

מדריך לאבטחת חסינות בפני טעויות תפעול

אבי הראל
ארגולייט
חיפה

ergolight@gmail.com,
+972-54-453-4501

ד"ר אביגדור זוננשיין
מרכז גורדון להנדסת מערכות, הטכניון
חיפה

avigdorz100@gmail.com,
+972 52 2891773

Copyright © 2014 by Avigdor Zonnenshain & Avi Harel. Published and used by INCOSE_IL with permission.

תקציר

מחקרים על תאונות קריטיות בתפעול מערכות מצביעים על כך שנהוג להצביע על הגורם האנושי כסיבה העיקרית לכשל. ממצאים אלו העלו את הצורך לפתח מדריך לתכן ולפיתוח של מערכות החסינות לטעויות תפעול. מאמר זה כולל דיווח על פיתוח מדריך כזה במסגרת מרכז גורדון להנדסת מערכות בטכניון. המדריך הנדון מניח כבסיס את גירסת גורמי אנוש של חוק מרפי, ומיישם את פרדיגמת STAMP על ידי בקרה עצמית בתכן מונחה תרחישים. המדריך מציע תכן המבוסס על שלש מערכות הגנה, למניעת טעויות סמויות, למניעת הסלמה וללימוד מאירועי כשל. אפקטיביות המדריך נבחנת בשיתוף קבוצת עבודה של אילטם, בשיתוף אינקווי. קבוצת העבודה בודקת את ישימות המדריך למספר ניתוח מקרה. המדריך מתוקף על ידי מדידה של ישימות ההנחיות בעזרת מאגר של 70 אירועי כשל.

מבוא

מילון אוקספורד בנושא מונחים היסטוריים (גירסא משנת 1973) מגדיר חסינות כתכונה של חזרה למצב מקור. ההגדרה מתייחסת לחומרים שחוזרים למצבים המקורי לאחר שעברו תהליך של עיוות. הגדרה מורחבת, ישימה למערכות מעשי ידי אדם, היא: היכולת של מערכת להתאושש מהפרעה (SEBK 2014).

המונח חסינות מערכת מוגדר כיכולת המערכת למתן את הסיכונים של כשל או אובדן, כאשר התפעול הוא במצבים חריגים (Harel and Weiss, 2011). מיתון הסיכונים מושג על ידי הסתגלות למצבים משתנים, ותגובה הולמת לאחר מכן (RSWG 2014).

המושג "הנדסת חסינות" מוסבר בספרם של Hollnagel ושות' (2006). עקרונות לתכן מערכות חסינות הוסברו בהרחבה במאמריו של Jackson (2010, 2013).

מאמר זה מציג מדריך חדשני המיועד לשימושם של מהנדסי מערכות. המדריך מציע עקרונות ושיטות לאבטחת תקשורת בטוחה בין המפעילים לבין המכונה.

מדוע מערכות נכשלות

קיימים הסברים רבים לגבי מקורות הכשל. להלן כמה מהם:

- גורמים ארגוניים (e.g. Reason, 1997; Dekker, 2006)
- מורכבות (e.g. Perrow, 1984)
- מצבי תפעול קיצוניים (e.g. Hollnagel et al., 2006; Weiler & Harel, 2011)
- טעויות אנוש (e.g. Norman, 1983)
- פגמים באיכות מפרטי הדרישות (e.g. Robert et al., 1998; Leveson, 2012)
- פגמים באיכות המימוש (e.g., Weinberg, 1971; Norman, 1990)
- ליקויים בהתאמה להקשר התפעול (e.g. Zonnenshain and Harel, 2009).

מדריך זה אינו עוסק בגורמים השונים, ובהסברים לגבי אופני הכשל. מדריך זה מתמקד בהגדרת אמצעי מיגון בפני אופני כשל אופייניים, המתוארים באמצעות מודל של חסינות מערכות.

טעויות תפעול

בדרך כלל נהוג לייחס כשל מערכתי לטעויות אנוש. כך, מיוחסות לגורם האנושי 60% אחוז מהתאונות האוירית (PlaneCrashInfo 2014), 80% מהתאונות הימיות (Baker & Seah 2004), 90% מהתאונות בדרכים (AlertDriving 2014) ו-60-80% מהתאונות בתעשייה (Kariuki & Löwe 2014). טעויות אנוש הן הגורם העיקרי לאובדנים במהלך תפעול: תאונות, נזקי רכוש, הפחתת תפוקה, חוסר שביעות רצון של השתמשים (Landauer, 1996). בדרך כלל, האובדן הוא תוצאה של תפעול במצבים חריגים, כתוצאה ממורכבות המערכת (Perrow, 1984).

תכופות, המצבים החריגים נובעים מבעיות בתיאום בין המכונה לבין המפעילים, כפי שמודגם בתרשים הבא:



המונח "טעות תפעול" מיוחס בדיעבד לפעולות לגיטימיות, אם ורק כאשר התוצאה אינה משיבת רצון (Hollnagel, 1983; Dekker, 2006). נהוג לייחס את הכשל לטעות אנוש בתנאים הבאים:

- המפעילים לא הגיבו כראוי לאירוע חריג (כגון, תקלה ברכיב או טעות הקלדה)
- כתוצאה מכך המערכת היתה במצב חריג

- המפעילים לא הצליחו להחזיר את המצב לקדמותו בעוד מועד.

שימושיות וטעויות תפעול

שימושיות וטעויות תפעול הן שני צדדים של אותה מטבע. לדוגמא, בעיות שימושיות נפוצות בתפעול מוצרי צריכה, כגון טלביזיה ביתית, מיוחסות לטעויות אנוש (Zonnenshain & Harel, 2009). התרשים הבא מדגים בעיות אופייניות לגירסאות מוקדמות של השלט הרחוק של טלביזיה ביתית:



הצורך לעסוק בגורם האנושי עלה לראשונה במלה"ע השניה, לאחר סדרה של אירועים כתוצאה מטעויות אנוש (Meister 1999). בשני העשורים האחרונים, מומחי שימושיות פיתחו פרקטיקות לחיזוי, גילוי וזיהוי של טעויות משתמש (Nielsen, 1993). פרקטיקות של הנדסת שימושיות שפותחו לאחרונה מאפשרות למנוע מספר טעויות משתמש נפוצות, על ידי תכנון פרקטיקות אלה עדיין לא קיבלו תוקף מחקרי, ולכן אינן מקובלות עדיין על כל המומחים.

איומים בתפעול מערכות

בניתוח אירועים כשל רבים מתבררים שני גורמי כשל עיקריים:

- **איומים סמויים**, כאשר המפעילים אינם מודעים למצב חריג, כגון, כשל של רכיב חומרה או תוכנה, או חוסר עקביות במצב המערכת. איומים סמויים נובעים מחוסר מידע או ממידע שגוי. בתאונה בכור הגרעיני TMI המערכת לא סיפקה למפעילים מידע לגבי מצבם של חמישה רכיבים קריטיים, מידע שהיה חיוני להתמודדות עם התקלות, וסיפקה מידע שגוי לגבי מצבם שסתום שחרור הלחץ, שהיה קריטי לפתרון הבעיה (Perrow, 1984). מונח זה קשור למונחים אחרים: כשל סמוי ומצב סמוי (Eurocontrol, 2006).
- **עיכובים בתהליך ההתאוששות מתקלה או טעות**, כאשר המפעילים אינם מצליחים לאבחן את ההפרעה בעוד מועד (כפי שאירע בתאונת TMI).

מחוללי הפרעות

אירוע שהיה ראשון בשרשרת של אירועים חריגים נקרא מחולל ההפרעה (Zonnenshain & Harel, 2013). מחוללי הפרעה טיפוסיים כוללים:

- אירוע חיצוני, כגון מכשול על דרך, או סירת אויב שהתגלתה על ידי מכ"ם
 - כשל ביחידת חומרה או ברכיב
 - נפילת מתח, כגון, בהחלפת סוללה או בתוצאה מחיבורים רופפים
 - תקלות או הפרעות בתקשורת
 - החלפת מצב כתוצאה מבאג בתוכנה
 - טעות או שגיאת מפעיל, כגון, הפעלה של פונקציה שאינה ישימה לתהליך התפעול
 - שינויים חריגים בקצב יצור.
- בנוסף, במהלך התפעול יתכנו מחוללי הפרעות אחרים, ספציפיות ליעוד המערכת.

ניהול סיכונים בגין אירועים בלתי צפויים

תיאורטית ניתן לנהל את הסיכונים בגין אירוע חריג על ידי אומדן של ההסתברות ושל הנזק בגין האירוע. אומדנים כאלו אפשר לקבל עבור אירועים שהתרחשו בעבר ושחזרו על עצמם מספר פעמים. הבעיה שהאירוע העוקב את האירוע החריג הוא לעתים קרובות בלתי צפוי, ולכן אומדנים כאלו אינם קיימים עבורו (Taleb, 2007). במצבים אלו, אין לנו ברירה אחרת, אלא להסתמך על מודלים המתארים כשל מערכת. גישה זו הודגמה על ידי ויילר והראל (2011).

ניתוח גורמי כשל

פרקטיקה מקובלת לחיזוי אירועי כשל היא על ידי יישום שיטות של ניתוח אירועי כשל, ביניהן FTA, FMEA, FMECA, HAZOP, ETA ושות' (2011) פירסמו השוואה של השיטות הללו.

