

הגנה על הדיוק שלך:
כיצד להתמודד עם שיבושים
והטעיות של אותות GNSS
לצורך השגת דיוק מרבי



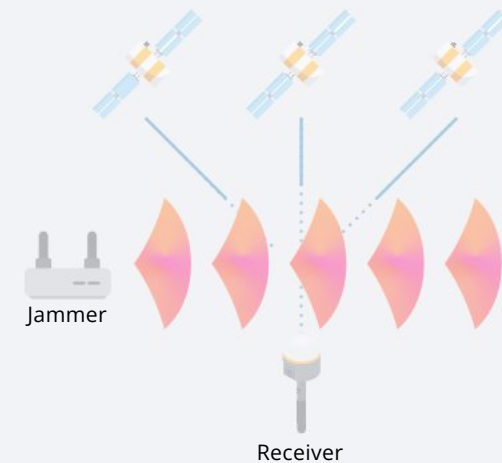
היערכות לשיבושי GNSS: הגנה על אמינות הנתונים בעידן של איומי RF

בעולם ההיפר מקושר של ימינו, רמת הסיכון הולכת ועולה בכל הנוגע לשמירה על אמינות אותות המיקום במערכות GNSS. כיום, אותות אלו אינם משמשים רק לניווט בסיסי, אלא מהווים תשתית קריטית למגוון רחב של יישומים הנדסיים, שווקים גלובליים ומערכות אוטונומיות.

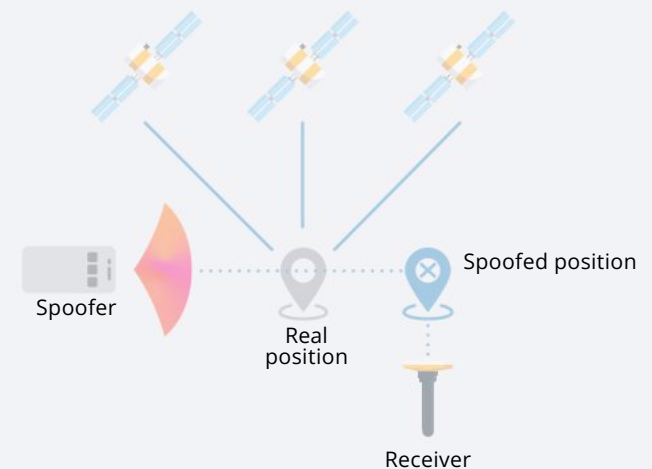
עם זאת, לאותות ה-GNSS קיימות נקודות תורפה מובנית: הם משודרים מלוויינים הנמצאים בגובה של כ-20,000 ק"מ מעל פני כדור הארץ, ועוצמתם ברגע הגעתם למקלט חלשה ביותר (ניתן להשוותה לעוצמת אלומה של נורת 40 וואט ממרחק עצום). נתון זה הופך את המקלטים לפגיעים במיוחד להפרעות בתדרי רדיו (RF), בין אם מדובר ברעש מקרי ובין אם בשיבוש מכוון.

כל הפרעה כזו, קלה כחמורה, עלולה לפגוע אנושות בדיוק המדידה או להוביל לאובדן מוחלט של פתרון המיקום. במציאות כזו, היכולת המבצעית והאמינות של הפרויקט כולו עומדות למבחן והיערכות מוקדמת היא כבר לא בחירה, אלא הכרח מקצועי.

