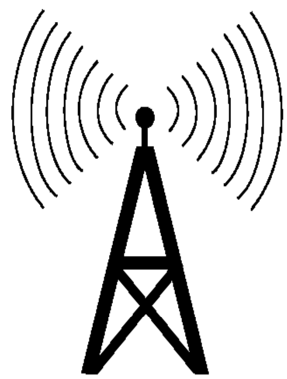
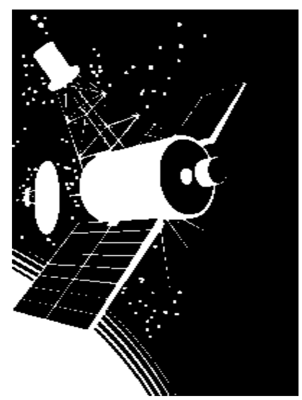
Bristol® BSAP

Bristol Standard Asynchronous/Synchronous Protocol

Features

- Compatible with SCADA and LAN networks
- ISO 1745/2111/2629 compliant
- Tree topology network
- Up to 6 network levels
- Up to 127 nodes from each node at a level
- Polled network
- Local and global addressing
- Peer-to-peer and RDB modes
- Report by exception
- Alarm handling
- Network time synchronization
- 16 bit CRC-CCITT error checking
- Communication statistics and diagnostics



