אבטחת איכות תפעולית: בין הכסאות

אבי הראל
ארגולייט בע"מ
גבעון 6, חיפה 34335
טל' 054-453-4501, avi.1@ergolight-sw.com

קלות ואמינות התפעול הם מרכיבים קריטיים של איכות מוצרים ומערכות. כ-10% מהפעולות של מפעילי מערכות ותהליכים הן בטעות. למרבית הפעולות השגויות המפעיל אינו מודע כלל, ולכן תגובה המערכת אליהן היא בלתי צפויה. כמחצית מזמן התפעול מתבזבז על הבנת ההתנהגות הבלתי צפויה של המוצר. היחס בין זמן התפעול המוצלח לבין הזמן המבוזבז הוא כ-1, בסדרי גודל נמוך יותר הערכים שנחשבים לסבירים עבור היחס MTBF ל-MTTR. למרות זאת, התהליכים המקובלים לאבטחת איכות מוצרים ותהליכים מתעלמים מבעיית התפעול.

בתהליך אבטחת איכות מוצרים ותהליכים, אנחנו מניחים שהמערכת תכשל בכל דרך אפשרית, ואנו מבקשים לוודא שהמערכת תשרוד את כל הכשלים, ותתאושש מהם תוך זמן סביר. באופן דומה, הנחת העבודה בתכנון ממשק הפעלה צריכה להיות שהמפעיל יעשה כל טעות אפשרית, והאתגר הוא להבטיח את תכונת השרידות וההתאוששות של המערכת.

באופן מסורתי, האחריות על הגדרת ממשקי ההפעלה של מערכות ותהליכים מוטלת על מומחים בתחום הנדסת גורמי אנוש, ובעיקר, אנשי שימושיות. הבעיה היא שמומחי שימושיות, ביחוד בעידן האינטרנט, נוטים להתמקד במאפיינים של קלות ההפעלה, ביחוד לשלבי הלימוד הראשוניים. מרבית זמנם מומחי השימושיות עוסקים בתהליכי הפעלה ראשוניים, תוך התעלמות מהבעייתיות של טעויות תפעול. כך, לדוגמא, למרות שחברת מיקרוסופט מעסיקה עשרות רבות של מומחי שימושיות בפיתוח מוצריה, כל מוצרי הקו הראשון שלה לוקים בתחום המיגון בפני כשל תפעולי. נושא ההגנה בפני כשל תפעולי נופל בין הכסאות.

תהליך אבטחת איכות תפעולית הינו חלק בלתי נפרד מתהליך אבטחת איכות המוצר או התהליך, עם חפיפה ניכרת בשיטות ובישומן. התהליך כולל ארבעה שלבים: תכנון, ביצוע, בדיקות ושיפור (PDCA). המאמר מציג את הצורך לשלב את נושא התפעול בתהליך אבטחת האיכות.

המטרה של שלב התכנון באבטחת איכות התפעול דומה לזו שבאבטחת איכות המוצר או המערכת: בשני המקרים אנחנו מבקשים לוודא שכל אופני הכשל אותרו והוגדרו במפרטים, ושהמפרטים כוללים תיאור של התנהלות המערכת במקרים של כשל. האתגר של אבטחת איכות התפעול בשלב זה הוא לנבא באילו אופנים המפעיל יכשל, ולהציע דרך לוודא שאופני כשל אלו אותרו, ושהמערכת שורדת אותם.

מבחינים בשני סוגי כשל תפעול: טעות מפעיל, כאשר המפעיל טעה בבחירת הפקד, ותקלות מדומות, כאשר הפקד שהמפעיל בחר הוא בהתאם לכוונתו, אבל תגובת המערכת אינה תואמת את ציפיותיו. גישה זו היא בעייתית, מכיוון שבעיות קריטיות בתפעול מערכות נמצאות בתחום האפור בין הנדסת מערכת לבין הגורם האנושי. בהקשר זה, התפקיד של מנהל האיכות הוא לתאם בין מהנדסי המערכת, מהנדסי התוכנה ומהנדסי גורמי אנוש, בנושאים של ניתוח תקלות, תהליכי איתור תקלות והגדרת דרכים למניעת הסלמה במקרים של תקלות.

