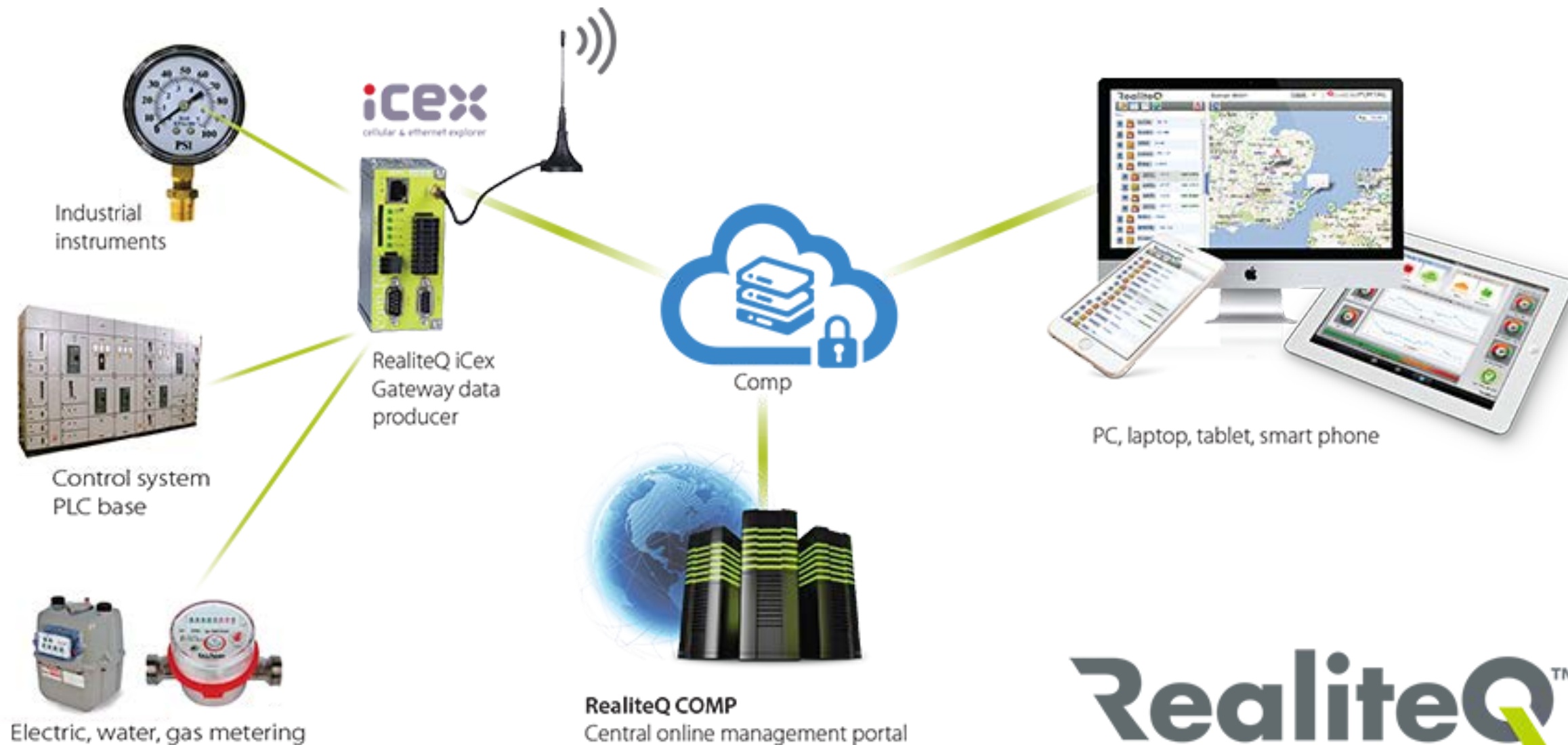




בקרה ושליטה (מרחוק) על מתקני מים (ומתקנים אחרים)

