety of Layer 2 and Layer 3 network services. For example, SNTP, RSH/SSH/Telnet/TFTP and Web servers. For more information about all the provided network services and configuration parameters, please refer to the latest *Rugged Operating System (ROS) User Guide for RS950G*.

4 Software

The Rugged Operating System (ROS) software on the RUGGEDCOM RNA module is accessible from a serial console (if equipped) and an Ethernet interface.

This chapter provides instructions for logging in to ROS. It describes the following topics:

- Section 4.1, “Accessing the ROS User Interface through a Serial Console”
- Section 4.2, “Accessing the ROS User Interface through the Ethernet Interface”
- Section 4.3, “Firmware Upgrade”
- Section 4.4, “System Design Constraints”

Section 4.1

Accessing the ROS User Interface through a Serial Console

To connect to the ROS User Interface using a serial console, do the following:

1. Attach a terminal or PC running terminal emulation software to the RS232 port, if equipped.
2. Configure the terminal as follows:
   - 8 bits
   - No parity
   - 57.6 Kbps
   - Hardware and software flow control disabled
   - VT100 terminal type
3. After connecting to the device, press any key on the keyboard. The terminal prompts for a user name and password.

   NOTE
   *The default user name is **admin** and the default password is **admin**.*

4. After logging in, the main menu appears. For complete instructions on working with the ROS Software, see the *Rugged Operating System (ROS) User Guide for RS950G*.

Section 4.2

Accessing the ROS User Interface through the Ethernet Interface

A web browser uses a secure communications method called SSL (Secure Socket Layer) to encrypt traffic exchanged with its clients. The web server guarantees that communications with the client are kept private. If the client requests access via an insecure HTTP port, it will be rerouted to the secure port. Access to the web server via SSL will be granted to a client that provides a valid user name / password pair.

> **NOTE**
> *It can happen that upon connecting to the ROS web server, a web browser may report that it cannot verify the authenticity of the server's certificate against any of its known certificate authorities. This is expected, and it is safe to instruct the browser to accept the certificate. Once the browser accepts the certificate, all communications with the web server will be secure.*

To access the ROS User Interface through the Ethernet interface, do the following:

1. Start a web browser session and open a connection to the switch by entering a URL that specifies its host name or IP address.

   > **NOTE**
   > *The factory default IP address is **https://192.168.0.1**.*

2. The user interface prompts for a user name and password.

   > **NOTE**
   > *The default user name is **admin** and the default password is **admin**.*

3. After logging in, the main menu appears. For complete instructions on working with the ROS Software, see the *Rugged Operating System (ROS) User Guide for RS950G*.

Section 4.3

Firmware Upgrade

ROS provides flexible, powerful mechanisms for the bulk update and backup of the system firmware and of the configuration database.

For complete instructions on working with the ROS Software, see the *Rugged Operating System (ROS) User Guide for RS950G*.

Section 4.4

System Design Constraints

> **CAUTION!**
> *Failure to follow these constraints may result in a non-functioning unit.*

RUGGEDCOM ROS makes the following hardware assumptions about the carrier board:

- Broadcom PHY device BCM54616S
- RTC (Real Time Clock) M41T82SM6 connected to I2C bus
- CPLD connected to I2C bus mainly for PHY management
- I2C MUX to managed Fiber SFPs

5 Specifications

This chapter provides the specifications for the RNA module. It describes the following topics:

- Section 5.1, "Pin-Out Specifications"
- Section 5.2, "Electrical Specifications"
- Section 5.3, "Dimensions"
- Section 5.4, "FPGA Heatsink Requirements"

Section 5.1

Pin-Out Specifications

NOTE
All digital pins are 3.3 V logical level.

Table: Module Connector (J2) Pin-out

Signal	J2 pin#	Pin Name	Pin Type	Description
RGMII signals				
Port 0	21	P0_TXCLK	OUTPUT	Port 0 Transmit clock
	11	P0_TXD[0]	Output	Port 0 Transmit data output. Nibble-wide transmit data is output synchronously with the rising and falling edges of TXCLK transmit clock. TXD{3} is the most significant bit.
	13	P0_TXD[1]	Output	
	15	P0_TXD[2]	Output	
	17	P0_TXD[3]	Output	
	25	P0_TXEN	Output	Port 0 Transmit Enable
	22	P0_RXCLK	Input	Port 0 Receive clock
	12	P0_RXD[0]	Input	Port 0 Receive data input. Nibble-wide receive data is input synchronously with the rising and falling edges of RXCLK receive clock. RXD{3} is the most significant bit.
	14	P0_RXD[1]	Input	
	16	P0_RXD[2]	Input	
	18	P0_RXD[3]	Input	
	26	P0_RXDV	Input	Port 0 Receive data valid.
Port 1	29	P1_TXCLK	Output	Port 1 Transmit clock
	37	P1_TXD[0]	Output	Port 1 Transmit data output. Nibble-wide transmit data is output synchronously with the rising and falling edges of TXCLK transmit clock. TXD{3} is the most significant bit.
	39	P1_TXD[1]	Output	
	41	P1_TXD[2]	Output	
	43	P1_TXD[3]	Output	

