SCADAPack E Technical Overview

Documentation

Table of Contents

Part I SCADAPack E Technical Overview 4

1 Technical Support ... 4

2 Safety Information ... 5

3 Introduction ... 7

3.1 Terminology ... 9

3.2 Glossary ... 11

4 References ... 15

5 SCADAPack E RTU Architecture ... 17

5.1 RTU Hardware ... 18

5.1.1 RTU Features ... 19

5.1.2 RTU Models ... 21

5.1.3 Hardware Accessories & User Servicing ... 23

5.2 Configuration Tools ... 24

5.3 Firmware Updates ... 26

5.4 RTU Operating System Components ... 28

5.5 RTU Points ... 32

6 Physical I/O Expansion ... 33

6.1 5000 Series I/O ... 34

6.2 SCADAPack ES Remote I/O ... 35

7 IEC 61131-3 ISaGRAF ... 36

7.1 ISaGRAF 3 Workbench ... 37

7.1.1 ISaGRAF Workbench Software ... 37

7.1.2 ISaGRAF Workbench Communication, LIBRARY, & Diagnostics ... 38

7.1.3 The ISaGRAF Pre-Processor & Transferring ISaGRAF Applications ... 39

7.1.4 ISaGRAF Target, Status, & Storage ... 40

7.2 SCADAPack Workbench ... 42

8 DNP3 - Distributed Network Protocol ... 43

8.1 DNP3 SCADA Protocol Standard ... 44

8.2 SCADAPack E DNP3 Support ... 45

8.3 DNP3 Networking ... 46

8.4 DNP3 Secure Authentication ... 48

8.5 AGA12 Encryption ... 49

9 RTU Communication ... 50

9.1 DNP3 Communication Interfaces ... 51

9.1.1 Direct & Multi-drop Communication Interfaces ... 52

9.1.2 Hayes Modem & TCP/IP Communications ... 53

9.2 Peripheral Device Communication Interface ... 54

9.2.1 Serial MODBUS Slave & PLC Driver Master Operation ... 55

9.2.2 Modbus RTU Master Driver & Rockwell DF1 PLC ... 56

9.2.3 MODBUS/TCP Client & Server Operation ... 57

9.2.4 ASCII & Virtual Terminal & TCP Serial Communications ... 59

9.2.5 IEC 60870-5-101, -104 & -103 Protocols ... 60

10 RTU Configuration ... 62

11 RTU Data Processing 63
11.1 Integrated RTU Data Processing & RTU Data Processing Facilities 64
11.2 Profiler & Trend Sampler 66
12 Using the SCADAPack E RTU 68
12.1 Parameter Changes, Engineering Mode, & RTU Configuration Revisions 69
12.2 Time Conversion 70
12.3 Maintenance Modes 72
12.4 Local & Remote I/O Status 74
12.5 Port Assignments 75
12.5.1 Default Port Settings 77
13 TCP/IP Integration 79
14 Diagnostics 80
14.1 Diagnostic Display Information 81
14.2 Start-Up & Command Line Diagnostics 82
14.3 SCADAPack E Status Codes 83
14.3.1 DNP3 Errors, PLC Communication Errors, & TCP/IP Errors 84
14.3.2 System Error Point 85
14.4 RTU Status 87
14.5 Communication Statistics 89
15 RTU File System 90
16 Data Concentrator 91
17 DNP3 Multi-Master 92
18 Conitel Slave Communications 93
19 IRIG-B Time Synchronisation 94

I SCADAPack E Technical Overview

Schneider Electric

Documentation

Version: 8.05.4

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed. Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

1 Technical Support

Support related to any part of this documentation can be directed to one of the following support centers.

Technical Support: The Americas

Available Monday to Friday 8:00am – 6:30pm Eastern Time

Toll free within North America	1-888-226-6876
Direct Worldwide	+1-613-591-1943
Email	TechnicalSupport@controlmicrosystems.com

Technical Support: Europe

Available Monday to Friday 8:30am – 5:30pm Central European Time

Direct Worldwide	+31 (71) 597-1655
Email	euro-support@controlmicrosystems.com

Technical Support: Asia

Available Monday to Friday 8:00am – 6:30pm Eastern Time (North America)

Direct Worldwide	+1-613-591-1943
Email	TechnicalSupport@controlmicrosystems.com

Technical Support: Australia

Inside Australia	1300 369 233
Email	au.help@schneider-electric.com

2 Safety Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

	The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.
	This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠DANGER
DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠WARNING
WARNING indicates a potentially hazardous situation which, if not avoided, **can result** in death or serious injury.

⚠CAUTION
CAUTION indicates a potentially hazardous situation which, if not avoided, **can result** in minor or moderate injury.

CAUTION
CAUTION used without the safety alert symbol, indicates a potentially hazardous situation which, if not avoided, **can result in** equipment damage..

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and the installation, and has received safety training to recognize and avoid the hazards involved.

BEFORE YOU BEGIN

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

⚠CAUTION
EQUIPMENT OPERATION HAZARD
• Verify that all installation and set up procedures have been completed. • Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.

• Remove tools, meters, and debris from equipment.
Failure to follow these instructions can result in injury or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and grounds, except those grounds installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove ground from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

OPERATION AND ADJUSTMENTS

The following precautions are from the NEMA Standards Publication ICS 7.1-1995 (English version prevails):

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer's instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer's instructions and the machinery used with the electrical equipment.
- Only those operational adjustments actually required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

3 Introduction

This document introduces the SCADAPack E architecture, and Technical Documentation. It is recommended that the reader of this technical overview and technical reference manuals be familiar with the concepts of SCADA and distributed telemetry communications. This manual is to be used by technical personnel such as Systems Engineers, Control System programmers, Communication Engineers, Maintenance Engineers, and Field Technicians.

The SCADAPack E is the technology term for a Telemetry hardware product range designed and manufactured by Schneider Electric. This manual describes the architecture and functionality of particular software for SCADAPack E systems.

Provided by the SCADAPack E technology is an extensive set of communications and control facilities for use in Telemetry and Supervisory Control And Data Acquisition (SCADA) applications, including Internet communication protocol (TCP/IP).

- ***Terminology*** 9
- ***Glossary*** 11

3.1 Terminology

This section describes terms used throughout the SCADAPack E documentation.

Analog : - A variable quantity represented numerically

Applications Level: - The RTU programming environment in which the users applications programs are running (IEC 61131-3 and vendor specific programming environment)

Applications Program: - An ordered set of instructions prepared by the user which may be loaded into the RTU and, once initialised, will continuously execute or as triggered by other applications programs or events

Binary : - A quantity with two discrete states: ON (1) or OFF (0). This term is often used in conjunction with DNP3 communication protocol objects. See also Boolean, Digital

Boolean : - A quantity with two discrete states: TRUE or FALSE. This term is often used in conjunction with ISaGRAF application variable types. See also Binary, Digital

Boot Monitor : - Software contained in Flash memory executed on an RTU at start-up (boot) time for the purposes of verifying, loading or modifying the main operating system firmware

Current Value: - associated with a point indicating the current value or state of the point. The current value of some points is read-only, and may be non-volatile. The current value is neither a point attribute nor a point property

Derived Point: - internal data within an RTU, being either a User defined point or a System point

Digital: - A quantity with two discrete states: ON or OFF. This term is often used in conjunction with physical input and output states. See also Binary, Boolean

Firmware: - Boot Monitor software and RTU Operating System software stored in Flash memory

Fragment: - DNP3 protocol application layer data unit – Max 2048 bytes

Frame: - DNP3 protocol link layer data unit – Max 292 bytes

Intelligent Electronic Devices (IEDs): - A programmed or programmable electronic instrument or controller having a communications interface, and not a Master Station or a PC

Internet Protocol: - Communication protocols and applications from the TCP/IP suite, used in Internet and Intranet local area and wide area communication architectures

Local Diagnostic Terminal: - A laptop or portable computer, connected directly to the RTU and is capable of executing Schneider Electric supplied applications to display and modify RTU parameters and user applications

Local Time: - Seasonally adjusted current time for the geographic location's time zone

Main RTU Unit: - RTU device responsible for communicating with a SCADA Master or Peer RTUs, executing user applications and controlling Remote I/O (see also Remote I/O)

Master Station: - The computer or computer systems that form the primary point of contact for communication to and from an individual RTU

Operating System Firmware: - Software contained in Flash memory on the RTU that controls RTU facilities except the Boot Monitor

Peer: - A like device, possibly to who direct communications may be established

Physical Points: - RTU internal representation of electrical terminations on a Main RTU Unit or Remote I/O Unit

Point: - an entity of data within an RTU corresponding to a physical or derived quantity

Point Attributes: - read/write field of a ***point configuration*** describing or controlling (to the RTU) a characteristic of the point

Point Index: - DNP3 point address of a point in the RTU point database

Point Properties: - read only field describing (to the SCADA Master or ISaGRAF user application) a status or characteristic of a point

Protocol: - communication description shared by multiple devices permitting interchange of information

Remote Engineering Workstation: - A computer workstation which is connected to the RTU through the telemetry network or dial up modem and is capable of executing CMI supplied applications to display and modify RTU parameters and user applications

Remote I/O: - RTU sub-system architecture providing I/O to expand the capacity of a Main RTU Unit. Units attached through serial or Ethernet communication channels and providing additional I/O capacity to a Main RTU unit are known as Remote I/O Units

RTU Sequence: - Same as applications program

Slave: - General term for a device that connects to a hierarchically higher level device for services (The higher level device is usually called by the General term “Master”)

Slave RTU: - A Main RTU unit that utilises the communication link of another RTU for communications with a Master station

Standard Time: - Non-seasonally adjusted current time for the geographic location’s time zone

Summer Time: - Standard Time + 1 hour, when RTU is notified during gazetted summer months

System Points: - RTU internal data managed by RTU operating system software

Telemetry Computer (TC): - A Master Station communications server

User: - Any person responsible for the installation, programming, operation or maintenance of RTUs

User Points: - RTU internal data created by a user defined configuration

User Program: - A compiled, end user written ISaGRAF application

UTC Time: - International standard time, not adjusted for local time zone or summer time

3.2 Glossary

This section describes acronyms used throughout the SCADAPack E documentation.

1xRTT	Single carrier (1x) Radio Transmission Technology (CDMA cellular wireless data standard)
ACCM	Asynchronous Control Character Map (PPP negotiated option)
ACFC	Address and Control Field Compression (PPP negotiated option)
AH	Ampere Hour (Battery capacity rating)
AI	Analog Input
ARP	Address Resolution Protocol (TCP/IP Ethernet component)
BI	Binary Input (DNP3 point type)
BNC	physical connector type (for 10Base-2 Thin-Ethernet cabling)
BOOTP	Boot Protocol (TCP/IP application layer remote boot services)
CASE	Computer Aided Software Engineering (tools suite)
CCITT	international standards organization now known as ITU-T
CDMA	Code Division Multiple Access (wireless cellular technology)
CHAP	Challenge Authentication Protocol (PPP security component)
CI	Counter (Pulse) Input
CRC	Cyclic Redundancy Check (error checking algorithm)
CRO	oscilloscope (cathode ray oscilloscope - Test instrument)
CROB	Control Relay Output Block (DNP3 control object)
CSLIP	Compressed Serial Line Internet Protocol (TCP/IP serial data-link layer)
CTS	Clear To Send (RS232 signal)
DCD	Data Carrier Detect (communication port signal)
DCE	Data Communication Equipment (communication port type)
DI	Digital Input
DNP	Abbreviation for DNP3 protocol
DNP3	Distributed Network Protocol (SCADA / RTU communication standard)
DNS	Distributed Naming Service (TCP/IP application layer name resolution)
DO	Digital Output
DTE	Data Terminal Equipment (communication port type)
Flash	electrically erasable programmable read only memory
FSM	Finite State Machine (PPP component)

FTP File Transfer Protocol (TCP/IP application layer file transfer)

GSM Global System for Mobile communication (wireless cellular technology). Hayes modem devices often provide communication on these networks

GPRS General Packet Radio Service (GSM cellular wireless data standard)

GPS Global Positioning System (satellite system used for time synchronization)

HDLC High-level Data Link Control (serial link layer protocol: PPP is based on this)

Hex Hexadecimal (Base-16 numbers are followed by 'h' or preceded by '0x')

I/O Inputs and Outputs (sometimes refers to an RTU or PLC sub-system)

I^2C Serial communication bus technology (used by 5000 series I/O modules)

IC Integrated Circuit

ICMP Internet Control Message Protocol (TCP/IP data-link layer services)

IEC International Electro-technical Committee (standards organization)

IEEE Institution of Electrical & Electronics Engineers (standards organization)

IETF Internet Engineering Task Force

IGMP Internet Group Management Protocol (TCP/IP network layer services)

IP Internet Protocol (TCP/IP network layer protocol)

IPCP Internet Protocol Control Protocol (TCP/IP network layer services)

IRIG Inter-Range Instrument Group (includes Time Synchronisation standards)

ISaGRAF IEC61131-3 Sequencing & control software & target used on SCADAPack E RTUs

ITU-T International Telecommunications standards organization, formerly CCITT

LAN Local Area Network (Ethernet is an example LAN technology)

LCP Link Control Protocol (PPP component)

LLC Link Layer Control (Ethernet MAC layer component)

MAC Media Access Control (Ethernet communication layer)

MODBUS PLC communications protocol (de-facto standard)

MRU Maximum Receive Unit (PPP negotiated packet length option)

NTP Network Time Protocol (time synchronization)

NV Non Volatile (memory that retains its data when powered off)

PAD Packet Assembler / Disassembler

PAP	Password Authentication Protocol (PPP security component)
PC	Personal Computer
PCB	Printed Circuit Board
PFC	Protocol Field Compression (PPP negotiated option)
PING	ICMP echo utility for determining TCP/IP device functioning
PLC	Programmable Logic Controller
POP3	Post Office Protocol (TCP/IP application layer E-mail receiver client)
PPP	Point-to-Point Protocol (TCP/IP serial data-link layer protocol)
PSTN	Public Switched Telephone Network. Hayes Modem devices often provide communication on these networks
PTT	Press To Talk (Radio)
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol (IP - Ethernet address resolution)
RFC	Request For Comments (TCP/IP standards documents)
RO	Relay Output
RoC	Rate of Change (signal processing)
RoF	Rate of Fall (signal processing)
ROM	Read Only Memory
RoR	Rate of Rise (signal processing)
RTS	Ready To Send (RS232 signal)
RTU	Remote Terminal Unit (telemetry device)
RX	Receive
RXD	Receive Data
SCADA	Supervisory Control And Data Acquisition
SLA	Sealed Lead Acid (Gel Cell) Battery
SLIP	Serial Line Internet Protocol (TCP/IP serial data-link layer)
SMTP	Simple Mail Transfer Protocol (TCP/IP application layer E-mail sender client)
SNAP	Sub-Network-Access-Protocol (Ethernet MAC layer LLC fields)
SNMP	Simple Network Management Protocol (TCP/IP application layer protocol)
SPDT	Single Pole Double Throw (change-over relay contact)
TC	Telemetry Computer (DNP3 protocol Master station host)
TCP	Transmission Control Protocol (TCP/IP transport layer protocol)

TCP/IP	Acronym typically referring to the entire Internet Protocol suite
TFTP	Trivial File Transfer Protocol (TCP/IP application layer file transfer for BOOTP)
Telnet	Virtual terminal protocol (TCP/IP application layer virtual terminal)
TTL	Time To Live (IP packet life-time)
TX	Transmit
TXD	Transmit Data
UDP	User Data-gram Protocol (TCP/IP transport layer protocol)
UTC	Universal Coordinated Time (international time standard)
UTP	Unshielded Twisted Pair (10Base-T Physical layer Ethernet cabling)
WAN	Wide Area Network

4 References

The following references form the Technical Documentation set for the SCADAPack E RTU.