תיאורטית, השיטות הללו עשויות לסייע לנו בחשיפת גורמי כשל ומהלכי כשל רבים ומגוונים. בפועל, התרומה של השיטות הללו מצומצמת, וזאת מהסיבות הבאות:

- תאונות בתפעול טכנולוגיות עתירות סיכון, כמו אלה של תחנות כח גרעיניות, הן תוצאה של סיבוכיות (Perrow, 1984). בניתוח גורמי כשל שנעשה ידנית, אין אפשרות מעשית לבחון את כל הצירופים האפשריים של אירועים המתרחשים במקביל. אירועי הכשל בפועל הם מימוש של אותם צירופים אותם לא השכלנו לכלול בניתוח.
 - ההבדל בין תפעול מוצלח לבין תאונה נעוץ ברגישות אופן התנהגות המערכת להבדלים זעירים בפרמטרים של ההפעלה (Hollnagel, 1983). בשימוש כלים המקובלים אין דרך לזהות את המוקדים בהם רגישות זו באה לידי ביטוי. ניתוח גורמי הכשל מאפשר לבחון אירועים שהתרחשו, אבל אינו יעיל לניבוי אירועים עתידיים.
 - על פי תיאוריית הברבור השחור, תאונות בגין אירועים בלתי צפויים לא ניתן לנבא מכיוון שחסר המידע הדרוש לצורך הניבוי (Taleb, 2007).
 - במקרים רבים טעויות תפעול הן תולדה של חוסר עקביות במצב של המערכת המורחבת או בהתאמה להקשר (Zonnenshain and Harel, 2009).
- לפיכך, יש צורך להשתמש בטכניקות אחרות בכדי לנבא מצבי סיכון.

עקביות פנימית

לעתים קורה שאחת מיחידות המערכת נחשפת לאירוע חריג, ותרחיש התפעול משתנה בהתאם. דוגמא לכך היא המקרה של תקלה ברכיב. אם כל יחידות המערכת פועלות על פי התרחיש החדש, אז המערכת מתואמת להקשר. אחרת, אם יחידות אחדות ממשיכות לפעול על פי התרחיש הקודם, המערכת מגיעה למצב של חוסר עקביות פנימית (Zonnenshain & Harel, 2009; Harel & Weiss, 2011).

מודל הגבינה השוייצרית

תאונות בתפעול מערכות מורכבות מתרחשות בדרך של הצטברות של מספר תקלות. המטפורה של גבינה שוייצרית מרמזת על כך שאירועי כשל נגרמים בתהליך של חדירה דרך מספר מחסומים, המיוצגים על ידי פרוסות של הגבינה (Eurpcontrol, 2006).

נהוג להשתמש במודל זה לתיאור אפקט מצטבר של פעולות, שמסתכם בכשל. במדריך זה אנו משתמשים במודל גם באופן שונה, לתיאור אפקט מצטבר של תגובות, שמסתכם בהתאוששות מאיומים סמויים.

אבטחת בטיחות פרואקטיבית

מפתחי מערכות אמורים לתכנן את המערכות באופן שיפעלו כראוי גם בתנאי תפעול חריגים. אבטחת בטיחות פרואקטיבית מיישמת את הרעיון שניתן למזער את מקרי הכשל על ידי זיהוי סיכונים לפני התרחשותם, ונקיטת פעולות למניעתם ולצמצום הנזקים (DOC 9859, 2009).

אסטרטגיה פרואקטיבית כוללת זיהוי איומים פוטנציאליים, בטרם הפיכתם לאירועי כשל או לתאונות, ונקיטת פעולות הדרושות למיזעור הסיכונים (Weiler & Harel, 2011).

תכן מונחה חסינות

תכן מונחה חסינות מאפשר להשיג את המטרה של אבטחת חסינות פרואקטיבית, על ידי תשומת לב לתהליכים הקשורים לתפעול המערכת במצבים חריגים (Zonnenshain & Harel, 2013).

פרדיגמת STAMP

פרדיגמת STAMP של ננסי לבסון (2004) מאפשרת להגדיר חסינות מערכת במונחים של ציות לחוקי התפעול. ההנחה היא שאירועי בטיחות נובעים מהפרה של כללים המגדירים (במפורש בו ע"פ מוסכמה) את התפעול התקין. עקרון הבקרה העצמית, הנגזר מפרדיגמה זו, הוא שהמערכת צריכה לבקר את הפעילות של עצמה, לאלץ את עצמה לפעול על פי הכללים.

ההנחות במדריך זה מתייחסות לתכן של יחידת בקרה המיועדת לממש את פרדיגמת STAMP. ספציפית, ההנחות מתייחסות אל מימוש הכללים ביחידת הבקרה, ואל תגובה המערכת במצבים של חריגה מהכללים.

בחירה בין פתרונות חליפיים

כל פתרון לבעיית בטיחות מייצר הזדמנויות לכשלים חדשים. לדוגמא, אם הוספנו נורית חיווי למצב של כשל באחת היחידות, אז הוספנו גם אפשרות לתאונה בגין חוסר תשומת לב למצב הנורית, או בגין תקלה בנורית.

באירוע שהתרחש בשנת 1977 בכור הגרעיני Davis-Besse-1, המפעילים זיהו באיחור מסויים ששסתום PORV היה תקוע במצב פתוח, והתגברו על התקלה מבלי שנגרם נזק. בעקבות אירוע זה ואירועים דומים, יצרן השסתום

הוסיף חיווי למצב השסתום. משיקולי עלות, החיווי התייחס לשליחת הפקודה לשסתום, ולא למצב בפועל. לרוע המזל, בתאונת TMI השסתום נשאר במצב פתוח, אבל החיווי הראה שנשלחה פקודה לסגירת מצב השסתום, המפעילים הסתמכו על חיווי זה, ולא ווידאו שהשסתום אכן נסגר כראוי (Perrow, 1984).

אחד האתגרים בתכן לחסינות הוא לזהות את הסיכונים שנוספו בגין פתרונות בטיחות, להשוות אותם לסיכונים המקוריים, ולהעריך את הבטיחות השולית של הפתרון, בהתחשב בסיכונים החדשים.

הפקת לקחים מאירועי בטיחות: הטיית האחריות

הנטייה הטבעית של האנשים המעורבים באירוע כשל היא לחפש אשמים. בארגון מונחה אמוציות, בו תרבות הבטיחות מוטה לעבר האחריות, תחקירי אירועים מתנהלים על פי תסריט של "האשמה והענשה".

תגובה מונחית אמוציות לאירועי כשל פוגעת באפשרות לשיפור החסינות, מכיוון שחוקרי האירוע אינם מתמקדים באיתור שינויים בתכן שעשויים לשפר את החסינות. לעומת זאת, בארגון שנוקט במדיניות של תרבות בטיחות, התחקירים כוללים המלצות לשינויי תכן, וההנהלה מקדמת את ישומם (Dekker, 2007).

באבטחת החסינות שומה עלינו להתחשב בהטית האחריות, ולספק אמצעים בתכן להתמודד עימה. מאמר זה מציע תהליך של שיפור מתמיד, על ידי הפקת לקחים מאירועים כשל (Weiler & Harel, 2011).

מטרות הפרויקט

מאמר זה כולל דיווח על פרויקט מתמשך במסגרת מרכז גורדון להנדסת מערכות בטכניון. המטרה של פרויקט זה היא לפתח מדריך להנדסי מערכות, הכולל הנחיות לאבטחת חסינות המערכות על ידי תכן. הגירסא הראשונה של המדריך הוצגה על ידי Zonnenshain & Harel (2013). המדריך מתמקד בהשגת היעדים הבאים:

- הצעת הנחיות למניעת כשל תפעולי, על ידי תכן
- הצעת הנחיות להערכת איכותנית של חלופות
- הצעת אמצעים לעקוב אחר מהלך התפעול קודם לאירוע, ושיטה לדווח ולהסיק מסקנות לגבי שינויי תכן שיאפשרו מניעת אירועי כשל דומים בעתיד.

הבסיס התיאורטי

חלק זה של המאמר מציג המושגים והעקרונות המשמשים את המדריך:

- הגדרת תפקיד התכן ההנדסי בתהליך אבטחת חסינות
- הגדרת גבולות התכן, מבוססת על שלש קטגוריות של פעילות בתפעול המערכת
- מודל המתאר את תהליך הווצרותם של אירועים בלתי צפויים
- מודל המתאר את ההתנהגות של מערכות חסינות
- עקרון הבקרה העצמית של מערכת, המבוסס על הפרדיגמה של STAMP
- מבנה של קוי הגנה, המבוסס על המטפורה של גבינה שוויצרית.

להלן הסבר של המושגים הללו.

תפקיד התכן ההנדסי בתהליך אבטחת חסינות

המחקר בנושא הנדסת חסינות מתמקד בניתוח אירועי כשל, ומדגיש את תפקיד ואחריות ההנהלה ביציאת תרבות בטיחות (e.g., Hollnagel et al., 2006). בניגוד לכך, מדריך זה מתמקד בהיבטים של תכן מערכתי. המדריך מניח שזהו תפקידו של מהנדס המערכת למנוע מצבים בלתי צפויים, וההנחיות מכוונות להשגת מטרה זו.

מונחי יסוד

להלן מונחי יסוד המשמשים למדריך זה:

- **המערכת.** במאמר זה, המונח מתייחס למערכת המורחבת, הכוללת בנוסף למכונה גם את מפעיליה (Zonnenshain & Harel, 2009).
- **מצב.** המונח משמש כקיצור ל"מצב המערכת".
- **תרחיש.** מערכות מתוכננות לפעול בהתאם לתרחישים, כלומר, התכן של התגובה של כל יחידה לכל מאורע מבוסס על הנחיות לגבי התרחיש הפעיל. בתפעול נורמלי ובפתרון בעיות, כל יחידות המערכת צריכות להתייחס אל התרחיש הפעיל, המשותף לכולן. התרחיש מוגדר על ידי פונקצית התפעול, בהקשר התפעולי.
- **תהליך תפעול.** סדרה של מעברי מצבים הקשורים בתרחיש תפעול.
- **מצב תפעולי.** המצב הפעיל, במסגרת של תהליך תפעול.
- **הפרעה.** האפקט של מחולל (טריגר), שנגרם על ידי מפעיל, כשל חומרה, באג בתוכנה, או איום חיצוני.
- **איום תפעולי.** באופן אידיאלי, המערכת יכולה להתאושש מהפרעה בקלות, ולהחזיר עצמה למצב תפעול נורמלי מיידית, מבלי לצרוך קשב רב וללא מאמץ מצד המפעיל. במקרה שהמערכת אינה מתמודדת עם ההפרעה מיידית, ההפרעה הופכת להיות איום תפעולי.

