8 יולי, 2016

הצעה להגדרת תפקיד מהנדס בטיחות - גירסא מורחבת

כתב: אבי הראל

רקע

חקר תאונות מייחס לגורם האנושי משקל רב ביותר[1]. למרות זאת, עד לאחרונה, פעילויות הבטיחות עסקו בעיקר במניעת כשל בציוד, ונמנעו בעיסוק בכשל של המפעילים. באופן מסורתי, ההנחה היתה שהמפעיל יכול לפעול על פי הציפיות, ובמקרים של חריגה שמסתיימת בתאונה, עליו לתת על הדין על כך.

לאחרונה חלה תפנית בגישה לכשל של המפעילים, בשני היבטים: בהיבט של מניעת תאונות, מקובלת כיום התפיסה שלא ניתן למנוע טעויות בתפעול. הגישה המקובלת היא שאם המערכת מאפשרת למפעיל לטעות, במוקדם או במאוחר הוא אכן יטעה.[2] בהיבט של אחריותיות, קיימת הכרה גוברת בכך שחיפוש אשמים בקרב המפעילים גורם לרתיעת העובדים מלדווח ולשתף פעולה עם צוות התחקור[3].

על רקע מגמה זו פותחו בשנים האחרונות מתודולוגיות, שמאפשרות לצוות העוסק בפיתוח מערכות הנדסיות לצמצם במידה ניכרת את הסיכונים בגין טעויות תפעול. לדוגמא, שיטת Poka-yoke שפותחה ביפן מאפשרת למנוע טעויות באופן החיבור של יחידות שונות במערכת[4]. מתודולוגיה חדשנית ומקיפה יותר זוהי מתודולוגית STAMP שפותחה ב-MIT, שכוללת המלצות לאלץ את המערכת לפעול על פי כללים המגדירים תפעול נורמלי[5].

בשיתוף ובתמיכה של מרכז גורדון להנדסת מערכות בטכניון, פותח לאחרונה מדריך למפתחי מערכות, ErgoSafe[6], הכולל המלצות ליישום מתודולוגיית STAMP בתהליך הפיתוח. הישום של מתודולוגיה זו מחייב שיתוף פעולה בין מהנדסי הבטיחות המשולבים בצוות הפיתוח, לבין מהנדסי המערכת ולבין מומחי עיצוב ממשקי תקשורת אדם-מכונה.

---

[1] ErgoSafe: statistics of failure: http://resilience.har-el.com/Guide/Terms/Error/Statistics.htm

[2] ErgoSafe: The Human Factors variant of Murphy's law: http://resilience.har-el.com/Guide/Terms/Design-quality/Design-principles.htm

[3] Dekker: quotes: https://www.goodreads.com/author/quotes/214803.Sidney_Dekker

[4] Wikipedia: Poka-yoke: https://en.wikipedia.org/wiki/Poka-yoke

[5] STAMP: http://sunnyday.mit.edu/STAMP-publications.html

[6] ErgoSafe: Guide to resilience-oriented system definition http://resilience.har-el.com/Guide/index.htm

סיווג האיומים

המדריך הנדון מגדיר שני סוגים של איומים: כאלו שניתן לצפות אותם וראש, וכאלו שמוגדרים כהפתעות[7]. המדריך כולל המלצות לזיהוי איומים משני הסוגים.

איומים צפויים

מדובר באיומים הנובעים מתקלות שניתן לצפות מראש, כגון, ברכיבים מערכת, נפילת מתח, בעיות תקשורת, וכיו"ב. קיימות מספר מתודולוגיות לניתוח ולהערכת הסיכונים של האיומים הללו[8]. האחריות על ביצוע הפעילויות הללו היא על מומחי התוכן, קרי, מהנדסי המערכת.

גורם עיקרי בכשל בהתמודדות עם איומים צפויים הינו במצבים בהם המפעיל אינו מודע לאיום הקונקרטי. סיבות אפשריות לכך כוללות חוסר אמצעים (חיישנים ואינדיקטורים) לגילוי האיום, או חוסר עירנות של המפעילים.

גורם כשל נוסף הוא כאשר המפעיל מודע לכך שהמערכת נמצאת תחת איום, אבל אינו יודע כיצד להתמודד עם המצב. סיבות לכך כוללות מגבלות בתחום התכן לאיתור תקלות, ליקויים בהדרכה, תחלופת עובדים וכיו"ב.

איומים בלתי צפויים

מדובר במצבים חריגים אותם לא ניתן לצפות מראש, כתוצאה מטעויות פסיכומוטוריות של המפעילים, חוסר תיאום בין מצב המערכת לבין כוונת המפעיל, חוסר תיאום בין תת-יחידות של המערכת, באג בתוכנה, טעות במפרטי הדרישות, ועוד.

