RealiteQ solución SCADA & Telemetría en la nube –

Detalles de la SEGURIDAD

Reali Technologies es un líder israelí en Web SCADA y tecnología de telemetría. Reali Technologies se estableció como una nueva empresa de tecnología israelí en 2007 que desarrolló **una nueva generación de soluciones SCADA y de telemetría llamada RealiteQ.**

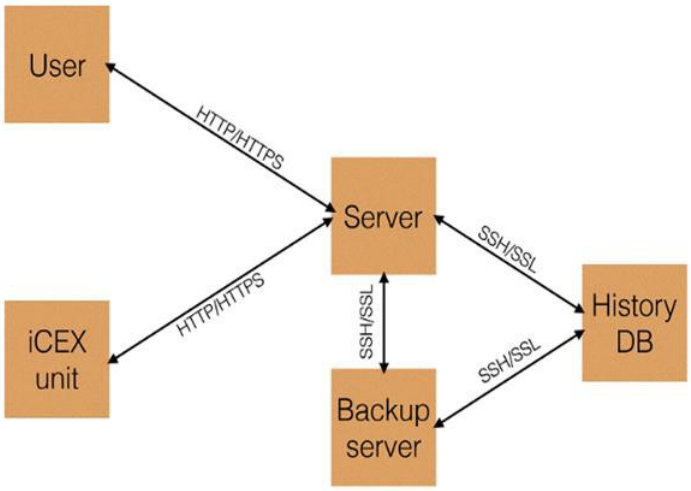
En la actualidad, Reali Technologies cuenta con **un avanzado sistema de telemetría SCADA basado en web de extremo a extremo** para una amplia gama de aplicaciones de agua y aguas residuales, con miles de sitios remotos que operan en cinco continentes.

Reali Technologies Ltd. invierte y aún aplica dosis, muchos esfuerzos y recursos en la provisión de la solución altamente confiable de SCADA y Telemetría basada en la nube de RealiteQ, usando varios niveles de seguridad:

- ✓ Servicio confiable - Alojamiento múltiple. Nuestros servidores se están ejecutando en Amazon pero para diferentes clientes y territorios, tenemos dos hosting más separados, uno en Alemania y otro en Israel. En Amazon RealiteQ, tiene tres servidores diferentes, uno para tiempo real, uno para el historial y uno para respaldo de estos dos servidores.
- ✓ Cada proyecto tiene su propia base de datos.
- ✓ La mayoría de los procedimientos de seguridad avanzados que aplican son los principales: No hay IP estático, SSL, 128 código hash S-Key, ninguna conexión transparente, todos son clientes, excepto COMP, encriptación de contraseña, retrasos adaptativos y bloqueo de usuarios con contraseñas incorrectas, y Más...
- ✓ El software no puede rastrear la ubicación en tiempo real del dispositivo ICEX (los RealiteQ Producers no necesitan corregir la IP, lo que previene los ataques de hackers).
- ✓ Alerta operacional remota: cualquier operación remota de valores críticos generará una notificación al personal relevante (bajo prueba).
- ✓ Opción para monitoreo solamente (Modelo "M") - la operación remota está bloqueada y solo se está ejecutando la supervisión remota. Instalaciones de equipos IS (intrínsecamente seguros).

RealiteQ se compone de las siguientes partes:

- **Servidor de estado (COMP)**: una máquina que maneja todo el estado de la aplicación y la interfaz de usuario.
- **Servidor de estado de copia de seguridad**: una máquina idéntica al servidor de estado, en el modo de espera activo en caso de que el primer servidor falle.
- **Servidor de base de datos histórica**: una máquina que sirve datos históricos.

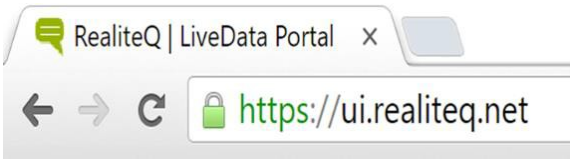


- **Unidades iCeX (Productores)**: unidades de campo que transmiten en tiempo real procesar datos en el servidor de estado.
- **Interfaz de usuario (UI)**: interfaz basada en navegador (consumidores) conectada al servidor de estado, para visualizar y controlar datos de proceso e históricos.