שאול רום

shaulr@realiteq.com

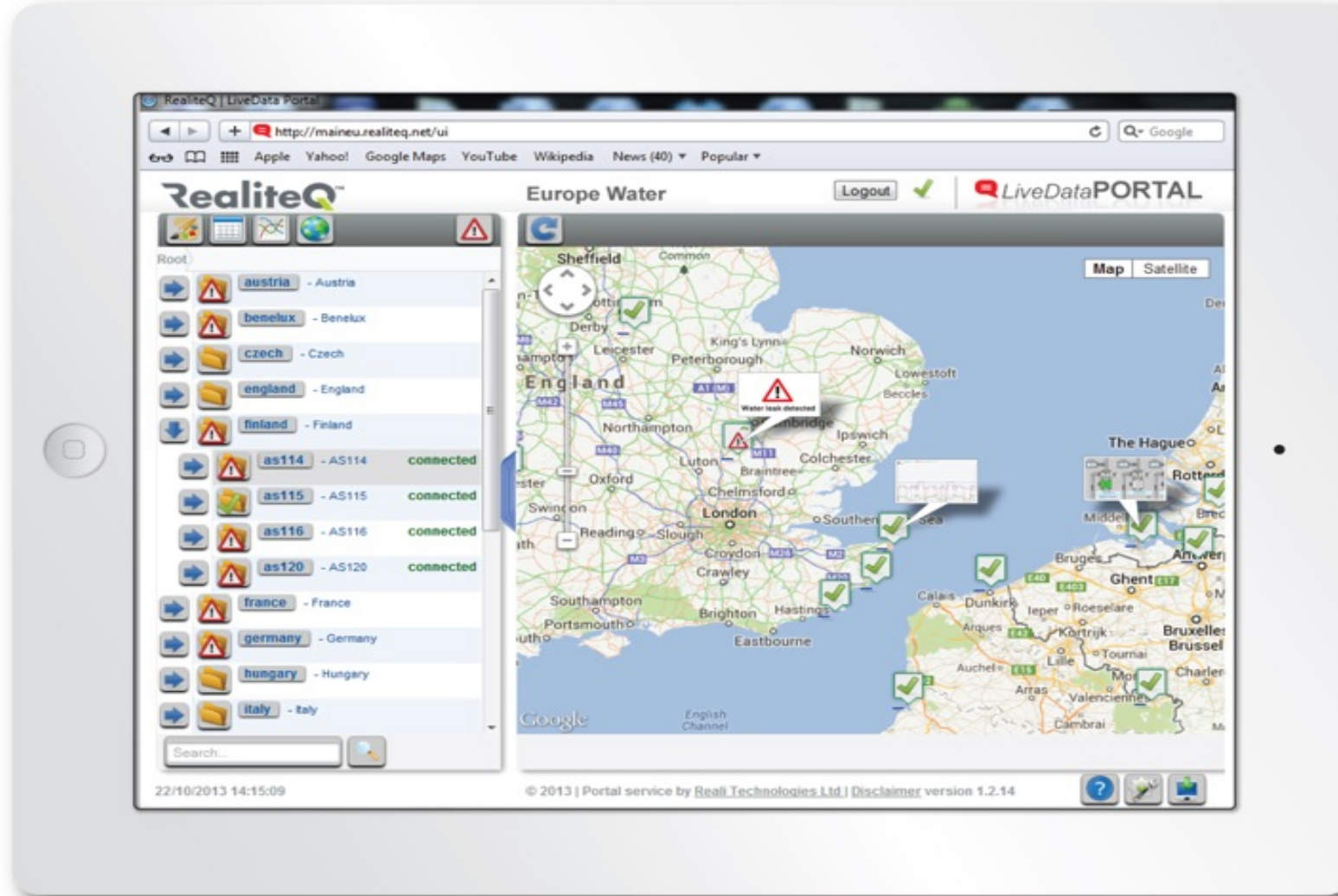
טלפון: 054-4958800

חדרי בקרה מסורתיים



חדרי בקרה מודרניים





“Fourth Generation – Cloud / Internet Based SCADA System....”

...” Cloud-based SCADA dramatically lower the costs associated with a traditional SCADA system... getting started with a cloud-based SCADA, users can achieve about 90% reduction in costs...”

...” Cloud-based SCADA improve the system's reliability. Cloud computing platform enables water and wastewater utilities to deploy redundancy and disaster recovery capabilities far beyond that found in the typical water and wastewater IT departments...”