הדרך המועדפת לטפל בכשלים היא על ידי המנעות ממצבי כשל. העקרונות להמנעות ממצבי כשל כוללים אוטומציה, צמצום המערכת, פישוט ממשק ההפעלה והגדרת תהליכים על פי תרחישים. במקרים מסויימים, אין לנו ברירה אלא לאפשר למפעיל לחרוג מהפעילות השגרתית, ולטעות. זאת, כשמדובר בפעולות חיוניות של המפעיל, כגון, לצורך פתרון בעיות תפעול, במיוחד במצבים בלתי צפויים, כאשר חייבים לאפשר למפעיל שליטה מלאה במערכת. מנהל האיכות נדרש לנקוט במספר אמצעים למקרים של פעילות מפעיל שהיא בלתי צפויה, כולל פרישת רשת בטחון למניעת הסלמה, ואמצעים ללמוד להכיר את אופני הכשל, לנתח אותם ולמנוע אותם בגירסאות עתידיות. המאמר מציג שיקולים ועקרונות באבטחת איכות התגובה במצבי תפעול חריגים.

איכות תפעולית

בתאריך 18 במרץ 1967 המיכלית טוריי קאניון עלתה על שרטון פולארד שנמצא מול החוף הדרום מערבי של אנגליה. כתוצאה מצירוף של מספר ארועים חריגים, המיכלית שייטה לעבר השרטון. קברניט הספינה ניסה ללא הצלחה להטות את הספינה מהשרטון, מכיוון שידית השליטה המאפשרת ניהוג ידני או אוטומטי הועברה בטעות למצב "בקרה" חריג, בו מערכת ההיגוי היתה מנותקת. היה זה האסון האקולוגי החמור

ביותר במאה שעברה. (http://en.wikipedia.org/wiki/Torrey_Canyon). אסון זה נגרם בגלל שני פגמים בתכנון המערכת, הקשורים לאיכות התפעול:

א. המערכת איפשרה לאנשי צוות המיכלית להעביר את ידית השליטה למצב ביניים, שמתאים לתפעול בזמן תחזוקה, אבל לא בזמן שיוט.
ב. המערכת לא התריעה לקברניט שהיא נמצאת במצב החריג.

בין הכסאות

המסמך ISO/IEC 9126-1 מגדיר איכות תוכנה על ידי שש תכונות, אחרת מהן היא השימושיות. האם אנחנו משקיעים מספיק בשימושיות? האם אנחנו מנסים לשפר אותה? כיצד? האם אנחנו דנים בכך בכנסים בנושא איכות? או, אולי אנחנו מעדיפים להשאיר את הנושא למהנדסי שימושיות? וכיצד אנחנו משלבים תהליך אבטחת שימושיות עם תהליך אבטחת איכות?

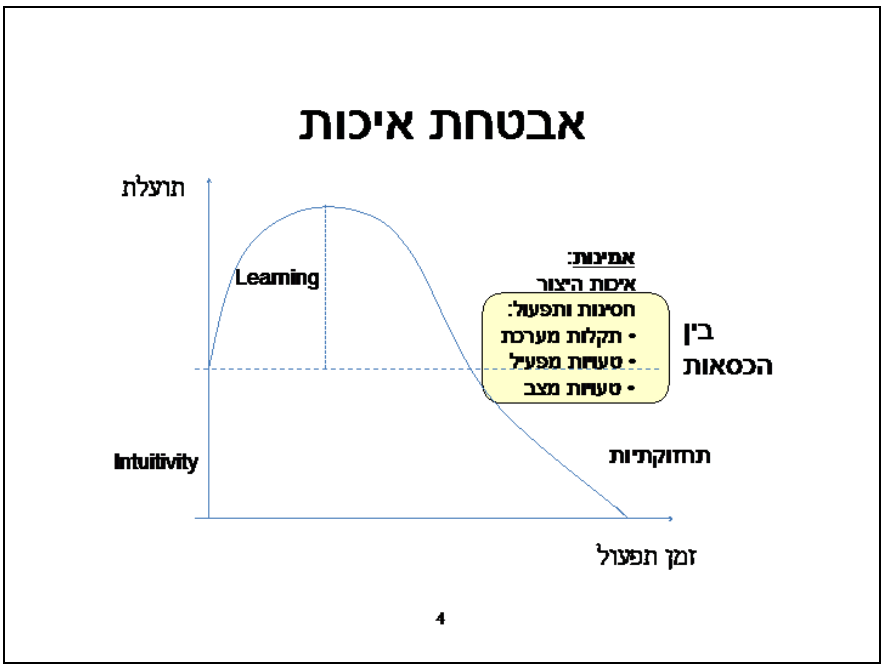
בתהליכי תכנון מסורתיים, הנדסת גורמי אנוש עוסקת בפרמטרים פיסיים של ממשקי ההפעלה. כך, למשל, בתכנון מערכת ההיגוי של מיכליות, זהו תפקידו של מהנדס גורמי אנוש לעצב את הגה הספינה כך שיהיה נוח לגישה ולתפעול במצבי הניווט השונים. באופן מסורתי, מהנדסי גורמי אנוש אינם מעורבים בתכנון לוגיקת ההפעלה, הם אינם מודעים למצבי ההפעלה החריגים. מפתחי מערכות אינם מודעים בדרך כלל לסכנות הכרוכות בתפעול במצבים חריגים, ואינם מצביעים בפני מהנדסי גורמי אנוש על מגבלות השימוש בתרחישים השונים. הם אינם מתודרכים לתכנן את מניעתם, ומהנדסי גורמי אנוש אינם מתודרכים להתריע עליהם.