שיבוש

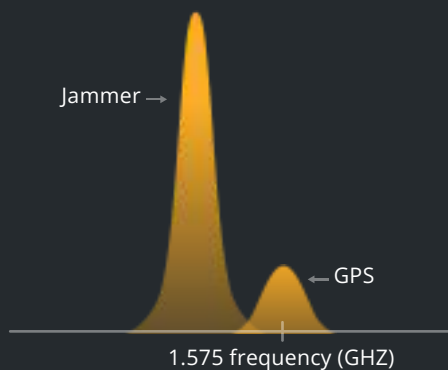


זיוף

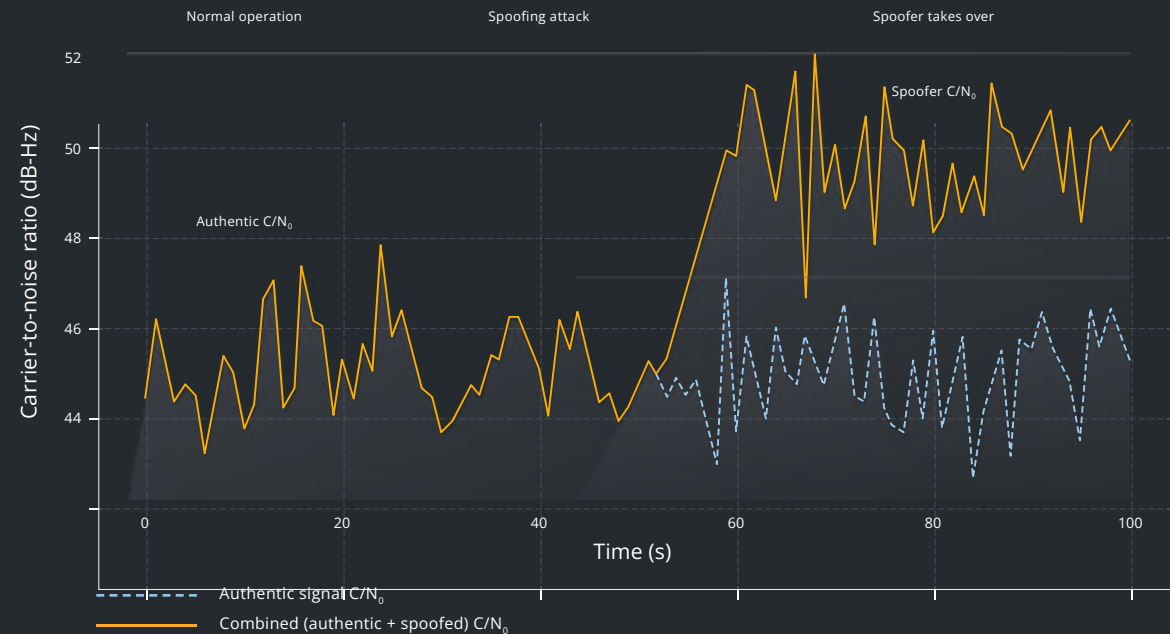


ויזואליזציה קונספטואלית של מתקפת זיוף GNSS

השוואה מהירה בין שיבוש לזיוף:
שיבוש מתרחש כאשר האות מופרע או נחסם, מה שמקשה על המקלט או מונע ממנו לחלוטין לפענח את המידע בצורה נכונה. לעומת זאת, הזיוף כולל שידור זדוני של אותות "מזוייפים" המחקים את האותות האמיתיים, ובכך מוליכים שולל את המקלט ומביאים להצגת נתוני מיקום שגויים.



הדמיה של מתקפת שיבוש על מקלט GNSS. אות ה-GNSS האמיתי הוא קטן ומדויק יותר, בעוד שאות המשבש הוא חזק ורחב יותר, וגובר במכוון על אות ה-GNSS באותו התדר.



ויזואליזציה של מתקפת הטעיה (Spoofing) על יחס אות לרעש (C/N₀) של מקלט GNSS, שבה האות המזוייף (קו צהוב) עוקב בתחילה אחר האות האותנטי (קו כחול) ולאחר מכן גובר עליו בהדרגה, כך שהמקלט ננעל על האות השגוי ומדווח על מיקום שגוי.

אנטומיה של פגיעות בשידור אותות

למרות שמערכות GNSS כמו GPS, BeiDou, GLONASS, Galileo משדרות בתוך פסי תדרים ספציפיים, אותות RF (תדר רדיו) רבים אחרים בסביבה יוצרים הפרעות. אלו עלולים "לזלוג" לתוך פסי ה-GNSS, לפגוע באיכות הדיוק של המיקום, ואף לגבור לחלוטין על אותות ה-GNSS.