**Source: 2017 Zion
Market Research**



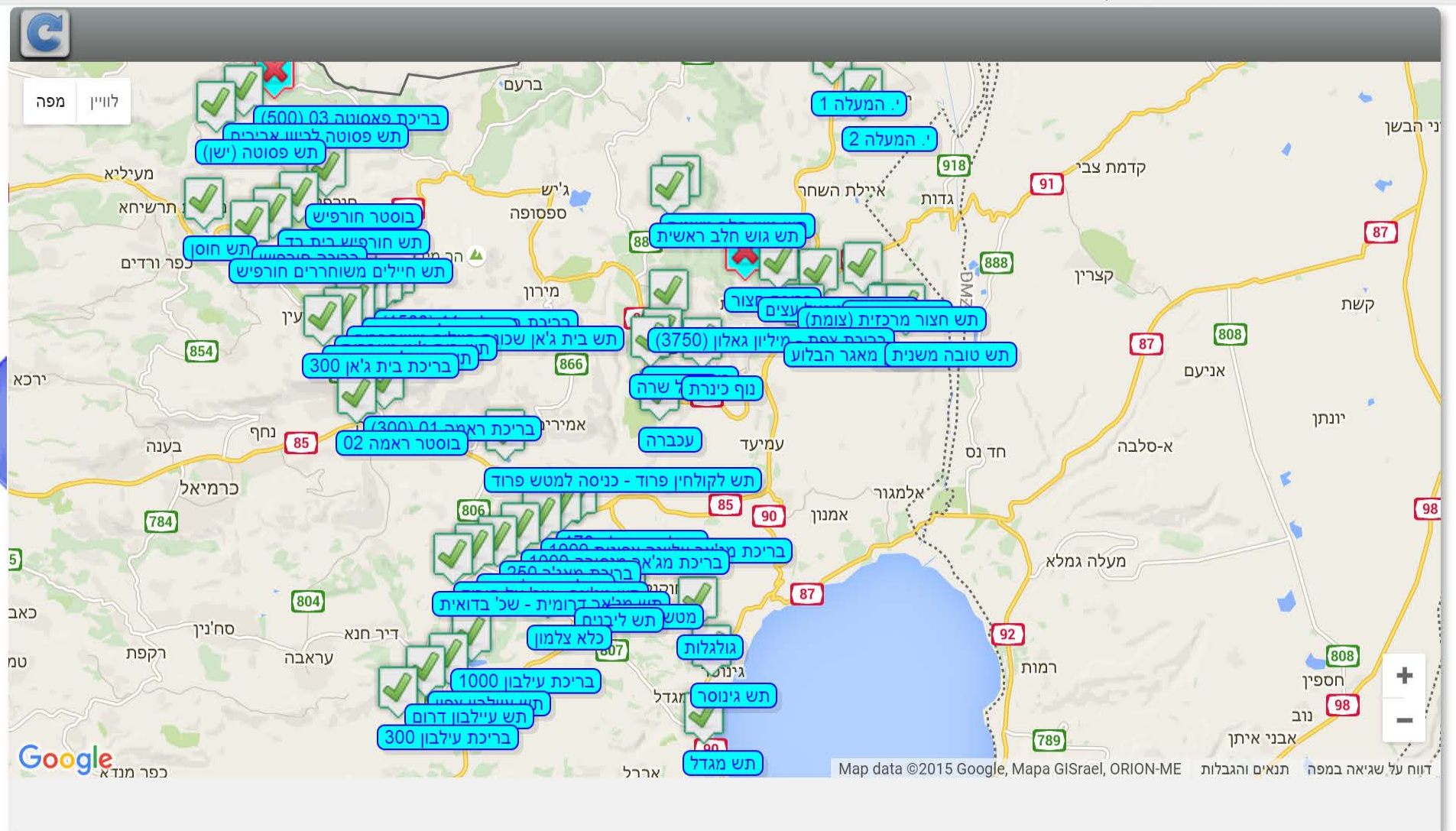
טכנולוגית ענן לניהול, שליטה ובקרה על מתקנים אשר מיישמת תקני תקשורת ואבטחה מתקדמים ומאפשרת ניהול יעיל ודינאמי של מערכי הבקרה בתחום המים, האנרגיה, הגז הטבעי ותחומים אחרים.



Root

- ☐ 1water - מים
מתקני בריכות מים
- ☐ 2biuv - תחנות ביוב
תחנות ביוב
- ☐ 3kolhin - קולחין
תחנות לאספקת קולחין
- ☐ livnim - רמת ליבנים
תחנות החברה לטיפול בשפכים
- ☒ motorola - Ilnrts **connected**
נקודות איסוף נתונים ממערכת מרכזית של מוטורולה
- ☐ time 2015-12-05 18:21:48 UTC
keep alive for pulse opc

Search...



עקרונות לניהול מערכות SCADA בענן

- ✓ שליפת נתונים קריטיים בזמן אמת
הפצת נתונים "בדחיפה" למפעילים ולאפליקציות תומכות. עדכון בסיס הנתונים להיסטוריה.
- ✓ תקשורת בעלת יתירות גבוהה
שימוש במגוון תקשורות אינטרנטיות רגילות, אלחוטיות, סלולאריות או לווייניות ובמספר ערוצי תקשורת מקבילים.
- ✓ ערוץ שליטה לתגובה מידית
ערוצי שליטה מאובטחים לשינוי נתונים והפעלות בשגרה או לתגובות מידיות במקרה של אירוע משברי.

ניהול מערכות SCADA בענן

ניהול תקלות והתראות ✓

זיהוי מצבי תקלה, הפצת התראות באמצעות SMS ודואר אלקטרוני לגורמים הרלוונטיים לתקלה.