From the SCADAPack E References Manuals set:

- SCADAPack E Product Overview
- SCADAPack E Technical Overview
- SCADAPack ES Quick Start Guide
- SCADAPack E ISaGRAF Quick Start Guide
- SCADAPack 300E Hardware manuals set
- SCADAPack ES Hardware Manual
- SCADAPack ER Hardware Manuals set
- SCADAPack E Configurator User Manual
- ISaGRAF 3 User Manual
- SCADAPack E ISaGRAF Function Block Reference
- SCADAPack E ISaGRAF 3 Pre-Processor Reference
- ISaGRAF 3 I/O Connection manual
- ISaGRAF Technical manual
- ISaGRAF 3 Modbus Communication Interfaces manual
- ISaGRAF 3 DF1 PLC Interface manual
- Idec PLC Interface manual
- Koyo PLC Interface manual
- SCADAPack E Target 5 Function Block Reference
- SCADAPack E Target 5 I/O Device Reference
- SCADAPack E Target 5 Technical Reference
- SCADAPack E Target 5 Modbus Communication Interfaces
- SCADAPack E Target 5 DF1 PLC Interface
- SCADAPack E Firmware Update User Manual
- SCADAPack E SCADAPack ES Remote I/O Technical Reference
- SCADAPack E DNP3 Technical manual
- SCADAPack E DNP3 Slave and DNP3 Master Device Profiles
- SCADAPack E Data Processing Technical manual
- SCADAPack E Data Concentrator manual
- SCADAPack E Configuration File Format
- SCADAPack E IEC 60870-5-101 and -104 Slave Technical Reference
- SCADAPack E IEC 60870-5-101 and -104 Slave Interoperability Profile

- SCADAPack E IEC 60870-5-103 Master Interoperability Profile
- SCADAPack E Conitel Technical Reference
- SCADAPack E Communication Interfaces Reference
- SCADAPack E Data Processing Technical Reference
- SCADAPack E Profiler manual
- SCADAPack E Security Technical Reference
- SCADAPack E Trend Sampler Technical Reference
- SCADAPack E Operational Reference
- SCADAPack E TCP/IP Technical Reference

From Standards and other documents (not included in the SCADAPack E reference manuals set):

- ICS Triplex ISaGRAF User's Manual
- ICS Triplex ISaGRAF Language Reference
- DNP3 Distributed Network Protocol 8 Volume Document Set
- DNP3 Distributed Network Protocol Conformance Test Procedures
- IETF TCP/IP RFC documents

5 SCADAPack E RTU Architecture

- *RTU Hardware* 18
- *Configuration Tools* 24
- *Firmware Updates* 26
- *RTU Operating System Components* 28
- *RTU Points* 32

5.1 RTU Hardware

The Schneider Electric SCADAPack E RTU hardware is based on state-of-the-art embedded technology. The following sections detail the SCADAPack E products.

Figure 5.1: SCADAPack E Smart RTUs

- ***RTU Features*** 19
- ***RTU Models*** 21
- ***Hardware Accessories & User Servicing*** 23

5.1.1 RTU Features

The SCADAPack E RTU hardware provides a wide range of facilities.

- Choice of I/O technology, I/O Boards and I/O expansion options
- Input power supply options (various technologies and voltage ranges available)
- Input power supply voltage monitoring
- Boot Monitor for local / remote re-programming of Operating System Firmware
- Hardware Watchdog
- Serial Communication Ports
- USB Communication Port (some models)
- Flash ROM and NV RAM
- Replaceable Lithium Battery
- Ethernet support : UTP
- Dual Ethernet interfaces (some models)
- Isolated secondary output power supply (some models)

SCADAPack E RTU I/O Interface features: (varies from model to model)

- Optically isolated Digital Input channels (some models)
- Pulse inputs on Digital Input channel (some models)
- De-bounce and Inversion on each Digital Input channel (some models)
- High speed counter inputs
- Relay Isolated Digital Output channels (some models)
- Digital Output channel Relay feedback (some models)
- Current / Voltage Analog Inputs selectable per channel (some models)
- Channel-to-Channel and Channel-to-Logic isolated Analog Input channels (some models)
- Channel-to-Channel and Channel-to-Logic isolated Analog Output channels (some models)
- A/D converter reference check (some models)

LED's on the Processor Boards and I/O Boards provide visual indication of RTU operation. These indicate:

- Energized Digital Input channels
- Activated Digital Output relays
- Controller running
- DNP3 Network communications activity
- SCADAPack ES Remote I/O communication activity (some models)
- PLC device communication activity

- TCP/IP LAN (Ethernet) and WAN (serial) communication activity
- UTP Ethernet connection active
- SCADAPack 300E FORCE LED indicates ISaGRAF has variable(s) locked

For more information see the hardware manual for each RTU hardware model

5.1.2 RTU Models

SCADAPack 300E

- wide range input power
- I/O time-stamping to 100ms (dependent on I/O quantity)
- Dual ISaGRAF IEC61131-3 target kernels for sequencing and control
- TCP/IP communications
- Open communication protocols
- Extensive SCADAPack E functionality
- Cost effective
- I/O expansion through 5000 Series I/O modules (SCADAPack 300E models)

The following models provide Ethernet + USB communications + 3 serial ports (RS232/485 vary per model):

- SCADAPack 330E I/O: 3 CI channels
- SCADAPack 334E I/O: 16 DI, 10 RO, 8 AI, 3 CI, 2 AO (optional)
- SCADAPack 350E I/O: 8 DIO (input or output channels), 6 AI, 3 CI, 2 AO (optional)
- SCADAPack 357E I/O: 32 DI, 16 RO, 14 AI, 8 DIO, 3CI, 4AO (optional)

The following models provide USB communications + 2 serial ports (RS232/485). Ethernet is not available:

- SCADAPack 314E I/O: 16 DI, 10 RO, 8 AI, 3 CI, 2 AO (optional)

(DIO = bidirectional digital input/output channels, DI = digital inputs, RO = relay outputs, AI = analog inputs, CI = counter inputs, AO = analog outputs)

SCADAPack ES

The SCADAPack ES RTUs are available in a variety of models and options including:

- High performance Processing and I/O
- 9-30VDC wide range input power
- 32 DI, 16 DO, 12 AI, 4 AO I/O model
- 16 DI, 8 DO, 4 AI, 2 AO I/O model
- 8 DI, 2 DO, 4 AI I/O model
- Digital time-stamping to 10ms (local I/O)
- Processor only model for high throughput communications with Dual Ethernet + 5 serial ports (no I/O)
- Dual ISaGRAF IEC61131-3 target kernels for sequencing and control
- TCP/IP communications
- Dual-Ethernet
- I/O expansion through SCADAPack ES Remote I/O (via serial and Ethernet interfaces)

- I/O expansion through 5000 Series I/O modules
- Open communication protocols
- High performance SCADAPack E features, compact size

SCADAPack ER

The SCADAPack ER RTU is a rack-based RTU which is available with a variety of options detailed as follows:

- 24V DC power supply card (isolated)
- 48V DC power supply card (isolated)
- 110V DC power supply card (isolated)
- Dual power supply support
- Rack-based I/O card system
- 32 DI card with high speed counters **(ER-32DI-A)**
- 16 RO (relay) card **(ER-16RO-A)**
- 16 AI card **(ER-16AI-A)**
- 4 AO card **(ER-4AO-A)**
- Hot-swap I/O cards
- Digital time-stamping to 1ms
- Hardware handshaking RS232 port on Port 0 (DB9 connector)
- Dual ISaGRAF IEC61131-3 target kernels for sequencing and control
- TCP/IP communications
- Dual Ethernet + 5 serial ports (**SCADAPack ER - P600 processor module**)
- Dual Ethernet + 9 serial ports – 6 support RS232/422/485, 4 of which are isolated from other ports (**SCADAPack ER - P620 processor module**)
- Conitel protocol support on up to 4 serial ports (v.28) – Conitel v.23 or Bell202 with external modem (**P620 processor module**)
- IRIG-B time synchronisation – modulated and un-modulated formats including IEEE1344 standard (**P620 processor module**)
- I/O expansion through SCADAPack ES Remote I/O (via serial and Ethernet interfaces)
- Open communication protocols
- High performance SCADAPack E features, large I/O capacity

5.1.3 Hardware Accessories & User Servicing

Hardware Accessories

Available accessories for SCADAPack E RTUs include:

- External isolated power supply
- Battery backup power supply with charging / discharge / test capability
- Solar power supply
- PSTN dial-up modem
- GSM dial-up modem
- CDMA dial-up modem
- Leased-line modem
- SCADAwave(R) Data radio
- Data radio
- GPRS, 1xRTT, HSDPA (3G) data modems
- Satellite communications
- TCP/IP Internet / Intranet communications equipment
- GPS Receivers
- Time synchronisation flexibility - DNP3, IEC60870-5, NTP, IRIG-B [SCADAPack ER - P620 only]

Hardware User Servicing

The SCADAPack E hardware includes user serviceable parts on many of its external interfaces (dependent on model).

Some models include:

- Fuses on input power supply and secondary output power supply
- Fuses on Analog Input channels
- Field replaceable Lithium battery

Typical I/O and Interface connections are available through Schneider Electric Support upon request.

More information on hardware aspects of the RTU is available in the relevant SCADAPack E Hardware User Manuals.

5.2 Configuration Tools

SCADAPack E Configurator

The SCADAPack E RTU is maintained and diagnosed using the SCADAPack E Configurator software package.

This package can also be used to build configurations offline and later load RTU configurations.

SCADAPack E Configurator executes on PC hardware using Microsoft Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, or Windows 7 32-bit or 64-bit, and provides graphical user interfaces for configuring and diagnosing SCADAPack E operations.

It also integrates with the ISaGRAF 3 Workbench and SCADAPack Workbench for building and diagnosing IEC 61131-3 sequences.

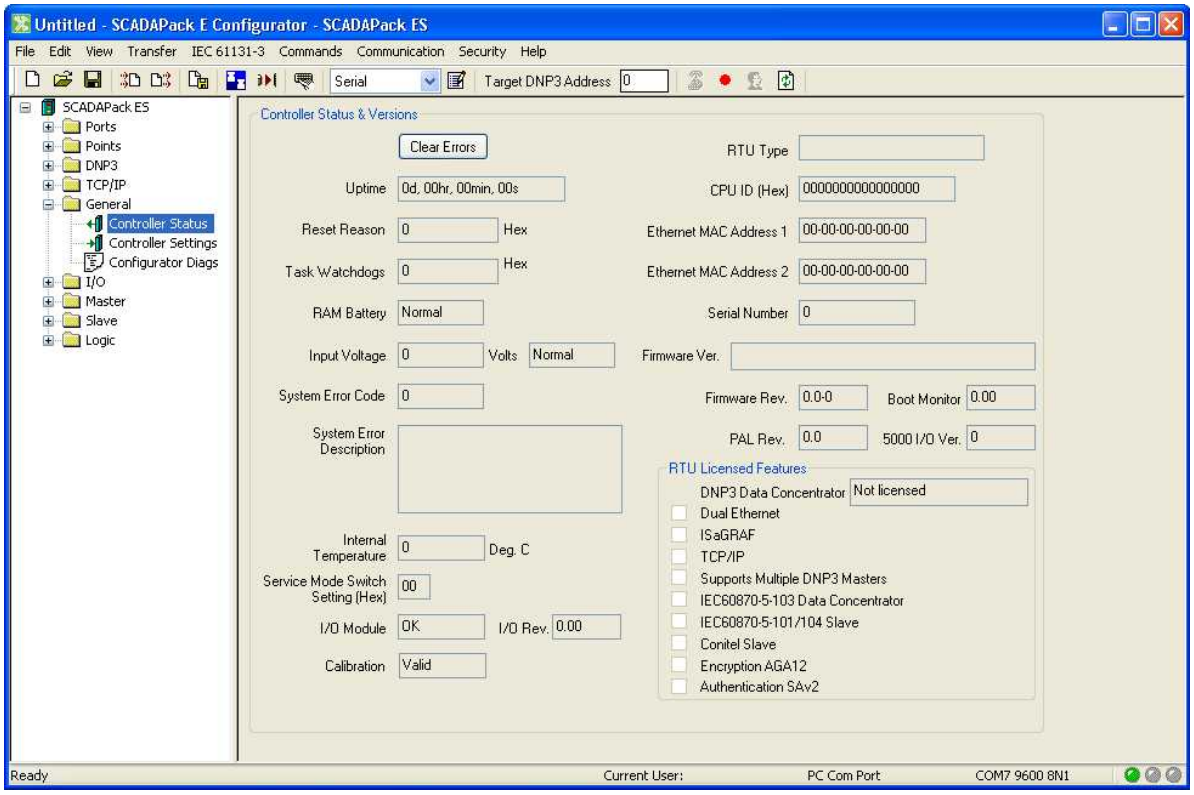


Figure 5.2: SCADAPack E Configurator Controller Status Page

SCADAPack E Configurator can create and modify configurations on-line with an SCADAPack E RTU or off-line, saving configurations for loading into the RTUs at a later time. SCADAPack E Configurator supports a wide variety of communication media access for remote communication with RTUs.

Supported communication links include:

- RS232
- PSTN dial-up

- GSM dial-up
- UDP/IP (across LAN/WAN networks)
- USB

Graphical forms are presented for each aspect of the RTU configuration. Ad-hoc user point enquiries may also be entered, and saved. Saved user data is associated with the RTU configuration file, so user data can be individually tailored for each RTU.

For more information on SCADAPack E Configurator refer to the *SCADAPack E Configurator User Manual*

ISaGRAF 3 Workbench

ISaGRAF 3 Workbench CASE tools manage the configuration and debugging of SCADAPack E sequence and control applications using IEC61131-3 languages, and target 3 firmware.

Through on-line interaction with the ISaGRAF 3 Workbench Debugger, SCADAPack E Configurator provides the ability for user applications to be debugged, remotely across a SCADA communications network including DNP3 communications links. For more information see section 5.2 in this Technical Overview.

For more information on IEC 61131-3 application programming interfaces for target 5, see the *SCADAPack E ISaGRAF 3 Reference* manuals.

SCADAPack Workbench

ISCADAPack Workbench manages the configuration and debugging of SCADAPack E sequence and control applications using IEC61131-3 languages, and target 5 firmware.

For more information on IEC 61131-3 application programming interfaces for target 3, see the *SCADAPack E Target 5 Reference* manuals.

5.3 Firmware Updates

Operating System Firmware Update

The Boot Monitor firmware on an SCADAPack E RTU resides in Flash memory on the processor Board. Its purpose is to start the SCADAPack E RTU, enable hardware peripherals, and to verify and start the main RTU Operating System Firmware.

It also provides facilities for re-programming the SCADAPack E Operating System Firmware Flash memory and re-programming the Boot Monitor Flash memory.

SCADAPack E Configurator provides update Wizards permitting local firmware updates for operating system firmware, or boot monitor firmware.

SCADAPack E Configurator can be used to load a ".BIN" binary image file locally, ".BIZ" compressed binary image file, or a ".BIP" compressed binary patch file into an RTU through DNP3 communication interfaces (locally or remotely).

The firmware files provided by Schneider Electric are firmware upgrades specifically for the SCADAPack E RTU hardware. The Boot Monitor re-programs the SCADAPack E RTU's operating system firmware Flash memory from these files.

A Windows® utility is provided on the Schneider Electric installation CD-ROM to allow generation of BIZ compressed binary image firmware files and BIP compressed binary patch firmware files. Using these file formats permits remote upgrading of RTU firmware. Due to the nature of the BIP files being "difference patch" files of a relatively small size, RTU firmware can be readily upgraded across remote DNP3 communications links.

The Boot Monitor can be forced to re-program the RTU operating system Flash memory at start-up rather than to start the RTU operating system firmware. This is achieved by following SCADAPack E Configurator *Transfer / Update System Firmware* wizard instructions.

Whilst operating, the RTU Operating System firmware supports loading of files (including firmware ".BIZ" and ".BIP" compressed files) across DNP3 communication links. Once remotely loaded, the Boot Monitor is instructed to re-program the RTU Operating System Firmware Flash ROM from this file. The disruption to RTU operation is minimized by the time consuming part of the operation occurring while the RTU continues to operate.

If the SCADAPack E Operating System Firmware is modified via DNP3 communications using SCADAPack E Configurator, the RTU preserves configurations of the RTU including the ISaGRAF application(s), ISaGRAF retained variables, RTU point configurations, etc.

Upon verification of the RTU operating system firmware after re-programming Flash memory, the **SCADAPack E RTU is automatically restarted**.

Local operating system update procedures are also provided that are independent of DNP3 communications.

Using these update modes (for example SCADAPack ES and SCADAPack ER Hex Switch 'FF' mode or SCADAPack E Configurator 'local serial port - offline' method), the RTU DOES NOT RETAIN ITS CONFIGURATION. Rather it reverts to FACTORY DEFAULT configuration. For more information see SCADAPack E **Firmware Update Technical Reference** manual.

Boot Monitor Firmware Update

The Boot Monitor may itself re-program the Boot Monitor Flash. To do this, follow the SCADAPack E Configurator *Transfer / Update Boot Monitor* wizard.

SCADAPack E RTUs allow the Boot Monitor firmware to be updated via a DNP3 link using SCADAPack E Configurator.

Alternatively for SCADAPack ES and SCADAPack ER RTUs, the HEX Switches may be set in special mode “F9” and SCADAPack E Configurator used to update the Boot Monitor firmware 'offline' (i.e. normal RTU operations are disrupted using this process).