- Los usuarios usan HTTP / HTTPS en los navegadores para conectarse al servidor de estado. La comunicación HTTPS / SSL se realiza mediante el cifrado SHA-256.
- La comunicación entre el servidor de estado y el servidor de respaldo se realiza a través de SSL.
- La comunicación entre el servidor de estado y el servidor de historial de DB se realiza a través de SSL.
- A cada usuario en el sistema se le asigna un nombre de usuario y contraseña. Las contraseñas se almacenan saladas mediante la generación de un UUID aleatorio

para cada usuario, y se encriptan usando hash MD5.

- El inicio de sesión en los navegadores siempre se realiza mediante HTTPS, por lo que las contraseñas nunca se envían en texto sin cifrar en el cable.



- Las sesiones de usuario caducan automáticamente después de 10 minutos de inactividad. El token de acceso del usuario, generado al iniciar sesión, es válido para iniciar la sesión durante una hora. Después de que caduque, el usuario deberá proporcionar sus credenciales para acceder al sistema.

- Hay un recordatorio automático para cada usuario cada 90 días para cambiar a una nueva contraseña.

- La fortaleza de la contraseña del usuario se puntúa. Se requiere contraseña compleja para una aprobación de puntaje alto.

- Credenciales detalladas para usuarios con varias reglas separadas.

User : mekorot - Title: mekorot

Permissions :

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

- El inicio de sesión de usuario falso activa un algoritmo de retraso que bloquea el pirateo. Después de 2 intentos más, el acceso se bloquea durante 30 minutos.

- Las unidades iCeX (productores) se conectan como clientes al servidor de estado usando HTTP/HTTPS (puerto 443). Eso hace que el sistema sea "amigable con el firewall" y no se deben abrir "agujeros".

- Cada iCeX tiene un nombre de usuario único. iCeX debe iniciar sesión en el servidor con una contraseña única (al igual que el usuario normal) o, para mayor seguridad, mediante el uso de un token de acceso exclusivo que el COMP genera para el iCeX/URL específico.

Del	Path	Access token
del	/icex	6424dd9b534746c69b02fa6444e7adde

- Todas las sesiones están aseguradas (además de SSL) por un código hash de 128 bits (S-Key) que se manipula con la IP real y se cambia rutinariamente. La S-Key manipulada y encriptada está asociada a cada transmisión HTTP / HTTPS.
- Los datos históricos se almacenan usando el cifrado AES-256.
- El productor y el consumidor no utilizan IP estática. Los productores y consumidores de RealiteQ son compatibles con DHCP con todas las redes (reparación o línea fija).
- Tanto los productores como los consumidores son clientes. Solo los clientes inicializan la conexión a COMP.
- Al trabajar con DHCP detrás de firewalls o enrutadores, no hay forma de exponer remotamente la IP (dinámica) real de los productores. Como tal, es imposible conectarse remotamente a los Productores (los Productores inician la conexión e inician sesión en COMP).

Conclusión:

En virtud de ser un sistema de control para infraestructura crítica, RealiteQ está protegido con el más alto algoritmo de seguridad y todos los datos protegidos por tecnologías que se utilizan en aplicaciones bancarias y militares. Además, cerrar una válvula, abrir un canal de suministro de agua alternativo o restablecer una alarma crítica debe hacerse con cuidado. El sistema usa un algoritmo avanzado que hace que el funcionamiento remoto sea seguro y confiable.

En los últimos 8 años, RealiteQ se instala de forma segura en muchos servicios de agua y aguas residuales, sistemas de distribución de Gas Natural y en otros miles de sitios en los cinco continentes, y entre nuestros usuarios puede encontrar empresas líderes mundiales y estadounidenses como Jonson Control, Schneider-Electric, banco de la ciudad, Coca-Cola, Tesla, Unilever, L'Oreal, Solenis, Hércules ...