עקרונות באבטחת חסינות

המדריך מציע את העקרונות הבאים:

- **מלחמה בבייש המזל.** התכן ימנע התערבות של יד המקרה. התכן יקח בחשבון את מצבי סיכון האפשריים ויכלול אמצעי הגנה בפני כולם, ככל הניתן.
- **גבולות התכן.** המפרטים יכללו הגדרה של גבולות התוקף שלהם. במסגרת הגבולות, מפרטי התנהגות המערכת יהיו שלמים.
- **מניעת טעויות.** התכן לא יאפשר כל טעות אנוש. התכן יתבסס על הנחת התוקף של גירסת גורמי אנוש של חוק מרפי:
אם המערכת מאפשרת למפעיל לטעות, במוקדם או במאוחר הוא אכן יטעה.
- **שימושיות.** תכן תפעול המערכת יתבסס על מודלים של המפעילים של המשתמשים, על מנת להבטיח שהם מבינים את תהליכי התפעול ואת התנהגות המערכת.

- **מודעות למצב.** התכן יתבסס על ההנחה שהמפעיל אינו מסוגל לעקוב אחר מצב המכונה באופן אמין. זוהי אחריות המפתח להבטיח שהמפעילים מודעים תמיד למצב המכונה.
- **הפחתת עומס התפעול.** התכן יתחשב בכל תפקידי המשתמשים, כולל אלו שאינם קשורים לתפעול המערכת. התכן ימנע הסחות, על ידי צמצום העומס המנטאלי הדרוש לצורך התפעול.
- **הגנה בפני שגיאות.** הסבירות לשגיאות משתמשים ומפעילים במצבים חריגים היא גבוהה. התכן צריך לכלול אמצעים להגן על המערכת בפניהן.
- **אימון ותרגול.** המפעילים צריכים להתאמן על מנת להכיר את המצבים החריגים, ולתרגל את אופן התפעול במצבים הללו. התכן צריך לכלול אמצעים לאימון ולתרגול.
- **בדיקות עם משתמשים.** תיקוף המערכת צריך להתבסס על בדיקות עם משתמשים ומפעילים אמיתיים, בסביבת עבודה אמיתית, שחושבים ומתנהגים כמו המשתמשים והמפעילים להם המערכת מיועדת.
- **אחריות ההנהלה.** הארגון האחראי על תפעול המערכת צריך, ולוודא תרגול התפעול במצבים חריגים.

מצבים חריגים

המצבים החריגים הם תוצאה של אירועים חריגים, כגון תקלת חומרה או טעות בהפעלת פונקציה. הבעיה במצבים החריגים היא שבתהליך פיתוח רגיל, המענה למצבים הללו הוא חלקי וחסר.

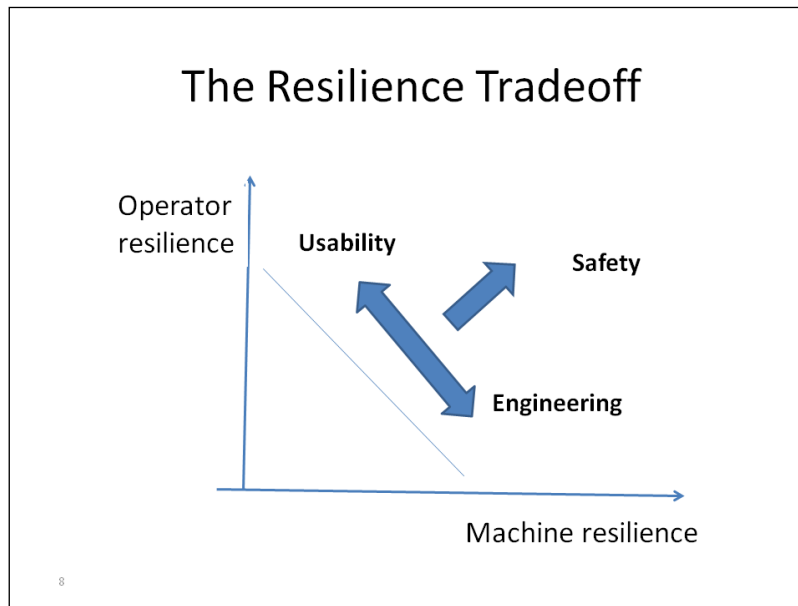
המורכבות של התנהגות המערכת במצבים חריגים עולה עשרות מונים על זו שבמצבי שגרה. לפיכך, עלות התיכון והבדיקות של תהליכי התפעול במצבים החריגים צריכים להיות גבוהים בהרבה מאשר אלה של המצבים השגרתיים. במציאות, המצב הוא הפוך. מאז ומעולם, תהליך פיתוח ובדיקות של מערכת הינו מוגבל בתקציב ובלו"ז. בהתחשב באילוצים הללו, בתהליך פיתוח אופייני מעדיפים להתמקד בתחילה בתהליכים המפעילים את הפונקציות העיקריות, בתפעול שגרתי.

בהתחשב בכך, המפרטים, התכן והבדיקות של התפעול המצבים החריגים לוקים בדרך כלל בחסר. כמו כן, בתפעול במהלך הבדיקות, המפעילים אינם זוכים בזמן מספיק על מנת להתנסות בתפעול המערכת בתנאים החריגים. בלוחות זמנים צפופים בעקבות אילוצי שיווק, יש לצפות לכך שהתכן כולל שגיאות משמעותיות, שאינן מתגלות בבדיקות. התוצאות של תפעול במצבים חריגים עלולות להיות חמורות.

התנהגות המערכת במצבים חריגים

במטרה למנוע מצבי כשל הנובעים מכך שהתנהגות המפעיל היא בלתי צפויה, מהנדסי מערכת עושים כמיטב יכולתם להעביר את תפקידי המפעיל אל המכונה. הבעיה היא שככל שהאוטומציה מינה יותר, למפעיל יש פחות הזדמנויות להתנסות בתפעול במצבים חריגים. כתוצאה מכך, כשהמערכת מגיעה למצב חריג, למפעילים חסר הידע הדרוש לתפעול במצב זה. לדוגמא, ב-40% מהתאונות האויריות שהתרחשו בין השנים 2001-2009 התברר שהיו ליקויים בהכרת הצוות את המערכת האוירית (Abbott, 2010). בעיה זו נקראת "האירוניה של האוטומציה" (Bainsbridge, 1983).

התרשים הבא, מתוך Zonnenshain & Harel (2013), מדגים את דילמת האיזון בין האוטומציה לבין שליטת המפעיל.



מצבים בלתי צפויים

אירועי כשל רבים קשורים במצבים שהם בלתי צפויים. למעשה, ניתן להגדיר את חסינות המערכת בתפעול כעמידות המערכת במצבים בלתי צפויים.

מצבים בלתי צפויים הם תוצאה של ליקויים במפרטים, טעויות בתכנון או שגיאות במימוש (בעיקר, באגים בתוכנה). דוגמאות של מצבים בלתי צפויים הן של חוסר תיאום מצב מפעיל-מכונה. במיוחד נפוצים המקרים בהם מפעיל אינו מודע לשינוי במצב המכונה. סוגים אחרים של מצבים בלתי צפויים כוללים:

- **חוסר עקביות תוך מערכתית.** הכוונה היא למצבי מכונה חריגים, שאינם תואמים את חוקי התפעול בשלב הפעיל של תהליך התפעול. חוסר העקביות נגרם מחוסר תיאום בין מרכיבי המכונה, כפי שמודגם על ידי התאונות במערכת הכימותרפיה Therac-25 (Casey, 1998).
- **חוסר עקביות בין מערכתית.** הכוונה היא להקשרים חריגים, שלא צוינו במסמכי הדרישו. חוסר העקביות הוא בין שתי תת-מערכות, כפי שמודגם על ידי תאונת האש הידידותית באפגניסטאן, בשנת 2001 (Casey, 2006).

מצבים לא עקביים נתפסים כבלתי ניתנים לחיזוי, ומשמעותם היא שהמפעילים אינם יכולים לזהות את המקור למצב הבעייתי.

אירועים בלתי צפויים

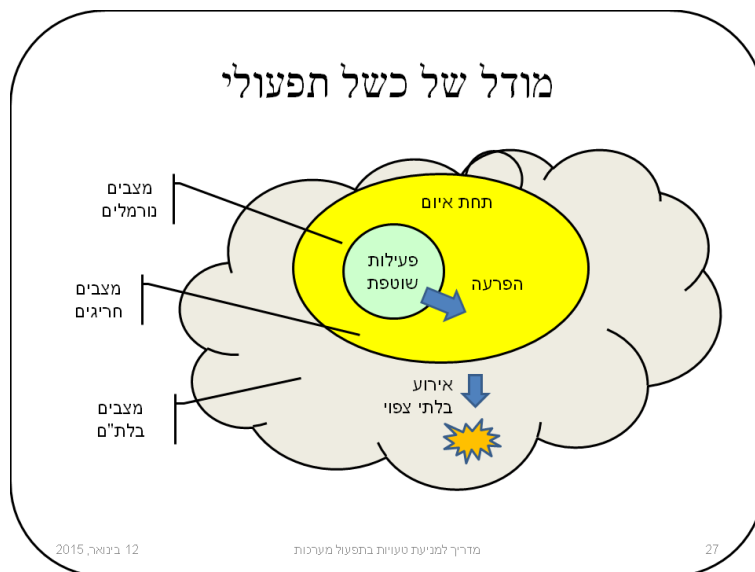
כאשר המערכת נמצאת במצב חריג, התכן עלול להתייחס אל אירוע רגיל באופן בלתי צפוי. כתוצאה מכך, המערכת עוברת למצב שהוא בלתי צפוי (Perrow, 1984). כאשר המפעיל נדרש להמשיך להפעיל במצב שהוא בלתי ידוע, הוא נדרש להתמצא במצב ולבחור את הפעולה הראויה, בתנאים בהם לא התנסה בעבר. תהליך ההתמצאות אורך זמן רב, ועלול להסתיים מאוחר מדי, או בפעולה שגויה. אם כתוצאה מכך נגרמו נזקים, אז האירוע שגרם לבעיה נקרא אירוע בלתי צפוי (Harel & Weiss, 2011).