מסקנות

א. תקלות מהסוג שהביא לאסון המיכלית, שנובעות ממצבים חריגים של המערכת, עלולות לקרות גם במערכות שאנחנו מפתחים כיום, במאה ה-21.
ב. להתמודדות עם תקלות מסוג זה, יש צורך לשלב את הנדסת גורמי אנוש בתהליכי אבטחת איכות המערכת

אבטחת איכות תפעולית

לעתים רחוקות אנחנו טורחים להגדיר באופן פורמלי את המושג "איכות". אחת ההגדרות המקובלות מתייחסת אל סך התכונות והמאפיינים שמאפשרים למערכת למלא אחר צרכי הלקוח (לדוגמא, ההגדרה ב-http://www.chesapeakebay.net/info/qa_glossary.cfm). בחיי היומיום המושג "איכות" מתייחס בדרך כלל לתכונות פונקציונליות, שניתן להתרשם מהן כבר במועד הרכישה של המערכת. כך, למשל, ה"איכות" של מערכת סטיראו נקבעת על ידי ההתרשמות שלנו מהצלילים שהיא מפיקה. בפרקטיקה, תהליכי אבטחת איכות מתייחסים להיבט צר של האיכות – להיבט של שימור האיכות לאורך זמן. כך, לדוגמא, אנחנו דואגים לכך שהרכיבים מהם מורכבת המערכת יפעלו כשורה לאורך זמן, על מנת להבטיח שקצב התקלות יהיה נמוך. התרשים הבא מתאר את מימדי האיכות במונחים של התועלת לאורך זמן:



התרשים מדגים את האפקט של גורמי איכות על התועלת לאורך זמן. התועלת הראשונית נקבעת על ידי הערך הפונקציונאלי ללקוח, על ידי השימושיות בהפעלה ראשונית – אינטואיטיביות ממשק ההפעלה, ועל ידי הקלות בה ניתן ללמוד להפיק מהמערכת את הפונקציונליות המירבית. שימור התועלת לאורך זמן קובע את אורך החיים של המערכת. כושר שימור התועלת נקבע על ידי גורמי אמינות ותחזוקתיות, גורמים שנקבעים בתהליכי אבטחת איכות מסורתיים. האיכות התפעולית מתייחסת אל כל הגורמים המשפיעים על תוספת התועלת אותה ניתן לייחס לקלות ההפעלה בשלב התפעול הראשוני ולשימור התועלת לאורך זמן - האמינות.

