מניעת טעויות בתפעול מערכות

אבי הראל*

בכתבה זו אסקור גישות מקובלות במניעה ובהתמודדות עם טעויות תפעול, ואציג גישה חדשנית לאבטחת חסינות מערכות בפני טעויות אלה.

בכל מערכת יש נקודות תורפה

הגורם העיקרי לתאונות בתעשייה הוא טעויות בתפעול ובשימוש במערכות.

מעל 60% מהתאונות מיוחסות בדיעבד לטעות של המפעיל. המושג "טעות תפעול" מתייחס אל פעילות של המפעילים במקרים בהם הפעילות מסתיימת באבדן: תאונות, נזק לרכוש, ירידה בתפוקה, או עוגמת נפש של המשתמשים בציוד. האובדן נגרם בדרך כלל כתוצאה מתפעול במצב חריג של המערכת. לעתים קרובות, הסיבות לחריגות הן מורכבות ומאופיינות על ידי קשיים בתיאום בין המכונה לבין המשתמשים והמפעילים. חוק מרפי (בגירסתו הקלאסית) בהנדסת מערכות גורס, שבכל מערכת יש נקודות תורפה, והכשל הוא תוצאה בלתי נמנעת של שימוש במערכת לאורך זמן. בתמצית, חוק מרפי קובע שבכל מקרה בו תכן המערכת כולל ליקוי שעדיין לא התגלתה, הליקוי יתגלה יום אחד באופן בלתי צפוי, והתוצאות עלולות להיות טראגיות. הבסיס לגרסת גורמי אנוש של חוק

מרפי הוא בתחום הפסיכולוגיה הקוגניטיבית. המפעילים אינם מכונות. הם אנשים, בשר ודם. יש להם יתרון על פני המכונה בפתרון בעיות במצבים חריגים, אבל הם אינם מדויקים בתפקודם. במצבים מסוימים, כגון בתנאי לחץ, הם נוטים לטעות.

קשה למנוע תאונות. קל יותר להגיב לתאונות, ולהסיק מסקנות לאחר מעשה. בגישה הריאקטיבית, הדגש אינו על מניעה, אלא על תגובה. כללית, ניתן לזהות שני אופנים של תגובה: הסקת מסקנות בגישה הפופוליסטית: הדרך הקלה היא על ידי הסקת מסקנות אישיות: חיפוש אשמים, והענשתם. ההליך של חיפוש אשמים מקובל, מכיוון שהציבור מבקש להשתכנע שהמערכת עושה ככל יכולתה בכדי למנוע את התאונה הבאה. הציבור אינו מתמצא בתהליכי התפעול המורכבים, ולכן הוא בא על סיפוקו מהידיעה על תהליך של הסקת מסקנות אישיות. התאונה הבאה, תתרחש בנסיבות שונות, יהיו מעורבים בה מפעילים אחרים, והתוצאות תהיינה שונות. הציבור אינו מודע לכך שהענשת המעורבים בתאונה הספציפית אינה תורמת מאום למניעתה של התאונה הבאה, שתהיה שונה בתכלית. הפקת לקחים: הדרך הקשה יותר, והמשמעותית יותר לנושא של מניעת תאונות, היא כאשר המסקנות כוללות הפקת לקחים ושיפור תהליכי התפעול.