מודל של כשל תפעולי

המדריך לאבטחת חסינות מבוסס על ההנחה שאירועים בלתי צפויים הם בעצם צפויים, והם נוצרים על פי סכימה המתוארת ע"י הראל ווייס (2011). בסכימה זו, האירועים הבלתי צפויים נוצרים בתהליך של חריגה מחוקי התפעול הנורמלי, שבעקבותיה הסלמה, כדלקמן:

- **שיבוש.** הפרעה גורמת לשינוי מצב התפעול מנורמלי לחריג. הפרעות הן אירועים צפויים, כאשר המערכת נמצאת במצב תפעול נורמלי, והיא ערוכה להתמודד עימם. במקרים רבים, המפעילים יכולים לזהות את המצבים החריגים, להתמודד עם הפרעה ולחזור למצב תפעול נורמלי.
- **אבדן אוריינטציה.** לעתים קורה שהמפעילים אינם מזהים את המצב החריג (המקרה של איום סמוי) או שהם פועלים לאט מדי בתהליך של איתור תקלות. בשני המקרים, המערכת נשארת במצב תפעולי חריג.
- **הסלמה.** במקרה של הפרעה נוספת, כאשר המערכת נמצאת עדיין במצב החריג, נוצר מצב בו המצב התפעולי הוא בלתי צפוי. המצב מעורפל, מורכב מדי מכדי שהמפעילים יוכלו להתמודד עמו.
- **אירוע.** כאשר מצב התפעול בלתי צפוי, תגובת המערכת לכל אירוע היא בלתי צפויה. בנקודה זו יש לצפות לכך שהמערכת תיכשל.

מצבי התפעול ותהליך היווצרותם של אירועים בלתי צפויים מודגמים בתרשים הבא:



שלש קטגוריות של מצבי תפעול

מודל החסינות משלב מודל של כשלים אופייניים עם תהליכים אופייניים של התמודדות עם מצבי הכשל. המודל המציג כשלים אופייניים מתואר במונחים של מצבי תפעול. המדריך מגדיר שלש קטגוריות של מצבי תפעול, המתייחסים אל שלשה סוגים של פעילות במהלך תפעול:

- **מצבים נורמליים,** המתייחסים לתפעול הנורמלי

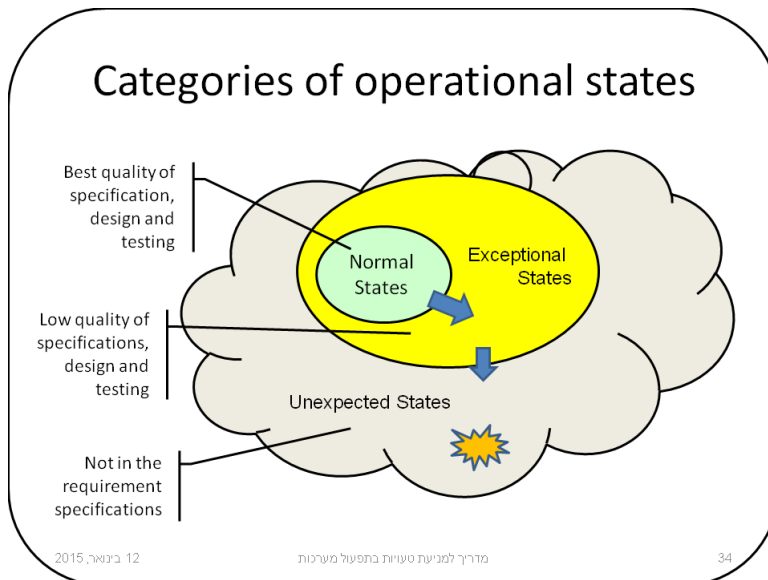
- **מצבים חריגים**, אליהם המערכת מגיעה כתוצאה של הפרעה (כולל מצבים סמויים וכולל מצבים של קושי של המפעילים לתקן את התקלה)
- **מצבים בלתי צפויים**, אליהם המערכת מגיעה כתוצאה של הפרעה, כאשר המערכת נמצאת עדיין במצב חריג.

האיכות של תכן האינטראקציה

האיכות של תכן האינטראקציה נגזרת מהמשאבים המושקעים במפרטים, בתכן ובבדיקות. השקעת המשאבים הללו שונה עבור שלשת הקטגוריות של מצבי תפעול:

- **מצבים נורמליים**. בתהליך פיתוח טיפוס, המיקוד הוא על התפעול הנורמלי. מרבית משאבי הפיתוח מוקצים לאבטחת איכות התפעול במצבים הללו.
- **מצבים חריגים**. בתהליך פיתוח טיפוס, משאבי הפיתוח המוקצים לשלב זה הם מועטים, והפיתוח מתנהל בדרך לא פורמלית, על ידי תיקון תקלות אד הוק, בתהליך של ניסוי וטעיה. כתוצאה מכך, איכות האינטראקציה במצבים הללו היא ירודה.
- **מצבים בלתי צפויים**. בתהליך פיתוח טיפוס, מצבים אילו אינם מוזכרים כלל במפרטים. התכן מסתכם במניעת קריסת המערכת, ובשיגור הודעת שגיאה למפעילים, שמשמעותה שהמערכת נמצאת במצב שהוא בלתי צפוי. הבדיקות אינן יכולות להתמודד עם מצבים שהם בלתי צפויים. המפעילים שמקבלים את הודעת השגיאה אינם מסוגלים להתמודד עמה.

איכות תכן האינטראקציה בשלשת הקטגוריות מודגמת בתרשים הבא:



מודל החסינות

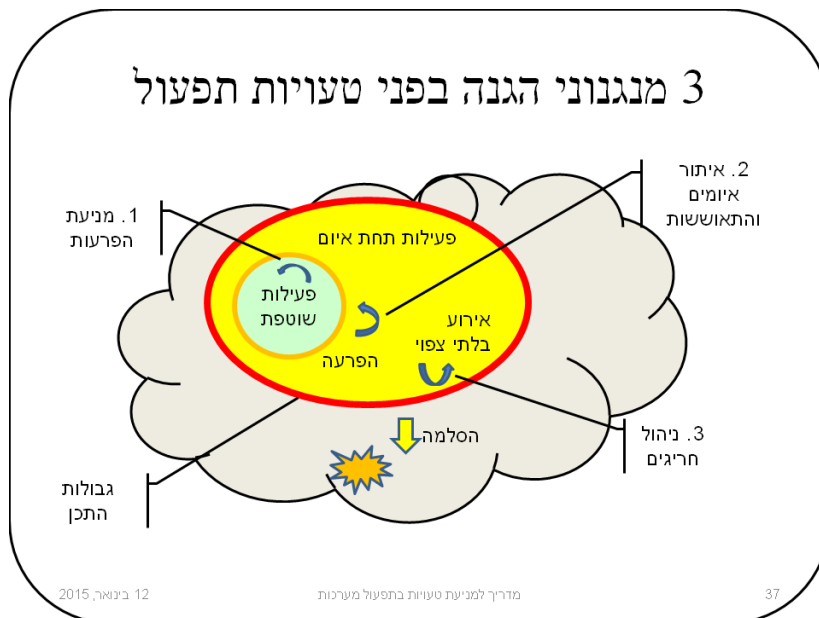
מודל החסינות מהווה מסגרת לתיאור מצבי כשל אופייניים. המודל מבוסס על מודל של התפיסה האנושית בהקשרים מעורפלים.

מודל החסינות המתואר כאן מבוסס על גירסא ראשונית שהוצגה על ידי Zonneschain & Harel (2011). הגירסא החדשה כוללת הגדרה של גבולות התכן, המגדירים את מנעד המצבים והפעילויות הקשורים למצבים נורמלים ולמצבים חריגים.

תכונת החסינות קשורה לשלש תכונות מערכת: אמינות, תגובתיות ויכולת התאוששות. היא נסמכת על שלשה קוי הגנה בפני אירועים בלתי צפויים:

- **מניעת הפרעות**, במטרה להמנע מהמצבים החריגים. קו הגנה זה ישים לכשלים שנובעים מפעולות מפעיל בלתי צפוי, וכן לאבטחת תואמות המצבים בין יחידות המערכת. קו הגנה זה אינו ישים להפרעות מסוגים אחרים, כגון, תקלות ברכיבים.
- **התאוששות מהפרעה**: מניעת איומים סמויים וניטור של תגובות לא רצויות במצבים החריגים. קו הגנה זה ישים להפרעות מסוג תקלות רכיבים, בדרך של איתור תקלות.
- **מניעת הסלמה**: אילוץ המערכת להשאר בגבולות התכן.

מודל החסינות, כולל שלשת קוי ההגנה, מתואר בתרשים הבא:



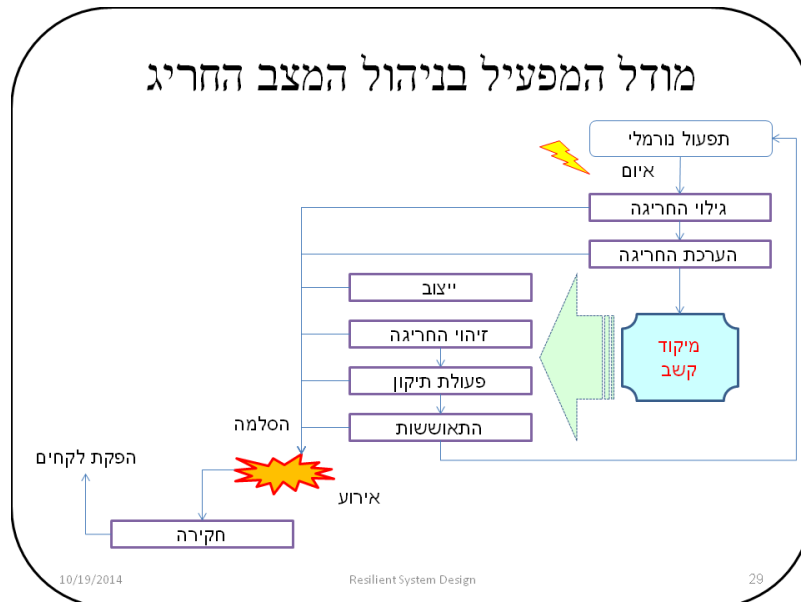
גבולות התכן

ההנחה במדריך היא שאין אפשרות מעשית להתייחס במפרטי ההתנהגות אל כל המצבים והאירועים האפשריים. לעומת זאת, המפרטים יכולים וצריכים להתייחס באופן שלם ומלא אל כל המצבים שנמצאים בגבולות התכן, דהיינו, כל המצבים הצפויים (כולל הנורמלים והחריגים).