שימור התועלת לאורך זמן

הגורמים המשפיעים על התועלת לאורך זמן קשורים בתקלות. לשימור התועלת אנחנו משתדלים למנוע תקלות במידת האפשר, ובמקרה של תקלה, אנחנו מבקשים לצמצם את הנזקים. תהליכי אבטחת איכות מסורתיים עוסקים בעיקר בתקלות בחומר ובתוכנה. בנושאים הבאים, תהליכי אבטחת איכות קלאסית אינם מטפלים, והם נופלים בין הכסאות:

- התאוששות מתקלות מערכת
- תקלות תפעול – מניעת והתאוששות
- טעויות מצב – מניעה והתאוששות

באופן מסורתי, האחריות על הגדרת ממשקי ההפעלה של מערכות ותהליכים מוטלת על מומחים בתחום הנדסת גורמי אנוש, ובעיקר, אנשי שימושיות. הבעיה היא שבאילוצי תקציב, ביחוד בעידן האינטרנט, מומחי שימושיות נוטים להתמקד במאפיינים של קלות ההפעלה, בשלבי הלימוד הראשוניים. מרבית זמנם מומחי השימושיות עוסקים בתהליכי הפעלה ראשוניים, תוך התעלמות מהבעייתיות של טעויות תפעול. כך, לדוגמא, למרות שחברת מיקרוסופט מעסיקה עשרות רבות של מומחי שימושיות בפיתוח מוצריה, כל מוצרי הקו הראשון שלה לוקים בתחום המיגון בפני כשל תפעולי. מהנדסי גורמי אנוש עוסקים בדרך כלל בהיבטים פיסיים של נוחות גישה לפקדים והבנת התצוגות. בדרך כלל, הם אינם מודעים למרבית התקלות האפשריות במערכת, והם אינם מעורבים בתהליכי תכנון ההתאוששות מהם. מהנדסי המערכת נוטים להטיל את האחריות למנוע תקלות תפעול על המפעילים, ומהנדסי גורמי אנוש נאלצים לקבל זאת התכתיב, בגלל מגבלות תקציב. בנושא טעויות מצב, הנטיה היא לייחס מקרים כאלו כאל כוח עליון, צירוף מקרים שלא בשליטה. נושא ההגנה בפני כשל תפעולי נופל בין הכסאות.

מבחינים בשני סוגי כשל תפעול: טעות מפעיל, כאשר המפעיל טעה בבחירת הפקד, ותקלות מדומות, כאשר הפקד שהמפעיל בחר הוא בהתאם לכוונתו, אבל תגובת המערכת אינה תואמת את ציפיותיו. גישה זו היא בעייתית, מכיוון שבעיות קריטיות בתפעול מערכות נמצאות בתחום האפור בין הנדסת מערכת לבין הגורם האנושי. בהקשר זה, התפקיד של מנהל האיכות הוא לתאם בין מהנדסי המערכת, מהנדסי התוכנה ומהנדסי גורמי אנוש, בנושאים של ניתוח תקלות, תהליכי איתור תקלות והגדרת דרכים למניעת הסלמה במקרים של תקלות.

המשך המאמר מציג דוגמאות של כשל תפעולי, שנובע מהעדר מתודולוגיה למנוע אותו, ומכך שהנושא נופל בין הכסאות.

איכות ההתרעות

בטיסה 296 של חברת אייר פראנס, שנערכה בשנת 1988 במסגרת מפגן אוירי , המטוס לא הגיב לפקודת נסיקה והתרסק (http://en.wikipedia.org/wiki/Air_France_Flight_296). בניתוח הסיבות לתקלה דווח על שני פגמים באמינות מערכת הבקרה:

- OEB 19/1 – פגם בהאצת מנועים במצבים של טיסה בגבה נמוך
- OEB 06/2 – פגם במדידת גובה המטוס.

פגם שלישי, עליו לא הדוח לא הצביע, היה בשיטת הדיווח לטייס לגבי מצב המערכת. בשניות שלפני ההתרסקות, המנועים פעלו במוד של סיבובי סרק. במצב זה, המנועים לא הגיבו לפקודת הטייס. המטוס היה במצב חריג, אבל הטייס לא היה מודע למצב החריג. לו היתה מערכת הבקרה מתוכננת על פי עקרונות האמינות התפעולית, היא היתה מתריעה לטייס על המצב החריג, והטייס היה יכול להגיב בזמן.

זהו מקרה קלאסי של נפילה בין הכסאות. מהנדס המערכת מצפה ממומחי השימושיות לתכנן את ההתרעות תוך התחשבות בגורמי אנוש, אבל נכשל בהגדרת כל מצבי המערכת עליהם צריך להתריע.