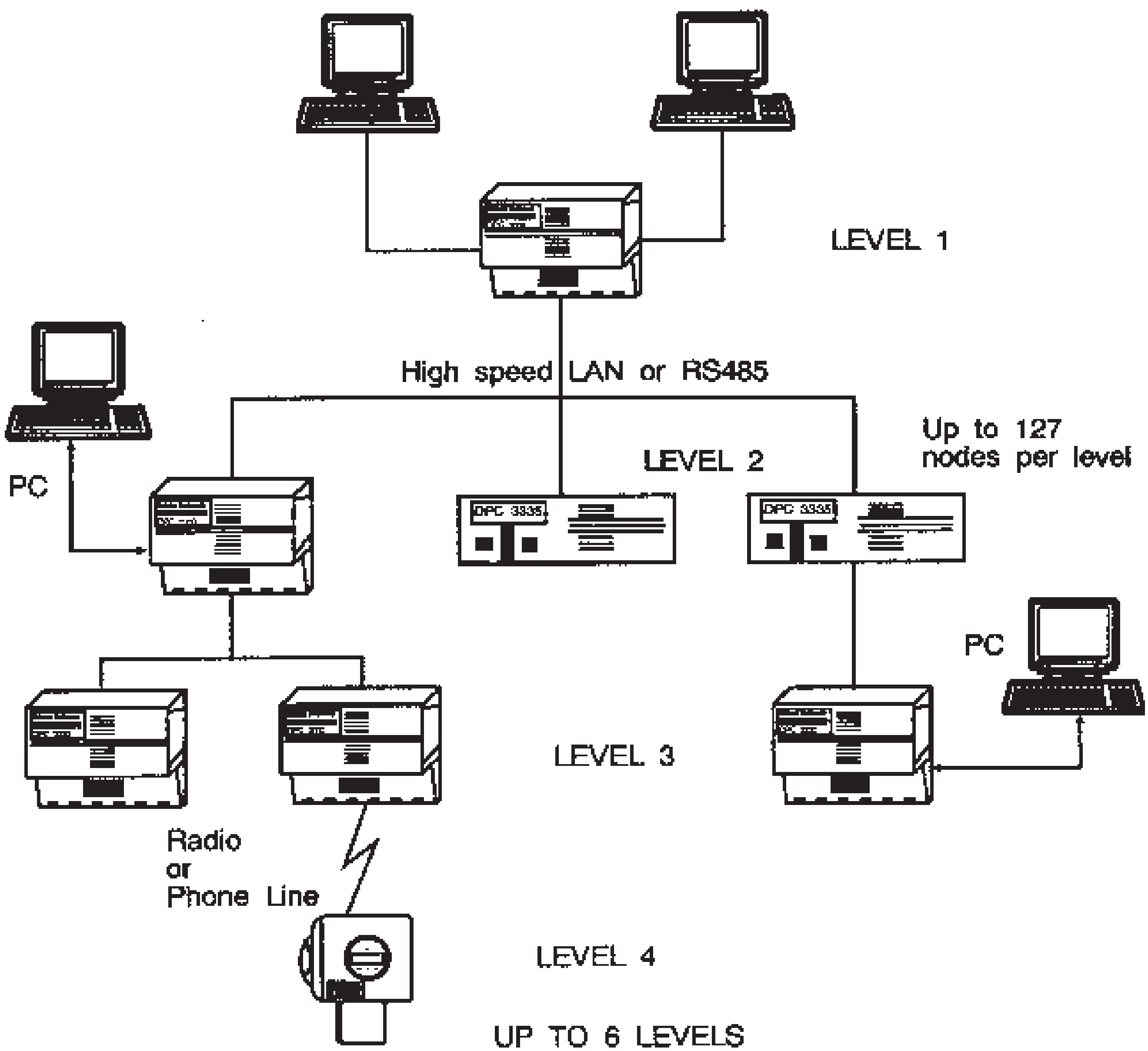


Bristol® Standard Asynchronous/Synchronous Protocol (BSAP), from Emerson Process Management, provides a complete communication framework for all Emerson's Bristol Network 3000 and ControlWave® products. It is a poll oriented communication system for horizontal LAN as well as vertical, multi-layer networks. Consequently, BSAP is equally well suited to both synchronous high speed local networks and asynchronous low speed wide area networks. BSAP is able to offer extremely high message security, required for phone line and radio networks, through the use of 16 bit CRC-CCITT error checking, handshaking, and extensive communication statistics reporting. The polling scheme employed by BSAP ensures that each node in the network has an equal opportunity to be polled and to respond. In addition, no node can dominate the network communication. BSAP supports both local and global addressing to all Network 3000 or ControlWavenodes in a network.

Network Topology

At the top of the network is the network master or host, typically a personal computer or mini computer performing graphical user interface functions. The network master normally connects to one (or sometimes more) Bristol process controllers commonly referred to as a data concentrator or communications front end. It in turn becomes a master node to up to 127 slave nodes. Each of those can then be a master to another level of slave nodes.

NETWORK EXAMPLE



This hierarchy can extend up to six levels deep. Each intermediate node has both master and slave capability through separate communication ports. This architecture lends itself very well to the typical geographical distribution of controllers in most SCADA system applications. It also allows multiple asynchronous communications to occur throughout the network since each network branch can communicate simultaneously.

Local and Global Addressing

The computer at the top of the network has the ability to communicate locally to its attached node or through it to any other node in the network. In addition, a computer attached to a lower level node, through a Pseudo-slave port, can have access to any data, except alarms, in any other node in the network. This computer will have access to alarms from its attached node and any nodes below it. Each Bristol process controller can actually support multiple personal computers.

In some systems it is convenient to have all data from all nodes collected by the top level node, commonly referred to as a data concentrator. The host computer will then communicate locally to that node only, since that is where all network data resides. Other systems may be configured to communicate globally through the data concentrator directly to the slave nodes. This communication mode is called Remote Data Base access (RDB), described later. Many systems will be configured to utilize both techniques, thus maximizing communication efficiency as well as ease of implementation.

Since BASP provides multi-message capability which is essentially transparent to the user, it is possible to connect a computer to any node in the network and communicate with the attached node or any other node in the network. This capability includes data collection, command changes, and reconfiguration and downloading of ACCOL and ControlWave control strategies. In fact, all of these communications can be occurring simultaneously, without interference, within the network.

Peer to Peer Communication

Peer to peer communication is a mechanism for transferring data blocks, such as signal lists and data arrays, between any two adjacent nodes in a network. Peer to peer uses Master/Slave and Client/Server software modules which should not be confused with BSAP master/slave communication. A BSAP slave may have a Master module and a BSAP master may have a Slave module. Master modules execute periodically at the rate of the program task in which they are included. Once a Master module executes the message request is passed off to BSAP for communication. Slave modules execute asynchronously with respect to tasks. When a command is received from a Master module, it is executed immediately.