בתרשימים לעיל, גבולות התכן מסומנים על ידי השטח הצהוב.

מודל של פתרון בעיות תפעול

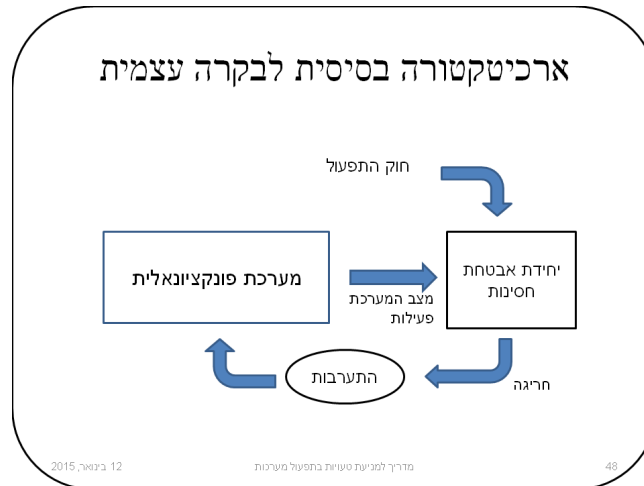
הדרך לשלוט באיומים היא על ידי המפעילים, בסיוע המכונה. ההתאוששות מאיומים נעשית בפעילות אינטראקטיבית, כאשר המכונה מיידעת את המפעילים לגבי מצבה, המפעילים משלבים מידע זה עם המידע והידע העומדים לרשותם, ופועלים בכדי להתגבר על האיום. התרשים הבא ממחיש את המודלים המנטאליים של המפעילים במהלך פתרון בעיות תפעול:



הפעילויות המנטאליות הנחוצות לפתרון הבעיות צורכות משאבי קשב ניכרים, ומחייבים התערבות של המפעיל. מאחר שבמקביל לתפעול המערכת, הקשב של המפעיל נדרש גם לפעילויות אחרות הקשורות לפתרון הבעיה, הפעילויות הללו רגישות לטעויות. במקרה שאחת מהפעילויות הללו נכשלת, כל התהליך נכשל, והמערכת מגיעה למצב שהוא בלתי צפוי.

בקרה עצמית של פעילות המערכת

מדריך זה נסמך על פרדיגמת STAMP, כלומר, המערכת צריכה להגביל את הפעילות שלה בהתאם לחוקי תפעול קשיחים, במטרה להמנע ממצבים בעייתיים. מכך משתמע שמפירטי הדרישות צריכים לכלול הנחיות מפורטות לגבי תהליכי התפעול המומלצים, והתכן צריך לכלול אמצעים לאיתור סטיות מהתהליכים הללו. כל סטייה מהחוקים נחשבת למחולל של אירוע כשל פוטנציאלי, והתכן צריך לכלול אמצעים לזיהוי המחוללים, ולהגיב כראוי. המימוש נעשה על ידי מודל של בקרה עצמית, המודגם בתרשים הבא:



סוגי אילוצים

המדריך מגדיר את הקטגוריות הבאות של אילוצים:

- אילוצים על אירועים:

- מעברי מצבים, מיפוי: (מצב נוכחי, אירוע) \leq מצב חדש
- תפוקת אירועים, מיפוי: אירוע \leq שינוי צפוי בפרמטרים של התפעול
- איתחול תהליכים, מיפוי: (מצב, עיתוי) \leq שינוי צפוי בפרמטרים של התפעול

- אילוצים מתמשכים:

- התנהגות, מיפוי: מצב \leq שינוי צפוי בפרמטרים של התפעול, כולל מרווח ערכים של הפרמטרים
- תיאום, מיפוי: מצב יחידה \leq מצב המערכת.

קוי הגנה על פי מטפורת הגבינה השוויצרית

מודל החסינות מיישם את מטפורת הגבינה השוויצרית בשני אופנים:

- **האפקט המצטבר של פעולות:** מהלך השינוי מסכנה לאירוע כשל, מיושם במודל החסינות בעזרת תיאור של שלשת קוי ההגנה העיקריים, המתוארים בעזרת מודל החסינות.
- **האפקט המצטבר של תגובות:** מהלך השינוי מסכנה להגנה, מיושם לתיאור הפעילויות המנטאליות של המפעיל במהלך איתור תקלות והתאוששות מהפרעות.

קוי הגנה

חסינות המערכת מושגת על ידי תכן שלשה קוי הגנה, בפני שלשה אופני כשל עיקריים:

- **מניעת כשל.** מניעת אופני כשל מסויימים על ידי תכן. קו הגנה זה ישים לטעויות תפעול מסויימות, כגון, הפעלת פונקציה בלתי רצויה. ההנחיות לביצור קו הגנה זה מבוססות על הדיסציפלינה של הנדסה קוגניטיבית
- **מניעת הסלמה.** הגנה בפני כשלים שלא נמנעו על ידי התכן, כגון, כשל של רכיבים, נפילות מתח והפרעות בתקשורת. ההנחיות לביצור קו הגנה זה מבוססות על עקרון הבקרה העצמית של STAMP. ההנחיות מבוססות על הגדרה מפורשת של תפעול נורמלי, חוקים פורמלים המגדירים את גבולות ההתנהגות התקינה של המערכת, וכן ארכיטקטורה התומכת בתגובה מתקנת במצבים של סטיות מהאילוצים.
- **לימוד מאירועים.** איתור וזיהוי אירועי כשל, והסקת מסקנות לגבי אמצעים למניעת אירועים דומים.

תיאור כללי של המדריך

המדריך כולל הנחיות להתמודד עם כשל ממקורות שונים (המדריך, חומרה, תוכנה, הקשר ...) ע"י מניעה, צמצום אפקטים שליליים, מניעת הסלמה, וכן הפקת לקחים מאירועי כשל. חלק זה של המאמר מציג את ההנחיות העיקריות במדריך.

מפרטי התנהגות המערכת

מפרטי התנהגות בגבולות התכן יכולים לכלול רשימה של המצבים הצפויים, וכן פירוט של התגובות החוקיות לכל האירועים האפשריים.

מניעת טעויות מפעיל

קו הגנה זה מתמקד במניעת טעויות מפעיל שעלולות להסיט את מצב התפעול מנורמלי למצב חריג.

בתכן לחסינות, אין לאפשר למפעיל לפעול באופן חופשי, כפי שנהוג בתהליכי ניסוי וטעיה. זאת, מכיוון שפעילות חופשית רגישה לטעויות, ועלולה לגרום בכך שהמערכת נמצאת במצב חריג, שאינו תואם את התרחיש הפעיל. לדוגמא, המשתמש במערכת טלביזיה ביתית עלול לכבות בטעות את הממיר הדיגיטלי במקום להדליק את הטלביזיה, כפי שהודגם על ידי Zonnenshain & Harel (2009).

בכדי למנוע טעויות כאלה, למעט מקרים חריגים, יש לאפשר למפעיל גישה אך ורק למבחר מצומצם של פונקציות, כאשר הפונקציות הנבחרות תואמות את השלב הפעיל בתהליך התפעול, המתייחס לתרחיש הפעיל. למשל, התכן יכול להגביל את הפונקציות בתפריטים, כך שהפונקציות הזמינות תהיינה אך ורק אלה הרלבנטיות לשלב בתהליך התפעול.

המשמעות היא שבתכן לחסינות, שליטת המפעיל במכונה צריכה להיות מוגבלת.

שליטת המפעיל במצבים חריגים

לו ידענו בזמן הגדרת הדרישות על כל המצבים החריגים, ועל דרך הפעולה המועדפת, לא היינו נזקקים למפעיל. במקום להפקיד את המערכת בידיהם של המפעילים, שמהימנותם בעייתית, היינו סומכים על המכונה. מכיוון שבזמן הגדרת המפרטים לא ברורים לנו עדיין כל מהלכי התפעול שהמפעיל יזדקק להם, אנחנו נאלצים לאפשר לו לבצע מספר מצומצם של פעולות "ליתר בטחון", בעיקר, במצבי חירום.

הבעיה בגישה זו היא שבתנאי לחץ, המפעילים אינם יצירתיים. הם מתקשים למצוא את הפתרון לבעיה אותה לא חוו בעבר. בדרך כלל, המפעילים נוהגים בתנאי חירום באותו אופן אליו הורגלו לפעול ברגיעה (Bainbridge, 1983). לפיכך, המדריך ממליץ לצמצם את חופש התמרון של המפעיל למינימום ההכרחי למצבי חירום בלבד, ולספק אזהרות מפני פעולות מסוכנות. המדריך ממליץ כיצד לנסח את האזהרות באופן שהמפעילים יתייחסו אליהם, למרות שהם פועלים בתנאי לחץ. המדריך ממליץ להמנע מהתרעות שווא, ולבחון את אופן התגובה של המכונה לפעולות הללו בקפידה.

מניעת טעויות מצב

טעויות מצב מאפיינות כשל הקשור בתפעול פקדים רב-שימושיים, המשמשים להפעלת מספר פונקציות, כאשר הפונקציה שמתבצעת בפועל נקבעת על פי מצב המערכת. למשל, אם לחצן ההפעלה בשלט רחוק של טלביזיה ביתית משמש להפעלת המסך ולהפעלת הממיר הדיגיטלי, אז השפעת הלחיצה עליו תלויה במצב השלט. במקרה של טעות מצב, המשתמש עלול להכבות את הממיר במקום את המסך, ולהיפך.

טעויות מצב ניתן למנוע על ידי הגבלת אפקט הפקד (בגבולות התרחיש) לפונקציה יחידה. לדוגמא, ניתן למנוע כיבוי בטעות של הממיר הדיגיטלי על ידי הגבלת לחצן ההפעלה (בגבולות של תרחיש הפעלה יומיומית) לשליטה במסך בלבד.