תפעול במצבי תקלה

סופת ברקים ב-13 ביולי 1977 גרמה לתקלות במספר תחנות כוח, וכתוצאה מכך לעומס יתר בתחנות כוח אחרות באזור ניו-ג'רסי וניו-יורק. במשך שעה, המפעיל של מרכז הבקרה של קון אדיסון לא מצא כיצד להפעיל את התוכנה שמאפשרת לפזר את העומס בין תחנות הכוח, עד שלבסוף כל המערכת קרסה והעיר ניו-יורק שקעה בעלטה (http://en.wikipedia.org/wiki/New_York_City_Blackout_of_1977) .

זוהי דוגמא נוספת של נפילה בין הכסאות, כאשר מהנדסי המערכת דואגים לכך שהמערכת תאפשר להתאושש מתקלות, מהנדסי התוכנה מפתחים את ממשק ההפעלה שמאפשר זאת, אבל אינם מתחשבים במגבלת המפעיל הבלתי מיומן.

איכות המידע של התרעות במצבי חירום

ב-28 במרץ 1979, הליבה של יחידה 2 בתחנת הכוח הגרעיני "אי שלשת המילין" בפנסילבניה הותכה. תהליך איתור התקלה נמשך חמישה ימים. הקושי באיתור התקלה נבע מריבוי התרעות בלתי ממוקדות, בלתי רלבנטיות, שגויות ומטעות.

בתהליכי התכנון המסורתיים, מהנדסי המערכת היו אלו שתכננו את מערכת ההתרעות. הכלל היה פשוט: לכל אינדיקציה למצב חריג, מתריעים. הבעיה היתה שההתרעות לא הצביעו על מקור הבעיה. בעקבות ארוע זה הוכנסו מהנדסי גורמי אנוש לתהליכי התכנון של תחנות כוח, והוגדרו תקנים שיבטיחו את יעילות תהליכי איתור תקלות.

אמינות ההתרעות לגבי תקלות

דוגמא זו מוכרת היטב למרבית בעלי הרכב. הדוגמא היא של התחממות מנוע הרכב במצב של חוסר נוזל קירור. במקרים כאלו, האינדיקציה לגבי חום מנוע מטעה, מכיוון שמד החום מודד את חום נוזל הקירור, והמדידה אינה אמינה במצב של חוסר בנוזל הקירור. מדי יום, מאות מנועים ניזקים באלפי שקלים בגלל הטעיה זו.

בתהליכי התכנון המסורתיים, מהנדסי גורמי אנוש משולבים בתהליכי תיכון כולל עיצוב ההגה, ידיות הפיקוד, המושבים, לוח המחוונים ועוד. באופן מסורתי, מהנדסי גורמי אנוש אינם נחשפים ללוגיקה של ההתרעות, ולכן טועים בהבנת משמעות ההתרעות לגבי מהות התקלות בכלי הרכב.

אמינות המידע לגבי מצב ההתרעה

מערכת שהורכבה ממצלמות אינפרא-אדום וממרכז בקרה שימשה לאיתור חדירות למתקנים בטחוניים. המצלמות תוכננו כך שאיפשרו זיהוי תנועה ושיערוך של המרחק לנקודות חקירה. המחשב במרכז הבקרה התריעה קולית בכל מקרה של גילוי תנועה. המערכת נבחנה ואושרה לשימוש בבדיקת שימושיות קלאסית. במספר תרגילי בדיקת עירנות, התברר שמפעילי המערכת מגיבים לאט מדי, או שאינם מגיבים כלל. הבעיה אובחנה כבעיית איכות תפעולית. הסיבה למחדלי המפעילים היתה ריבוי התרעות לגבי תנועת בעלי חיים, כלי רכב שנעו באזור המתחם ושיחים שנעו ברוח. מהנדסי המערכת לא היו מודעים לצורך למנוע התרעות שווא, ומהנדסי השימושיות לא היו מודעים למצבים הבעייתיים שגורמים להתרעות הללו. גם כאן, האיכות התפעולית נפלה בין הכסאות.

