

אחריות מנהל הפרויקט למניעת טעויות מפעיל

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

מיהו האדם בצוות הפרויקט שתפקידו למנוע טעויות מפעיל?

כ-10% מהפעולות של מפעילי מערכות ותהליכים הן בטעות. 60-80% מתאונות המטוסים מקורן במצבים חריגים, המיוחסים לטעויות טייס. מעל למחצית מזמן התפעול מתבזבז על הבנת ההתנהגות הבלתי צפויה של המערכת, כתוצאה מטעות מפעיל. מרכיב נכבד של עלות שירות הלקוחות של מכשור ביתי ותקשורת הוא תמיכה בפניות הציבור, בעקבות טעויות הפעלה שגרמו לשיבוש במצב המערכת.

דוגמא

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.

אחריות המפעיל

למרבית הפעולות השגויות המפעיל אינו מודע כלל, ולכן תגובה המערכת אליהן היא בלתי צפויה. למרות זאת, הדרך המקובלת להתייחסות למצבי טעות היא להטיל את האחריות למצב על המפעיל. דרך זו נוחה למפתח ולאחראים על הבטיחות, מכיוון שהיא משחררת אותם מאחריות למחדלי תיכון. באופן טיפוסי, מפתחי מערכות נוטים להכחיש את עצם קיום הבעיה. ההליך המקובל של הכחשת בעיה הוא על ידי בחינה עצמית: אם אני מסתדר עם הפעלת המערכת, אין שום סיבה מדוע אחרים לא יוכלו להסתדר עם זה. באופן תגובה זה, המפתחים מתעלמים מקבוצה חשובה של משתמשים, אנשי עסקים, אנשי אקדמיה, מנהלים ומפקדים בכירים, שאין להם עודפי זמן, לבזבז על לימוד דרך החשיבה של מפתחי המערכת.

במקרים של טעות שמסתיימת בתאונה, אין אפשרות להתכחש לקיום הבעיה. במקרים בהם חוקרי התאונה מתקשים לפענח את מנגנון הכשל, הדרך המקובלת לחפות על האין-אונות שלהם או על חלקם ביצירת מצב שאיפשר את התאונה, היא על ידי הענשת הקורבן, דהיינו, המפעיל שנפל בפח שהטמינו לו, בחוסר תשומת לב, המפתחים. כך, למשל, קברניט המיכלית שגרמה לאסון האקולוגי בשנת 1967 פוטר מעבודתו, והושעה מכל פעילות ימית. להצדקת האשמת הקורבן, בדרך כלל נוהגים לחקור את האירוע באופן יסודי ולמצוא מספר נקודות בהן הקורבן לכאורה התנהג שלא כראוי. כך, למשל, קברניט מטוס האיירבאס 320 בטיסה 296 של אייר-פרנס, הואשם בשורה של נושאים שאינם קשורים כלל לסיבת התאונה, כגון, חוסר מוכנות לתמרון, חוסר תיאום בין אנשי הצוות, תמרון שלא על פי התכנון, רצף אירועים מהיר מדי, זחיחות דעת, יהירות, אווירת החג במפגן האוירי והשפעת הדיילות שביקרו בתא הטייס. טייס אחר שהיה עד לתאונה והעיד מטעם ההגנה, הושעה מעבודתו ללא פיצויים, בטענה של אי-שפיות. כל זאת, על מנת לאפשר את הרשעת הקברניט באשמת הריגה, ולדון אותו למאסר (http://en.wikipedia.org/wiki/Air_France_Flight_296). כך גם, בין השאר, קציני צה"ל שהיו מעורבים בתאונת האימונים בצאלים, הורשעו בדין והוכנסו לכלא, באמתלות שאינן קשורות לפליטת הפה של קצין הקישור ([קישור למאמר ב-Wiki](#)).

אחריות המפתח

הדרך של הענשת קורבן הטעות היא בעייתית בכך שהיא מונעת פתרון בעיית התיכון, מכיוון שהיא מסיחה את הדעת מהגורמים המבניים לתאונה. במקום לחקור את התאונה, לנתח ולהבין את הסיבות לה, משליכים כמה אנשים לכלא. בגישה זו, החוקרים של תאונות קטלניות נכשלים בכך שאינם פועלים למנוע בעיות דומות בעתיד (Norman, 1990). התוצאה היא שהתאונה חוזרת על עצמה. כך, 19 חודשים לאחר התאונה של מטוס האיירבאס 320 במפגן האוירי, התרסק מטוס נוסעים מדגם זה בבאנגלור שבהודו ו-94 אנשים מצאו את מותם, בגלל אותה תקלה ([קישור למאמר ב-Wiki](#)). חקירה רצינית של הגורמים לתאונה הראשונה החלה רק אחרי התאונה השנייה. כך גם, שנתיים לאחר תאונת צאלים א', קרתה תאונת צאלים ב', בגלל כשל חוזר של מניעת ירי

על כוחותינו [\(קישור למאמר ב-Wiki\)](#). נהלי הבטיחות של הסיוע הארטילרי, שלא מנעו את תאונת צאלים אי' נבחנו מחדש רק לאחר תאונת צאלים ב'.

