



Real-time weather data in 2000

STORM Watch data collection and dissemination

The STORM Watch data collection base station is a highly graphical, Microsoft Windows application that collects, stores, analyzes and displays real-time hydrometeorological information. A STORM Watch data collection base station receives ALERT-formatted data from one or more serial ports on the local PC. With additional, optional modules, the base station application can also integrate data collected from other sources, support LAN clients, upload data to an FTP server for rapid dissemination to inter- or intra-networked clients, automatically fail over from being a network client to collecting data locally, and support hydrologic forecast tools.

Hosts and clients

STORM Watch is now widely deployed as an enterprise-level application, allowing users to have full STORM Watch functionality from locations other than the data collection base station. Data hosting can be accomplished in one of two ways: Client applications can attach directly to a STORM Watch host database, or clients can be supported via an FTP server site. These two solutions are priced and sold separately, with the FTP server approach being the method of choice for robust, enterprise-level data dissemination.

A STORM Watch host is a base station that, in addition to collecting data, makes its open, relational database available to networked clients. The clients periodically retrieve updated configuration and sensor data. A STORM Watch client collects its data from a STORM Watch host rather than from an ALERT port or other data sources. It stores and displays data in its own open database the same way as the host. Its initial configuration, site locations and sensor definitions are set by information from the host. The client's user displays are supported by the local database. The data updating process is automatic and as frequent as required.

Host method one: Local area network (LAN) host and clients

LAN clients attach directly to the host's database and transfer information to theirs over the network. After its initial connection, a client connects to the host just long enough to bring over the incremental data since its previous connection. LAN clients can communicate with the host to acknowledge or clear alarms. A dial-up networked client can either stay connected to the LAN or host between updates, or it can reconnect for each update.

The LAN implementation is simple and can serve a few clients well, particularly if they are on a fast network connection. It does not scale well to support large

numbers of clients. The network database access is not very efficient with respect to use of bandwidth, and dial-up clients could find the connection time onerous. If heavy client use correlates in time with an extreme weather situation, the host PC could become the bottleneck for clients' access to mission critical information. Finally, this approach can generate network security issues for any client users outside the primary agency, with firewalls making implementation potentially complicated.

Host method two: FTP uploader and FTP clients

These clients use internet-standard file transfer protocol (FTP) to transfer data, rather than a direct network database connection to the host. The FTP clients attach to an FTP server site, usually configured on a separate machine from the host PC. A program called the FTP Uploader runs on the host machine. It creates a new set of data files every minute and moves them to the FTP site where the clients pick them up.

In a network context, the FTP server can be outside the host agency's firewall, thus serving clients at remote sites without exposing the agency network. It can also be used inside the firewall to serve an enterprise's intranet clients. Dial-up clients can be supported in both cases, using either an outside internet service provider or the agency's own sanctioned intranet dial-up. Only authorized FTP clients using usernames and passwords have access to the restricted site, further reducing security concerns.

The FTP implementation is standardized and fits well with the architecture of most agencies' networks today. It also makes efficient use of the network bandwidth, and it offloads all client activity from the host onto a logical server site, allowing the host PC to continue its data collection and dissemination operations without any outside interference. It will scale well to support even very large numbers of clients at any remote location.

Basic and independent clients

Both LAN and FTP clients come in two flavors: Basic and independent. A basic client can define its own base maps and rain displays, but all sensor configurations and alarm settings are determined at the host. A basic LAN client allows alarm acknowledgements on the client to be transferred back to the host at the next connection. A basic FTP client cannot acknowledge alarms on the host, but it can define and initiate its own notification actions based on the host alarms, including automated paging and running outside programs.

Whether LAN- or FTP-based, a STORM Watch independent client can define its own alarms and notification procedures. This application is highly useful to STORM Watch users with missions that differ from that of the primary data collection host. For example, many agencies host their data collection PCs in an emergency services environment but support users in engineering, water quality, natural resources, land use and planning that require the same data for very different uses. Whereas the emergency manager would want to have alarms set on high water thresholds for flood detection, the wildlife resource or water quality division may use

low water thresholds to establish low flow boundaries. Independent clients enable users to define their STORM Watch tool set so it will best serve their unique needs.

Central data definition, collection and integrity

A fundamental principle behind choosing ALERT is that every mission critical user should be able to hear their real-time data transmissions directly. This advantage comes with a challenge: Another characteristic of ALERT systems is that the data collection software must contain knowledge about the field sensors from which it receives data. This sensor definition and calibration information is used to translate the incoming data transmissions into meaningful engineering units. If these definitions are not correctly matched to the field units, the incoming data will not be interpreted correctly.

In most ALERT implementations, having centralized data collection and host/client dissemination is the key to maintaining data integrity across all users. The person or entity in charge of sensor maintenance is tasked with maintaining the calibration information in the host database. Any changes they make are automatically propagated out to the client users as soon as they next receive host data. An enterprise system operated in this fashion will maintain mirrored databases and enable all its users to have the most accurate data.

Robust systems: Failover for mission critical users

Should a mission-critical client lose contact with its host, whether due to host failure or network failure, they may choose to have the option of running their own data collection base station using the same local database their client application was using. If they are ordinarily running a client, their sensor definitions will be up to date with the host's last contact.

This process can be automated using the Failover application. Failover is an outside program running on a STORM Watch client database. The user sets a timeout period, which is the maximum time the client should expect to receive no new data. If this time is exceeded, the failover module will terminate the client application and start up a standalone base station. With antenna, receiver, ALERT decoder and port definitions in place, the base station will immediately start collecting data directly from the field units, assuring almost no interruption in data flow.

Please contact DIAD to find out more about our products and how they can be used. We encourage input from the community of data consumers, as these are the experts that help us determine our future product direction.

Contact information:

303-774-2033 voice

303-774-2037 fax

www.diad.com, diadinfo@diad.com