מניעת טעויות מפעיל

לא מעט מנויים של חברת הכבלים מתקשים להשתלט על השלט ולצפות בטלוויזיה בגלל ההפעלה הדו-שלבית של השלט - ראשית עליהם להדליק את הטלוויזיה ולאחר מכן הם צריכים להפעיל את הממיר ולזפזפ בו לערוץ המבוקש. צופים רבים נתקעים בדרך, למרבה מבוכתם. שלט הממיר הדיגיטלי תוכנן כך שניתן להפעיל באמצעותו גם את הממיר וגם את מקלט הטלוויזיה על מנת לחסוך שימוש בשני שלטים. זאת, במטרה לאחד את השלט של הממיר עם שלט הטלוויזיה ולחסוך מהמשתמשים, לפחות באופן חלקי, את הרדיפה הבלתי פוסקת אחר אחד השלטים שאבד בנבכי הסלון. לשם כך מעצבי השלטים הוסיפו לשלט של הממיר את המקשים השימושיים ביותר של שלט הטלוויזיה, כולל כיבוי והפעלה, שליטה בעוצמת הקול, סקירה ובחירת תחנה. על מנת להמנע מהגדלת מימדי השלט, המפתחים הוסיפו לו שני מקשים חדשים, שמאפשרים מעבר בין מצב שליטה בטלוויזיה לבין מצב שליטה בממיר. ההנחה היתה כי למשתמש נוח להשתמש באותם מקשים כאשר מדובר בפונקציות דומות (כפתורי הערוצים משמשים גם למעבר ערוצים בטלוויזיה וגם בממיר הדיגיטלי), "כי הוא כבר רגיל אליהם". הנחה זו נראית סבירה והגיונית, ומשתמשים רבים מוכנים ללמוד את דרך הפעולה, ומפעילים את המערכת ללא קושי. משתמשים רבים אחרים, לעומת זאת, מתקשים לעקוב אחר מצב המערכת. כתוצאה מכך, הם טועים בכך שהם מכבים את הממיר הספרתי במקום את הטלביזיה, ובכך שבניסיון לשנות ערוץ בממיר הם מסיטים את הטלביזיה מערוץ הקליטה. המשמעות הפיננסית של בעיית השלט היא עלייה בלתי סבירה בהוצאות התפעול של חברות הטלוויזיה וירידה במכירות כתוצאה מחוסר שביעות רצון הלקוחות.

גם בדוגמא זו, מהנדסי גורמי אנוש היו שותפים בעיצוב הצורה, המקשים והתצוגות בשלט רחוק, אבל לא היו שותפים בהגדרת לוגיקת ההפעלה. בהנדסת גורמי אנוש קלאסית הדגש הוא על התמצאות בתהליכי הפעלה במצבים נורמליים, והדעת אינה ניתנת במידה מספקת למצבים של טעויות תפעול. גם בדוגמא זו, האיכות התפעולית נפלה בין הכסאות.

משמעות לתפוקה של תהליכי יצור

מערכת יצור מבוקרת GUI מאפשרת למפעיל לשלוט במספר פרמטרים של מספר קווי יצור. התיכנון התבסס על ארכיטקטורת SOA, כאשר מכונות ומרכיבים אחרים מיוצגים על ידי אובייקטים, הפרמטרים מיוצגים על ידי התכונות של האובייקטים והפעולות שמתבצעות על המכונות מיוצגות על ידי שיטות שמגדירות את השירותים. ממשק המשתמש כלל מסך יעודי לכל אובייקט, שאיפשר למפעיל להציב ערכים לכל התכונות ולהפעיל את כל השירותים.

מפעילים רבים סברו שהתכנון הוא לוגי. למרות זאת, קרה לעתים קרובות שכששינו את קו היצור, הם שכחו להציב את כל הפרמטרים הרלבנטים לקו היצור החדש. לפיכך, כדי להבטיח שכל הפרמטרים הוצבו כנדרש, בכל שינוי של קו היצור, הם נאלצו לפני תחילת היצור לבדוק את תקינות התהליך בדרך של ניסוי. תהליך זה ייקר את עלות היצור וגרם להפסדים. בהמשך, המפעילים הגדירו טופס פרמטרים של כל תהליך יצור, ובגירסת השידרוג, הם מימשו את הטופס בתוכנה, והוזילו בכך את עלויות היצור.

