21 בינואר, 2014

פיתוח מדריך למניעת טעויות בתפעול מערכות

אבי הראל - מאמר בכנס האגודה הישראלית לארגונומיה – פברואר 2014

הסיבה העיקרית לתאונות באויר (כ-60%, סימוכין) בים (כ-80%, סימוכין) בנהיגה (כ-90%, סימוכין) ובתעשיה (60-80%, סימוכין) היא טעויות בתפעול ובשימוש במערכות.

טעויות אנוש מתייחסות אל מקרים של אובדן במהלך התפעול: תאונות, נזק לרכוש, ירידה בתפוקה, או עוגמת נפש של המשתמשים בציוד. בדרך כלל, האובדן נגרם כתוצאה מתפעול במצבים חריגים, כאשר הסיבות לחריגות הן מורכבות, ומאופיינות על ידי קשיים בתיאום בין המכונה לבין המשתמשים והמפעילים .

הנטייה הטבעית של חוקרי אירועי כשל, בעיקר תאונות, היא לייחס את הכשל לאדם שאיתרע מזלו והיה סמוך אליו ביותר במקום ובזמן, ושתיאורטית יכול היה למנוע אותו. אופן התחקור הנפוץ הוא על ידי הקמת וועדה אד-הוק, בתגובה לאירוע, שתפקידה למצוא גורמי כשל במונחים של התרשלות של בעלי תפקידים. מטרת הוועדות הללו היא להצביע על האחראים לכשל (כגון, הש"ג), על מנת למצות עימם את הדין.

על פי הגישה הפרואקטיבית אין להטיל את האחריות לתאונה על הגורם האנושי. במקום זאת, חשוב להשקיע את המשאבים הדרושים לשיפור התהליכים. במקום לעסוק ברשלנות ברמת הפרט, הגישה הפרואקטיבית עוסקת ברשלנות בתכן, ברמת תהליכי תפעול.

מרכז גורדון להנדסת מערכות בטכניון מקדם בשנים האחרונות יוזמות בתחום של בחינת דרכים למנוע טעויות אנוש בתפעול מערכות. מחקר החלוץ הראשון עסק באפיון התנהגות מערכות בתגובה לאירועים בלתי-צפויים, כגון, טעויות ספונטאניות של המפעילים, והגדיר עקרונות במניעה ובלימוד מטעויות (סימוכין). מחקר החלוץ השני עסק בתועלת של מערכות התרעה בנהיגה בכלי רכב, וכלל איפיון של טעויות בהבנת ההתרעות ובתגובה נכונה אליהן (סימוכין), וכן עקרונות ליישום מערכות התרעה בנהיגה. העקרונות הוצגו במסגרת כנס ITS (סימוכין).

בהמשך לשני מחקרי החלוץ הללו, המרכז מקיים לאחרונה מחקר שתכליתו פיתוח של מדריך לאבטחת חסינות מערכות. המדריך, המיועד למפתחי מערכות, אמור לסייע להם להבין את הגורמים לטעויות בתפעול, ולמנוע את גורמי הכשל. גירסא ראשונה של המדריך הוצגה בכנס INCOSE להנדסת מערכות בהרצליה (סימוכין). ככל הידוע לנו, מדריך זה הוא הראשון מסוגו בעולם.

שיטה

המדריך מבוסס על מודל של חסינות מערכות, שפותח אף הוא במסגרת מחקר זה. פיתוח המדריך נעשה על ידי שיפורים באיטרציות, כאשר השיפורים מבוססים על ניתוח אירועי כשל מהספרות, ועל משוב ממהנדסי מערכת וממהנדסי גורמי אנוש לגבי יעילות המדריך.

גירסאות ראשונות של המודל והמדריך אורגנו כדו"חות טכניים. אירועי הכשל מאורגנים במאגר אירועים שמוצג לכל דיכפין באינטרנט בכתובת
http://resilience.ergolight-sw.com/Event-DB/MishapDB-1.htm .
המשוב מהמהנדסים התקבל במסגרת קבוצת עבודה ייעודית שהוקמה לצורך זה במסגרת אילטם.

עד כה, קבוצת העבודה קיימה ארבע פגישות. במהלך המפגשים מוצגות בעיות עקרוניות באבטחת חסינות, הצעות לפתרון, ודיון בישימות ובתועלת שבהצעות הללו.

אחת הנקודות שעלו כבר בישיבה הראשונה של קבוצת העבודה היתה המורכבות של ההנחיות, שמקשה על השימוש בהן. לפתרון בעיה זו, פותחו גירסאות אינטראקטיביות של המודל ושל המדריך.

תוצאות

כל המידע על בעיית החסינות, מאגר אירועי הכשל, מודל החסינות, המדריך לאבטחת חסינות, קבוצת העבודה, דרך פעולתה, המשוב מחברי הקבוצה, ותהליך השיפור, מוצגים באופן שוטף באתר מיוחד שהוקם לצורך זה, בכתובת
/http://resilience.ergolight-sw.com .

מסקנות

המשוב מחברי קבוצת העבודה הוא בדרך כלל חיובי ביותר. חברי הקבוצה חושבים שהנושא חשוב, שהפתרונות אינם פשוטים, ושראוי להמשיך ולחקור את הנושא.

סיכום

לקראת סוף שנת 2014, בכוונתנו להציג גירסא ראשונה של המדריך באנגלית, המיועדת לקהילת מהנדסי מערכות העולמית.