אבטחת תיאום בין יחידות המערכת

חוסר תיאום יכול להתבטא במספר אופנים. אחד מהם הוא כאשר אחת מהיחידות אינה מעודכנת לגבי שינוי בתרחיש הפעיל. בתפעול נורמלי במצב זה, המערכת עלולה להגיע למצב חריג. התכן צריך לוודא שתמיד, כל היחידות מעודכנות לגבי התרחיש הפעיל. המדריך ממליץ להקצות יחידה יעודית שתפקידה לתאם בין היחידות.

ההנחיות לתכן מונחה תרחישים הן:

- יש לציין את התרחישים במפורש במפרטי הדרישות
- יש לפרט את חוקי התפעול בכל אחד מהתרחישים
- יש להגדיר את התרחיש כמשתנה מערכת, ולממש אותו כך שיהיה זמין לכל יחידות המערכת. (מומלץ לאכסן אותו ביחידת התיאום היעודית).
- יש להגדיר את הסמכויות של היחידות השונות לגבי שינויי תרחיש
- יש להגדיר את האופן בו היחידות המוסמכות צריכות לעדכן את התרחיש הפעיל.

מניעת איומים סמויים

מניתוח תאונות מתברר שבמקרים רבים המערכת היתה תחת איום, אבל המפעילים לא היו מודעים לכך. למשל, בתאונת הכור הגרעיני TMI מספר שסתומים לא פעלו כמצופה, חלקם בגלל תקלת חומרה, וחלקם כתוצאה מרשלנות.

אחת המטרות המאתגרות בתכן לאבטחת חסינות היא למנוע איומים סמויים. איומים סמויים יכולים להגרם מכשל רכיב, טעות תפעול, באג בתוכנה, מעבר מצבים בלתי מתואם, הפרעת תקשורת ועוד. אם המפעילים אינם מודעים לאיום, הם אינם יכולים לפעול בזמן.

איום סמוי מוגדר כמצב של חריגה מחוקי התפעול אליו המפעיל אינו מודע. התכן ממליץ על הקצאת יחידה לאיתור חריגים, שצריכה לאתר מצבים של הפעלה בניגוד לחוקי התפעול התקין. היחידה לאיתור חריגים צריכה להעביר את המידע לגבי המצבים הבעייתיים אל יחידת ההתרעות. התכן צריך להגדיר שיטות לבחינת מצב המערכת, כגון, על ידי חיוויים יעודיים.

איתור טעויות מפעיל

לעתים המפעיל נדרש לבצע פעילויות החורגות מתהליך התפעול. למשל, במצבים בהם המפעיל מבחין בשינוי חריג במצב המערכת, או בסיכון הקשור בגורם חיצוני. התכן צריך לאפשר למפעיל חריגות מסוימות, למשל, במצבי חירום. הבעיה היא שהמפעילים עלולים להפעיל את הפונקציות החריגות בשוגג.

התכן ממליץ שבמסגרת תפקידיה, היחידה לאיתור חריגים צריכה לאתר גם מצבים של הפעלה של פונקציות באופן שנוגד את חוקי התפעול התקין.

התרעות על תקלות ברכיבים

כל רכיבי המערכת מועדים להכשל בשלב זה או אחר. בתכן של מערכות התרעה, עלינו להתחשב בכל אופני הכשל האפשריים, כולל תקלה בחיישנים או בהתרעה, הסחת המפעיל מתפקיד הבקרה, ועוד (Weiler & Harel, 2011).

מפתחי מערכות נמצאים תמיד תחת לחץ לפשט את המערכת, במטרה להוזיל אותה, ולפשט את תהליכי ההרכבה, ההתקנה והתחזוקה. בדרך כלל, מפתחי מערכות נמנעים מלקצץ בפונקציונאליות, ולכן הנטייה היא לקצץ ברכיבים המשמשים לאבטחת חסינות: חיישנים, תצוגות וחיוויים, התרעה קולית, וכיו"ב.

שאלה ראשונה שכל מתכנן חייב לשאול בנוגע להוספת חיוויים על תקלה ברכיב היא:

- מהו הסיכון הכרוך בכך שהרכיב יהיה תקול, ואף אחד לא יבחין בכך?

אם המצבים בהם המפעילים לא הבחינו בתקלה מהווים סיכון, אז צריכה להשאל השאלה הבאה:

- האם ניתן לסמוך על מדד ה-MTBF?

ה-MTBF זהו מדד סטטיסטי. מה יקרה אם הרכיב בספציפי נמצא בזנב של פונקציה ההתפלגות, כפי שאירע במקרה של ה-PORV בתאונת TMI? האם בעלי העניין במערכת מוכנים לקבל ברבורים שחורים כתוצאה מטעות מסוג זה?

אם בעלי העניין מוכנים לקבל כשלים סמויים בקשר לרכיב ספציפי, סביר להניח שרכיב זה אינו חיוני לתפעול המערכת, וראוי לשקול לפשט את המערכת על ידי גריעת הרכיב מהתכן. אחרת, אם תקלה מסוג זה תגרום מבוכה לבעלי העניין, התכן צריך לספק אמצעים לגילוי תקלות ברכיב, ולדווח עליהן כראוי.

MTBI - ה-MTBF של אירועי כשל

נצא מנקודת הנחה שבעלי העניין במערכת מעוניינים לקחת סיכון של איומים סמויים, במטרה להוזיל את המערכת. מפתחי המערכת יכולים לסייע להם בהערכת הסיכון. מכיוון שמדובר בתוצאות שהן בלתי צפויות, ושהרגישות שלהן בנסיבות האירוע היא גבוהה ביותר (Hollnagel et al., 2006) לא נוכל לספק הערכה אמינה של מחיר הטעות. אבל, נוכל לחשב שיערוך של הזמן הממוצע בין אירועי כשל (Mean Time Between Incidents).

$$MTBI = 1 / \sum_{Component} FR (Component)$$

כאשר FR (Fault Rate) זהו קצב התקלות, מחושב לפי

$$FR(Component) = 1 / MTBF (Component)$$

לצורך הדגמה, בכדי להתרשם מהערכים האפשריים של מדד זה, נבחן מערכת הכוללת 120 רכיבים לא קריטיים, כל אחד מהם נבחר כך שה-MTBF שלו הוא של 10 שנים. מכיוון שהרכיבים הללו אינם קריטיים, המפתח מחליט לחסוך את החיזויים הדרושים לאבחון תקלות בהם. החישוב לעיל מראה ששיעור התקלות במערכת זו הוא תקלה בכל חודש. נתון זה יש להציג לבעלי העניין, כדי שיוכלו להחליט האם הם מוכנים לקחת את הסיכון.

ההנחה הנגזרת מהדיון לעיל היא שבתכן המערכת יש שני סוגים של רכיבים: כאלו שהם חיוניים, וכאלו שהם מיותרים. את הרכיבים החיוניים יש לצייד באמצעים לגילוי ולחיזוי תקלות, ואת הרכיבים המיותרים עדיף להסיר מהתכן, על מנת לפשט את המערכת.

איתור תקלות בחיוויי הבטיחות

הרכיבים הנוספים לאבחון תקלות (חיישנים, אלגוריתמים, תצוגות וחיוויים, התרעות קוליות) מייקרים את המערכת, אבל בנוסף, הם עצמם גורמי סיכון חדשים, מכיוון שהם מהווים מקורות נוספים לתקלות (ראה דוגמת תקלת PORV בתאונת TMI). רכיבי הבטיחות מועדים אף הם להכשל, והתכן צריך להבטיח שהמפעילים ידעו כשזה קורה.

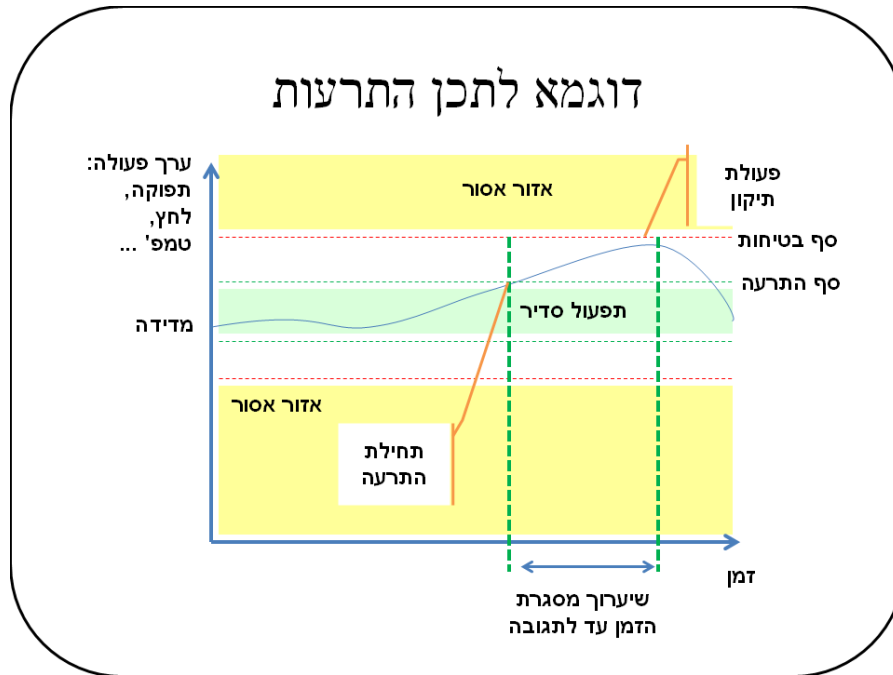
בתכן, יש להבחין בין המקרה של תקלה ברכיב עצמו לבין תקלה בדיווח על תקלה ברכיב. המדריך ממליץ להוסיף חיווי משני לכל חיווי ראשי, ומנחה כיצד ניתן לעשות זאת מבלי להוסיף לסיבוכיות המערכת, על ידי קידוד. במצבי כשל בחיישן או בתקשורת לחיישן, לא נשלח ממנו אות למערכת ההתרעה. לפיכך, ניתן לתכנן את החיוויים כך שהחיישן תמיד ישלח אות, גם במצב בו לא נתגלתה תקלה. המערכת תזהה תקלה ברכיב על ידי האות הספציפי לתקלה, ותקלה בהתרעה תזוהה על ידי מצב של חוסר מידע מהחיישן.

