10 באוגוסט, 2017

שילוב אדם מערכת – הלכה ומעשה

כתב: אבי הראל

כללי

בפיתוח מערכות מורכבות נדרשת מומחיות של מהנדסי מערכות ושל מהנדסי קוגניציה. השילוב בין שני סוגי המומחיות הללו הוא לעתים בעייתי. את הכשל של מערכות רבות, שמתבטא לעתים באסונות, ניתן לייחס לכשל בשילוב זה. הדוגמאות לכך רבות מספור, בתחום התחבורה, התעשיה הכימית, תעשיית האנרגיה, ציוד ביתי, מערכות מידע, תוכנות משרדיות ומערכות תקשורת. קיים צורך לנתח את גורמי הכשל ולהציג דרך להמנע מהם. חברת ארגולייט, בשיתוף עם מרכז גורדון להנדסת מערכות בטכניון פיתחה בשנים האחרונות מודל ומתודולוגיה המאפשרים למפתחי מערכות לצמצם את הסיכונים בגין בעיות בשילוב אדם-מערכת.

גורמי כשל בשילוב אדם מערכת

באופן טיפוסי הבעיה היא שמהנדס המערכת מסתמך על הנחות שגויות לגבי יכולת המשתמשים והמפעילים, ומהנדס הקוגניציה אינו מכיר את פרטי התכן, ואינו מודע לשגיאות שעושה מהנדס המערכת.

בעיה נוספת נובעת מכך שהנושא של גורמי אנוש בהנדסת מערכות נמצא עדיין ברמה של הצהרת כוונות, והוא חסר עדיין ברמה הפרקטית. עדיין אין מסורת ומתודה סדורה של הגדרת דרישות וקריטריונים לאיכות בשימוש ובתפעול, שצריכות לכוון את מהנדסי הקוגניציה. באופן טיפוסי, מפרטי המערכות אינם כוללים הנחיות בנוגע למדדי ביצוע שונים, ולשימוש בהם להגדרת קריטריונים לאבטחת איכות התפעול. הקריטריונים להם הנדסי הקוגניציה נדרשים צריכים להתייחס למהירות ביצוע ולרמת הטעויות המותרת בשלבים השונים של רכישת מיומנות בתפעול. זאת, כאשר הדרישה למהירות ביצוע נוגדת את הדרישה למניעת טעויות. כמו כן, במפרטי המערכת חסרה בדרך כלל התייחסות להתאמה לתפקידי המפעיל השונים: הזנת נתונים, בקרה, תחזוקה, בדיקות וכיו"ב.

בעיה נוספת קשורה לשיטות המקובלות לניתוח גורמי הכשל ולמניעתם. באופן מסורתי, הניתוח מתייחס לאירועי כשל צפויים, ברמת הטריגר. הניתוח מתבצע בשיטות של עץ תקלות, HAZUP, FMEA וכיו"ב. המניעה היא בדרך של אבטחת איכות ברמת הרכיבים ובדיקות ברמת המערכת. הנדסת מערכת אינה עוסקת בנושא הבעייתי יותר, של אופני התמודדות המפעיל עם אירועי כשל. בין היתר, הנדסת מערכות עוסקת גם בנושאים של חסינות מערכות, אבל השיטות לאבטחת חסינות מתמקדות באירועי כשל פשוטים וצפויים. הנדסת מערכות מסורתית אינה מתמודדת עם מצבים שנחשבים לבלתי צפויים, בגין שילוב של מספר גורמי כשל שסבירותם נמוכה, ועם בעיות של התמצאות המפעיל במצבים הללו.

בעיה נוספת נובעת מכך שהנדסת קוגניציה עדיין לא הגיעה לבשלות. דיסציפלינה זו מבוססת על בסיס ידע נרחב של מדעי הקוגניציה, אבל ידע זה עדיין אינו מתורגם לכללים הנדסיים ברי תוקף. ביחוד, מורגש מחסור בקריטריונים להתאמת ממצאי מחקר במדעי הקוגניציה לסיטואציה שונות בתפעול ושימוש במערכות. דוגמא בולטת למחסור זה היא הנושא של התאמת ממשק התפעול למאפיינים של תפקיד המפעיל, כגון עומס התפקיד, על פי תכונות קוגניטיביות כגון קיבול הזכרון לטווח הקצר, על פי תיאוריות של ניהול משאבים מנטאליים וכישורים פסיכומוטוריים.