Whilst operating, the RTU Operating System firmware supports loading of Boot Monitor firmware “.BIN” binary image files across DNP3 communication links.

Once remotely loaded, the RTU Operating System firmware can re-program the Boot Monitor Firmware Flash ROM from this file.

The SCADAPack E RTU is automatically restarted at the completion of the Boot Monitor update.

For more information on the Boot Monitor see **SCADAPack E Firmware Update Technical Reference** manual.

5.4 RTU Operating System Components

The major components of the SCADAPack E Operating System Firmware are as follows:

Real Time Executive
- responsible for scheduling internal RTU task operations and providing interfaces between other RTU system facilities. Many real time executive operations are transparent to the user, but some diagnostics are provided through the RTU's command line interface

Point Database
- contains configurations and current values for RTU points
- contains Trend records for trend sampling

I/O Sub-system
- receives data from physical input channels and controls data to physical output channels on the local RTU I/O
- performs low level I/O processing such as digital input de-bounce, digital input state inversion, pulse input counting, analog channel calibration

Remote I/O
- expands the I/O capacity of an RTU by interconnecting multiple RTU devices
- utilizes Serial or Ethernet communication links between remote I/O units
- Remote I/O units are identified by SCADAPack E HEX Switch settings

ISaGRAF
- provides user sequencing and control support using IEC61131-3 international standard programming languages
- interfaces with Point Database for access to I/O, derived data and configuration information
- interfaces with DNP3 for peer communication, manipulation of DNP3 communication parameters
- up to two (2) user applications may execute simultaneously on the same RTU

DNP3
- provides DNP3 Slave capability for RTU to SCADA Master Communication
- up to three (3) DNP3 Master Stations may connect simultaneously to the same SCADAPack E RTU. This can be via individual serial links, a common serial link, PSTN, GSM, TCP/IP, etc.
- provides DNP3 Master and Slave capability for RTU to RTU peer-to-peer communication
- provides DNP3 Master capability for Data Concentrator facilities
- manages historical record of point events for transmission to SCADA Master(s)
- carries Master Station requests for controls, configuration
- carries configuration and diagnostic data including SCADAPack E Configurator information
- Remote ISaGRAF Workbench Debug communication
- Support for AGA12 secure communications
- provides a number of communication interfaces for DNP3

Comm Interfaces
- includes PSTN dial-up, GSM dial-up, keyed RS-232
- provides serial TCP/IP communications including PPP serial, PPP for GPRS / 1xRTT

Peripheral Interface	- provides external communication services with peripheral equipment such as PLC's (typically, RTU is Master, PLC is Slave), I/O bricks - interfaces with ISaGRAF for configuration and exchange of data - includes protocol drivers for Rockwell DF1 Master, MODBUS RTU Master, MODBUS RTU Slave, MODBUS/TCP Client and MODBUS/TCP Server communications
Data Processor	- provides integrated data processing and manipulation - uses Point attributes to drive the data processing and sets Point properties with the results of the processed data - interfaces with DNP3 for event generation, storage and transmission
Profiler	- manipulates point attributes or point values based on loaded time schedule configurations
Trend Sampler	- summarizes and stores historical records of point data for Transmission to a SCADA Master
File System	- stores RTU data such as configuration files, profiles, sample files, ISaGRAF applications, and logged data files.
Command Interface	- provides user access to RTU commands and diagnostic information
TCP/IP	- provides communication facilities and applications on the RTU for Internet or Intranet networks through Ethernet (LAN) or serial (WAN) RTU interfaces. - integrates RTU facilities with standard TCP/IP applications for remote management of the SCADAPack E RTU. - provides advanced facilities such as NTP time synchronization. - GPRS (mobile IP over GSM) and 1xRTT (mobile IP over CDMA) is supported natively

Figure 5.3 30 summarizes the relationship between these major SCADAPack E RTU Operating System components.

Figure 5.4 31 showing the relationship between RTU system components and TCP/IP services. (The system component relationships shown in ***Figure 5.3*** 30 are implied for ***Figure 5.4*** 31, but these are not shown for clarity).

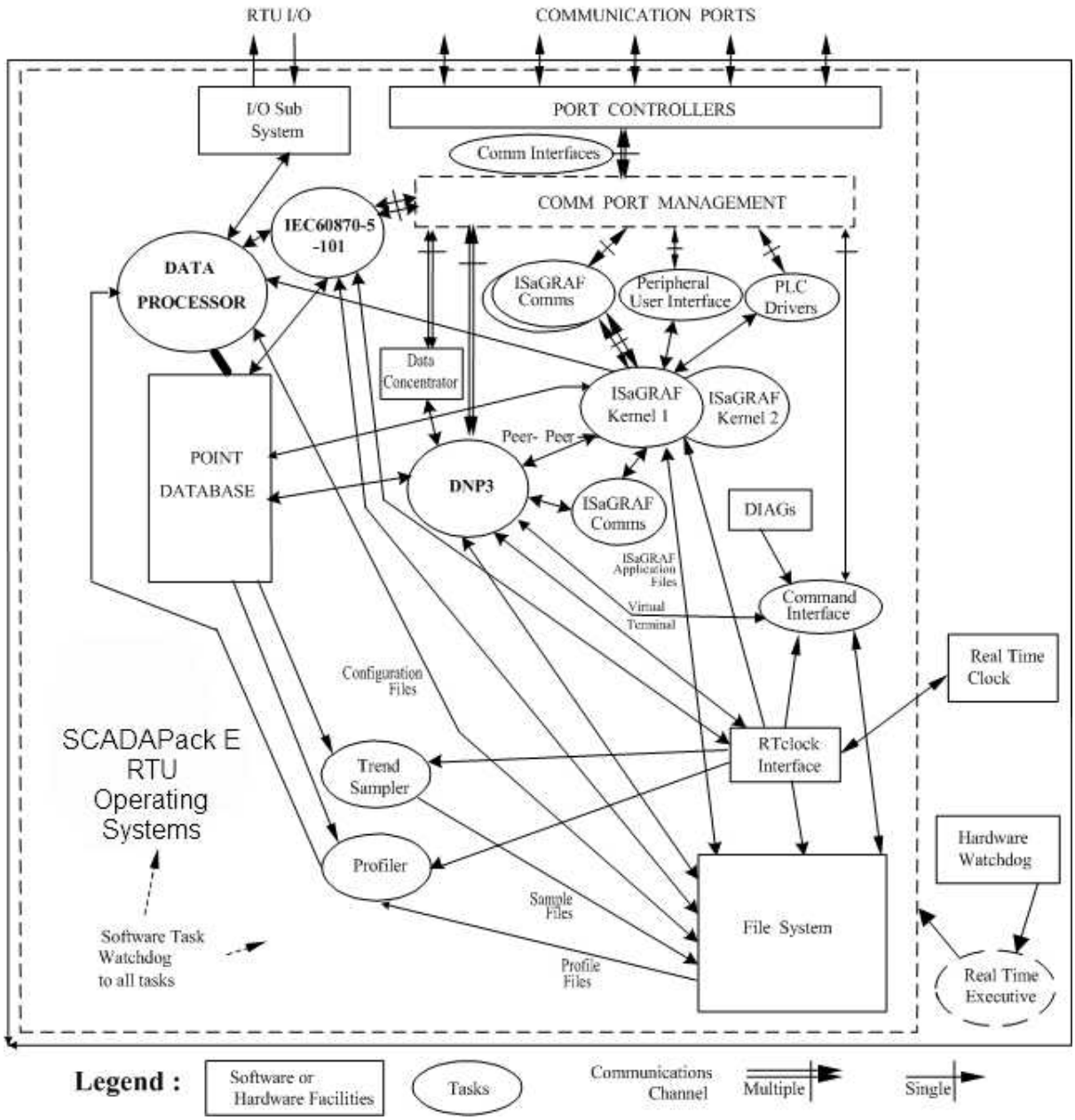


Figure 5.3: SCADAPack E RTU Operating System Architecture

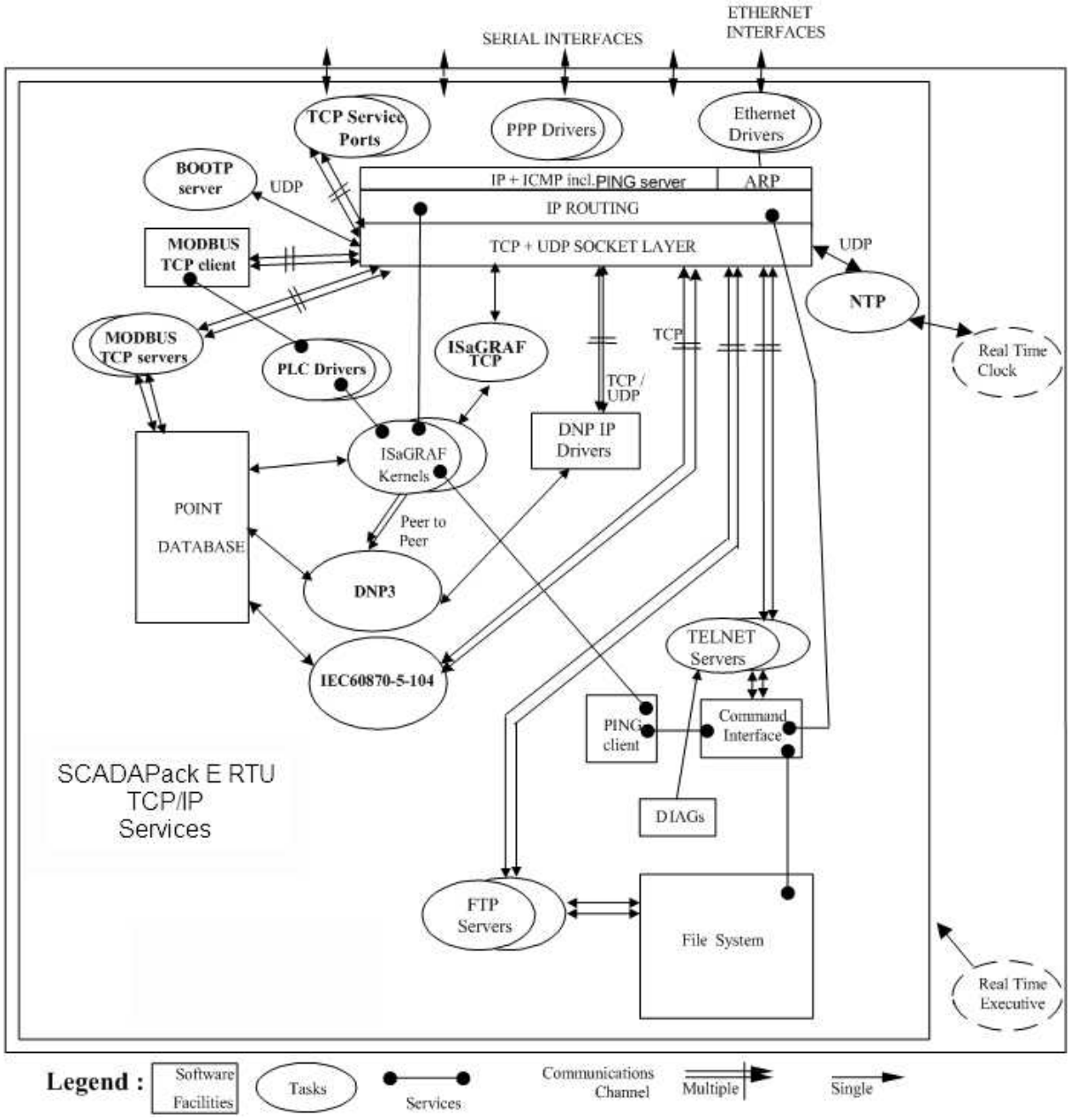


Figure 5.4: SCADAPack E RTU TCP/IP Services Architecture

5.5 RTU Points

"Points" are used in the SCADAPack E RTU to access data and some RTU system configurations.

Each RTU point is accessible through the following protocols, but not every point is necessarily presented to the SCADA Master.

- DNP3
- Modbus
- IEC60870-5-101
- IEC60870-5-104

See individual device hardware manuals for specifications of point capacity for each RTU model.

Points fall into one of two categories: Physical Points and Derived Points.

Physical Points

RTU internal representation of electrical terminations on a Main RTU, Remote I/O unit, external I/O modules.

These may be either **Input Points** or **Output Points**.

Derived Points

RTU internal data.

These may be either **User Points** (created by a user defined configuration) or **System Points** (managed by the SCADAPack E operating system)

Point Types

Various point types are supported by the SCADAPack E RTU.

"Point Type" and "Point Number" uniquely identify each point in the SCADAPack E RTU.

See the *SCADAPack E Configuration Technical Reference* manual for information on Point Numbering methodologies.

"Point Type" may be one of the following:

- **Digital Point** (also referred to as "Binary Point" throughout the DNP3 protocol documentation and SCADAPack E RTU documentation). These may be **Input**, **Output**, **User** or **System** points.
- **Analog Point**. These may be **Input**, **Output**, **User** or **System** points.
- **Counter Point**. These are **Input** points on the RTU.
- **String Point**. These are **System** points on the RTU.

6 Physical I/O Expansion

- *5000 Series I/O* 34
- *SCADAPack ES RTU Remote I/O* 35

6.1 5000 Series I/O

The physical I/O of a SCADAPack 300E or SCADAPack ES can be expanded by connecting 5000 Series Expansion I/O modules to the 5000 Series I/O bus interface on the RTU.

Configurations, that specify the modules to be used and the mapping of configuration points, can be created OFFLINE using the SCADAPack E Configurator and transferred to the RTU as required. The following diagram displays a configuration window, from the SCADAPack E Configurator, used to configure a SCADAPack E RTU connected to a 5606 Expansion I/O module.

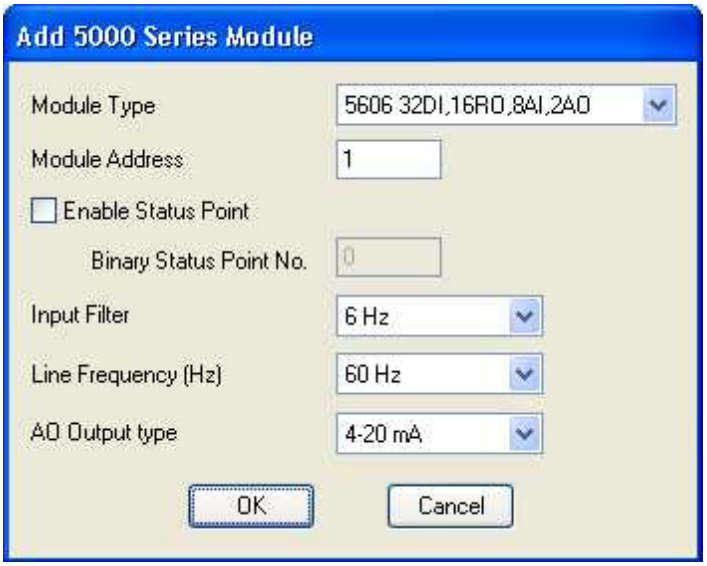


Figure 6.2: Add 5000 Series Module Dialog

The 5000 Series I/O modules can be daisy-chained in order to expand the quantity of physical I/O as required. SCADAPack E RTUs support up to 16 connected series 5000 I/O modules.

6.2 SCADAPack ES Remote I/O

Remote I/O is the mechanism provided by the SCADAPack E RTU that expands the I/O capacity of a Main RTU unit using SCADAPack ES devices. A SCADAPack ES and SCADAPack ER RTU can be a Main RTU. Only SCADAPack ES devices can be Remote I/O units.

Each Remote I/O system "group" needs to have only one "Main" RTU unit, and up to 15 "Remote I/O" units. RTU HEX Switches select between "Main" and "Remote" unit numbers.

A Main RTU unit is a normal RTU, providing the full range of RTU services. Remote I/O units provide facilities for monitoring and controlling I/O on behalf of the Main RTU. The Normal RTU facilities, such as ISaGRAF user applications, data manipulation, Profiling, Trend Sampling, etc. are not provided by Remote I/O units.

I/O on Remote I/O unit(s) is accessed through additional I/O points in the Main RTU point database. All facilities provided by the local RTU (Main unit) on its I/O are also provided by Remote I/O units. This includes de-bounce, invert, and pulse counter functions. Calibrations need to be performed on each RTU unit individually prior to connection in a Remote I/O system.

Communication links are established between a Main RTU unit and its Remote I/O unit(s). Remote I/O communications is supported on Serial links RS-232 or ETHERNET to SCADAPack ES RTUs.

A "Main" RTU unit may be configured with multiple Remote I/O ports if necessary.