מהנדסי השימושיות עזרו בעיצוב מסכי ממשקי ההפעלה, וכן ביצעו ניסויי שימושיות עבור תהליכי יצור עיקריים. בדיקת השימושיות של המעברים בין תהליכי היצור היתה יכולה ללא ספק לאתר מראש את המצבים של טעויות מפעיל בהצבת הפרמטרים, ולמנוע את ההפסדים בגירסא הראשונה. גם בדוגמא זו, ההפסדים נבעו מכך שהאיכות התפעולית נפלה בין הכסאות.

תהליך אבטחת איכות תפעולי

בתהליך אבטחת איכות מוצרים ותהליכים, אנחנו מניחים שהמערכת תכשל בכל דרך אפשרית, ואנו מבקשים לוודא שהמערכת תשרוד את כל הכשלים, ותתאושש מהם תוך זמן סביר. באופן דומה, הנחת העבודה בתכנון ממשק הפעלה צריכה להיות שהמפעיל יעשה כל טעות אפשרית, והאתגר הוא להבטיח את תכונת השרידות וההתאוששות של המערכת.

תהליך אבטחת איכות תפעולית הוא חלק בלתי נפרד מתהליך אבטחת איכות המוצר או התהליך, עם חפיפה ניכרת בשיטות ובישומן. התהליך כולל ארבעה שלבים: תכנון, ביצוע, בדיקות ושיפור (PDCA).

המטרה של שלב התכנון באבטחת איכות התפעול דומה לזו שבאבטחת איכות המוצר או המערכת: בשני המקרים אנחנו מבקשים לוודא שכל אופני הכשל אותרו והוגדרו במפרטים, ושהמפרטים כוללים תיאור של התנהלות המערכת במקרים של כשל. האתגר של אבטחת איכות התפעול בשלב זה הוא לנבא באילו אופנים המפעיל יכשל, ולהציע דרך לוודא שאופני כשל אלו אותרו, ושהמערכת שורדת אותם.

הדרך המועדפת לטפל בכשלים היא על ידי המנעות ממצבי כשל. השיטות להמנעות ממצבי כשל כוללות אוטומציה, צמצום המערכת, פישוט ממשק ההפעלה והגדרת תהליכים על פי תרחישים. במקרים מסויימים, אין לנו ברירה אלא לאפשר למפעיל לחרוג מהפעילות השגרתית, ולטעות. זאת, כשמדובר בפעולות חיוניות של המפעיל, כגון, לצורך פתרון בעיות תפעול, במיוחד במצבים בלתי צפויים, כאשר חייבים לאפשר למפעיל שליטה מלאה במערכת. מנהל האיכות נדרש לנקוט במספר אמצעים למקרים של פעילות מפעיל שהיא בלתי צפויה, כולל פרישת רשת בטחון למניעת הסלמה, ואמצעים ללמוד להכיר את אופני הכשל, לנתח אותם ולמנוע אותם בגירסאות עתידיות.

הדרך המקובלת לבדיקות תפעול היא על ידי אבי טיפוס של ממשקי ההפעלה. לבדיקת התועלת בשלב הראשוני נהוג לבצע בדיקות שימושיות, שמתבצעות בעזרת מומחי שימושיות. בדיקות אלה אינן משתמשות לבדיקת מצבי תקלה למיניהן. בתהליכים המקובלים בתעשיה, אבי הטיפוס משמשים להדגמת אופן השגת הפונקציות העיקריות, אך לא לבדיקת תקלות תפעול או לבדיקת התפעול במקרים של תקלות מערכת. לאבטחת איכות התפעול יש צורך להרחיב את אופן השימוש באבי-טיפוס כך שהם יאפשרו יזום של מצבי תקלה צפויים ובלתי צפויים, על מנת לבחון את עמידות המערכת בפני התקלה ואת תהליך ההתאוששות.

סיכום

הגורמים המשפיעים על התועלת לאורך זמן קשורים בתקלות. כ-10% מהפעולות של מפעילי מערכות ותהליכים הן בטעות. למרבית הפעולות השגויות המפעיל אינו מודע כלל, ולכן תגובה המערכת אליהן היא בלתי צפויה. כמחצית מזמן התפעול מתבזבז על הבנת ההתנהגות הבלתי צפויה של המוצר. היחס בין זמן התפעול המוצלח לבין הזמן המבוזבז הוא כ-1, בסדרי גודל נמוך יותר הערכים שנחשבים לסבירים עבור היחס MTBF ל-MTTR.