לרוע המזל, הדבר הופך את המערכות לפגיעות גם ל"הפרעות" בעלות אופי חתרני יותר, באמצעות שיבוש וזיוף שני איומים ממשיים מאוד המשפיעים על מערכות המיקום כיום.

השתמש בטכנולוגיה כ"שומר סף" מפני נתונים כוזבים

מערכות חדשניות בעלות מנגנוני זיהוי מובנים יכולות לצמצם את ההשפעה של מניפולציות GNSS באמצעות ניטור אמינות ומערכות ניווט יתירות, כגון מערכות ניווט אינרציאליות (INS) ובכך לשמור על השליטה בידיים שלך.

הפרעות אותות נמצאות בכל מקום

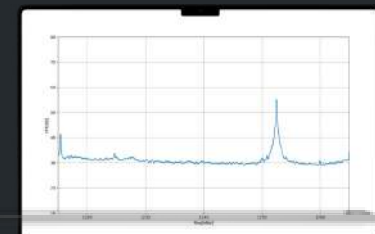
בעידן הנוכחי, המאופיין בריבוי מכשירי "אינטרנט של הדברים", הפרעות בתדרי רדיו הפכו לדבר שבשגרה, בין אם הן נגרמות בזדון ובין אם כתוצאה מנסיבות טכניות. אחת הסיבות המרכזיות לכך היא הצפיפות הגבוהה של חיישנים המותקנים זה לצד זה על גבי ציוד הנדסי, כלי רכב ורחפנים. פתרונות טכנולוגיים מתקדמים נגד חסימה והטעיה אינם מספקים רק מענה לאיומים המוכרים כיום, אלא מתפתחים ללא הרף כדי להקדים סיכונים עתידיים וטכנולוגיות שיבוש מתהוות.

מקורות ההפרעה עלולים להיות מפתיעים: לפי דיווחי הקרן לניווט ותזמון חסינים, נמצא כי אפילו אנטנות טלוויזיה ימיות תקולות גרמו לשיבושים קשים באותות המיקום הלווייניים. בנוסף, העלייה בשימוש במערכות למעקב אחר ציי רכב ובמנגנוני גביית אגרות מבוססי מיקום, הובילה לגידול משמעותי בהפצת משבשים זולים ובלתי חוקיים המותקנים בכלי רכב דבר המהווה איום ישיר על דיוק המדידה במרחב הציבורי.

משבשי "Chirp" רחבי סרט: קטנים, עוצמתיים וקשים לסינון

משבש Chirp בודד בהספק נמוך של 10mW בלבד, המתחבר לשקע המצית ברכב (12V), מסוגל לשתק קליטת GNSS ברדיוס של מספר קילומטרים. בניגוד להפרעות "אקראיות" צרות סרט, ההתגוננות מפני משבשי Chirp מורכבת בהרבה; אופי האות המשתנה במהירות ("דילוגי תדר") הופך את מסנני ה-Notch הסטנדרטיים לבלתי יעילים.

כדי להבטיח דיוק ואמינות, מקלטים מתקדמים מנטרים כיום מספר תדרים וקונסטלציות לוויינים במקביל. עם זאת, כאשר הפרעה רחבת סרט משפיעה על מספר אותות באותו פס תדרים, היא עלולה לגרום לשיבוש קליטה מוחלט. מצב זה מחייב אימוץ אסטרטגיות הגנה מתקדמות ומערכות חסינות יותר (Hardened GNSS) כבר בשלב התכנון.





נקטו באמצעי זהירות, אל תקחו סיכונים

כשמדובר בדיוק במיקום, "קרוב מספיק" פירושו כישלון. שמירה על אמינות נתוני המיקום שלך חיונית לא רק עבור העבודה עצמה, אלא גם עבור המוניטין שלך. הסתמכות על אבטחת GNSS לקויה מותירה את המכשור שלך חשוף להפרעות ומעמידה את העסק כולו בסכנה.