המתודולוגיה של STAMP מאפשרת התמודדות עם האיומים הבלתי צפויים בדרך של איתור בעוד מועד. המדריך לאבטחת מסינות ממליץ על ארכיטקטורה יעודית לאבטחת מסינות, שמאפשרת זיהוי בעוד מועד של מצבים של חוסר תיאום כנ"ל, התרעה למפעילים, ותהליך של הפקת לקחים, לצורך מניעה איומים כאלו בעתיד[9]. יישום הארכיטקטורה מחייב שיתוף מידע בין מהנדסי הפיתוח, המבוסס על כלי תוכנה לניהול בסיסי נתונים הכוללים הגדרות של פעילות תקינה[10].

---

[7] Hazard definition: http://resilience.har-el.com/Guide/Terms/Hazard/index.htm

[8] דוגמאות: FMEA, HAZOP, FTA

[9] Resilience-oriented system architecture: http://resilience.har-el.com/Guide/Models/Architecture/index.htm

[10] Resilience-oriented system development http://resilience.har-el.com/Guide/Models/V-model/index.htm

משימות החסינות בהנדסת בטיחות

מהבחינה ההנדסית, משימות החסינות זהות למשימות הבטיחות. האתגרים העומדים בפני מהנדס הבטיחות זהים לאלו שמוגדרים בהנדסת חסינות, והם, למנוע איומים צפויים, ולצמצם את הנזקים בפני האיומים אותם לא הצלחנו למנוע (כולל איומים בלתי צפויים). ההבדלים הם סמנטיים בלבד, בשני היבטים:

- רמת הסיכון: בעוד שהמונח "בטיחות" מתייחס אל נזקי נפש וגוף, המונח "חסינות" מתייחס אל נזק כלשהו, כולל נזקי ממון, מוניטין, וכיו"ב.
- ארגז הכלים: בעוד שהיסטורית, המונח "בטיחות" מעורר אסוציאציה של שיטות אד-הוק, תכנון ריאקטיבי בתגובה לאירועי בטיחות, המונח "חסינות", שהוא מודרני יותר, קשור לגישה של מניעה, על ידי תכן פרואקטיבי.

אבטחת חסינות בפני האיומים

עקרונות התכן לחסינות

התכן לחסינות מבוסס על מודל של כשל בתפעול מערכת ועל נקיטת אמצעים למניעת אופני הכשל שבמודל. מקובל לתאר את מערכת ההגנה בפני כשל בעזרת המטפורה של גבינה שוויצרית[11]. במונחים של אבטחת חסינות, מודל הכשל מתואר על ידי אופנים שונים של היווצרות והתפתחות איומים[12]. ההתמודדות עם הסיכונים היא על ידי חמש שכבות הגנה המתוארות ביצוג של תרשים זרימת מצבים[13] של מודל החסינות.[14]

תהליך אבטחת החסינות

התפקיד של אבטחת חסינות בפני האיומים הוא בין דיסציפלינרי, ונמשך לאורך חיי המערכת[15].

- בשלב הפיתוח, החסינות מושגת בדרך של שיתוף מידע בין מהנדסי מערכת, מעצבי האינטראציה, ומהנדסי בטיחות
- בשלב התפעול, החסינות מושגת על ידי שיתוף מידע בין מהנדסי הבטיחות לבין ממוני בטיחות.

---

[11] Wikipedia: https://en.wikipedia.org/wiki/Swiss_cheese_model
[12] ErgoSafe: Failure model: http://resilience.har-el.com/Guide/Models/Failure/index.htm
[13] ErgoSafe: Defenses: http://resilience.har-el.com/Guide/Models/Resilience-states/index.htm
[14] ErgoSafe: Resilience model: http://resilience.har-el.com/Guide/Models/Resilience/index.htm
[15] ErgoSafe: Iterative resilience assurance: http://resilience.har-el.com/Guide/Models/Iteration/index.htm

תפקידי מהנדס בטיחות במהלך הפיתוח

המשימה של הגדרת תכונות הבטיחות של מערכת צריכה להיות באחריות מומחה תוכן, שמכיר את רזי המערכת, ויכול לזהות אופני כשל פוטנציאלי. ההנחה היא שמהנדס הבטיחות מכיר את המונחים והשיטות הספציפיות למערכת, אך אינו מומחה תוכן. לכן בדרך כלל הוא לא יוכל למלא את תפקיד הגדרת תכונות הבטיחות באופן משביע רצון. תפקידיו כוללים:

- חיזוי סיכונים אפשריים בעבודה
- פיתוח וישום דרכים למניעה או צמצום של הסיכונים הללו
- פיתוח וישום דרכים לאיתור מצבי סיכון בזמן אמת
- פיתוח וישום דרכים לאבטחת מודעות ההנהלה והעובדים למצבי הסיכון.