המפעיל כקורבן התאונה

הנטייה הטבעית של חוקרי אירועי כשל, בעיקר תאונות, היא לייחס את הכשל לאדם שאיתרע מזלו ובזמן האירוע היה סמוך ביותר אל מקום התאונה. בדרך כלל, זהו המפעיל. אופן התחקור הנפוץ הוא על ידי הקמת וועדה אד–הוק, שתפקידה לזהות גורמי כשל ולנסח אותם במונחים של התרשלות בעלי תפקידים. המנדאט הפורמאלי של הוועדה הוא להצביע על האחראים לכשל, אבל בפועל, במקרים רבים, חברי הוועדה ממונים על ידי האחראים על הבטיחות בארגון. במקרים חריגים, המינוי נעשה על ידי גופים ציבוריים, תוך התייעצות עם האחראים בארגון. בכל מקרה, לחברי הוועדה יש נטייה להגן על האינטרסים של האחראים על הבטיחות. נטיית הלב שלהם היא לנקות את האחראים על הבטיחות מכל אשמה, ולהטיל את האחריות על המפעילים, על מנת למצות עימם את הדין. העמדת הש"ג לדין נועדה לשרת שתי מטרות: מטרה אחת היא לרצות את הציבור. הציבור רוצה לראות את המערכת מנקה את עצמה, כדי שמקרים כאלה לא יקרו בשנית. לציבור לא ברור כיצד המערכת יכולה לנקות את עצמה, ולכן הוא מבקש שהאחראים למחדל יוצאו מן המערכת.

מטרה שנייה היא לחפות על ההנהלה, שלא הצליחה למנוע את הכשל. לציבור לא ברור מיהם האחראים למחדל, והוא סומך על ועדת הבדיקה. הציבור אינו מודע לכך שחברי ועדת הבדיקה הם נציגיהם של האחראים למחדל, והמסקנות שהם מסיקים נועדו לחפות עליהם. הציבור מקבל את המסקנה שהש"ג אשם. אופן הפעולה של וועדות הבדיקה כולל איסוף עדויות ונתונים לגבי הפעילות של המפעילים שהיו נוכחים בשטח בזמן התרחשות התאונה, ולהצביע על דרכים בהם המפעילים יכלו לנקוט בכדי למנוע את האירוע המביך. משנמצאה דרך כזו, המפעיל הופך להיות קורבן של התאונה. חוקרי האירוע נוטים להתעלם מכך שהמפעיל לא היה מודע למצב הסיכון, או לא זכר את תהליך התפעול המאפשר להתמודד עם הסיכון. בחכמה לאחר מעשה, המסקנה השכיחה היא שהמפעיל לא הכיר היטב את תהליכי התפעול, ולכן אפשר להאשים אותו ברשלנות. חברי הוועדה מתעלמים מהכלל הידוע שלטעות זה אנושי, ושהענשת המפעילים אינה תורמת מאום למניעת הטעויות שהם עושים.

הגישה הפופוליסטית לעומת הגישה ההנדסית

מחקרים שנערכו בשנים האחרונות מראים שככלל, הגישה הפופוליסטית מזיקה יותר מאשר מועילה לבטיחות: עריפת ראשים בדרגות הנמוכות לא רק שאינה תורמת לפתרון הבעיה, אלא אף מעצימה ומחריפה אותה: במקרה של