בעלי עסקים ומומחי מידע גאו-מרחבי (Geospatial) צריכים לשקול היטב מספר שאלות מפתח בעת הערכת מידת היעילות של הגנת הנכסים והמערכות הדיגיטליות שלהם מפני מתקפות סייבר, במיוחד כאלו הכוללות שיבושים:

- אילו אמצעים קיימים כיום להגנה על המערכות שלנו מפני שיבושים, ומהי מידת יעילותם?
- האם ביצענו הערכת סיכונים לזיהוי נקודות תורפה ספציפיות לאיומי שיבוש?
- אילו לקחים הפקנו מאירועי עבר, וכיצד התאמנו את האסטרטגיות שלנו בהתאם?

קל יותר מאי פעם לפגוע באותות

זמינותם של מכשירי רדיו זולים וניתנים לתכנות מאפשרת כיום ליצור בקלות משדרים המפיצים אותות הטעיה. מקלטי ייחוס עלולים לזהות אותות אלו כלגיטימיים, מה שמוביל לשגיאות קריטיות בנתוני המיקום והזמן ולסטיות של מאות קילומטרים. מעבר להפרעה הטכנית, לחסימות ולהטעיות יש כוח הרסני: הן מעוותות נתונים, משתקות ביצועי מכשירים ופוגעות בתהליכי עבודה אוטומטיים. מציאות זו מסכנת לא רק את הרווחיות הכלכלית, אלא גם חיי אדם באתרים הנדסיים ובחוות חקלאיות מבוססות טכנולוגיה.

הגנת אותות מובנית: תכנון מראש כסטנדרט מקצועי

הפחתת הפרעות יעילה אינה יכולה להיות פתרון חיצוני או מאוחר; עליה להוות חלק בלתי נפרד מארכיטקטורת המקלט. עבור המודד בשטח, המשמעות היא הסתמכות על ציוד שבו ההגנה מתחילה כבר ברמת החומרה בדגש על האנטנה ודרגות הכניסה של המכשיר.

קליטת האות היא רק מחצית מהמשימה. ברגע שבו הנתונים הופכים מאנלוגיים לדיגיטליים, המקלט נדרש לאלגוריתמיקה מתקדמת. כאן בא לידי ביטוי כוחו של הסינון: הוא פועל כשומר סף המבודד את תדרי העבודה הדרושים ודוחה באגרסיביות רעשים המאיימים על הדיוק. ללא יכולת זו, המערכת חשופה למצב של "קלט שגוי פלט שגוי", מה שהופך מדידה הנדסית לנתונים חסרי ערך.



מה ההבדל בין שיבוש לזיוף?

השיבוש מתמקד בהפרעה. הוא מציף את המכשירים ברעש מוגזם או בנתונים פגומים, וגורם להם לשגעאות.

הזיוף מתבסס על רמאות. הוא שולח אותות מזויפים המחקים את האמיתיים, ומוליך שולל את המערכות. הדבר עלול להוביל למדידות שגויות, לפעולות לא תקינות ואף לקריסה מוחלטת של המערכת.

המניעים מאחורי זיוף או שיבוש מכוון נעים בין ריגול תעשייתי והונאה פיננסית ועד לחבלה, במטרה לגרום לשגיאות או לתאונות. שניהם מציבים אתגרים חמורים, אך ההבדלים ביניהם דורשים אסטרטגיות ייחודיות לזיהוי ולמניעה. ההפרעה אמנם בלתי נראית, אך עלות זמן ההשבתה נראית לעין היטב. כדי להעניק שקט נפשי ללקוחותיכם, עליכם להיות ערניים לגבי אמינות הנתונים. בין אם אתם עובדים במרכז עירוני צפוף ובין אם סמוך למשדרים בעלי הספק גבוה, המטרה היא זהה: להישאר צעד אחד לפני הפגיעה באות. הפרעה שאינה מטופלת מובילה לתיקוני מיקום שגויים ולביצוע עבודה מחדש בעלות גבוהה. השלכות שאף עסק מדידות אינו יכול להרשות לעצמו להתעלם מהן.