"Remote I/O" units require no configuration other than the HEX switch settings. They do require individual RTU hardware calibration.

Remote I/O using Ethernet links on the RTU uses IEEE 802.3 framing and may be connected to a standard Ethernet LAN using 10/100-BaseT (UTP) for the SCADAPack E RTUs.

Multiple Remote I/O system "groups" are supported by SCADAPack E RTUs on the same communication link. RTU HEX Switches select the "Group" number as well as the "Unit" number. This is particularly useful for ETHERNET communications where up to 15 Groups may be present on the same ETHERNET LAN, with each group having 1 main RTU unit and up to 15 Remote I/O units.

Figure 6.1 35 shows an example Remote I/O configuration using ETHERNET.

For more information on Remote I/O see *SCADAPack E Remote I/O Technical Reference* manual.

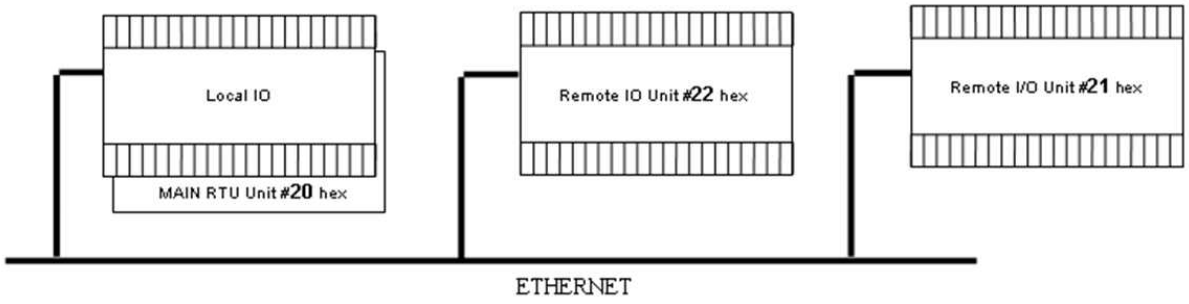


Figure 6.1: Typical SCADAPack E System Using Remote

7 IEC 61131-3 ISaGRAF

- ISaGRAF 3 Workbench 37 (target 3)
- SCADAPack Workbench 42 (target 5)

7.1 ISaGRAF 3 Workbench

- ISaGRAF Workbench Software 37
- ISaGRAF Workbench Communication, LIBRARY, & Diagnostics 38
- The ISaGRAF Pre-Processor & Transferring ISaGRAF Applications 39
- ISaGRAF Target 40

7.1.1 ISaGRAF Workbench Software

ISaGRAF Workbench software is used to create, manage and simulate sequencing and control applications using the five (5) IEC61131-3 international standard programming languages. ISaGRAF Workbench CASE Tools provides an environment for complete off-line application development. ISaGRAF Workbench is compatible with Windows 2000 / XP.

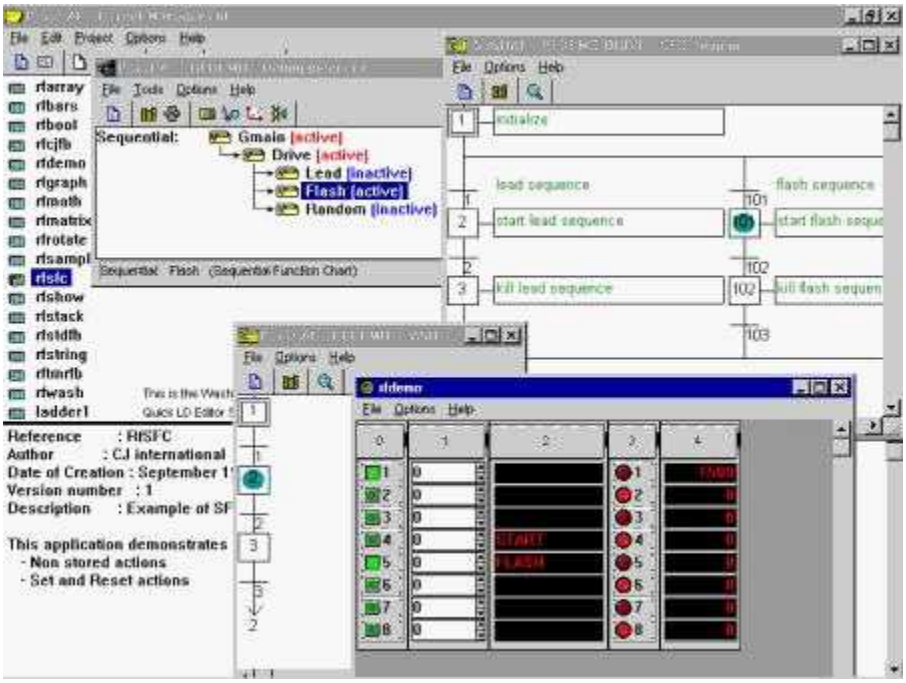


Figure 7.1: ISaGRAF Software Dialog Boxes

The ISaGRAF Workbench debugger transfers ISaGRAF application programs to the target (SCADAPack E RTU in this case) and also provides on-line target application debugging facilities.

ISaGRAF supports basic data types such as BOOLEAN, INTEGER, REAL, TIMER, MESSAGE variables. ISaGRAF also supports ARRAY types of these variables.

For more information see *SCADAPack E ISaGRAF 3 User and Technical Reference* manuals.

7.1.2 ISaGRAF Workbench Communication, LIBRARY, & Diagnostics

ISaGRAF Workbench Communication

The ISaGRAF Workbench debugger operates with SCADAPack E RTUs directly on an RTU serial port configured as "ISaGRAF" and via TCP/IP LAN/WAN in the RTU processor board.

In addition, SCADAPack E RTUs provide the ability for the ISaGRAF workbench debugger to be operated remotely via the RTU's DNP3 data communication channels. The remote debugging facility uses DNP3 protocol 'Virtual Terminal' objects.

The SCADAPack E Configurator software (as well as providing a configuration interface for setting parameters such as RTU port functions & data rates, SCADA data configuration, DNP3 configurations, etc) provides a software connection to the ISaGRAF Workbench debugger running on the same PC.

SCADAPack E Configurator transports ISaGRAF Workbench debugger communications via DNP3 protocol to the ISaGRAF target in the remote RTU. Similarly, the DNP3 driver in the remote RTU sends ISaGRAF target data via DNP3 protocol to SCADAPack E, which returns the data to the ISaGRAF Workbench debugger. For more information see the *ISaGRAF Technical* manual and the *SCADAPack E Configurator User Manual*.

ISaGRAF LIBRARY

Schneider Electric provides a set of ISaGRAF Library modules for use with the ISaGRAF Workbench. These provide the interfaces between the Workbench and RTU target facilities, i.e. they provide ISaGRAF user application access to RTU software and hardware facilities through standard IEC 61131 interfaces. The Library modules include:

- I/O Board definitions
- I/O Complex Equipment definitions
- Common Defines
- Function definitions
- Function Block definitions

For more information see the *ISaGRAF Technical* manual and the *SCADAPack E ISaGRAF Function Block Reference* manual.

ISaGRAF Diagnostics

The format of the Diagnostic Display of ISaGRAF user applications messages is as follows:

ISaGRAF Warning: XXX:YYY

Where XXX is the ISaGRAF message code number, and YYY is an information number provided to the Workbench. This meaning of the information number depends on the particular message code, and indicates the ISaGRAF Target number for some message codes.

See the *ISaGRAF Technical* manual for a complete list of ISaGRAF Application Status Codes.

7.1.3 The ISaGRAF Pre-Processor & Transferring ISaGRAF Applications

The ISaGRAF Pre-Processor

Schneider Electric provides an ISaGRAF pre-processor for the ISaGRAF Workbench to assist in defining constants for use with the SCADAPack E telemetry system.

The ISaGRAF Pre-Processor allows the use of a string “define” in place of a DNP Point Number as an input parameter to some SCADAPack E ISaGRAF function blocks. It is useful for the following function blocks: “SETATR_I”, “SETATR_R”, “RDFLD_I”, and “RDFLD_R”

When installed, the ISaGRAF pre-processor is transparent to the user and automatically generates application definitions for the DNP3 point index of ISaGRAF variables connected to DNP3 I/O boards. If an ISaGRAF I/O variable is moved on an I/O board, the pre-processor re-generates the definition string automating the link between an I/O variable and its DNP3 point index.

For more information see the *ISaGRAF Technical Reference* manual.

Transferring ISaGRAF Applications

ISaGRAF applications can be transferred to the SCADAPack E RTU (target 3) in one of several ways:

- Connect Workbench Debugger to an RTU “**ISaGRAF**” port
- Connect Workbench Debugger to the RTU via Ethernet or TCP/IP WAN
- Use Workbench Debugger, through SCADAPack E Configurator, via the DNP3 communication network
- Transfer the ISaGRAF application file(s) via the DNP3 communication network (DNP3 file transfer)
- Use the SCADAPack E Configurator "Write IEC 61131-3 Application” facility

ISaGRAF Target Application Files

An ISaGRAF application produced by the Workbench for an SCADAPack E RTU target is stored in the following file on the PC (for Intel targets):

C:\ISAWIN\ESeries\SMP\project_name\appli.x8m

This file can be copied to an RTU file called **isa11** or **isa21**, for ISaGRAF target kernels 1 and 2, respectively.

File transfer to the RTU can use FTP, using SCADAPack E Configurator, or can be transferred by the SCADA Master Station.

Once the file has been successfully transferred to the RTU, the ISaGRAF task(s) can be restarted to activate the new application. The SCADAPack E Configurator provides a toolbar facility that automatically performs these steps using DNP3, so can be performed across any DNP3 communications link.

7.1.4 ISaGRAF Target, Status, & Storage

ISaGRAF Target

The SCADAPack E RTU is equipped with ISaGRAF target kernel software.

This allows the RTU to perform PLC control functions using the IEC61131-3 international standard. The control functions provided by the ISaGRAF targets are completely autonomous of any supervisory (SCADA Master) system or communications network (e.g. DNP3). The ISaGRAF application operates on the RTU regardless of the state of remote communications.

The ISaGRAF target version supported by SCADAPack E RTUs is 3.40, which is compatible with ISaGRAF Workbench versions 3.20 and later.

SCADAPack E RTU firmware supports the simultaneous execution of up to two ISaGRAF target kernels on the same RTU. This allows up to two independent ISaGRAF applications to execute simultaneously on the same RTU. The

two ISaGRAF targets within the RTU have ISaGRAF Slave addresses of 1 and 2 respectively. The Workbench "Slave Number" communications parameter needs to be set to match the appropriate target kernel slave address prior to connecting the ISaGRAF Workbench debugger to the RTU.

The ISaGRAF Workbench software running a PC connects to an RTU serial port selected for 'ISaGRAF' communications mode.

ISaGRAF Status

The following RTU system points are provided in the RTU point database to indicate the status of each of the ISaGRAF Target tasks and applications within the RTU:

- ISaGRAF Target Application Halted
- ISaGRAF Target Task Started
- ISaGRAF Target Appl. Incorrect Checksum
- ISaGRAF Target Application Version
- ISaGRAF Target Application Size
- ISaGRAF Target Application Load Time
- ISaGRAF Target Application Checksum

ISaGRAF Storage

The SCADAPack E RTU provides several storage mechanisms for ISaGRAF applications and application data.

ISaGRAF uses the RTU file system in Non-volatile memory and FLASH memory to store its applications. An application transferred from the Workbench Debugger will be stored in the following files when validated by the ISaGRAF Targets on the RTU:

RTU ISaGRAF Application File: **isa11** (first ISaGRAF target)

RTU ISaGRAF Application File: **isa21** (second ISaGRAF target)

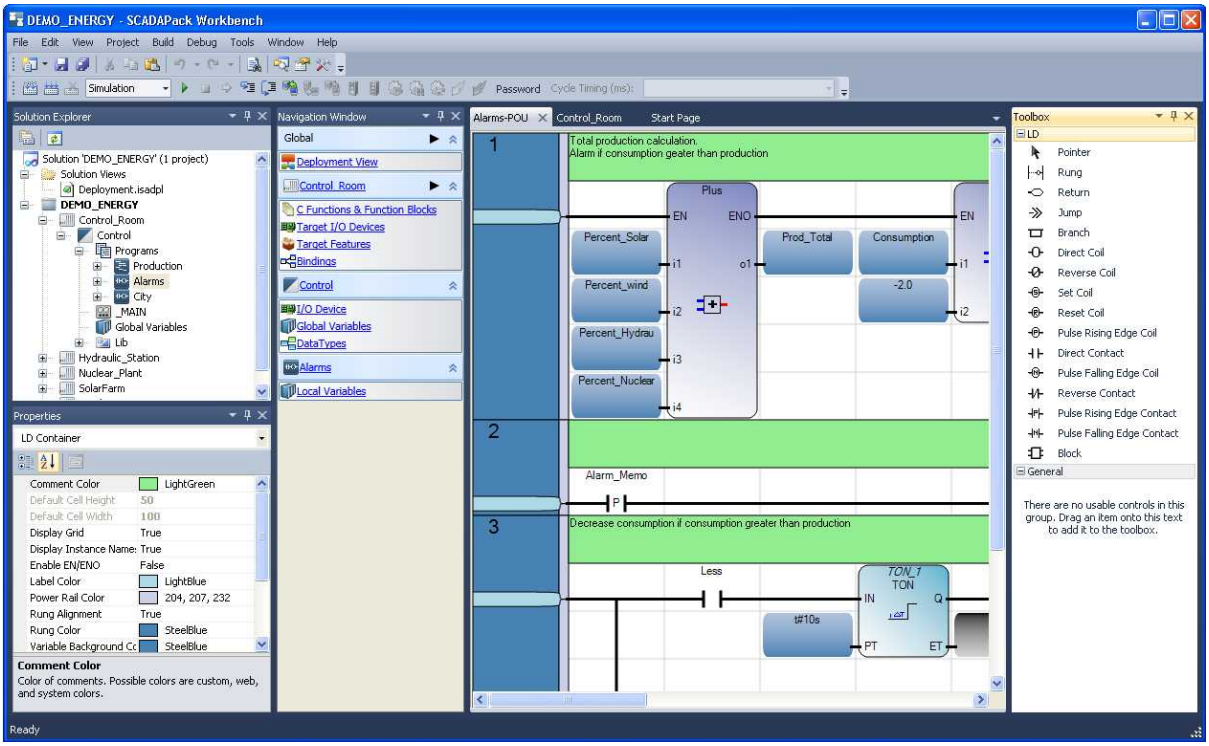
The executed version of each ISaGRAF application is loaded from the RTU file system if present. The FLASH memory copy will be used to load the user application if file system application cannot be loaded. In addition, the FLASH memory copy is used to regenerate the application file if it can not be loaded.

ISaGRAF application *Retained Variables* for each ISaGRAF target are also stored in RTU non-volatile memory.

7.2 SCADAPack Workbench

SCADAPack Workbench Software

SCADAPack Workbench software is used to create, manage and simulate sequencing and control applications using four (4) IEC 61131-3 international standard PLC programming languages and the target 5 firmware. SCADAPack Workbench is compatible with Windows XP SP3, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 operating systems.



The SCADAPack Workbench debugger loads IEC 61131-3 application programs to the target 5 resource (SCADAPack E RTUs in this case) and also provides on-line application debugging facilities.

Up to two independent resources can be loaded in to the same SCADAPack E RTU.

SCADAPack Workbench Communication

The SCADAPack Workbench debugger operates with SCADAPack E RTU's via serial or Ethernet.

Transferring IEC 61131-3 Applications

IEC 61131-3 applications can be transferred to the SCADAPack E RTU (target 5) in one of several ways:

- Connect Workbench Debugger to an RTU "**ISaGRAF**" port
- Connect Workbench Debugger to the RTU via Ethernet
- Use the SCADAPack E Configurator "Write IEC 61131-3 Application" facility to transfer an *.I5P file package

For more information see *SCADAPack E Target 5 Reference* manuals.

8 DNP3 - Distributed Network Protocol

- ***DNP3 SCADA Protocol Standard*** 44
- ***SCADAPack E DNP3 Support*** 45
- ***DNP3 Networking*** 46
- ***DNP3 Secure Authentication*** 48
- ***Encryption using the AGA12 Protocol*** 49

8.1 DNP3 SCADA Protocol Standard

DNP3 *(Distributed Network Protocol)* is an industry standard SCADA communications protocol. It originated in the Electricity Industry in the USA and was based on drafts of the IEC870-5 SCADA protocol standards (now known as IEC60870-5). DNP3 is now in widespread use in many industries across the world and is managed by the internationally represented DNP User Group.