Signal	J2 pin#	Pin Name	Pin Type	Description
	33	P1_TXEN	Output	Port 1 Transmit Enable
	30	P1_RXCLK	Input	Port 1 Receive clock
	38	P1_RXD[0]	Input	Port 1 Receive data input. Nibble-wide receive data is input synchronously with the rising and falling edges of RXCLK receive clock. RXD{3} is the most significant bit.
	40	P1_RXD[1]	Input	
	42	P1_RXD[2]	Input	
	44	P1_RXD[3]	Input	
	34	P1_RXDV	Input	Port 1 Receive data valid.
Port 2	103	P2_TXCLK	Output	Port 2 Transmit clock
	93	P2_TXD[0]	Output	Port 2 Transmit data output. Nibble-wide transmit data is output synchronously with the rising and falling edges of TXCLK transmit clock. TXD{3} is the most significant bit.
	95	P2_TXD[1]	Output	
	97	P2_TXD[2]	Output	
	99	P2_TXD[3]	Output	
	107	P2_TXEN	Output	Port 2 Transmit Enable
	104	P2_RXCLK	Input	Port 2 Receive clock
	94	P2_RXD[0]	Input	Port 2 Receive data input. Nibble-wide receive data is input synchronously with the rising and falling edges of RXCLK receive clock. RXD{3} is the most significant bit.
	96	P2_RXD[1]	Input	
	98	P2_RXD[2]	Input	
	100	P2_RXD[3]	Input	
	108	P2_RXDV	Input	Port 2 Receive data valid.
Link/SDET signals	57	LINK0	Input	Port 0 link up indication, active high
	56	LINK1	Input	Port 1 link up indication, active high
	55	LINK2	Input	Port 2 link up indication, active high
	64	SDET0	Input	Port 0 Fiber optic transceiver signal detect input when port 0 in fiber mode, active high.
	63	SDET1	Input	Port 1 Fiber optic transceiver signal detect input when port 0 in fiber mode, active high.
	62	SDET2	Input	Port 2 Fiber optic transceiver signal detect input when port 0 in fiber mode, active high.
Control signals	47	MDC	Output	SMI clock output, Master
	49	MDIO	Input/Output	SMI Data Input/Output, Master.
	50	I2C_CLK	Output	I2C clock output, Master
	48	I2C_DATA	Input/Output	I2C data input.output, Master.
	89	UART-RXD	Input	Console UART RXD
	91	UART-TXD	Output	Console UART TXD

Signal	J2 pin#	Pin Name	Pin Type	Description
Other signals	67	CLK25	Input	25MHz clock input
	66	Reset_MB	Output	Reset PHYs, active low
	90	Reset	Input	Reset the module, active low
	70	PRP-MODE-LED	Output	PRP MODE INDICATION
	72	HSR-MODE-LED	Output	HSR MODE INDICATION
	92	ALARM-LED	Output	ACTIVE HIGH
	84	FAIL-SAFE-RELAY	Output	ACTIVE HIGH
	88	INT_MB	Input	INTERRUPT FROM PHYS
POWER	1, 2, 3, 4, 5, 6	3.3V	Input	3.3V INPUT
	7-10, 19, 20, 23, 24, 27, 28, 31, 32, 35, 36, 45, 46, 65, 69, 101,102, 105, 106, 109, 110, 113, 114	GND	Input	
Other	51-54, 58-61, 68, 71, 73-83, 85-87, 111, 112, 115-120	RFU		Reserved for future use, do not connect to anything.

Section 5.2

Electrical Specifications

Stressing the module outside the ratings listed in Table "Recommended Operating Conditions" may cause permanent damage to the module. These are stress ratings only, and operation of the module at these, or any other conditions outside those indicated in the Operating section of this specification, is not implied. Exposure to Absolute Maximum Rating conditions for extended periods may affect the module's reliability.