מהי ההשפעה הפוטנציאלית של שיבוש או הטעיה על מכשירים וחומרה?

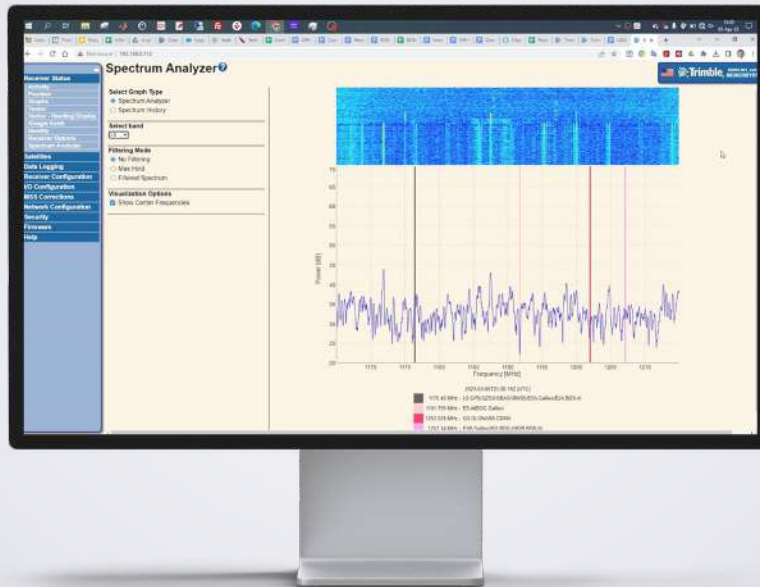
השפעת שיבוש וזיוף על מערכות וחומרה ללוחמה אלקטרונית השפעה קריטית על תפקוד המכשירים ועל שרידות החומרה:

שיבוש: שימוש ברעש, טון או פולסים מוביל לירידה באיכות האות ולנתק בתקשורת. התוצאה היא אובדן נתונים ופגיעה חמורה במודעות המצבית.

זיוף: שידור חוזר או כיסוי אותות מחדירים נתונים כוזבים למערכת בצורה מעודנת. הדבר מוביל לקריאות שגויות ולפעולות הרסניות, כמו הסטת רחפני הצלה ממסלולם במשימות קריטיות.

נזק לחומרה: עוצמת שידור גבוהה בסמוך לאנטנה עלולה להזיק פיזית לרכיבי הקליטה. בנוסף, עיבוד אינספור אותות פגומים מעמיס על המערכת, גורם להתחממות יתר, מקצר את אורך חייו הציוד ומייקר את התחזוקה..

מהם הסימנים לכך שמקלט ה-GNSS עובר שיבוש או הטעיה? הפרעה מתבטאת בדרך כלל בביצועי מכשיר לא יציבים או תזזיתיים, ניתוקים תכופים באות או ירידה ניכרת בדיוק הנתונים. הזיוף חושפת את עצמה לעיתים קרובות באמצעות "נורות אדומות" כגון:



- רכישה מחדש תכופה של אותות.
- חוסר עקביות חריג בנתוני המיקום.
- פערים גדולים המזוהים על ידי מסנני קלמן.
- שינויים פתאומיים ובלתי מוסברים בתבניות הנתונים.
- קפיצות בלתי צפויות בעוצמת האות.
- ירידה באיכות האות (לדוגמה: נפילה ביחס אות לרעש או רצפת רעש גבוהה).
- זיהוי מהיר של הפרעות והטעיות הוא חיוני לשמירה על תקינות המערכת.
- סטיות מיקום פתאומיות.

באזור הבלטי בלבד,

46,000 כלי טיס

הציגו סימני שיבוש אפשריים
בין אוגוסט 2023 למרץ
2024.

