SCADA-Aware Mobile far exceeds the capabilities of SMS, e-mail, and pagers, and delivers alarms to the mobile device in the most reliable way. It uses both pull and push technologies to ensure that no alarm is lost or arrives late.

The alarm comes with data, its acknowledgment is easy and visible across a designated group, and it escalates at defined intervals until someone acknowledges. All interactions with alarms are on a single mobile device. No need to use a browser. The screens are easy to understand and navigate through.

SCADA-Aware Mobile runs on iPhone, Android, and Blackberry. The mobile devices work as both client and server. The application can be implemented non-intrusively with existing SCADA systems. The application requires very little bandwidth. The verification heartbeat between the server and the client is less than 250 bytes.

Features discussed here:

- User Login
- Connectivity
- Settings and Notifications
- Alarms on Mobile Device
- Database Editor
- Secure Client Connectivity
- Reliability of Access
User Login

Start the application on your mobile device using the SCADA-Aware Mobile icon. The initial screen differs, depending on the phone being used (Android, iPhone, or Blackberry). In general they will have:

• The application name
• The current server name
• User ID field
• Login button

Always Connected

Once logged-in, you can stay so indefinitely. There is no automatic session timeout. Even if you close the application on your device or your device is turned off, you’ll be considered logged in. When the application is closed, the SCADA-Aware Mobile icon will be displayed on the home screen of your device when there is an alarm (picture on the right). The number next to the notification icon shows the current number of unacknowledged alarms.

If your device is not available to receive alarms when it should be available, an automated alarm is sent out to designated personnel. These alarms get processed just like alarms associated with a tag. SCADA-Aware Mobile raises alarms about itself when

• The server fails to talk to the SCADA system
• The server fails to talk to the Historian
• A logged in user’s mobile device fails to talk to the server

Settings and Notifications Options

The options may vary depending on the phone being used (Android, iPhone, or Blackberry). In general, the settings screen manages the event notifications, displays the current configuration (logged in user, login time, log file name, and other info), and manages the server descriptions when not logged in. The device notifications screen chooses the platform actions for an event (alarm acknowledgment, alarm escalation, alarm arrival, failure to communicate with the server). Available actions are to play a sound, vibrate the device, and/or turn on the LED.
Alarms on Mobile Device

On SCADA-Aware Mobile, specific events can make a sound, vibrate, and/or flash the LED. These events are: new alarm, alarm acknowledgement, alarm escalation, and “no server contact”. The SCADA-Aware Mobile icon on the home screen will take the user to the alarm list screen.

The alarm list screen shows tags in alarm state and their status. Each row shows the tag name, either a check mark or the escalation level starting at zero, and either who acknowledged the alarm or when escalation is scheduled. Each row is color coded to show the escalation level. Level 0 is shown in cyan, Level 1 in yellow, Level 2 in orange, and Level 3 in red. The alarms are sorted by either of two sequences: who acknowledged it (my acknowledgments, unacknowledged, others’ acknowledgments); or oldest to newest.

The screen shows the time of the most recent update or update attempt. A large difference in the times means the device and server are not talking to each other. If the device and server fail for a configurable time, the time’s font changes to bold italic and the device notifies the user.

Selecting a row provides detailed info on the alarm, related data, and historical data. The detail screen shows, for an unacknowledged alarm, the tag name, the time the tag entered an alarm state, the escalation level, the current alarm state, when the next escalation is scheduled, and the current value of the tag. For an acknowledged alarm, the detailed screen shows the tag name, the time the tag entered an alarm state, the escalation level “None”, the current alarm state, when the alarm was acknowledged, who acknowledged the alarm, the current value of the tag. The related data covers up to ten related tags and their values. On Blackberry, the detailed and related info are on the same screen; in iPhone and Android they are in different screens.

If history values are available, a graph of the most recent values of the tag is shown, along with the the time the history values were retrieved. The X axis shows the time as minutes within an hour of each graphed value, oldest to newest. The Y axis shows the graph scale and the unit of measure.

The alarms and the data can be also be seen using a desktop application.
Database Editor

The Database Editor provides the ability to input alarm descriptions, user descriptions, and specification of which user gets which alarm and at which escalation level. Tag groups and user groups can be created to facilitate this. The Editor also provides the ability to configure the behavior of the event server with timeouts, network addresses, and specification of how it receives the alarm events from the underlying system.
Secure Client Connectivity Options

VPN client on smartphone device to existing corporate VPN: Utilizes existing corporate infrastructure. No additional ports required to be open in the corporate firewall. May have to adjust client disconnect timeouts if set too low.

WiFi enabled for internal use: Utilizes existing corporate infrastructure. No additional ports required to be open in the corporate firewall since access is internal to the facility. Usage is restricted to coverage area of WiFi hotspots.

Open port in corporate firewall: Carrier usage requires the connection be created by the smartphone client to a well-known host/port. Customer must open one port in the firewall for incoming connectivity. Typically the Secure Proxy Server listens for connections to the open port.

Deploy secure proxy server in the cloud: Carrier usage requires all connections be created by the smartphone client to a well-known host/port. No changes to corporate firewall for incoming connections. Depends on 3rd party availability for alarm delivery.

Authentication and encryption: SCADA-Aware Mobile users can be authenticated against the corporate Open LDAP servers or Microsoft’s Active Directory servers. Other authentication methods can be incorporated. Encrypted password is stored in the SCADA-Aware Mobile database. Besides authentication, another security measure is to encrypt the data transmitted. SCADA-Aware Mobile supports SSL between all devices, and can be extended to handle additional encryption protocols.

Reliability of Access

SCADA-Aware Mobile interacts with the operating system on the smartphone to detect network changes and responds accordingly. Users may experience a dropped connection, but the application will recover automatically.

SCADA-Aware Mobile can use the carrier’s TCP/IP network or the Wi-Fi interface on smartphones. The application can be tuned for unreliable networks. 3G or higher speeds are not required depending on the amount of data shared with the device. The application can handle disruptive network as it moves from no coverage, minimal connectivity, to full 3G or 4G.

In some locations, the carrier network bounces between EDGE, 2G, 3G, and 4G connectivity. As the mobile device switches between the different cellular networks, the TCP/IP connection is dropped and reestablished. The application framework needs to handle the unreliable environment and maintain or reinitiate connectivity to the network and application. SCADA-Aware Mobile handles this changing environment.