DNP3 describes standards for SCADA protocol facilities such as polling, ad-hoc data requests, controls, report by exception (RBE) and Unsolicited communications. Master-slave and Peer-to-Peer communication architectures are supported by DNP3.

Inter-operability is one of the key aspects of DNP3. It is enforced by way of minimum implementation subsets to which vendors needs to adhere. Currently, the DNP3 standard is supplemented by Subset Definitions document describing 3 minimum subset levels. In addition, a vendor's DNP3 implementation needs to be provided with a *Device Profile* document describing information required by the DNP User Group, including details of the implementation of one of the three minimum subset levels, and other protocol information.

The DNP3 protocol also caters for expansion & evolution of the standard without detracting from the strengths of inter-operability that it promotes. This is achieved by an object-oriented approach to the data. Data objects can be added to the DNP3 Standard without affecting the way that devices inter-operate.

For further information see the DNP User Group Web Site at www.dnp.org, the *DNP3 eight volume document set, conformance test procedures, DNP3 Technical Bulletins, etc.*

8.2 SCADAPack E DNP3 Support

The SCADAPack E RTU supports DNP3 communication protocol facilities to the DNP User Group's DNP3 Subset Level 4 with a range of additional features being provided from the DNP3 standard.

The RTU supports DNP3 communication across TCP/IP and UDP/IP interfaces in accordance with the DNP User Group DNP3 standard for IP communication.

In summary the SCADAPack E RTU provides the following facilities for use of DNP3:

- Polling, Report by Exception, Unsolicited Response transmission to SCADA Master
- RTU configurations for data reported to SCADA Master
- Up to three (3) SCADA Master Stations supported with points individually configured for exposure to each Master (licensing may be required). See DNP3 Multi-Master 92.
- DNP3 Slave address can be individually set for communication with each Master Station
- Simultaneous DNP3 Master, Slave and Peer operation on the same SCADAPack E communication Port, or on multiple communication Ports
- Networking (Routing) of DNP3 frames
- Peer-to-Peer interchange of data between RTU nodes, including point quality
- Control operations from SCADA Master or Peer nodes
- Wide range of DNP3 data objects including:
- Integrated support for DNP3 object status flags
- integer and floating point analog objects
- counter objects
- File identifier objects
- Virtual terminal objects
- DNP3 Secure Authentication
- AGA12 Encryption security 49

Each SCADAPack E RTU on a DNP3 network needs to have a unique DNP Node Address to identify it. This node address is set as part of the RTU configuration, through SCADAPack E Configurator.

A single SCADAPack E RTU (controller) can have up to three DNP3 node addresses. 2 or 3 different addresses can be used when the SCADAPack E RTU connects to multiple DNP3 Master Stations (licensing required).

Valid DNP3 node addresses are in the range 0-65519. (DNP3 node addresses 65520-65535 are reserved by the DNP3 protocol).

It is recommended that DNP3 device Address ‘0’ not be used in SCADAPack E RTU as this is the default DNP3 address when an RTU is set to its factory default configuration.

For more information on DNP3 and operation of the RTU, see the *SCADAPack E DNP3 Technical Reference* manual and *SCADAPack E DNP3 Device Profile* documents.

8.3 DNP3 Networking

Communications received by the SCADAPack E RTU may be re-directed to other SCADAPack E RTU communication ports based on routing (packet forwarding).

Each DNP3 data-link layer frame contains both a Source and Destination DNP node address. This addressing scheme, by identifying both the sender and receiver of DNP3 frames, allows peer-to-peer RTU communication, and allows DNP data-link layer frames to be routed.

The SCADAPack E RTU networking facility determines if the destination node for a received DNP3 frame appears in a network routing table. The network routing table contains user configured Static Route entries that fully qualify received DNP3 frame source information (including RTU port and DNP3 source node address) and DNP3 frame destination node address, resolving a destination SCADAPack E communication channel. If a received frame, through serial or TCP/IP interfaces, qualifies the route filtering configuration in the network routing table's static entries, the DNP3 frame is routed for transmission to the DNP3 communication link on the specified SCADAPack E physical channel.

DNP3 frames are discarded if they are not for this node & not to be routed by this RTU to another node.

Any SCADAPack E RTU is capable of routing DNP3 frames, and can be configured with network routing table entries for this purpose. The RTU continues to provide RTU facilities and at the same time can perform routing functions. Typically, though, only a small number of nodes in a DNP network are required to route frames. These nodes usually have two or more DNP3 communication ports.

An SCADAPack E RTU can potentially route DNP3 frames to one of multiple DNP3 communication links on the RTU, including via TCP/IP interfaces. This is achieved efficiently and with a minimum of configuration when DNP3 node addresses on each DNP3 communication link are in small fixed address range, rather than addresses being randomly scattered across multiple links.

Some network communications infrastructure or Master Station implementations may restrict the routing capabilities.

For more information see the *SCADAPack E DNP3 Technical Reference* manual.

Where network communications infrastructure will support it, the SCADAPack E RTUs may send Peer messages to any other SCADAPack E RTU in the network.

Figure 8.1 47 shows a typical SCADAPack E RTU network using SCADAPack E RTU routing of DNP3 frames.

For example, DNP #200 can communicate with Peer DNP #301. In this case, SCADAPack E RTUs DNP #101 and DNP #103 route the DNP3 frames between the various communication sub-networks.

The Master station may also communicate transparently with every node in the communication network, with DNP nodes #101 and #103 routing DNP3 frames to RTUs on different communication sub-networks, as required.

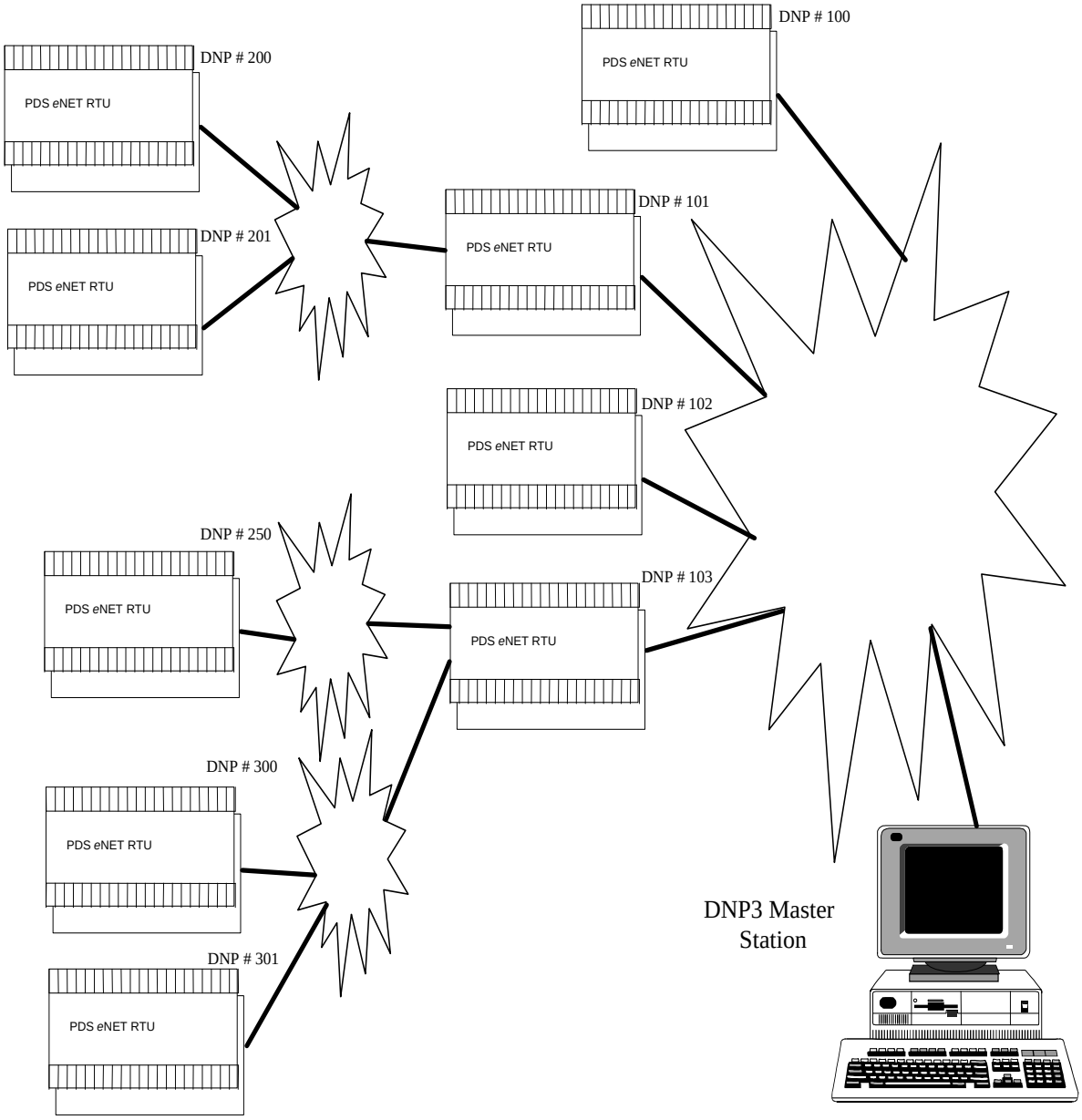


Figure 8.1: Typical SCADAPack E Network Using DNP3 Routing

8.4 DNP3 Secure Authentication

SCADAPack E RTUs support DNP3 Secure Authentication to the DNP User Group's secure authentication specification v2.0

The Integrated Security functionality provided by the RTU firmware requires a feature licence for activation. It secures DNP3 communication ports for Slave, Master and Peer communications.

The following RTU communications media supports DNP3 Secure Authentication:

- DNP3 RS232 serial ports
- DNP3 Dial-up (Hayes Modem) ports
- DNP3 RS422 serial ports
- DNP3 RS485 serial ports
- DNP3 / IP communications (TCP and UDP), including Ethernet, PPP, GPRS, 1xRTT, etc.

Integrated DNP3 Secure Authentication is a licensed feature of the RTU. After licensing, integrated security is activated when a security configuration is loaded into the device.

Security configurations are loaded via COMPACT Flash card for the SCADAPack ES and SCADAPack ER RTUs, and via SCADAPack E Configurator USB port for the SCADAPack 300E RTUs.

DNP3 Secure Authentication challenges requests to the controller for critical operations (controls, configuration change, firmware change, etc).

Optional configuration for DNP3 Secure Authentication includes:

- Master Key configuration for devices and Security Administrator application, for system privacy
- Common Key mode for Configurator software, for ease of deployment and maintenance of configuration computers
- Unique Key mode for Configurator software, for maximum protection of configuration computers
- Controller User Login, authenticating individual users for critical operations
- Concurrent operation with AGA12 Encryption 49

Security configurations are managed by the Security Administrator software. For more information see *Security Administrator User Manual.*

Refer to the *SCADAPack E Security Technical Reference* for detailed information regarding SCADAPack E RTU security functions.

8.5 AGA12 Encryption

SCADAPack E RTUs support the AGA12 security protocol through a “Virtual SCM” (SCADA Cryptographic Module), integrated with the various operational aspects of the RTU. The implementation adheres to the AGA12-2 recommendations and inter-operates with the AGA12-2 reference Application.

The Integrated Security functionality provided by the RTU firmware includes Virtual SCM facilities on DNP3 communication ports, implemented to the AGA12-2 recommendations.

Encryption services provided using AGA12 security on SCADAPack E firmware applies only to DNP3 communications.

The following RTU communications media supports AGA12 encryption:

- DNP3 RS232 serial ports (excluding Hayes Modem ports)
- DNP3 RS422 serial ports
- DNP3 RS485 serial ports
- DNP3 / IP communications (TCP and UDP), including Ethernet, PPP, GPRS, 1xRTT, etc.

Integrated AGA12 Encryption is a licensed feature of the RTU. After licensing, integrated security is activated when a security configuration is loaded in to the device.

Security configurations are loaded via COMPACT Flash card for the SCADAPack ES and SCADAPack ER RTUs, and via SCADAPack E Configurator USB port for the SCADAPack 300E RTUs.

A number of DNP3 communication port types are used when security is active. In summary the port types are:

- AGA12 Ciphertext ports
- DNP3 Local Access Port
- DNP3 Clear Device Port (AGA12 Gateway only)

There are two ways that RTU DNP3 communications may be used with AGA12 security:

- **As an AGA12 Node RTU** where every but one of the DNP3 communication ports (including Ethernet and PPP ports) are **Ciphertext ports** (protected). One port on the RTU is set-aside as a Local Access DNP3 port for configuration of the RTU (as normal)
- **As an AGA12 Gateway,** where the SCADAPack E RTU (the integrated virtual SCM) is used to take DNP3 messages received from a SCADA master on a **Clear Device Port**, protects it through AGA12 encoding, then sends the secure data out a **Ciphertext Port**.

AGA12 Encryption can be used concurrently with DNP3 Secure Authentication 48.

Refer to the *SCADAPack E Security Technical Reference* for detailed information regarding SCADAPack E RTU security functions and the AGA12 recommendations.

9 RTU Communication

- *DNP3 Communication Interfaces* 51
- *Peripheral Device Communication Interface* 54

9.1 DNP3 Communication Interfaces

Communication with the SCADAPack E RTUs via DNP3 protocol can be accomplished through several physical interfaces: Direct physical interfaces, Multi-drop physical interfaces, Hayes Modem interfaces and ETHERNET interface.

Each RTU physical port has a *Port Interface Type* parameter to select the appropriate interface. SCADAPack E RTUs support direct physical communication using RS232 and RS422 interface standards.

RS485 operation is only supported on selected ports on each of the SCADAPack E RTUs.

Detailed information on RTU communication interfaces are provided in the *SCADAPack E Communication Interfaces Technical Reference*.

- ***Direct & Multi-drop Communication Interfaces*** 52
- ***Hayes Modem & TCP/IP Communications*** 53

9.1.1 Direct & Multi-drop Communication Interfaces

Direct Communication Interfaces

Port Interface types using direct communication interfaces are:

- RS232
- RS422 **
- RS485 4-wire Master (same as RS422) **

Multi-drop Communication Interfaces

Port Interface types using multi-drop communication drivers are:

- Keyed RS232
- FSK modem (option)
- RS485 4-wire Slave **
- RS485 2-wire

** RS422 and 4-wire RS485 modes are supported by SCADAPack ES and SCADAPack ER RTUs. RS485 2-wire modes are supported by SCADAPack E RTUs.

9.1.2 Hayes Modem & TCP/IP Communications

Hayes Modem Communications

The SCADAPack E RTU can provide DNP3 network communications using Hayes Modem communications.

This type of RTU communication is often called “PSTN” (Public Switched Telephone Network) or dial-up communication, and requires the use of commercial modem equipment. Hayes modem devices on wireless networks are also supported including GSM and CDMA.

GPRS and 1xRTT wireless networks using public cellular infrastructure are also supported. Also see TCP/IP Integration 79.

The SCADAPack E RTU communications support using Hayes modems includes both dial-in and dial-out operation, both on the same communication channel.

Similarly, the same modem can be used for dial-out and dial-in DNP3 Peer-to-Peer communication between RTUs, or for dial-in for configuration or diagnosis using SCADAPack E Configurator.

A DNP3 Route Table ‘static entry’ can be associated with a Modem Dial number. This allows an RTU to contact an individual DNP3 such as a Peer RTU, Master station, etc. Where groups of nodes are contacted through the same modem phone number, route entries with DNP address ranges can have a single phone number. Multiple route entries for DNP nodes can have the same phone number, or any combination can be used.

The RTU firmware include specific support for low power modems.

For more information see *SCADAPack E Communication Interfaces Reference* manual.

TCP/IP Communications

The SCADAPack E RTU supports communications on Internet or Intranet TCP/IP networks.

DNP3 communication protocol is transported using TCP and/or UDP transport in accordance with the DNP User Group LAN/WAN specifications.

TCP/IP communications is supported via Ethernet, PPP (including GPRS and 1xRTT) on the RTU.

RTU to Master Station DNP3 communications is supported via TCP/IP, including to multiple backup Telemetry Computer systems use different IP addresses.

RTU to RTU communications is also supported via TCP/IP using DNP3 protocol for Peer-to-Peer calls.

SCADAPack E Configurator supports TCP/IP communication to remote RTUs using DNP3 over UDP via Windows® TCP/IP communication stack.

For more information on the RTU interfaces to TCP/IP see *SCADAPack E TCP/IP Technical Reference Manual*.

9.2 Peripheral Device Communication Interface

The SCADAPack E RTU can communicate with Peripheral devices, such as PLC's, in various ways.