לשימור התועלת אנחנו משתדלים למנוע תקלות במידת האפשר, ובמקרה של תקלה, אנחנו מבקשים לצמצם את הנזקים. תהליכי אבטחת איכות מסורתיים עוסקים בעיקר בתקלות בחומר ובתוכנה. בנושאים הבאים, תהליכי אבטחת איכות קלאסית אינם מטופלים, והם נופלים בין הכסאות:

- התאוששות מתקלות מערכת – במאמר זה בחנו את תאונת מטוס 320A בטיסת איירפראנס 296 בשנת 1988, את המקרה של קריסת מערכת אספקת החשמל לעיר ניו-יורק בשנת 1977 ואת פרשת היתוך הכור בפנסילבניה בשנת 1979 להדגמת הצורך באבטחת איכות התפעול במקרים של תקלות מערכת. כמו כן ניתחנו את איכות ההתרעה לגבי חום מנוע כאשר מדידת החום מתבצעת לגבי נוזל הקירור
- תקלות תפעול – מניעת והתאוששות – במאמר זה בחנו את תאונת המיכלית טוריי קאניון בדרום מערב אנגליה בשנת 1967 להדגמת הצורך באבטחת איכות התפעול בהגנה בפני טעויות מפעיל, וכן את תפקודם של מערכת לניטור מתקנים בטחוניים ושל מערכת לבקרת יצור בהיבטים של מגבלות המפעיל.
- טעויות מצב – מניעה והתאוששות – במאמר זה בחנו את תאונת המיכלית טוריי קאניון בדרום מערב אנגליה בשנת 1967, וכן תקלות תפעול אופייניות של שלט-רחוק במערכות טלביזיה בכבלים, להדגמת הצורך באבטחת איכות התפעול בהגנה בפני טעויות מצב.

תהליך אבטחת איכות תפעולית הוא חלק בלתי נפרד מתהליך אבטחת איכות המוצר או התהליך, עם חפיפה ניכרת בשיטות ובישומן. התהליך כולל ארבעה שלבים: תכנון, ביצוע, בדיקות ושיפור (PDCA). המאמר הציג את הצורך לשלב את נושא התפעול בתהליך אבטחת האיכות ואת הפעילויות הנדרשות בשלבים אלו על לצורך אבטחת איכות התפעול.

מקורות

Bevan N., 2001, International standards for HCI and usability, *International Journal of Human-Computer Studies*, Volume 55, Number 4, pp. 533-552(20), Academic Press (available at: http://www.usabilitynet.org/tools/r_international.htm)

Casey, S., 1998, *Set Phasers on Stun*, Aegean Publishing Company, Santa Barbara, Ca.

Harel, A., 2006 - Alarm Reliability, User Experience Magazine, Vol 5., Issue 3.

Norman, D. A., 1983, Design rules based on analyses of human error, *Communications of the ACM*, v.26 n.4, p.254-258, April 1983 (available at http://cpe.njit.edu/dlnotes/CIS/CIS732_447/Cis732_1R.pdf)

Norman, D. A., 1990, Commentary: Human Error and the Design of Computer Systems, Editorial published in *Communications of the ACM, 1990*, 33, 4-7.

Palanque, P., Kornneef, F., Johnson, C., Szwillus, G. and Write, P., 2004, Safety-Critical Interaction: Usability in Incidents and Accidents. CHI 2004 Special Interest Group on Safety

Critical Interaction: Usability in Accidents and Incidents. 28 April 2004, Vienna, Austria, CHI Extended Abstracts 2004: 1600-1601 (available at http://liihs.irit.fr/palanque/Ps/CHI2004SIGSafetyCritical.pdf)

Reason, J., 1990, *Human Error*, Cambridge University Press, New York.

הראל, א., 2007a, מיגון מערכות בפני טעויות אנוש, הכנס הרביעי של INCOSE ISRAEL הרצליה

הראל, א., 2007b, לקחים מהפעלת הצופרים במלחמת לבנון השניה הכנס הלאומי להנדסת בטיחות

הראל, א., 2007c, מיגון מערכות בפני טעויות מצב, פוסטר בכנס הרביעי של INCOSE ISRAEL הרצליה