שילוב הנדסת בטיחות בתהליך הפיתוח

מהנדס הבטיחות צריך להוביל את הפעילויות הקשורות למניעת איומים בתכן ולאיתור איומים בלתי צפויים בזמן התפעול. התאמתו למשימת הובלת נושא הבטיחות נגזרת מההתמחות שלו בשיטות ובתהליכים של אבטחת חסינות, ובזוית הראיה שהוא רוכש עם הנסיון בתפקיד. תפקידיו כוללים[16]:

- הובלה של פעילות אבטחת התרעה במקרה של כשל ברכיב כלשהו במערכת, באינטראקציה עם מהנדס המערכת האחראי על שילוב רכיב זה במערכת
- הובלה של פעילות אבטחת התמצאות המפעילים באירועי כשל, באינטראקציה עם מפתחי מערכת ההתרעות
- כתיבת מפרטי הבדיקות לאימות התמצאות המפעילים באירועי כשל
- הובלה של פעילות הגדרת מפרטי התפעול, באינטראקציה עם מהנדסי המערכת ועם מפתחי ממשקי ההפעלה
- הגדרת הדרישות מיחידות הבקרה היעודיות (תרחישים[17], מצבים[18], פעילות[19]) המאפשרות איתור מצבים חריגים תוך כדי תפעול.
- כתיבת מפרטי הבדיקות לתיקוף היכולת לאתר מצבים חריגים.
- הובלה של תהליכי בדיקות איתור מצבים חריגים ותפעול במצבים הללו.

---

[16] ErgoSafe: interdisciplinary interaction http://resilience.har-el.com/Guide/Models/Interdisciplinary/index.htm

[17] ErgoSafe: scenario control: http://resilience.har-el.com/Guide/Models/Scenario-control/index.htm

[18] ErgoSafe: situation control: http://resilience.har-el.com/Guide/Models/Situation-control/index.htm

[19] ErgoSae: activity control: http://resilience.har-el.com/Guide/Models/Activity-control/index.htm

תפקידי מהנדס הבטיחות במהלך התפעול השוטף

במהלך התפעול השוטף, מהנדס הבטיחות פועל באינטראקציה עם ממוני הבטיחות, כאשר ממוני הבטיחות אמורים לזהות מצבי כשל, לדווח עליהם ולהציע פתרונות. מהנדס הבטיחות צריך לבחון את החלופות השונות בשיתוף עם מהנדסי המערכת ולהוביל את יישום הפתרון הנבחר. תפקידיו כוללים:

- זיהוי מצבי כשל במניעה, צמצום או תגובה לסיכונים בפועל
- זיהוי סיכונים בלתי צפויים (שאינם נכללים ברשימת אילו שנצפו בשלב התכנון)
- ניהול בנק אירועים, כולל כשל במניעת סיכונים וזיהוי סיכונים בלתי צפויים
- הצעת שינויים בגין האירועים הללו
- פירסום הממצאים

תפקידי מהנדס הבטיחות בתחקור תאונות

מהנדס הבטיחות צריך לוודא שתהליך התחקור ממוקד בהפקת לקחים, ואינו עוסק בחיפוש אשמים. תפקידיו כוללים:

- ניהול תחקיר לגבי מהלך האירועים ומצבי הסיכון בשלבים השונים
- פירסום התחקיר
- הצעה לשינוי אופן התפעול במטרה למנוע חזרה על מהלך האירועים שהוביל לתאונה
- מיתון וריסון כוחות הפועלים להסטת הדיון לפסים אישיים.

איוש

בכל ארגון כדאי שיהיה מישהו אחראי על הפעילויות הללו, גם אם הסיכונים הם פיננסיים בלבד.

גם בארגונים קטנים, שאינם זקוקים ואינם יכולים להרשות לעצמם מהנדס בטיחות במשרה מלאה, כדאי שיהיה מישהו שהפונקציות לעיל הן במסגרת תפקידיו ואחריותו.

אחריות

כל שינוי באופן התפעול עלול להשפיע וליצור סיכונים שאינם מזוהים ברמת העובד שאינו מיומן בניהול סיכונים. יש לדרוש בחינה של מהנדס בטיחות של כל הצעה לשינוי באופן התפעול.

רצוי להמנע מדרישה לאישור פורמלי בחתימה של מהנדס הבטיחות על שינויים, על מנת למנוע זילות של החתימה שלו. במקום חתימה, עדיף לדרוש ממהנדס הבטיחות לסכם בכתב את התייחסותו לשינוי, כולל סיכונים חדשים, השפעה על סיכונים מוכרים אחרים והמלצות לצמצום הסיכונים.

מקצועיות

יש לאפשר למהנדס הבטיחות ללמוד ולהשתפר בתחומים רלבנטיים.

חסינות (אחריותיות)

יש להבטיח את חסינות מהנדס הבטיחות בפני תביעות במקרים של תאונה, במקרים בהם הוא עמד בדרישה הבסיסית של תיעוד והפצה של מסמכי בטיחות (כלעיל).

יש לחייב את אחראי התפעול לאשר את מסמכי הבטיחות, ואת המלצות מהנדס הבטיחות.