*מומחה ארגונומיה באבטחת חסינות מערכות, בטיחות וגיהות

תאונה, האנשים שהיו מעורבים בה, גם אם הם בטוחים בחפותם, מנסים לטשטש ולהעלים ראיות, מכיוון שהם יודעים שוועדת החקירה מחפשת עדויות במטרה להאשים את הש"ג. במקום לתרום לשיפור תהליכי התפעול, הגישה הפופוליסטית מביאה למצב של חוסר אמון של העובדים בהנהלה וממוני הבטיחות. התוצאה היא חוסר נכונות של העובדים לשתף פעולה בתחקור מצבי כשל. העובדים אינם מדווחים על טעויות שהם עושים בתום לב, מתוך חשש שדיווחים אלו יביאו להאשמתם ברשלנות. המחקרים מצביעים על הצורך בהבחנה בין מקרים של נזק שנגרם כתוצאה ישירה של כוונת זדון או רשלנות, לבין מקרים של כשל בתום לב, הנובע מהצורך לפעול בתנאי אי–וודאות, בלחץ זמן. העיוות בשיטה של האשמת המפעילים בולט לעין, אבל לציבור אין כלים לבחון אותה. המחקר על תאונות בינלאומיות מצביע על כך שהעיתונות נוהגת לפרסם את הגירסה של האחראים על המחדל. אין לעיתונאים מקורות שיאפשרו להם לזהות את האחראים למחדל, שבמסגרת תפקידם היו צריכים לדאוג לשיפור הבטיחות. חוקרי תאונות ידועי שם הצביעו על הצורך בחקיקה שתסדיר את מינוי וועדות הבדיקה על ידי גורמים שאינם שותפים לאחריות על הבטיחות, ושתגביל את המנדאט של ועדות הבדיקה ותחייב אותן לעסוק אך ורק בדרכים למניעת הישנות מקרי הכשל. החקיקה צריכה להבטיח שחברי וועדות הבדיקה אינם מייצגים את האינטרסים של הממונים על הבטיחות. בנוסף, החקיקה צריכה לאסור על וועדות הבדיקה להצביע על אשמים ברמת הפרט, למעט במקרים של חבלה בזדון. כך, לדוגמה, חוק התעופה האווירית של נורווגיה אוסר על שימוש במידע שהתקבל בוועדות הבדיקה למטרת הרשעת המעורבים בתאונה. חקיקה כזו מאפשרת יצירה של אקלים בטיחות, בו עבודת הוועדות מתמקדת בחיפוש דרכים לשיפור הבטיחות.

גישה מעשית למניעת מצבי תאונה זוהי הגישה ההנדסית, העוסקת בשיפור חסינות המערכת. הענשת המפעילים אינה יכולה למנוע את הטעויות שהם עושים. לכן, במקום להעניש את המפעילים, עדיף לתכנן את המערכת כך שתהיה חסינה לטעויות התפעול. הגישה ההנדסית מבוססת על הגישה הפרואקטיבית, הדוגלת במניעת מצבי תפעול שמאפשרים את התאונה. זאת, בניגוד לגישה הפופוליסטית, שעוסקת במציאת אשמים למצב התאונה. במקום לעסוק ברשלנות ברמת הפרט, הגישה ההנדסית עוסקת ברשלנות בתכן, ובהגדרת תהליכי תפעול. דוגמה ליישום הגישה ההנדסית היא התקן ת"י 18200 "ניהול מערכות התרעה בתעשייה התהליכית" שאושר לפני למעלה משנתיים.

חסינות בפני טעויות תפעול

חסינות המערכת זוהי היכולת להמשיך ולפעול במצבים חריגים, אליהם המערכת מגיעה כתוצאה מאירועים חריגים. החסינות של מערכת נקבעת על ידי התגובה האוטומטית (של המכונה) להפרעות, ועל ידי האינטראקציות בין מרכיביה כאשר המערכת נמצאת תחת איומים (הפרעות שלא נפתרו אוטומטית). החסינות נקבעת על ידי איכות תכן המערכת בהיבטים של מניעת אירועים חריגים, התמודדות עמם בזמן התפעול, והפקת לקחים במצבי כשל.

אבטחת חסינות מערכות: גירסת גורמי אנוש לחוק מרפי מעבירה את מוקד הדיון מעיסוק באחריות האישית ברמת הפרט לעיסוק באחריות של הארגון. למעשה, היא מטילה את האחריות למניעת תאונות על יצרני הציוד, ועל הנהלת הארגון המתפעל את הציוד. מרכז גורדון להנדסת מערכות בטכניון מקדם בשנים האחרונות יוזמות למציאת דרכים למנוע טעויות אנוש בתפעול מערכות. מחקר החלוץ הראשון עסק באפיון התנהגות מערכות בתגובה לאירועים בלתי–צפויים, כגון, טעויות ספונטניות של המפעילים, והגדיר עקרונות במניעה ובלימוד מטעויות. מחקר המשך היה בנושא ניהול הסיכונים בגין טעויות תפעול, כולל ניתוח התועלת של מערכות התרעה במניעת טעויות בנהיגה בכלי רכב.