In-built drivers for MODBUS protocol, for example, provide both serial and TCP/IP communications for Master, Slave, Client & Server protocols.

Other peripheral device communications supported by SCADAPack E includes DF1 PLC communications.

The user can also implement their own communications with ASCII devices.

- ***MODBUS/TCP Client & Server Operation*** 57
- ***Serial MODBUS Slave & PLC Driver Master Operation*** 55
- ***Rockwell DF1 PLC & Modbus RTU Master Driver*** 56
- ***ASCII & Virtual Terminal Serial Communications*** 59
- ***IEC 60870-5-101, -104 & -103 Protocols*** 60

9.2.1 Serial MODBUS Slave & PLC Driver Master Operation

Serial MODBUS Slave Operation

The SCADAPack E RTU supports a driver for native MODBUS RTU Slave protocol.

The RTU can be configured to have multiple Modbus Slave ports functioning simultaneously. This MODBUS Slave implementation maps directly into the RTU's point database and supports MODBUS function codes: 1, 2, 3, 4, 5, 6, 7, 15 and 16.

Consult the *SCADAPack E Modbus Communication Interfaces* document for more information.

PLC Driver Master Operation

As an extension of the data interface provided by the SCADAPack E RTU, access by ISaGRAF applications to external PLC or peripheral device data is supported.

Standard ISaGRAF I/O boards access RTU I/O points and RTU database points. An additional set of ISaGRAF boards is provided for the RTU that allow data to be extracted from external PLC device(s) into ISaGRAF variables.

When using ISaGRAF I/O boards for peripheral device communication, ISaGRAF is a protocol Master, communicating with PLC or peripheral devices on one or more RTU communication ports. Various protocols can be supported between the RTU and slave peripheral devices via the ISaGRAF PLC Device I/O boards mechanism.

Peripheral device drivers are part of the RTU Operating System firmware.

LED(s) on the SCADAPack E RTU indicates external peripheral device communication activity.

9.2.2 Modbus RTU Master Driver & Rockwell DF1 PLC

Modbus RTU Master Driver

The SCADAPack E ISaGRAF MODBUS PLC Device I/O Boards communicate to PLC devices using MODBUS RTU Master communications protocol.

Multi-drop MODBUS PLC's are supported provided that interface adapters, external to the RTU, permit it.

The RTU *Port Function* needs to be set to "**PLC Device**" and the RTU "Port Baud" and port parity settings need to match those of the PLC device for correct operation.

ISaGRAF PLC Device I/O Boards specify MODBUS device address and MODBUS register address.

ISaGRAF PLC Device Input Boards also specify input data update rate.

ISaGRAF PLC Device Output Board data is updated upon change, and at a periodic background rate.

The RTU ISaGRAF MODBUS PLC Device I/O Boards generates communication link requests for MODBUS function codes: 1, 2, 3, 4, 5 and 6.

Rockwell DF1 PLC Driver

The SCADAPack E ISaGRAF DF1 PLC Device I/O Boards communicate to PLC Devices using Rockwell (Allen Bradley) DF1 Master communications protocol.

DF1 protocol is also known as Rockwell Data Highway protocol. Multi-drop PLC's are supported.

The SCADAPack E RTU DF1 driver supports communication with a wide range of Rockwell (AB) PLCs including: PLC5, SLC/500 and Generic DF1 devices.

Communication modes supported include:

- DF1 Half/Full Duplex,
- BCC/CRC error checking

Data types supported are:

- SLC500 Discrete, SLC500 INT, SLC500 REAL,
- PLC5 Discrete, PLC5 INT, PLC5 REAL,
- Generic Discrete, Generic INT

For more information see *SCADAPack E DF1 PLC Driver* manual.

9.2.3 MODBUS/TCP Client & Server Operation

MODBUS/TCP Client Operation

MODBUS/TCP Client operation allows an SCADAPack E RTU to utilize ISaGRAF PLC I/O boards to generate requests to MODBUS/TCP server devices such as PLCs, block I/O devices, etc. This is similar to serial MODBUS Master operation described in Section 7.2.4.

For example, the RTU can read data from, or write data to Conformance Class 0 or Class 1 Open Modbus/TCP Ethernet PLCs. Many data formats are supported including 984 discrete, IEC discrete, IEC UINT, INT, DINT, REAL & Swapped Real formats.

In addition, BOOTP server facilities are supported by the RTU for providing Ethernet network configuration of devices such as block I/O units.

For example, PLC I/O blocks can be used to expand I/O for the SCADAPack E RTUs. Up to 20 TSX Momentum I/O blocks can be connected to the same SCADAPack E RTU.

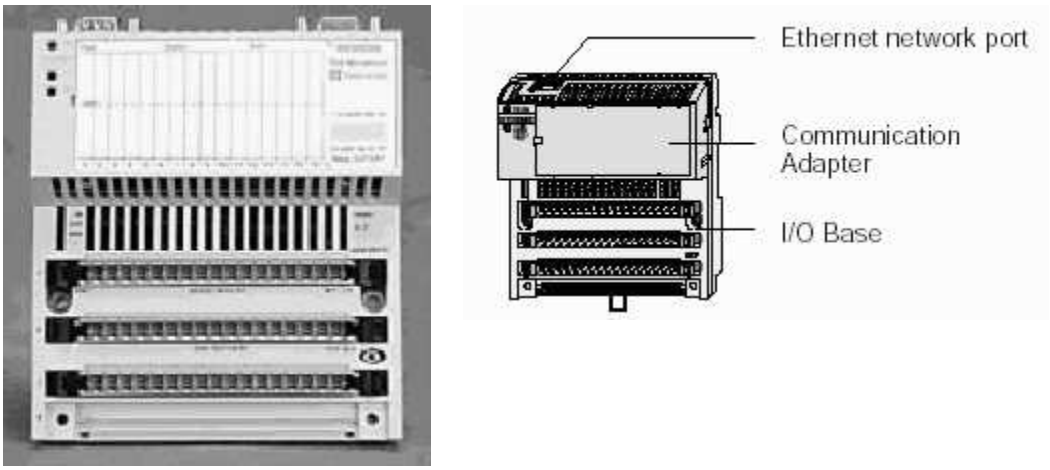


Figure 9.1: PLC I/O Module

MODBUS/TCP Server Operation

MODBUS/TCP Server operation allows SCADAPack E RTU data (I/O and/or derived data) to be made available to MODBUS/TCP client devices such as a local SCADA master station, or Ethernet PLCs.

Using this facility, the RTU can be used like a full-featured Ethernet PLC, or like an I/O module.

Other than enabling the MODBUS/TCP Server, no additional configuration is required to access RTU point data. Modbus register accesses are automatically mapped to the SCADAPack E RTU point database.

RTU physical, derived and system points can be accessed and controlled via the MODBUS/TCP server.

The RTU MODBUS/TCP server supports simultaneous access to multiple clients, utilizing any TCP/IP interface (e.g. Ethernet, PPP, GPRS, etc.).

The SCADAPack E supports Open MODBUS/TCP Conformance Class 0 & Class 1 device function codes: 1, 2, 3, 4, 5, 6, 7, 15 and 16.

Modbus/TCP data requests are served directly from the RTU point database, supporting IEC discrete, UINT, INT, DINT, UDINT & REAL formats.

9.2.4 ASCII & Virtual Terminal & TCP Serial Communications

ASCII Serial Communications

The ISaGRAF user application may optionally open an RTU serial port, or multiple RTU serial ports, as communication port(s) to serial devices.

Both ASCII and BINARY port transmit and receive function blocks are provided by ISaGRAF.

The user's ISaGRAF application can send and receive ASCII message strings, and interchange information with peripheral devices. The user has complete control over the process, and can create ASCII protocol drivers within the IEC61131-3 ISaGRAF sequencing and control application.

Examples where the ASCII serial communications facility has application includes: LCD display terminals, Personal Digital Assistant (PDA) palm-top devices, instrumentation interfaces, data logger interfaces, intelligent motor controllers, other ASCII devices.

Virtual Terminal Serial Communication

Serial ports on SCADAPack E RTUs can be used as remote DNP3 Virtual Terminal service ports.

This allows a DNP3 Master Station supporting Virtual Terminal functions to send and receive ad-hoc byte oriented data to RTU serial port(s) across DNP3 communication links.

Upon receiving a virtual terminal Write from a DNP3 Master, the RTU will transmit this to a local serial communications port.

Upon receiving data from the local serial communications port, it will generate DNP3 virtual terminal event data, which can be polled or unsolicited to the DNP3 Master station.

For more information see the *SCADAPack E DNP3 Technical Reference* manual.

TCP Service Port Serial Communication

Serial ports on SCADAPack E RTUs can be used as remote TCP Service ports.

This allows TCP/IP applications to send and receive ad-hoc byte oriented data to RTU serial port(s) across TCP/IP links.

TCP service ports permit remote connection to RTU serial ports for terminal-server style multi-protocol applications. Both Client & Server TCP service ports are supported in various configurations including Host client to SCADAPack E TCP service port server, RTU TCP service port client to RTU TCP service port server & TCP service port client to remote TCP service port server.

For more information see the *SCADAPack E TCP/IP Technical Reference* manual.

9.2.5 IEC 60870-5-101, -104 & -103 Protocols

IEC 60870-5-101 Protocol

The IEC 60870-5-101 protocol is designed for data transmission between Master Stations and Slave RTUs. The SCADAPack E RTU supports communications using the 60870-5-101 protocol on every serial port, and is supported for RS485/422* and RS232 modes. In each case the RTU operates as a 60870-5-101 Slave.

Configurations for up to two IEC60870-5-101 Master devices are supported. These configurations define communication fundamentals such as the Master address, RTU serial port for Master communications, etc. These configurations also define how information object identifiers (i.e. function type and information number) are mapped to configuration points in the RTU.

The support for the IEC 60870-5-101 protocol is discussed in more detail in the *SCADAPack E IEC 60870-5-101 and -104 Slave Technical Reference* manual and the *SCADAPack E IEC 60870-5-101 Slave Interoperability* document.

* RS422 and RS485 4-wire & 2-wire interfaces are supported on SCADAPack ES and SCADAPack ER RTUs. Other SCADAPack E RTUs support RS485 2-wire.

IEC 60870-5-104 Protocol

The IEC 60870-5-104 protocol is designed for data transmission between Master Stations and Slave RTUs using TCP/IP communciations. The SCADAPack E RTU supports communications using the 60870-5-104 protocol on Ethernet ports, whereby the RTU operates as an IEC60870-5-104 Slave.

Configurations for up to 2 IEC60870-5-104 Master devices are supported (shared with IEC60870-5-101 master configurations). These configurations define communication fundamentals such as the Master address, etc. These configurations also define how the information object identifiers (i.e. function type and information number) are mapped to configuration points in the RTU.

There is a large degree of commonality between the SCADAPack E support for IEC60870-5-104 and IEC60870-5-101 protocols.

The support for the IEC 60870-5-104 protocol is discussed in more detail in the *SCADAPack E IEC 60870-5-101 and -104 Slave Technical Reference Manual* and the *SCADAPack E IEC 60870-5-104 Slave Interoperability* document.

IEC 60870-5-103 Protocol

The IEC 60870-5-103 protocol is designed for data transmission between protection equipment and control systems. The SCADAPack E RTU supports communications using the 60870-5-103 protocol on each serial port, and is supported for RS485* and RS232 modes whereby the RTU behaves as a 60870-5-103 Master.

The configurations for the 60870-5-103 Slaves devices are defined in the SCADAPack E Data Concentrator Technical Reference manual. These configurations define communication fundamentals such as the Slave address, RTU serial port for slave communications, poll intervals, etc.. These configurations also define how the information object identifiers (i.e. function type and information number) are mapped to configuration points in the RTU.

IEC 60870-5-103 Controls and Generic data are supported in addition to conventional protection equipment polled data.

The support for the IEC 60870-5-103 protocol is discussed in more detail in the *SCADAPack E Data Concentrator Technical Reference.*

* RS485 4-wire & 2-wire interfaces are supported on SCADAPack ES and SCADAPack ER RTUs. Other SCADAPack E RTUs support RS485 2-wire.

10 RTU Configuration

RTU Configuration File Format

The SCADAPack E RTU Configuration file is a human readable ASCII text file that enables the RTU to build, modify, or restore its configuration.

The configuration file is can created by SCADAPack E Configurator or by a SCADA Master station. It can be created and edited with a standard text editor, or database application. Additionally, a configuration file can be built from the current configuration of an SCADAPack E RTU.

The configuration file can be loaded or activated in the RTU in two possible ways – full configuration or incremental configuration. The file format and content is identical for the two configuration techniques, the differences being the affect upon the RTU when the configuration is activated. A full configuration removes current RTU configurations and re-loads the new configuration, whereas an incremental configuration modifies existing configurations in the RTU. Activation of a configuration will produce the file “config.log” in the RTU, which summarizes the activation of the configuration and any errors encountered.

For details on the configuration file format see the *SCADAPack E Configuration File Format*.

Point Configurations

Points are configured by means of *Point Attributes* that describe information used by various RTU facilities. RTU facilities take the Point Attributes, current point state or value, information from other RTU facilities, and derive the *Point Properties*.

Point Attribute and Point Property information is described in detail in the *SCADAPack E Configuration Technical Reference* manual.

Point Attributes

Point Attributes are read/write fields of point configurations describing point functionality (to the RTU) and characteristics of a point.

Every configurable point in the RTU shares a common set of point attributes. Individual point types have unique point attributes in addition to the common point attributes.

Point Properties

Point Properties are generally read only point database fields describing (to the SCADA Master, SCADAPack E Configurator and ISaGRAF application) a status or characteristic of a point.

11 RTU Data Processing

- ***Integrated RTU Data Processing & RTU Data Processing Facilities*** 64
- ***Profiler & Trend Sampler*** 66

11.1 Integrated RTU Data Processing & RTU Data Processing Facilities

Integrated RTU Data Processing

Integrated RTU data processing is managed by the Data Processor.

It is directed by configurations defined for each point, mostly through point attributes. The data processing facilities provided in the SCADAPack E RTU includes:

- Physical I/O Point Processing
- Derived Point Processing
- Configurable System Point Processing
- Data Manipulation Processes

The role of the Data Processor is central to the primary functionality of the SCADAPack E RTU. It interacts with other services to provide data processing and co-ordination of data distribution within the RTU. While, in general, RTU services read point properties and attributes directly from the Point Database, tasks changing (writing) point attributes and properties use the Data Processor to validate and co-ordinate the change.

For each potential change to point fields (attributes or properties), the Data processor considers the impact of the changed value, processing interlocks and dead-bands where necessary, and initiating or stopping timers, performing floating point math, etc.

RTU Data Processing Facilities

The following list summarizes the data processing facilities that are integrated with the SCADAPack E RTU:

- Physical Digital Input De-bounce (provided by I/O sub-system)
- Physical Digital Input Invert (provided by I/O sub-system)
- Software Counters with de-bounce & Invert (provided by I/O sub-system)
- Integer scaling range & Engineering scaling range
- Rate Of Rise, Rate Of Fall, No Change detection
- Over-range detection, Under-range detection
- Multiple Engineering Alarm Limits
- Into Alarm Time dead-band
- Out-of-Alarm Time dead-band
- Out-of-Alarm Value dead-band
- Alarm Inhibit, Trend Inhibit
- Point Quality
- Remote Control Interlock
- Output Pulse time
- Event generation on Significant Change Deviation

- Set Point properties to User binary points

Detailed information on RTU data processing facilities is presented in the *SCADAPack E Data Processing Technical Reference Manual*.

11.2 Profiler & Trend Sampler

Profiler

The Profiler allows the SCADAPack E RTU to manipulate values and attributes of binary, analog and counter data points based on time profiles. The Profiler provides time-based control of data points on a time-of-day and day-of-week basis. The time information is stored in files in the RTU File System that schedule changes to point attributes.

Point attribute or value changes controlled by the Profiler are synchronized to occur on the one minute boundary of the RTU real time clock. Profile operations are based on Local RTU time, and ARE affected by the RTU's Time Zone Modifier system point.

The Profiler can manipulate the following point attributes:

- Analog points: Current Value (integer or floating point), Alarm Limits 4L..4H
- Counter points: Current Value (integer), High Counter Limit
- Binary points: Current State

The user configuration interface for the Profiler is as follows:

- Database "Profile ID" field for each point used by the Profiler. This associates points with profiles by a number in the profile filename
- Profile files
- Restart the Profile task

For more information see *SCADAPack E Profiler Technical Reference* manual.

Trend Sampler

The Trend Sampler allows RTU data points to be periodically sampled, the values being recorded in files in the RTU File System. The storage of data using this mechanism provides a more sophisticated and efficient data storage mechanism than is provided by DNP3 Event storage.