והבעיה שלשמה התכנסנו, אופן השילוב בין הדיסציפלינות, גם היא לוקה בחסר. שילוב בין הדיסציפלינות פירושו הגדרת תפקידים והקצאתם למכונה ולמפעילים, ואופן זרימת המידע בין האדם למכונה. שילוב זה חסר במודלים של הדיסציפלינות הרלבנטיות. המודל של הנדסה קוגניטיבית הוא של תפיסה, תהליכים מנטאליים וביצוע, כאשר המכונה היא בבחינת קופסא שחורה. המודל של הנדסת מערכות הוא של קלט, תהליך עיבוד ופלט, כאשר האדם נמצא בחוץ, בבחינת חידה. המפעיל אמור להבין את כוונת המתכנן, לזכור פרטים טכניים הקשורים ליישום, ולדעת ליישם את הידע בסיטואציות בלתי צפויות. שני המודלים, המערכתי והקוגניטיבי, אינם עומדים במבחן המציאות, מכיוון שהם אינם מתייחסים אל ההשפעה ההדדית במצבים חריגים.

במצב הנוכחי של חוסר בשלות בשתי הדיסציפלינות, מי שקובע למעשה את איכות השילוב זהו מהנדס התוכנה, שנדרש לעצב אינטראקציה על בסיס דרישות חלקיות ומעורפלות. התוצאה תלויה בכישורים ובנסיון של מהנדס התוכנה. האחריות לפעול על פי הגחמות (הנטיות האישיות והנסיון האישי) של מהנדס התוכנה מוטלת על המפעיל, והוא לפעמים טועה, בין בפעולה ובין בזיהוי מצב המכונה. בפרקטיקה, חסרות הגדרות של טעות, אחריות ואחריותיות. הנטיה הטבעית של בעלי התפקידים היא לחפש את גורם הכשל במישור האישי. נטיה זו היא הרסנית בהיבט של הפקת לקחים ממצבי כשל או כמעט כשל. בהעדר הגדרות כאלו, לא ניתן למנוע את הטיית הדיון לנתיב האשמה.

מתודולוגיה לחסינות מערכות בפני טעויות תפעול

חברת ארגולייט, בשיתוף עם מרכז גורדון להנדסת מערכות בטכניון (קרי, ד"ר אביגדור זוננשיין) פיתחה בשנים האחרונות מודל ומתודולוגיה המאפשרים למפתחי מערכות לצמצם את הסיכונים בגין בעיות בשילוב אדם-מערכת.

מודל החסינות מבוסס על האבחנה שכשל מקורו בצירוף אירועים שהסתברותם נמוכה, ושקיים קשר הדוק בין מצבי כשל לבין תפעול במצבים חריגים. מודל החסינות כולל תיאור של תגובה לאיומים שמקורם בהפרעות, שמאפשרת למערכת לסכל את האיום ולהתאושש ממנו. סיכול האיום מבוסס על זיהוי המצבים החריגים, והנחיית המפעיל כיצד לפעול בתנאים שאינם מוכרים לו. המודל כולל תיאור של תכונות המעניקות למערכת יכולת חסינות במצבים כאלו.

בבסיס המתודולוגיה לאבטחת חסינות עומד הרעיון של הגנה בשכבות המתייחסות לשלבים השונים של התפתחות האיום על פי המודל: מניעת הפרעה, תיקון אוטומטי או מבוקר, גילוי מצבי איום, התרעות למפעיל, הכוונה בתהליך איתור תקלות, תפעול במצבי חירום וכיו"ב. בנוסף, המתודולוגיה כוללת גם התייחסות לאירועים בלתי צפויים, הנשענת על רעיון הבקרה העצמית של מערכות, כאשר המפעיל נמצא בחוג הבקרה. ההנחה, שהיא ואריאציה של חוק מרפי, היא שאם התכן מאפשר למפעיל לטעות, במוקדם אם במאוחר הוא אכן יטעה, ולכן התכן צריך למנוע את האפשרות לטעות. המימוש הוא על ידי הכללה של חוקי התפעול בבסיס ידע שמשמש למעקב אחר הפעילות, ולבדיקה שהפעילות נעשית על פי חוקי התפעול. המתודולוגיה כוללת כללים ושיטות להתנהלות תקינה במקרה של מצבים חריגים, וכן ארכיטקטורה לניהול תהליך התגובה לאיומים.