את חסינות המערכת ניתן להשיג בשתי דרכים: בפיתוח המערכת: על ידי תכן לאבטחת חסינות בשלב התפעול: על ידי הנחיות מנהליות. תכן לאבטחת חסינות: הפרעה שנוצרת במצב חריג היא בלתי צפויה, ולפיכך היא הופכת אוטומטית לאיום, שמחייב את התערבות המפעיל. אתגר התכן לחסינות הוא לצמצם את הסיכונים בגין האירועים החריגים. ניתן להביא לשיפור החסינות על ידי תכן, שמיועד למטרות הבאות:

מניעה: יישום שיטות למניעת אירועים ומצבים חריגים. תגובה נכונה לאירועים חריגים: יישום שיטות להבטיח איתור מצבים חריגים, מניעת הסלמה, התרעה לגבי המצבים הללו, ותהליכי התאוששות. המוטיבציה לפירסום העקרונות לאבטחת החסינות נובעת מהרצון להתגבר על הטבע האנושי, לחפש מתחת לפנס. בנושא הנדסת מערכות, טבע זה מתבטא בנטייה לעסוק בנושאים טכניים, ולהזניח את הגורם הקריטי לחסינות, דהיינו, מגבלות המפעיל. להלן רשימה של עשרה עקרונות המנחים את מפתחי המערכות בתהליך הגדרת הדרישות.

עקרונות באבטחת חסינות

1. עקרון המלחמה בביש המזל: עקרון המלחמה בביש המזל אומר שאין להניח ליד המקרה את האפשרות לכך שהמערכת תיכשל. בתהליך הפיתוח צריך להיערך לקראת מצבים בעייתיים במהלך התפעול, כולל המקרה שהמפעיל אינו זמין, ולוודא שהתכן נותן להם מענה ראוי.
2. עקרון הבקרה העצמית: עיקרון זה מבוסס על המודל האילוצים של ננסי לבסון (STAMP) המגדיר את החסינות כאילוץ המערכת לפעול בהתאם לכללים קבועים מראש, כגון, חוקי סינכרון בין המכלולים ופרוטוקולי תקשורת.
3. עקרון המלחמה בטעויות אנוש: טעויות אנוש הן תוצאה של רשלנות בתכן המכונה או במימוש. את חלקן ניתן למנוע, וכנגד האחרות, אפשר להיערך, באופן שהנזק בגינן יהיה מיזערי.
4. אימון לתפעול במצבים חריגים: תרגול מצבים חריגים נדרש על מנת לאפשר למפעיל להתנסות במצבי חירום בזמן רגיעה, לפתח רפלקסים שיאפשרו תגובה ההולמת את האיום.
5. עקרון אחריות המפתח: התכן צריך להתחשב בכך שהמפעיל אינו מסוגל לעקוב תמיד באופן מדויק אחר מצב המכונה, ושהוא עלול לפעול בדרך שאינה הולמת את המצב.
6. אבטחת שלימות התכן: אירועי כשל רבים הם תוצאה של פעילות מערכת במצבים בלתי צפויים. התכן צריך להתייחס להתנהגות המערכת בכל המצבים האפשריים.
7. תכן ממוקד מפעיל: יש להבטיח שהמשתמש תופס את התנהגות המכונה (מודל המשתמש) באותו אופן שאליו מתכנן המכונה התכוון (מודל המפתח).
8. הפחתת העומס המנטאלי: התכן צריך להתחשב במגבלות הקשב, ולמנוע הסחה מהמטלות העיקריות של המפעיל.
9. תיקוף ואימות: התיקוף והאימות של חסינות המערכת צריכים להיות כאשר המערכות מאוישות, בתנאי הפעלה אמיתיים, תוך שימוש בסימולציה לצורך תיקוף התפעול בתנאים חריגים.
10. עקרון אחריות הארגון: אבטחת החסינות צורכת משאבי כסף וזמן פיתוח. עקרון אחריות הארגון אומר שהארגון צריך להגדיר את התנאים בהם מפעילים יוכלו להתמודד עם מצבים חריגים. ■