איתור בעקיפין של מצבי תקלה

חיישני מצב מאפשרים איתור וזיהוי מהיר של רכיבים תקולים, אבל לא בכל מצב. תקלות מסויימות, כגון, דליפה משסתום או ממיכל, קשה לגלות ישירות על ידי חיישנים, אבל ניתן לגלות בעקיפין, על ידי בדיקות חוקיות של פרמטרים תפעוליים. לדוגמא, דליפה ממיכל יכולה להשפיע על הלחץ במיכל. אם הלחץ הנמדד חורג מתחום של לחצים סבירים לתפעול נורמלי, היחידה לאיתור חריגים יכולה לאתר את התקלה ולדווח עליה ליחידת ההתרעות.

דוגמא פשוטה לשימוש בשיטה זו היא זו המשמשת בבקרת תהליכים סטטיסטית (SPC) בבקרת ייצור. אופן השימוש בשיטה זו מודגם בתרשים הבא:

דוגמא לתכנ התרעות



בכדי לאפשר איתור תקלות, מפרטי התפעול צריכים לכלול תיאור של התנהגות המערכת במצבי תקלה. תיאורים כאלו ניתן לפתח בטכניקות של FMEA.

איתור גורם ההתרעה

לאחר שהמכונה התריעה על תקלה, המפעיל נדרש לאתר את הרכיב שגרם להתרעה. הבעיה של המפעיל היא במצבים בהם הוא אינו יודע לזהות את מקור ההתרעה על סמך מאפייני ההתרעה, כי מעולם לא הוכשר לכך, ולא התנסה בסוג זה של תקלה במידה מספקת על מנת שיזכור אותה.

בעיה נוספת היא כאשר מספר רכיבים יכולים להיות הגורמים לאותה ההתרעה. דוגמא לכך היא המצב של ירידת לחץ במיכל. לירידת הלחץ יכולות להיות מספר סיבות, כולל דליפה מהמיכל, דליפה מאחד השסתומים, מצב בלתי צפוי של אחד השסתומים ועוד. במצבים אלו התהליך של איתור גורם התקלה עלול להיות בלתי יעיל, ולכן איטי מדי (כפי שאירע בתאונת TMI, בעקבות התקלה ברכיב ה-PORV).

בכדי להבטיח התאוששות מהירה ממצב התקלה, התנהגות המערכת במצב תקלה צריכה לייצג את גורם התקלה באופן חד ערכי. המיפוי מגורם התקלה להתנהגות המערכת צריך להיות הפיך. חוקי התפעול צריכים להיות ברמת פירוט כזו שיאפשרו בניית מודל של התנהגות המערכת במצב תקלה. מודל כזה יאפשר זיהוי גורם התקלה על סמך מדידת השינויים בפרמטרים של התנהגות המערכת (כגון, מדידות לחץ וטמפרטורה במיכל). ניתן ליצור חוקים כאלו בדרך של ניתוח, בשיטות הנקוטות ב-FMEA, ובעזרת סימולציה.

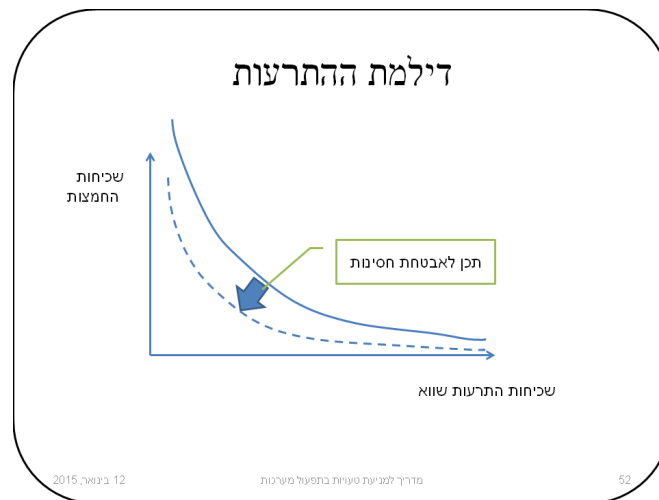
מניעת הסלמה

על פי מודל החסינות, הסלמה פירושה חריגה מגבולות התכן. למניעת הסלמה, התכן צריך להגביל ולבקר את האירועים במערכת כאשר היא במצב חריג, למינימום ההכרחי, כלומר, לאירועים שתואמים את תהליכי ההתאוששות, ולפעולות חירום. במקרה של פעולת חירום יש לוודא שהפעולה אינה גורמת לחריגה מחוקי התפעול. במקרה של חריגה, יש להפעיל רשת בטחון, שמשמעותה מעבר לתפעול במוד חירום.

השוואת פתרונות חלופיים

לעתים, התכן נדרש לבחור בין פתרונות חלופיים. למשל, בקביעת ערך סף להתרעה, יש לבחור בין אופציה של מיעוט החמצות לעומת אופציה של מיעוט התרעות שווא. במצבים מסויימים, ניתן על ידי שינוי יעד התכן לקבל פתרון טוב יותר מהחלופות המקוריות. בדוגמא של התרעות, השיפור יכול להתקבל על ידי מניעת התרעות טורדניות בעזרת חיוויים ואישורים המאורגנים בהתאם למהלך אירועים אופייני במצבי התרעה. דוגמא ליישום פתרון כזה מוגדרת בתקן ANSI/ISA 18.2 לניהול התרעות בתעשייה התהליכית.

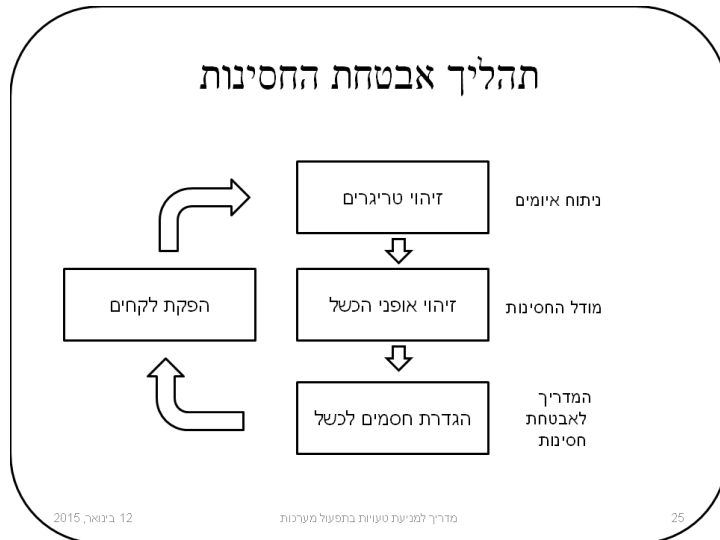
המדריך כולל המלצות לשיפורים הנדסיים, כפי שמתואר בתרשים הבא:



תהליך השיפור המתמיד

כאשר התכן הוא מונחה חסינות, מפרטי התפעול כוללים הגדרה של חוקי תפעול, המבוססים על ידע של מומחי תוכן, ומתקבלים בתהליכים של ניתוח מערכת. כל טעות בהגדרה של חוקי התפעול בא לידי ביטוי בכשל תפעולי: חוקים קשיחים מדי יגרמו לדיווחי סרק על כשל. חוסר בחוק תפעול מסויים יגרום לאירועי כשל סמויים, שהמערכת לא זיהתה בעוד מועד.

בדרך כלל, יש לצפות לכך שבמהלך התפעול יתברר שיש צורך בביצוע שינויים של חוקי התפעול. את השינויים הללו יש לנהל בתהליך מבוקר. החסינות מתפתחת באופן הדרגתי, במחזורים, כאשר כל מחזור כולל איבחון של מצבי כשל, הפקת לקחים, ויישום השינויים. מחוללי המחזורים הם אירועי כשל, כמודגם בתרשים הבא:

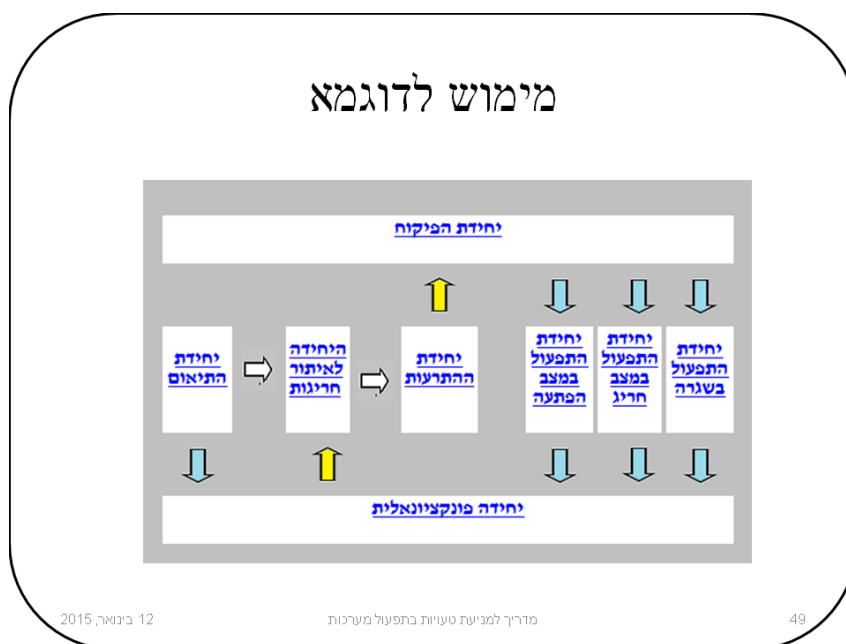


המדריך כולל המלצות לפיתוח וישום כלים לדיווח ולשיתוף מידע לגבי אירועי כשל. כלים אלו מאפשרים את המעבר מתרבות של האשמה וענישה לתרבות בטיחות. המדריך ממליץ לפתח חיישני כשל, שמאפשרים מעקב אחר הפעילות במהלך התפעול, איתור חריגות וניתוח אירועים של טרום כשל, על ידי בדיקת הפעילות והתאמתה לאילוצים. המדריך ממליץ על דיווח בשתי רמות:

- ברזולוציה גבוהה, מקרים של מעבר מפעילות נורמלית לפעילות חריגה
 - ברזולוציה נמוכה, מקרים של מעבר מפעילות חריגה למצבים בלתי צפויים.
- התוצר של כל מחזור הוא מסמך דרישות לשינויים בהגדרת החוקים ו-או בתהליכי התפעול.