— מגזין Wired



אילו תעשיות הן הפגיעות ביותר לשיבוש או לזיוף?

מעבר למדידות ולבנייה, תעשיות הכוללות תשתיות ציבוריות, אבטחת סייבר, תחבורה, ספנות, צבא, בטיחות הציבור וחקלאות הן בעלות רגישות גבוהה, דבר המהווה איום משמעותי. שיבושים ברשתות תחבורה מרכזיות עלולים להוביל להסטת כלי רכב ממסלולם, מה שעלול לגרום להתנגשויות, ואף להפיכתם ליעד לפעולות זדוניות כמו גניבת מטענים. בשנת 2024, שתי משאיות שהובילו טקילה מיוחדת בשווי של למעלה ממיליון דולר נחטפו בלרדו, טקסס, ומאז לא נודעו עקבותיהן. חקירות הובילו את רשויות אכיפת החוק ונציגי החברה לחשד כי בוצע זיוף אותות, שגרם לכך שייראה כאילו המשאיות נמצאות במקום הנכון, בעוד שבפועל הן לא היו שם. לאחרונה הפכו גם מסילות הרכבת ליעד משמעותי לאיומי סייבר באמצעות זיוף, וזאת בשל השימוש הגובר בטכנולוגיות דיגיטליות.

"מתקפות כופר הפכו לאיום הבולט ביותר נגד מגזר הרכבות" בשנים האחרונות ברחבי האיחוד האירופי, מה שהוביל להנחיות נרחבות הכוללות אמצעים נגד זיוף. **מריאנטי תאוקרידו, סוכנות האיחוד האירופי לאבטחת סייבר.**

גם תעופה, ספנות ולוגיסטיקה יבשתית עומדות בפני סכנות משמעותיות בשל תלותן במערכות ניווט ותקשורת מדויקות. בחקלאות, טכנולוגיות לחקלאות מדויקת דורשות נתונים אמינים ומדויקים כדי לייעל את לוחות הזמנים של השתילה, ההשקיה והקציר. שיבושים פירושם זמן השבתה. זמן השבתה מבזבז משאבים ומכלה את הרווחים.



עד כמה קל לגורמים עוינים לשבש מערכות מיקום לווייניות?

בעוד שבעבר תחום זה נשלט על ידי האקרים מיומנים בלבד, כיום השוק מוצף במשבשים זולים. למרות שהשימוש בהם אינו חוקי ברוב מדינות העולם, מכשירים אלו הפכו לנגישים וזולים יותר ויותר, ולעיתים קרובות הם מוסווים כהתקני זיכרון ניידים (USB) תמימים או כמטענים לרכב. זיוף אותות, שבעבר נחשב למשימה טכנולוגית מורכבת, נמצא כיום בהישג יד באמצעות תוכנות בקוד פתוח או רכיבים בעלות נמוכה. המשמעות היא שהצורך באמצעי הגנה חזקים מעולם לא היה קריטי יותר לשמירה על מערכות הפועלות בתחומי החקלאות, הבנייה, הספנות, הכרייה והתחבורה בדרכים פתוחות.



עד כמה קל לגורמים עוינים לשבש מערכות מיקום לווייניות?

בעוד שבעבר תחום זה נשלט על ידי האקרים מיומנים בלבד, כיום השוק מוצף במשבשים זולים. למרות שהשימוש בהם אינו חוקי ברוב מדינות העולם, מכשירים אלו הפכו לנגישים וזולים יותר ויותר, ולעיתים קרובות הם מוסווים כהתקני זיכרון ניידים תמימים או כמטענים לרכב. זיוף אותות, שבעבר נחשב למשימה טכנולוגית מורכבת, נמצא כיום בהישג יד באמצעות תוכנות בקוד פתוח או רכיבים בעלות נמוכה. המשמעות היא שהצורך באמצעי הגנה חזקים מעולם לא היה קריטי יותר לשמירה על מערכות הפועלות בתחומי החקלאות, הבנייה, הספנות, הכרייה והתחבורה בדרכים פתוחות.

