Hi Tech Low Cost RealiteQ™ New Generation of SCADA & Telemetry Solution

RealiteQ Cloud based SCADA & Telemetry solution –

Security white paper

Reali Technologies is an Israeli leader in Web SCADA and telemetry technology. Reali Technologies established as an Israeli breakthrough technology startup in 2007 that developed a **new generation of SCADA & Telemetry Solution named RealiteQ.**

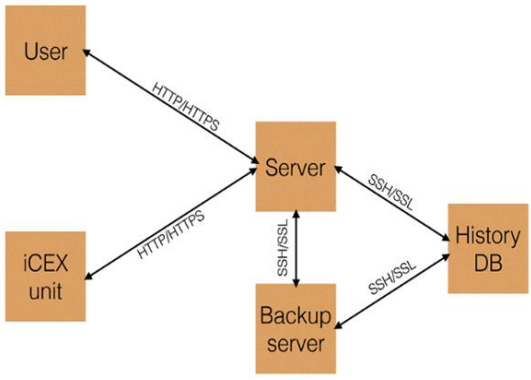
Today, Reali Technologies has an advanced proven **End-to-End web base SCADA & telemetry system** for a wide range of water and wastewater applications, with Thousands of remote sites that operate in five continents.

Reali Technologies Ltd. invests and still dose, many efforts and resources in providing the RealiteQ highly secured Cloud based SCADA & Telemetry solution, using several security levels:

- Reliable Service – Multiple hosting. Our servers are running at Amazon but for different customers and territories, we have two more separated hosting's, one in Germany and one in Israel. In Amazon RealiteQ, have three different servers, one for real time, one for history and one for backup these two servers.
- Each project has its own database.
- Most advanced Security procedures applied which the main ones are: No static IP, SSL, 128 hash code S-Key, no transparent connection, All are clients but the COMP, password encryption, adaptive delays and blocking of users with wrong passwords, and more...
- The software can't track ICEX device real time location (RealiteQ Producers need no fix IP, preventing hacker attacks.)
- Remote operational notification – any remote change of critical values will generate notification to the relevant personal.
- Option for monitoring only – remote operation is blocked and only remote monitoring is running.

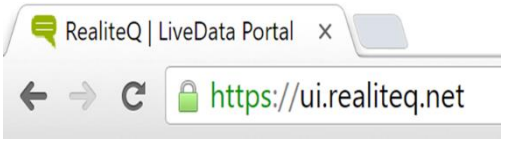
RealiteQ is composed of the following parts:

- State server (COMP) - a machine handling all application state and user interface.
- Backup state server - a machine identical to the State server, in hot standby in case the first server fails.
- History DB server - a machine serving historical data.
- iCeX units (Producers) - field units transmitting real-time process data to the state server.



- User Interface (UI) – Browser based interface (Consumers) connected to the state server, in order to display and control process data and historical data.

- Users use HTTP/HTTPS on browsers to connect to the state server. HTTPS/SSL communication is performed using SHA-256 encryption.
- Communication between the state server and the backup server is done over SSL.
- Communication between the state server and the history DB server is done over SSL.
- Each user on the system is assigned a username and password. Passwords are stored salted by generating a random UUID for each user, and encrypted using MD5 hashing.
- Log-In on browsers is always performed using HTTPS, so passwords are never sent in plaintext on the wire.



- User sessions expire automatically after 10 minutes of inactivity. The user's access token, generated on log-in, is valid for starting session for one hour. After it expires, the user will need to provide their credentials in order to access the system.
- There is automatic reminder for every user every 90 days to change to new password.
- User password strength is scored. Complex password is required for a high score approval.
- Detailed credentials for users with several separated rules.

User : mekorot - Title: mekorot

Permissions :

Del	path	Read	Write	Modify	Upload	Config
del	/icex	☑	☐	☐	☐	☐
del	/icex/registers	☑	☑	☐	☐	☐

- False user log-in activates a delay algorithm that block hacking. After 2 more retries the access is blocked for 30 minutes.
- iCeX units (Producers) connect as clients to the state server using HTTP/HTTPS (port 443). That's make the system "firewall Friendly" and no "holes" should be opened .
- Each iCeX has a unique user name. iCeX are required to sign into the server either as with a unique password (just like normal user) or, for better security, by using a unique Access Token that is generated for the specific iCeX/URL by the COMP.

Del	Path	Access token
del	/icex	6424dd9b534746c69b02fa6444e7adde

- All sessions secured (in addition to SSL) by a 128 bits hash code (S-Key) that is manipulated with the actual IP and routinely changed. The manipulated and encrypted S-Key and is attached to every HTTP/HTTPS transmission.
- Historical data is stored using AES-256 encryption.
- No static IP is in use by the producer nor the consumer. RealiteQ Producers and Consumers support DHCP with all networks (fix or landline).
- Both Producers and Consumers are clients. Only the clients initialize the connection to COMP.
- Working with DHCP behind firewalls or routers, there is no way to expose from remote the actual (Dynamic) IP of the Producers. As so it is impossible to remotely connect to Producers (the Producers initiate the connection and Log-In to COMP).

Hardware –

- An advanced Firewall has been added to iCex (field gateway) new hardware.

Conclusion:

By virtue of being a control system for critical infrastructure, RealiteQ protected with the highest security algorithm and all the data protected by technologies that are used in banking and military applications. In addition, closing a valve, opening an alternative water supply channel, or resetting a critical alarm must be done carefully. The system uses an advanced algorithm that makes remote operation secure and safe.

In the last 8 years, RealiteQ is safely installed in many Water & Wastewater utilities, Natural Gas distribution systems as well as in other thousands of sites in five continents, and among our users you can find global & American leading enterprises such as Jonson Control, Schneider-Electric, City bank, Coca-Cola, Tesla, Unilever, L'Oreal, Solenis, Hercules...