The SCADAPack E RTU's *TREND SAMPLER* provides selective storage based on deviation control for each sampled point, a binary trigger point for selective control of sampling, and a file format with some data reduction facilities.

Multiple trend streams on the same RTU point are supported. Trend samples may optionally include data quality flags.

Each data sample may be stored in one of various formats including 16-bit, 32-bit, signed, unsigned, floating-point format, with or without quality flags.

The Sampler requires the following user configuration information:

- DNP point index and point type of Point to sample
- Sample Rate (Secs)
- Deviation change for recording Analog or Counter samples
- Binary trigger point for controlling sampling
- Trend Stream (Statistic) Type

Trend data recorded by the SCADAPack E RTU can retrieved by:

- a Master Station via the communications channel,
- SCADAPack E Configurator locally at the RTU, or remotely via the communications channel,
- by a user ISaGRAF application copying data to external storage media (e.g. SCADAPack ES and SCADAPack ER COMPACT Flash)

For more information see the *SCADAPack E Trend Sampler Technical Reference* manual.

12 Using the SCADAPack E RTU

The *SCADAPack E Operational Reference* manual describes operational aspects of using the SCADAPack E RTU.

- ***Parameter Changes, Engineering Mode, & RTU Configuration Revisions*** 69
- ***Time Conversion*** 70
- ***Maintenance Modes*** 72
- ***Local & Remote I/O Status*** 74
- ***Port Assignments*** 75

12.1 Parameter Changes, Engineering Mode, & RTU Configuration Revisions

SCADAPack E Parameter Changes

Other than RTU point database attribute changes, RTU parameter changes in general will not take effect immediately. The exception to this is the SCADAPack E DNP Network Routing table. Changes to entries in this table *do* take effect immediately.

Parameter changes relating to hardware configuration require RTU restart (e.g. power on, SCADAPack E Configurator **Restart Controller**, or DNP3 Cold Restart) to take effect.

DNP3 parameter changes require DNP3 driver initialization (e.g. SCADAPack E Configurator *Reinitialize DNP3* or DNP3 Warm Restart) or hardware reset to take effect (e.g. DNP3 Cold Restart, hardware reset, power-on)

Engineering Mode

Whenever a privileged SCADAPack E Configurator user sends a control or configuration information to the RTU, the RTU's ENGINEERING TIMER is started and the RTU's "ENGINEERING MODE" system binary point is activated. If set as an alarm point, this can report RTU re-configuration to the Master Station.

The SCADAPack E Configurator restarts the Engineering Timer value at 60 secs for each configuration or control sent to the RTU. When the Engineering Timer expires after 60 secs, the Engineering Mode alarm is de-activated.

RTU Configuration Revisions

The SCADAPack E RTU provides a revision number tracking facility for RTU configurations.

Re-loading an entire RTU configuration results in the "CONFIGURATION MAJOR REVISION NUMBER" system point being incremented.

Small configuration changes through Record Exchange from SCADAPack E Configurator results in the "CONFIGURATION MINOR REVISION NUMBER" system point being incremented.

For more information see *SCADAPack E Operational Reference* manual.

12.2 Time Conversion

The SCADAPack E RTU operates using Standard Time or UTC Time in the RTU Real Time Clock.

UTC time is recommended for SCADAPack E RTUs. The DNP User Group recommends UTC time for RTU operation.

If UTC Time is used, “Local Time Offset from UTC” is an offset number of hours away from UTC time (as set in float point system point **63201**).

Alternatively, Standard Time may be used in the RTU real time clock by setting the “Local Time Offset from UTC” system point to “0” and setting the real time clock to local (non-summer) time.

Consider the following factors when choosing which time format is appropriate for an individual system:

- is SCADA equipment for the system located in multiple time zones ?
- is time synchronization such as NTP or GPS used to align RTU real time clocks ?
- does the Master Station require data reported from RTUs in UTC time ?

If the answer to any of these questions is yes, it is highly recommended that UTC time be used in the SCADAPack E RTU.

If Summer time activities are required, it is not necessary to adjust the RTU Real Time Clock.

Rather, the “Time Zone Modifier” (Daylight Savings / Summer Time) system point (binary system point **50302**) can be activated that affects Local Time by 1 hour. This is normally the responsibility of the Master Station.

The following RTU facilities use Local (Summer time adjusted) or UTC / Standard (Summer time independent) times as indicated.

Table 12.1: Time Conversion Usage

RTU FACILITIES USING **UTC or STANDARD TIME** (Independent of Summer Time)		RTU FACILITIES USING **LOCAL TIME** (Adjusted for UTC offset and Summer Time)
RTU Real Time Clock		Profile Task
Trend sample time-stamps		ISaGRAF TIMEDATE Function Block
DNP3 event time-stamps		ISaGRAF TIME Function Block
ISaGRAF OS_TIME Function		ISaGRAF DAY_TIME Function

Times shown in RTU diagnostics		ISaGRAF LOC_TIME Function

12.3 Maintenance Modes

LED Button Modes (SCADAPack 300E)

SCADAPack 300E RTU controllers provide a LED button for operation and maintenance modes.

Under normal operating conditions, the function of the LED Button is determined by configuration.

- When the **Controller Modes / LED Power always On** mode is enabled, the LED button has not effect on operation when the RTU is running.
- When the **Controller Modes / LED Power always On** mode is disabled, the LED button controls the state of the RTU's status LED indicators. Press the LED button to turn LEDs on, press again to turn off.

LED Button Maintenance Modes

At startup, the LED Button can be used to activate various Maintenance Modes:

These include:

Maintenance Mode	Description
Service Boot	Stops the ISaGRAF user applications and overrides RTU ports with DNP3 communications at node address “0” This mode can be used to locally establish communications with the RTU if its node address is not known. This mode also sets the Port 4 to ‘Command Line’ mode at 9600bps for alternative identification of the RTU via an ASCII terminal.
Cold Boot	Initializes SCADAPack E configurations to factory defaults. Doesn't affect Flash file system
Factory Boot	Initializes SCADAPack E configurations to factory defaults and format the Flash file system

For more information on using the LED Button see the appropriate SCADAPack 300E hardware manuals.

Hex Switch Settings (SCADAPack ES and SCADAPack ER)

RTU HEX Switch settings are supported by the SCADAPack ES and SCADAPack ER RTUs only.

Switch setting **00 - EF** are used for Main RTU Remote I/O unit identification. For more information see *SCADAPack E Remote I/O Technical Reference* manual

Switch settings **F0 - FF** are used only for special RTU maintenance modes.

Changing the RTU switch settings ***to*** a value in the range 00 - F0 will cause a reset (equivalent to a Hardware reset).

Switching ***to*** the addresses F1 - FF will require the RTU to be separately reset (e.g. powered off & on) in order for the special operation to take affect.

Switch Settings (Hex)	Description
F0	Service Mode - Override RTU ports with DNP3 communications at node address "0" This mode can be used to locally establish communications with the RTU if its node address is not known. This mode also sets the Port 4 to 'Command Line' mode at 9600bps for alternative identification of the RTU via an ASCII terminal.
F1	Initialize ISaGRAF applications. Alternatively issue a command line "CLEAR ISaGRAF" or DNP3 File Exec "CLEAR ISaGRAF" command.
F8	SDRAM Memory Test. Refer to the *SCADAPack E Boot Monitor User Manual* for more details
F9	Boot Monitor Re-program mode. See **Boot Monitor Firmware Update** 26.
FB	Format Boot Mode. This mode forces the command line on the Port 4 at 9600 bps. The standard tasks are NOT started so that the controller file system can be formatted. For more information see *SCADAPack E Operational Reference* manual
FC	Cold Boot - Initializes SCADAPack E configurations to factory defaults. Doesn't affect Flash file system
FE	Calibrate SCADAPack E Hardware via ASCII terminal on Port 4
FF	Force Boot Monitor to operating system download mode, for using SCADAPack E Configurator to load new operating system firmware on the Port 4

For more information on special RTU HEX Switch maintenance settings see *SCADAPack E Operational Reference* manual.

12.4 Local & Remote I/O Status

Local I/O Status

The following RTU system points are provided to indicate operational status of local RTU I/O.

- Local I/O Module Failure
- Local Input Power Supply Low
- Local On-Board Battery Low
- Local Calibration Parameters Invalid
- Local Input Supply Voltage
- I/O Card Status (SCADAPack ER only)

Refer to the *SCADAPack E Operational Reference* manual for details of these status system points.

Remote I/O Status

The following RTU system points are provided for operational status indication on the Main RTU and for each Remote I/O Unit.

- Remote I/O Module Failure
- Remote Input Power Supply Low
- Remote On-Board Battery Low
- Remote Calibration Parameters Invalid

Refer to the *SCADAPack E Operational Reference* manual for details of these status system points.

12.5 Port Assignments

Serial Ports

Each RTU serial port can be configured for a variety of communications protocols, functions, speeds and data formats.

The configurable port functions are:

- DNP3 (multiple ports supported)
- IEC60870-5-101 (multiple ports supported) - requires RTU license
- IEC60870-5-103 Master (multiple ports supported) - requires RTU license
- Modbus Slave (multiple ports supported)
- Command Line & Diagnostics (single port supported)
- ISaGRAF (workbench debug software) / Command Shell when IEC 61131-3 Target 3 is enabled. Command line shell is not available with Target 5.
- ISaGRAF 2 (additional ISaGRAF workbench port)
- Modbus Slave (multiple ports supported)
- Command Line & Diagnostics (single port supported)
- ISaGRAF User - ASCII communications (multiple ports supported)
- PLC Device communcations via ISaGRAF PLC Device I/O boards (multiple ports supported)

  (E.g. MODBUS RTU Master protocol, DF1 Master protocol)
- Remote I/O (multiple ports supported – 57600 bps fixed format)
- PPP – TCP/IP (multiple ports supported)
- TCP Service (multiple ports supported – client or server mode)
- DNP Virtual Terminal (VT) Service (multiple ports supported)
- NTP GPS Receiver (NMEA-0183 standard)
- Conitel Slave – SCADAPack ER - P620 Processor only (multiple ports supported) - requires RTU license
- NONE (port disabled)

Ethernet Ports

Depending on the SCADAPack E RTU model, Ethernet ports can be enabled for the following facilities:

- TCP/IP
- SCADAPack ES Remote I/O (SCADAPack ES and SCADAPack ER only)

TCP/IP

TCP/IP communications is supported on SCADAPack E PPP serial interfaces and Ethernet interfaces.

The supported TCP/IP services (need to be enabled by configuration) are:

- DNP3 / TCP (enabled)

- DNP3 / UDP (enabled)
- ISaGRAF / TCP
- IEC60870-5-104 - requires RTU license
- Telnet Server
- FTP Server
- Modbus/TCP Client
- Modbus/TCP Server
- BOOTP Server
- NTP Network Time

The default port settings for the SCADAPack E RTUs are listed in the tables in the following section.

12.5.1 Default Port Settings

- The default Port Format for each serial port is:

  8-bit, No-parity, 1-stop-bit

- Serial communication ports support data rates from 300 to 115200 bps.

Table 12.4: Default Port Settings on SCADAPack 300E RTUs

PORT 0	PORT 1	PORT 2	PORT 3*	Ethernet 1*
DNP3	NONE	DNP3	ISaGRAF	TCP/IP Enabled
USB	RS485 2-wire	RS232 (RTS On)	RS232 (RTS On)	
	9600 bps	9600 bps	9600 bps	

*** Port 3 and Ethernet 1 are not available on SCADAPack 314E**

- SCADAPack 300E RS485 2-wire interfaces are supported on serial Ports 1 and 2

Table 12.2: Default Port Settings on SCADAPack ES and SCADAPack ER RTUs

PORT 0	PORT 1	PORT 2	PORT 3	PORT 4	Ethernet 1	Ethernet 2
ISaGRAF	DNP3	DNP3	DNP3	Cmdline	TCP/IP + Remote I/O	TCP/IP + Remote I/O
RS232 (RTS On)	RS232 (RTS On)	RS232 (RTS On)	RS232 (RTS On)	RS232 (RTS On)		
9600 bps	9600 bps	9600 bps	9600 bps	9600 bps		

- SCADAPack ES and SCADAPack ER RS485 2-wire and 4-wire interfaces are supported on serial Ports 2,3, and 5-8.

Table 12.3: Default Settings for additional Ports on SCADAPack ER - P620 RTUs

PORT 5	PORT 6	PORT 7	PORT 8	IRIG
DNP3	DNP3	DNP3	DNP3	Disabled
RS232 (RTS On)	RS232 (RTS On)	RS232 (RTS On)	RS232 (RTS On)	
9600 bps	9600 bps	9600 bps	9600 bps	

- SCADAPack ER - P620 ports 5-8 are isolated from all other ports..

13 TCP/IP Integration

The *SCADAPack E TCP/IP Reference* manual describes specific aspects of using the RTU on TCP/IP networks.

The SCADAPack E RTU supports TCP/IP networking and communications integration. The RTU conforms to the relevant IEEE and TCP/IP RFC standards, and may be used in a wide range of LAN and WAN topologies, including systems using Routers, Bridges, Terminal Servers, Hubs, Switches, etc.

The following TCP/IP networking facilities are available with the SCADAPack E RTU.

- PPP serial communications including extensive options negotiation including IP address, ACCM character map, MRU, loop-back detection (via magic number) and ACFC & PFC compression negotiation
- PPP communications integrated with Hayes Modem commands for GPRS communications (IP over GSM wireless networks) and 1xRTT communications (IP over CDMA wireless networks)
- LCP echo (PPP link status) via command line & ISaGRAF function block
- Ethernet TCP/IP communications including ARP
- ICMP support including PING server
- PING client via command line & ISaGRAF function block
- IP forwarding between TCP/IP interfaces (e.g. PPP to PPP, PPP to ETH, etc.)
- IP routing table, configurable via RTU configuration, command line and ISaGRAF
- BOOTP server capability for configuring network device addresses across an Ethernet network, configurable via RTU configuration or command line
- TCP/IP diagnostics on the RTU diagnostic stream, including selectable filtering
- UDP and TCP transport over IP
- DNP3 integration with TCP/IP
    - UDP and TCP support as per DNP User Group requirements for DNP3 over LAN/WAN TCP/IP networks
    - Routing DNP3 frames between DNP3 serial and/or TCP/IP interfaces
- ISaGRAF Workbench debugger using TCP (e.g. via PPP links, Ethernet, etc)
- MODBUS/TCP client providing connectivity for SCADAPack E RTUs with Ethernet PLC systems and I/O brick units. The SCADAPack E RTU conforms with the Open Modbus/TCP specification for Class 0 and Class 1 devices.
- MODBUS/TCP server providing multiple simultaneous communication services to the Open MODBUS/TCP specification requirements for Class 0 and Class 1 devices.
- Modbus RTU in TCP client providing connectivity with Modbus RTU in TCP server devices.
- Telnet server accesses the RTU command-line and diagnostic stream (multiple users supported simultaneously)
- FTP server accesses the RTU file system (multiple users supported simultaneously)
- TCP service ports permitting remote connection to RTU serial ports for terminal-server style multi-protocol applications. Both Client & Server TCP service ports are supported in various configurations including Host client to SCADAPack E TCP service port server, RTU TCP service port client to RTU TCP service port server & TCP service port client to remote TCP service port server.
- Security for denying and permitting RTU TCP/IP services
- NTP Network Time Protocol for synchronization of the RTU real time clock from time sources across a TCP/IP network (typically Ethernet). Includes correction for clock drift. Also integrated with GPS and IRIG-B time synchronisation

14 Diagnostics

A range of diagnostic information is provided by the SCADAPack E RTUs in order to facilitate trouble-shooting and understand RTU operation.

- ***Diagnostic Display Information*** 81
- ***Start-Up & Command Line Diagnostics*** 82
- ***SCADAPack E Error Codes*** 83
- ***RTU Status*** 87
- ***Communication Statistics*** 89

14.1 Diagnostic Display Information

The SCADAPack E RTU, through the Diagnostic Display session, may indicate exceptional RTU operating conditions.

This is available from a “CmdLine” command line port on the RTU using “DIAG” command.

Alternatively, access to the diagnostic display session is provided by a Command Line shell through an RTU “ISaGRAF” port when IEC 61131-3 Target 3 is enabled (shell is not available with Target 5), or via TELNET.

Where a direct serial connection or TELNET is not available, diagnostics can be remotely acquired by directing the diagnostics to an RTU file. This is achieved using the FILEDIAG command described in *SCADAPack E Operational Reference* manual. This diagnostics log file can then be retrieved using DNP3 file transfer for analysis.