Table: Absolute Maximum Ratings

Parameter	Description	Value
Tstg	Storage temperature	-65°C to 150°C (-85°F to 302°F)
VCC	Supply voltage relative to GND	-0.2V to 3.75V

Table: Recommended Operating Conditions

Parameter	Description	Value
TA	Ambient operating temperature.	-40°C to 85°C (-40°F to 185°F)
VCC	Supply voltage relative to GND	3.15V(min) 3.3V(Typ) 3.45V
ICC	Supply Current	1.8A min

Section 5.3

Dimensions

For the RNA module dimensions, refer to the figure below.

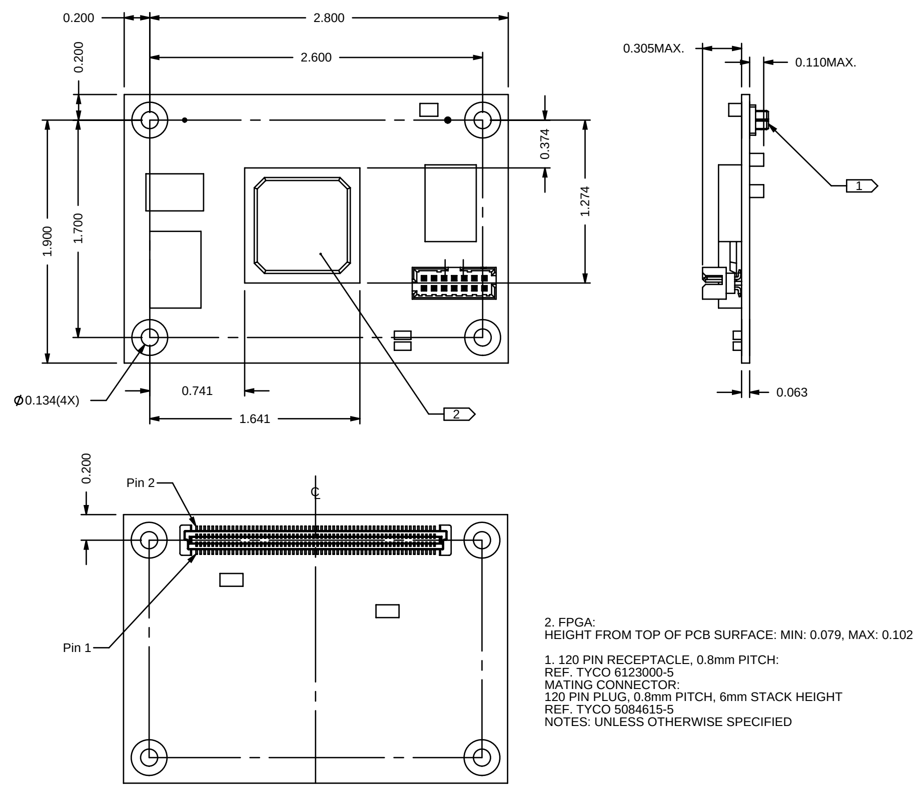

Figure 6: Dimensions

Section 5.4

FPGA Heatsink Requirements

For the FPGA heatsink requirements, refer to the figure and table below.

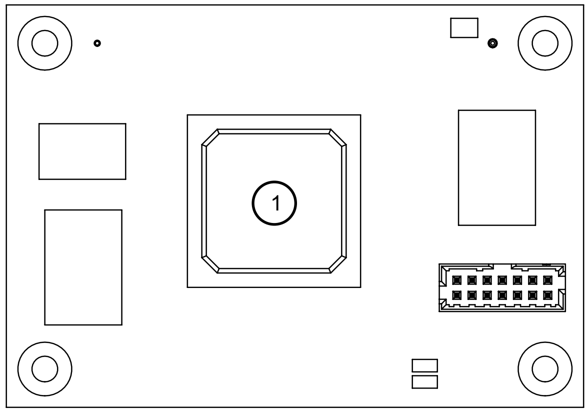

Figure 7: FPGA Heatsink Location

1. Heatsink location

Table: FPGA Heatsink Requirements

Max. Junction Temperature	Thermal Resistance (Junction to Ambient, No Air Flow)	Thermal Resistance (Junction to Case)	Max. Power Consumption
100°C (212°F)	15.8°C/W (60.44°F/W)	3.7°C/W (38.66°F/W)	5.0W