

## מדריך לניהול וניתוח סיכונים הנגרמים מטעויות אנוש

אבי הראל<sup>1</sup>, ד"ר אביגדור זוננשיין<sup>2</sup>

מנכ"ל, חברת ארגולייט, חיפה, ישראל<sup>1</sup>  
מרכז גורדון להנדסת מערכות, הטכניון, חיפה, ישראל<sup>2</sup>

### מבוא

מחקרים על תאונות קריטיות בתפעול מערכות מצביעים על כך שנהוג להצביע על הגורם האנושי כסיבה העיקרית לכשל. ממצאים אלו העלו את הצורך לפתח מדריך לתכן ולפיתוח של מערכות החסונות לטעויות תפעול. מאמר זה כולל דיווח על פיתוח מדריך כזה בסיוע ובתמיכה של מרכז גורדון להנדסת מערכות בטכניון.

### תיאור העבודה

המדריך מניח כבסיס את גירסת גורמי אנוש של חוק מרפי ומיישם את העקרון אחריות המפתחים למנוע את טעויות התפעול. הישום נעשה במספר דרכים:

א. יישום טרמינולוגיה של גורמי הכשל: במקום טעות מפעיל משתמשים במונחים של כשל בתפעול, שמקורו בטעות בתכן. במקום לייחס את הכשל לטריגר, מייחסים אותו למצב התפעול.

ב. תכן פרואקטיבי: התגובה הטבעית לאירועי כשל היא של התגוננות וגלגול אחריות. התכן הפרואקטיבי מאפשר מניעה של מצבים כאלו על ידי התייחסות מפורטת לגורמי הכשל בעזרת מודל של חסינות מערכות, על ידי ארכיטקטורה שמאפשרת איתור מצבים חריגים, ועל ידי הנחיות לאיתור המצבים החריגים ולהתאמת תגובת המערכת למצב התפעול.

ג. תכן ריאקטיבי: ניהול מצבי כמעט-תאונה. העיסוק בהאשמות מסיט את הדיון מהעיקר. המדריך מציע כלים והנחיות לאיתור מצבי כמעט-תאונה ולמידע על תהליך הכשל.

### תיקוף המדריך

אפקטיביות המדריך נבחנה בשיתוף קבוצת עבודה של אילטם, בשיתוף אינקווי. קבוצת העבודה בדקה את ישימות המדריך למספר ניתוחי מקרה. המדריך תוקף על ידי מדידה של ישימות ההנחיות בעזרת מאגר של 67 אירועי כשל.

### מסקנות

המדריך עשוי לסייע למפתחי מערכות למניעת כשל על ידי מניעת טריגרים, מניעת מצבים חריגים, ניתוב התפעול במצבים חריגים לאיתור תקלות ולשיקום. בנוסף, המדריך עשוי לסייע למפתחי מערכות בהיערכות לאיתור, ניתוח ותיעוד מצבי כשל בעוד מועד לצורך הפקת לקחים.