טכנולוגיות מתקדמות לזיהוי ודחיית אותות מזויפים

- דחיית אותות זיוף באמצעות עיבוד אותות דיגיטלי: אלגוריתמי מעקב מתוחכמים מזהים אם מתקבלים מספר אותות עבור כל לוויין, ומבטיחים שרק האות האמיתי ינוטר.
- אימות נתוני לוויין: באמצעות ניהול יומן היסטורי של הפרמטרים המסלוליים המשודרים על ידי כל לוויין, טכנולוגיית טרימבל יכולה להבחין בכל שינוי בלתי צפוי או חריגה מהטווחים הסבירים. המערכת מבצעת אימות צולב של נתונים מסלוליים ממקורות שונים, כגון השוואת נתוני תדר אחד של ה-GPS לתדרים אחרים, מה שמגביר משמעותית את האמינות.
- ניטור אמינות אוטונומי: שיטה המוכרת היטב בתעשיית התעופה, החיונית לזיהוי ודחייה של נתוני לוויין שעלולים להיות מזויפים, תוך איתור מדויק של כל קריאת לוויין שאינה תואמת את פתרון המיקום.

כיצד טכנולוגיית טרימבל מפחיתה את הסיכונים הללו?
מקלטי ה-GNSS של טרימבל מתוכננים עם מגוון תכונות המוטמעות בתוך טכנולוגיית "מקסוול", השואבת השראה מחדשנות פורצת דרך בפרוטוקולי אבטחה של תדרי רדיו וטכנולוגיות עיבוד נתונים, במטרה להבטיח מיקום מדויק וחסין.



תכונות מנתח ספקטרום

עם הצגת טכנולוגיית "מקסוול", פתרונות טרימבל מסוגלים לנטר ולנתח את האותות המתקבלים בכל אחד מפסי התדרים של הלוויינים באמצעות ממשק המשתמש הגרפי של המקלט. תכונת מנתח הספקטרום המובנית מסייעת למשתמשים לזהות הפרעות בבדיקות מעבדה או לאחר סיום המשימה, ולנקוט בצעדים להסרתן.



- יכולת ניטור של כל פסי התדרים של הלוויינים ותחנות הייחוס.
- ניטור רציף הפועל ברקע.
- אפשרות להשמעת נתונים מימים קודמים בתצוגת מפל או בפורמט מסונן.
- תצוגת נתונים בזמן אמת בפורמטים של מפל, סינון, החזקת שיא או ללא סינון.
- פעולת מקלט ללא הפרעה, כגון פלט מיקום, יצירת תיקונים או הזרמת תצפיות.

השוואה לצד לצד של מנתח הספקטרום של טרימבל לצורך זיהוי חזותי של הפרעות תדרי רדיו. התמונה השמאלית מציגה שיבושי תדרי רדיו המיוצגים כקווים בתכלת בנתוני הספקטרום הנגללים בתצוגת המפל העליונה. התמונה הימנית אינה מראה הפרעות בתצוגת המפל העליונה, מה שמעיד על תנאי עבודה אידיאליים עבור מקלט הלוויינים.

אל תיקחו סיכונים ונקטו באמצעי זהירות!

ככל ששיבושים וזיופים הופכים לנפוצים יותר, המחיר של פגיעות המתבטא בביצוע עבודה מחדש ובפגיעה במוניטין, גבוה מכדי להתעלם ממנו. הזמן לבצר את הטכנולוגיה שלך הוא עכשיו, לפני שאות פגום ישבש פרויקט קריטי.
עם טכנולוגיית ההפחתה המתקדמת של טרימבל, תוכל לפעול בביטחון גם בסביבות העוינות ביותר.

**סלאמה עואודה מנכ"ל חברת
Axis - פתרונות מדידה מתקדמים
מהנדס ומודד מוסמך**