על מנת לאפשר חקירה יסודית של גורמי הכשל, יש להימנע מהטלת האשמה על המפעיל, ולחקור את הגורמים המערכתיים אשר אפשרו את הכשל. כך, למשל, וועדת חקירה שנייה שחקרה את תאונת המטוס הניו-זילאנדי בקוטב הדרומי הפכה את מסקנות וועדת החקירה הראשונה, זיכתה את צוות המטוס מאשמה, וסללה בכך את הדרך לחקירה יסודית של גורמי הכשל (http://en.wikipedia.org/wiki/Air_New_Zealand_Flight_901).

תהליך אבטחת איכות תפעולית

באופן מסורתי, האחריות על הגדרת ממשקי ההפעלה של מערכות ותהליכים מוטלת על מומחים בתחום הנדסת גורמי אנוש, ובעיקר, אנשי שימושיות. 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. בנושא טעויות מצב, הנטיה היא לייחס מקרים כאלו כאל כוח עליון, צירוף מקרים שלא בשליטה. נושא ההגנה בפני כשל תפעולי נופל בין הכסאות.

אבטחת שימושיות

באילוץ 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, לדוגמה, למרות שחברת מיקרוסופט מעסיקה עשרות רבות של מומחי שימושיות בפיתוח מוצריה, כל מוצרי הקו הראשון שלה לוקים בתחום המיגון בפני כשל תפעולי.

הנדסת גורמי אנוש

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 כתכתיב, בגלל מגבלות תקציב. 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.

הנדסת איכות

מהנדסי איכות בודקים תכונות של עמידות ותפעול המערכת ביחס למפרטים. הבעיה היא שהמפעיל בדרך כלל אינו בקי בפרטי המפרטים, וטועה בהבנת דרך פעולת המערכת ובמעקב שוטף אחר השינויים במצבה.

בין הכסאות

הנחת העבודה בתכנון ממשק הפעלה צריכה להיות שהמפעיל יעשה כל טעות אפשרית, והאתגר הוא להבטיח את תכונת השרידות וההתאוששות של המערכת. 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. בעיות קריטיות בתפעול מערכות נמצאות בתחום האפור בין הנדסת מערכת לבין הגורם האנושי. הנושאים הבאים נופלים כיום בין הכסאות:

- תקלות תפעול – מניעה, צמצום הסיכוי לתקלות ואבטחת שימושיות מנגנון ההתאוששות
- טעויות מצב – מניעה, צמצום הסיכוי לתקלות ואבטחת שימושיות מנגנון ההתאוששות
- אבטחת שימושיות תהליכי תפעול שמיועדים להתמודד עם תקלות מערכת

אחריות מנהל הפרויקט

תקלות מהסוג שהביא לאסון המיכלית, שנובעות ממצבים חריגים של המערכת, עלולות לקרות גם במערכות שאנחנו מפתחים כיום, במאה ה-21. להתמודדות עם תקלות מסוג זה, יש צורך לשלב את הנדסת גורמי אנוש בתהליכי אבטחת איכות המערכת, להגדיר אחראי לטיפול בנושאים הללו, למנות מהנדסים שהוכשרו למשימות אלו, שמכירים את השיטות שמאפשרות להתמודד עם הבעיות הללו, ושיכולים לקחת אחריות על פתרונן.

בהקשר זה, התפקיד של מנהל הפרויקט הוא לתאם בין מהנדסי המערכת, מהנדסי התוכנה ומהנדסי גורמי אנוש, בנושאים של ניתוח תקלות, תהליכי איתור תקלות והגדרת דרכים למניעת הסלמה במקרים של תקלות. בין השאר, מנהל הפרויקט נדרש להבטיח ישום של מתודולוגיות להבטחת שימושיות בתחומים של ניתוח מערכת, מפרטי דרישות, ארכיטקטורת מערכת, לוגיקת הפעלה, עיצוב תצוגה, בדיקות שימושיות ועוד. המאמר יסקור את ההבדלים בין מתודולוגיות אלו לבין המתודולוגיות המקובלות בהנדסת מערכת מסורתית.