מדריך לאבטחת חסינות בתפעול מערכות
כמרכיב להבטחת איכות ובטיחות מערכות

אבי הראל[1], ד"ר אביגדור זוננשיין[2]

מנכ"ל, חברת ארגולייט, חיפה, ישראל [1]
מרכז גורדון להנדסת מערכות, הטכניון, חיפה, ישראל [2]

מבוא

מחקרים על תאונות קריטיות בתפעול מערכות מצביעים על גורמי כשל הקשורים בתפעול במצבים חריגים. ממצאים אלו העלו את הצורך לפתח מדריך לתכן ולפיתוח של תהליכי תפעול המאפשרים מניעה והתמודדות עם מצבים חריגים. מאמר זה כולל דיווח על פיתוח מדריך כזה בתמיכת מרכז גורדון להנדסת מערכות בטכניון.

תיאור העבודה

המדריך מיישם את פרדיגמת **STAMP** על ידי בקרה עצמית בתכן מונחה תרחישים. היישום נעשה על פיתוח איטרטיבי כאשר:

א. פיתוח פרואקטיבי: התייחסות אל גורמי הכשל בעזרת מודל של חסינות מערכות. התכן מבוסס על ארכיטקטורה שמאפשרת איתור מצבים חריגים, ועל הנחיות זיהוי המצבים החריגים ולהתאמת תגובת המערכת למצב התפעול. הבדיקות מבוססות על ייזום מצבים חריגים בתנאי מעבדה, וכן אצל הלקוח.

ב. פיתוח ריאקטיבי: תכן לניהול מצבי כמעט-תאונה, המבוסס על כלים והנחיות לאיתור מצבי כמעט-תאונה ולמידע על תהליך הכשל. הבדיקות מבוססות על ייזום מצבי כמעט-תאונה בתנאי מעבדה.

תיקוף המדריך

אפקטיביות המדריך נבחנה בשיתוף קבוצת עבודה של אילטם, בשיתוף אינקוזי. 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.