Remote Database Access

Remote Data Base (RDB) communication is used for reading and writing of individual variables. Individual variables may be requested by name or by physical address within the node. RDB can also be used to read or write data arrays and data array elements. RDB requests for data and commands are initiated by the host computer. There are no function blocks required to pass these messages throughout the network. In many cases network communication is structured to use peer to peer for data collection and RDB for commands.

RDB is implemented such that the host computer will read a variable by name the first time that variable is requested. The response to the request will include the memory address in the node which contains the value of the variable. All further communications to the node requesting that variable will be by memory address rather than variable name. Reading by address requires less communication overhead than reading by variable name, thus reducing communication time.

Report By Exception

Report By Exception (RBE) provides an effective technique to maximize communication efficiency. Since RBE reduces network communication traffic it is particularly useful in low speed SCADA systems communicating over modem and radio networks. When RBE is enabled, a node will respond to a poll by transmitting only the values that have changed since the last poll and any alarms. RBE communication is selectable on an individual variable basis.

It is possible and often advantageous to mix communication modes within the same system and even in the same node. For example, historical data may be passed up the network to the data concentrator using peer to peer, commands from the host computer will be sent down the network to the destination node by RDB, and display data may be gathered on an RBE basis.

Alarm Handling

ACCOL and ControlWave alarm signals produce buffered, time stamped alarm messages which are automatically transferred up the network to the host computer. When a node is polled by its master it will, if requested, respond with an alarm message, with time/date stamp, that have been posted since the last poll. Alarm reports have a higher communication priority than all other messages cued to go up the network. Each node contains space to buffer alarm messages from nodes below it. If the buffer becomes full due to a communication failure at a higher level the node will not permit additional alarm message transfer from its slave nodes. The slave nodes will then begin buffering alarm messages. This throttling effect is used to prevent a node from becoming overwhelmed with alarm messages at any one time.

Individual alarms may be acknowledged by an operator at the host computer. This activity will send the acknowledged status down the network to the node initiating the alarm. BSAP also supports alarm report initialization. This feature, initiated by the host computer, will instruct all nodes in the network to report all current alarms that are unacknowledged.

Time Synchronization

The Time Syncronization/Node Routing Table (TS/NRT) combined message enables each node in the network to know the topology of the network including the nodes unique global address and current time and date. The TS/NRT message emanates from the host computer to the top level node which in turn broadcasts it to its slave nodes which send it to their slave nodes. A network may have only one master capable of issuing a TS/NRT ensuring the entire network is in sync.

Polling Philosophy

Each node in the network, except the lowest level nodes, is both a master to the nodes below it and a slave to the master node above it. A master node sends data request messages to the slave nodes then periodically polls its slave nodes for alarms and response data messages. The polling philosophy used maintains four types of polls to maximize throughput by minimizing extraneous communication. The four poll types are:

1. Main poll
2. Reactivation poll
3. Preferred poll
4. Dead node poll

The main poll loop interrogates each slave at the start of each poll period to determine if it is alive and if it has any response messages. A live slave which responds with a data message becomes a candidate for a preferred poll. If the slave responds but has no messages it will be ignored until the next main polling cycle. If a slave node fails to respond to three consecutive polls it is assumed dead and will be subject to reactivation polling.

The reactivation poll is attempted only once per polling cycle to determine if a known dead slave has come alive. One dead slave is polled each polling cycle on a rotating basis to ensure that every dead slave node gets an equal chance to respond. If a dead node responds its status is changed to live and becomes a member of the main poll loop.

The preferred poll loop interrogates, on a round robin basis, all of the slaves that responded to the main poll or reactivation poll with data messages. Responding slave nodes will continue to be polled in sequential address order until the end of the poll period or until there are no more response messages.