אבטחת מידע וביטחון מערכת ✓

יישום מנגנוני אבטחה ברמה גבוהה כנדרש במתקני תשתית חיוניים. מנגנונים ואלגוריתמים מתקדמים לביצוע בטוח של הפעלות במתקנים מרוחקים.

ממשקים מוכרים ונוחים ✓

ממשקי דפדפן מודרניים מותאמים לפלטפורמות השונות (מחשבים, טאבלטים, סמארטפונים).



dreamstime.com

מספר עובדות על אבטחה והתאמה לדרישות רשות המים

דרישות רשות המים – עיקרי הדברים

- ניהול משתמשים והרשאות שימוש.
- הכנסת רכיבי אבטחה לניטור הרשת ורכיבי אבטחה לשרתים ותחנות הקצה.
- יש לקיים הפרדה פיזית ברכיבי התקשורת בין מערכות המחשוב העסקיות לבין התהליכיות לדוגמה מתגים נפרדים לכל רשת ומעבר לכך ארונות תקשורת נפרדים לכל הפחות באותו החדר.
- נדרש ליישם מנגנון הצפנת תעבורה תוך שימוש באלגוריתם מסחרי בעל מפתח הצפנה של AES 256.
- יתירות בערוצי תקשורת מהבקר למערכת לדוגמא סלולר ויתירות במקרה נפילה של התקשורת למרכז הבקרה.

דרישות רשות המים (המשך)

- שם משתמש ייעודי לכל בעל הרשאה/תפקיד ומדיניות סיסמה תווים ותוחלף כל ארבעה חודשים.
- יש לוודא קיום של מידור הרשאות במערכת השו"ב לפי בעלי תפקיד הן ברמת פעולות אפשריות לביצוע והן ברמת נגישות לכלל מערכות הסקאדה או חלקן.
- ניטור ברמת יש לוודא רישום פעולות בעל ההרשאה (לדוגמא –סגירת משאבה) בלוג ייעודי הניתן לקריאה וחקירה.
- בסיס הנתונים במערכות שו"ב אשר לרוב אפליקטיבי נדרש להיות מופרד מהאפליקציה (תצורה מבוזרת) בסביבות בהן הוא משמש כחלק מתשתית SCADA תומכת החלטה וליישם הגנות עליו.

דרישות רשות המים (המשך)

- סגמנטציה בתוך רשת התהליך: התקנת Fire Wall (חומת אש ומסנן תוכן) תעשייתי, ככל שניתן, בכל מתקן ובין המתקן לרשת הבקרה.
בקרים תעשייתיים מאובטחים – מומלץ בהתקנת מערכת חדשה להתקין בקרים PLC מאובטחים, בהתאם לזמינות הטכנולוגיה
- מומלצת הקלטת ה- Session ושמירתו לצורך בקרה והסטוריה.

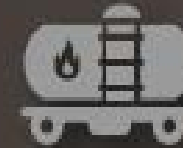
חיזוק האבטחה ברמת תוכנת הבקר

- הגדרת ערכי Min/Max וחסימת ערכים "לא סבירים".
- בדיקת סבירות זמני עבודת משאבות (או זמני מנוחה).
- בחוסר תקשורת או נתונים כוזבים שליחת התראה ומעבר לרוטינה עצמונית.
- במתקנים הפועלים בתקשורת רוחבית (בין מתקן אחד לשני) הרצת Watch Dog פנימי לבדיקת חיות מערך התקשורת.
- שימוש במנגנוני אבטחה מובנים של הבקרים (הגנה על תוכנת הבקר, פורטים בחיבורי ETH ועוד).

מרכיבי אבטחה נוספים הקיימים במערכת RealiteQ

- אין שימוש ב- IP קבוע, אין צורך ב- APN ייעודי.
- כל סיסמא מקבלת ציון חוזק.
- משתמשים מקבלים תזכורת החלפת סיסמאות כל 90 ימים.
- מופעלים (בקרוּב) מנגנות "נודניק" לשליחת התראות למפעילים וכן מנגנון אסקלציה.
- מפעיל בכיר יקבל התראה על שינוי ערך קריטי על ידי מפעיל זוטר.
- ניתן לחבר יחידות קצה מאחורי שרתי Proxy.
- מפתח S-Key מתחלף כל מספר דקות ומועבר ביחד עם כל הודעה במערכת.
- מופעל (בקרוּב) ממשק ל- Telegram המאפשר קבלת התראות וביצוע Ack בקליק.

פלטפורמת SCADA בענן מאפשרת התייעלות תפעולית יחד עם הקפדה על רמת אבטחה גבוהה



שאול רום

shaulr@realiteq.com

טלפון: 054-4958800