RTU diagnostics are provided for each aspect of communications and exceptional RTU operating conditions. The following operational diagnostics are specifically supported:

- DNP3 diagnostics at each protocol layer including network routing
- TCP/IP diagnostics including DNP3 over IP, IP servers, TCP service ports, etc.
- PLC communication diagnostics including protocol packet displays, communication status and device status for serial and network PLC services
- RTU system diagnostics
- NTP server/client and Receiver diagnostics
- IEC60870-5-103 diagnostics
- IEC60870-5-101 / 104 diagnostics
- AGA12-2 diagnostics

RTU diagnostics may indicate operational information that assists in trouble shooting. To sort these diagnostics from normal operational messages, it may be advantageous to disable DNP, TCP/IP, PLC and SYSTEM diagnostics using DNPDIAG, TCPDIAG, PLCDIAG and SYSDIAG commands from the command-line.

Other RTU diagnostics use the following format to assist in identifying messages from various SCADAPack E tasks:

Task-name>>diagnostic text

14.2 Start-Up & Command Line Diagnostics

Start-Up Diagnostics

At start-up, the SCADAPack E RTU can display information about its start-up sequence and configuration.

If a “CmdLine” command line port is configured on the RTU, ASCII text is displayed through this port as the RTU starts up.

After completion of the RTU start-up, the SCADAPack E RTU usually terminates the diagnostic session and enters command mode.

The entry to command mode after start-up can be optionally disabled, leaving the RTU in the diagnostic display session. This is achieved using the SYSDIAG “OVERRIDE” command described in *SCADAPack E Operational Reference* manual and via SCADAPack E Configurator .

Command Line Diagnostics

RTU command line operations & diagnostic display can be accessed using an ASCII terminal via an RTU port configured as “Cmd Line”, or its “ISaGRAF” port.

Telnet can be used via TCP/IP links.

The RTU also supports a “Remote Command Line” whereby the command line interface can be accessed for remote SCADAPack E units over DNP3 links. This uses DNP3 standard Virtual Terminal capability. A “Remote Command Line (Virtual Terminal)” window is provided in SCADAPack E Configurator to access this functionality in the RTU.

At RTU start-up, configuration information and diagnostics are displayed on an ASCII terminal on the RTU’s “Cmd Line” port. The RTU then defaults to command line mode. *Diagnostic Display* mode can be connected by entering the *DIAG* command. To enter *Command* mode from *Diagnostic Display* press **<Escape**>. In SYSDIAG “OVERRIDE” mode, the RTU remains in Diagnostic Display mode after start-up rather than entering Command mode. To enter Command mode press **<Escape>**.

Command mode provides a wide range of commands for interrogating the operational status of an SCADAPack E RTU.

These are detailed in the *SCADAPack E Operational Reference* manual.

Command line operations and diagnostic display are also supported on the “ISaGRAF” workbench port. The RTU need not be configured with a “Cmd Line” port in this case. An ASCII terminal can be connected to the ISaGRAF workbench port, and after inputting **<Enter><Enter><Enter>**, the port enters Command mode. To return to ISaGRAF Workbench debugging mode, enter the command “BYE”.

The “**BYE**” command should be issued prior to disconnecting the ASCII terminal for correct ISaGRAF operation.

Command line operations and diagnostic display are also supported via TCP/IP interfaces using TELNET. In addition, command line operations are also supported via DNP3 “Virtual Terminal”. The RTU need not be configured with a “Cmd Line” or “ISaGRAF” port in these cases. Multiple TELNET sessions may be established with the SCADAPack E RTU on the same TCP/IP interface, or multiple sessions may be established on multiple TCP/IP interfaces, simultaneously.

14.3 SCADAPack E Status Codes

Status codes are reported by the SCADAPack E RTU from various RTU facilities. RTU status codes fall into the following major categories:

- DNP3 communication
- PLC Device communication
- System
- ISaGRAF user application
- TCP/IP

Refer to the *SCADAPack E Operational Reference Manual* for details of these system status codes.

- ***DNP3 Errors, PLC Communication Errors, & TCP/IP Errors*** 84
- ***System Error Point*** 85

14.3.1 DNP3 Errors, PLC Communication Errors, & TCP/IP Errors

DNP3 Communication Errors

DNP3 communication errors are reported by the RTU through the Diagnostic Display session as DNP3 driver diagnostic information. These error codes are also reported through the ISaGRAF Peer Communication function blocks in the output STATUS variable.

The DNP3 communication errors are NOT reported via the RTU System Error Point.

See *SCADAPack E DNP3 Technical Reference Manual* for a complete list of DNP3 Communication Error Codes.

PLC Device Communication Errors

Error codes reported from PLC Device drivers on the SCADAPack E RTU are through Analog System Points that represent an error code resulting from communication between an ISaGRAF PLC Device I/O Board and a PLC Device.

The PLC Device communication errors are NOT reported via the RTU System Error Point.

These error codes are detailed in the following manuals:

- *ISaGRAF Technical* manual
- *ISaGRAF 3 Modbus Communication Interfaces* manual
- *SCADAPack E Target 5 Technical* manual
- *SCADAPack E Target 5 Modbus Communication Interfaces* manual

TCP/IP Errors

TCP/IP communication and configuration errors are reported by the SCADAPack E RTU through the Diagnostic Display session as TCP/IP diagnostic information. These error codes are also reported through the ISaGRAF TCP/IP function blocks in the output STATUS variable.

The TCP/IP errors are reported via the System Error Point for TCP/IP configuration problems.

See the *SCADAPack E TCP/IP Technical Reference* manual for a complete list of TCP/IP Communication Error Codes.

14.3.2 System Error Point

The SCADAPack E RTUs provide a system error code through an RTU Analog System Point.

The recent error is retained as the value of the system error code. DNP3 event reporting may be configured for the system error code point to provide a time-stamped history of error codes.

RTU system errors are reported through the RTU System Error Point.

User defined error codes may be generated via ISaGRAF using RTUPARAM function block with the "SYS_ERR_CODE" parameter.

ISaGRAF user application errors are reported using the following RTU facilities:

- to the ISaGRAF Workbench Debugger if connected (locally or remotely)
- through the RTU System Error Point
- via the RTU Diagnostic Display session
- SCADAPack E Configurator Status Page in numeric and text format

Error Code	Name	Description
0	Normal Operation	Normal operation
1-99	ISaGRAF Target Errors	See the *ISaGRAF Technical* manual
100-999	User defined Errors	See the *SCADAPack E ISaGRAF Function Blocks Reference* manual -RTU_PARAM function block
1001-1009	ISaGRAF Application Load Errors	Error loading ISaGRAF application files or memory application for ISaGRAF Targets
1010-1019	Configuration Errors	Configuration File errors
1020-1029	Profile Errors	Profile configuration errors
1030-1039	Event & Trend Warnings & Errors	Event storage threshold warnings and errors
1040-1049	Data Processing Errors	Run time data processing error codes
1050-1059	Remote I/O Errors	Firmware mismatch error codes
1060-1099	IO Error (SCADAPack ER only)	SCADAPack ER I/O errors reported by main OS firmware
1100-1139	IO Error (SCADAPack ER only)	SCADAPack ER I/O errors reported by I/O Processor CPU firmware
2000-2999	TCP/IP Errors	TCP/IP configuration & run-time errors See the SCADAPack E *TCP/IP Technical Reference* manual

Error Code	Name	Description
3000-3099	Extended Configuration Errors	More Configuration File errors.

For “RTU System Error Point” details see the *SCADAPack E Operational Reference* manual.

14.4 RTU Status

The following system status points are provided by the SCADAPack E RTU to indicate status of various aspects of RTU operation.

Point Type	Description
System Binary Points	RTU Initialized
	RTC Time Synchronized
	RTC Time Invalid
	DNP3 Protocol Driver Running
	Engineering Mode
	Local I/O Module Failure
	Local Input Power Supply Low
	Local On-Board Battery Low
	Local Calibration Parameters Invalid
	Hex Switch Settings Changed (SCADAPack ES / SCADAPack ER only)
	Task Software Watchdog
	Time Zone Modifier
	Configuration Corrupt
	Trend Storage Priority
System Analog Points	SCADAPack E Smart RTU Type
	Firmware revision
	Switch Setting (SCADAPack ES / SCADAPack ER only)
	Processor Board PAL revision
	Processor Board Boot Monitor revision
	I/O Board Firmware revision
	Hardware revision ID
	Up Time (Secs)
	Up Time Delta (0-1000 ms)
	Reset/Error Reasons Mask
	Task Watchdogs Mask
	Engineering Timer
	System Error Code
	RTU Dynamic System Memory Free

Point Type	Description
	RTU Dynamic System Memory Size
	Configuration memory Size
	Configuration memory Slack
	File System Number of Files Used
	File System Bytes Used
	File System Bytes Free
	Configuration Major Revision
	Configuration Minor Revision
System Float Points	Local Time Offset from UTC
	Input Supply Voltage
	Low Volts Alarm Level

For the SCADAPack ER there is also a range of I/O card status points available in order to provide information on a per slot basis. These system points along with the system points listed in the above table, are described in detail in the *SCADAPack E Operational Reference* manual.

14.5 Communication Statistics

A variety of communication statistics are provided by the SCADAPack E RTU via System Analog points. These analog points may be read from the RTU using specific DNP3 point range read requests. Alternatively they may be read into an ISaGRAF user application via Input Boards, or Function Blocks.

Communication Statistic point values may be reset at any time by controlling the relevant System Point value and setting it to 0. This may be done by an ISaGRAF user application or via DNP3 point controls.

The Communication Statistics System Analog points cannot be directly added to the RTU point database and returned in DNP3 Class data polls. To map Communication Statistic points to a SCADA Master, the values may be imported in to an ISaGRAF user application, manipulated if required, then exported to a derived point which can be configured for access by a SCADA Master.

There are three types of communication statistic points provided by the SCADAPack E RTU.

- RTU (global) communication statistics
- Port communication statistics
- TCP/IP communication statistics

Communication Statistics System Analog points may be accessed as 16-bit or 32-bit Analog Input points.

For “Communication Statistics” details see the *SCADAPack E Operational Reference* manual.

15 RTU File System

The SCADAPack E RTU has an on-board file system is typically used to store or load the following information:

- configuration files (RTU configurations, NTP configurations, license files, security files, etc)
- configuration logs
- ISaGRAF application files
- Profile files
- Trend Sample files
- output data from specific tasks
- Logged diagnostics

The main file system (Drive C:) is stored in FLASH memory with directory support.

The file system supports a maximum filename length (including path) of 255 characters. Spaces in the filename (and or path) are not supported.

The file system on SCADAPack ES and SCADAPack ER RTUs also allows for COMPACT FLASH drives.

The use of COMPACT FLASH drives is application specific. ISaGRAF function blocks are provided for user access to the external drive.

The mounted drives and directories on the SCADAPack E RTU are as follows:

- C: drive. **Non-volatile drive**. Resides in FLASH memory
- **C:\Sampler** directory. Used for Trend Sampler file storage
- D: drive (RAM disk). **Volatile drive**. Resides in RAM. Used by Trend Sampler and File Diagnostics for performance reasons
- E: drive. COMPACT FLASH Slot (SCADAPack ES and SCADAPack ER RTUs only)
- F: drive. **Non-volatile drive**. Resides in FLASH memory (SCADAPack ES and SCADAPack ER RTUs only)

File system sizes are as follows:

Drive	Type	Size (SCADAPack 300E)
C:	**Flash**	**7 MB**
D:	**RAM Drive**	**128 KB**

Drive	Type	Size (SCADAPack ES and

		SCADAPack ER)
C:	**Flash**	**12 MB**
D:	**RAM Drive**	**2 MB**
E:	**COMPACT FLASH**	**up to 2 GB**
F:	**Flash**	**16 MB**

16 Data Concentrator

The SCADAPack E RTU can be configured as a Data Concentrator where the RTU manages the communications and polling regimes to other remote devices. This approach abstracts the SCADA master from the remote devices, and is often used to allow a SCADA master (or multiple SCADA masters) to regularly communicate with only the data concentrator. The data concentrator acts an intermediate master to the remote outstations.

The data concentrator configuration in the SCADAPack E RTU involves two configuration tables.

- The *Remote Devices* table details the necessary information for the data concentrator to communicate with the remote device, i.e.
  - communications protocol
  - device address
  - polling schedule
- The *Remote Points* table details the mapping of remote outstation points to points on the data concentrator.

The protocols currently supported for outstation communications are:

- DNP3 Master
- IEC60870-5-103 Master
- Remote I/O

Where supported by the protocol (for example DNP3 Master), time-stamps and point quality data received from IEDs or remote outstations are preserved within the data concentrator. A Master Station polling the data concentrator receives the original timestamps, quality flags and data (as generated by the remote outstation). In addition, the data concentrator modifies point quality flags on data mapped from remote outstations to reflect data concentrator information, such as point Offline, Comms Lost, etc.

Refer to the *SCADAPack E Data Concentrator Technical Reference* for more information regarding the Data Concentrator.

17 DNP3 Multi-Master

The SCADAPack E RTU supports DNP3 Multi-Master operations when acting as a DNP3 slave. The RTU fully supports communications with multiple DNP3 masters. Up to three DNP3 Masters may be configured.

The DNP3 addresses of the multiple DNP3 masters need to be different for correct operation.

The DNP3 address of the SCADAPack E RTU (as a DNP3 slave) may be the same for each of the DNP3 masters, or alternatively may be configured to have a different DNP3 slave address for each DNP3 master. Communications to the multiple DNP3 masters may be on single or multiple communications ports

The RTU supports separate event lists for each DNP3 Master, and also allows configurations on a per point basis, allowing points to be selectively returned in poll responses for a given DNP3 Master E.g a given point may be configured as Class 1 for DNP3 Master 1, and Class 0 (static) for DNP Master 2, not configured for DNP Master 3.

The DNP3 Multi-Master functionality requires licencing. Refer to the *SCADAPack E DNP3 Technical Reference* for more information regarding DNP3 Multi-Master support.

18 Conitel Slave Communications

The SCADAPack ER - P620 processor supports Conitel Slave and Baker Slave communications on up to 4 serial ports, concurrently.

The RTU can be configured to respond to multiple Station / Group addresses. The RTU's support for Conitel includes RTU current value and event data scanning, MCD scanning, trip/close, execute, raise/ lower and setpoint controls, time synchronisation and status reporting. The RTU's support for Baker includes RTU current value scanning, MCD scanning, trip/close, execute and reset controls.

User configuration permits RTU digital, analog and counter objects to be mapped in to the Conitel frame format, with a high degree of flexibility. The user interface also visually guides the user as to valid mappping combinations within Conitel frames. Other configurations include adjustable control / execute timeout and raise / lower timebases.

The P620 serial interfaces support direct Conitel v.28 communications, or with external modem(s) can support Conitel v.23 or Conitel Bell 202 formats. Each serial interface presents the same Conitel data, so multiple interfaces can be used with redundant communication paths. Similarly, individual interfaces can be polled for different Station / Group data to increase throughput.

The RTU can combine any other functionality with Conitel Slave operation. E.g. as a data concentrator for multiple protocols presenting data back to Contiel.

The Conitel functionality requires licencing. Refer to the *SCADAPack E Conitel User Reference* for more information.

19 IRIG-B Time Synchronisation

The SCADAPack ER - P620 processor module supports an IRIG-B time synchronization interface. This permits external time synchronization along with other equipment that may be using the IRIG-B.

Both modulated and unmodulated IRIG-B formats are supported.

The following is a list of supported IRIG-B formats:

- IRIG-B000 (un-modulated, IEEE control functions, straight binary seconds)
- IRIG-B003 (un-modulated, straight binary seconds)
- IRIG-B120 (1KHz modulated, IEEE control functions, straight binary seconds)
- IRIG-B122 (1KHz modulated)
- IRIG-B123 (1KHz modulated, straight binary seconds)
- Supports IRIG-B IEEE-1344 extensions

The following formats (although less common) are also supported:

- IRIG-B001 (un-modulated, IEEE control functions)
- IRIG-B002 (un-modulated)
- IRIG-B121 (1KHz modulated, IEEE control functions)

The RTU can combine other functionality with IRIG-B time synchronization operation:

- RTU clock synchronisation used for local time-based control, DNP3 event time-stamping, IEC60870-5-101 and -104 event time-stamping, profiler parameter control & trend sampler logging, etc.
- The NTP time synchronization server in the RTU can serve time to IEDs and other devices based on the time it has synchronized from IRIG-B.
- When being used as a Master to other device protocols (e.g. DNP3, IEC60870-5-103, etc), the RTU can serve time based on the time it has synchronized from IRIG-B.