If there is time left after the preferred poll, the dead poll loop is used to give any remaining dead nodes an opportunity to advise the master that they are alive.

Poll Periods

Each communication line within a network has a user defined poll period configurable from .1 sec. The poll period is the minimum time between each main polling cycle of the slave nodes from the master node. It is a function of the number of slave nodes, baud rate, physical link (i.e. leased line, dial line, radio, RS 485, coax, or fiber), message type, and the number of analog and discrete values to be transmitted. The following table shows the relative rates assuming a master communicating 20 analog signals and 40 discrete values from each of ten slave nodes. The total time is the time required to communicate all values from all 10 slaves and includes 25% spare time for alarms.

Baud Rate	Message	Recommended Poll period	Required # of polls	Total Time
1200 baud leased line	RDB	24.5 sec	2	49 sec
1200 baud leased line	peer to peer	18.8 sec	1	18.8 sec
1200 baud radio	RDB	39.8 sec	2	59.6 sec
1200 baud radio	peer to peer	34.1 sec	1	34.1 sec
9600 baud	RDB	3.1 sec	2	6.2 sec
9600 baud	peer to peer	2.4 sec	1	2.4 sec
1 Mbaud	RDB	.2 sec	2	.4 sec
1 Mbaud	peer to peer	.2 sec	1	.2 sec

Message Security

BSAP employes 16 bit CRC-CCITT error checking to ensure message security. This 16 bit CRC technique catches all single and double errors, all errors with an odd number of bits, all burst errors of 16 or less, 99.997% of 17-bit error bursts, and 99.998% of 18-bit and longer bursts. These statistics are based upon pure bit data. Since BSAP is a message structure with handshaking and additional diagnostics, the overall security is even greater than stated.

All Bristol RTUs retain on-line statistics reflecting the integrity of all communication transactions. An independent set of statistics is maintained for each communication line (serial port) at each node.

The embedded handshaking of message communication in BSAP provides an additional level of security be ensuring that messages are not assumed to have arrived at their destination. All messages initiated by a node are acknowledged by the receiving node. If an acknowledgment is not received the message is assumed not to have arrived. Also, a unique serial number is assigned to all messages to ensure that a response is matched to a specific request.

Within a network it is essential that certain communications take precedent over others. BSAP prioritizes communication messages such that commands being sent down the network, ie. to change set points or turn outputs on or off, have the highest priority and interrupt the normal polling cycle. Alarms have the highest priority of all messages traversing up the network but do not interrupt the normal polling cycle.

Specifications

- SO 1745/2111/2629
  - 1745 - asynchronous character oriented
  - 2111 - transparent messages
  - 2629 - conversational mode
- Protocol layering
  - Physical level
  - Link level
  - Network level
  - Transport end-to-end
- Message length
  - Variable up to 253 bytes
- Data lengths
  - Analog - 4 bytes (floating point)
  - Logical - 1 byte
  - Packed logical - 8 values/byte
  - Alarm time stamp - 5 bytes
  - Alarm data - 6 to 10 bytes
- Addressing
  - Local and global
- Network levels supported
  - 6 levels
- Nodes per level

  Up to 127 nodes from each existing node at a level. In a property configured network, one level could contain several thousand nodes.
- Communication modes
  - peer to peer
  - Remote Data Base access (RDB)
  - Report By Exception (RBE)
- Alarm handling
  - Automatic
- Message security
  - 16 bit CRC-CCITT
- Supported serial communication rates
  - Asynchronous - 300 baud to 115 K baud
- Line media supported
  - RS 332, RS 485 multidrop
  - Leased phone line
  - Dial up phone line
  - Satellite
  - Ethernet
  - Cellular

Emerson Process Management
Remote Automation Solutions

Watertown, CT 06795 USA — T 1 (860) 945-2200
Mississauga, ON 06795 Canada — T 1 (905) 362-0880
Worcester WR3 8YB UK — T 44 (1) 905-856950

Website: www.EmersonProcess.com/Remote

EMERSON
Process Management