מימוש

המדריך ממליץ על ארכיטקטורה שמאפשר ליישם את העקרונות לאבטחת חסינות, כמודגם בתרשים הבא:



ארכיטקטורה זו מאפשרת פיתוח מודולרי של פונקציות חסינות עיקריות, כדלקמן:

- יחידת תיאום, תפקידה לנהל את השינויים בתרחיש הפעיל, ולאפשר גישה לכל יחידות המערכת, לצורכי אבטחת עקביות
- היחידה לאיתור חריגות, בודקת את התאמת הפעילות לאילוצים, ודווחת על הפרות ליחידת ההתרעות
- יחידת התרעות, מדווחת למפעילים על חריגות ומנחה אותם למציאת מקור התקלה
- יחידות לניהול האינטראקציה: במצב נורמלי, חריג, ובחירום
- יחידת פיקוח, המגדירה את מצב התפעול (נורמלי, חריג, חירום) המפעילה את יחידות האינטראקציה בהתאם.

פיתוח המדריך

מדריך זה הינו תולדה של שני מפגשים במסגרת קבוצת העבודה לניהול סיכונים של אילטם, בשנת 2010. במהלך שני מפגשים של קבוצת העבודה ניהלנו דיון על הסיכונים בגין טעויות תפעול. לאחר המפגשים, תיעדנו את הדיונים במסמך המגדיר ששה סוגים של טעויות תפעול, ומציע הנחיות להמנע מהטעויות הללו.

בהמשך, מרכז גורדון קידם שני פרויקטי חלוץ, בנושא הסיכונים של אירועים בלתי צפויים (Harel & Weiss, 2011) ובנושא ניהול סיכונים של טעויות שימוש (Weiler and Harel, 2011).

הפרויקט של כתיבת מדריך לאבטחת חסינות התחיל בשנת 2012. מטרת הפרויקט היתה לייצר שני מסמכים:

- מודל חסינות, המתאר את התנהגות אופיינית של מערכות במצבים חריגים
 - מדריך להמנע ממצבי כשל המתוארים בעזרת מודל החסינות
 - מאגר של אירועי כשל, הכולל ניתוח של 60 מקרים, לצורך תיקוף התועלת של המדריך.
- העקרונות עליהם מבוסס המדריך תוארו במאמר קודם (Zonnenshain & Harel, 2013). הגרסא הנוכחית של המדריך היא אינטראקטיבית, והיא נגישה לכל דיכפין באינטרנט. זאת, מתוך מחשבה שמהנדסי מערכת יכולים לבחון את ישימות המדריך לפרויקטים שלהם, ולתרום לשיפור המדריך.

דוגמת שימוש במדריך

אחד מאופני הכשל הנפוצים הוא כאשר במהלך התפעול הנורמלי, המערכת מאפשר ביצוע פעולות הנדרשות לתפעול לצרכי תחזוקה. ביצוע פעולות מסוג זה עלול להביא למצבים של איומים סמויים. אופן כשל זה זוהה כגורם עיקרי לתאונות רבות, כולל הכור הגרעיני TMI (Wikipedia 2014a), המיכלית טוריי קניון (Wikipedia 2014b), והרעלת הציאניד בבהופל (Wikipedia 2014). כמו כן, אופן כשל זה זוהה כגורם עיקרי לטעויות מצב בתפעול מכשירים ביתיים, כגון טלביזיה. ההנחיות במדריך לתכן מונחה תרחישים, ולאילוץ המערכת לפעול על פי חוקים שהם ספציפים לתרחישים, מאפשרים למנוע סוג זה של תקלה.

שיטת תיקוף המדריך

תכנית התיקוף ביקשה להתייחס אל מגוון רחב של טעויות שימוש, כפי שבאו לידי ביטוי באירועי כשל ממקורות שונים. התכנית היתה להקים מאגר של נתונים על אירועי כשל, ולהיעזר בנסיון של מהנדסי מערכות מנוסים במגוון של עיסוקים ויישומים. התכנית שיושמה כוללת:

- ביקורת של עמיתים, מומחים בתחום של הנדסת מערכות, במסגרת קבוצת עבודה של INCOSE_IL ואילטם. חברי הקבוצה התבקשו לתרום מנסיונם למאגר האירועים, ולסייע בהערכת המקרים שהוצגו במהלך הפגישות.
- הערכה של התועלת הפוטנציאלית של ההנחיות במדריך במניעת כל אחד מהאירועים שבמאגר, והצגת סטטיסטיקות של ההערכות הללו.

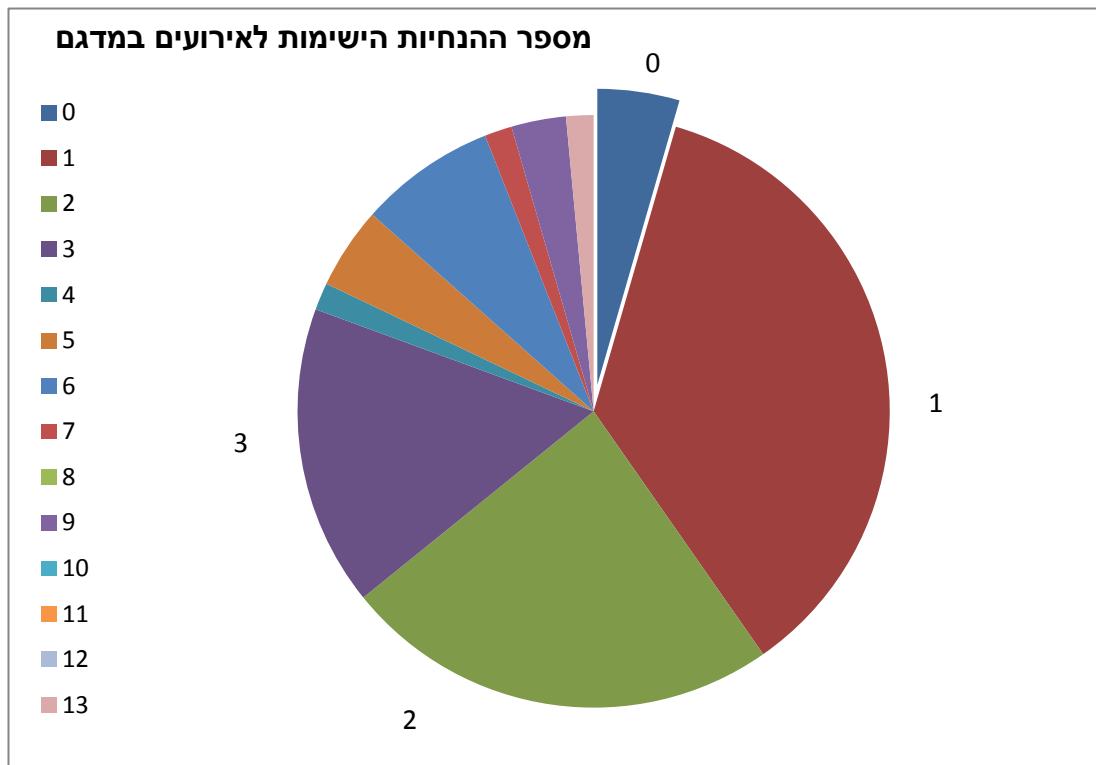
מאגר האירועים

לצורך תיקוף המדריך הוקם מאגר של כ-70 אירועי כשל, ממקורות שונים, כולל ניתוחים של תאונות מפורסמות, וכן דיווחים של חברי קבוצת העבודה של INCOSE_IL. כל אחד מהאירועים שהוכנסו למאגר כלל את המידע הבא:

- תיאור של האירוע
 - תיאור של אופני הכשל שתרמו לאירוע
 - קישורים להנחיות במדריך שעשויות פוטנציאלית ללמנוע אופני כשל מסוג זה.
- הקישורים להנחיות שימשו לצורך הערכת התועלת של ההנחיות הספציפיות שבמדריך, אל ידי חישובים סטטיסטיים. ניתוח של כשל לדוגמא הוצג במאמר על מניעת תאונות בגין אי ציות להתרעות לציבור (Zonnenshain & Harel, 2013a).

ממצאי התיקוף

ממצאי התיקוף מוצגים בתרשים להלן:



התוצאות העיקריות הן:

- 96% מהאירועים במאגר ניתן למנוע בעזרת ההנחיות במדריך
- 60% מהאירועים ניתנים למניעה בעזרת שתי הנחיות או יותר
- 44% מהאירועים ניתנים למניעה בעזרת שלש הנחיות או יותר.

תהליך התיקוף הביא למספר מסקנות לגבי ההנחיות, ולצורך לבצע שינויים בתוכן ובפורמט של המודל ושל המדריך. השינויים העיקריים בתוכן כללו:

- הוספת פרק מבוא, הכולל הסבר כיצד להשתמש במדריך
- גירסת גורמי אנוש של חוק מרפי
- המלצה על ארכיטקטורה למערכת חסינה
- הגדרה פורמלית של ממשקי הפעלה ידידותיים, התנהגות נורמלית ומצבי תפעול
- הרחבת ההגדרה של איומים, הכוללת הסחות ותנאים קיצוניים
- איפיון של אירועים נדירים, במונחים של ברבורים שחורים ואפורים
- הגדרה של רגעי זהב וזמן חסד עד לנקודת אל-חזור
- הנחיות להוספת חיישנים לאיתור מהיר של גורם הכשל
- הנחיות לגבי ניהול התפעול במוד חירום
- אזהרות לגבי הנזק לבטיחות בגין תוספי בטיחות
- הנחיות להערכת התועלת והנזק של תוספי בטיחות, ובחירת פתרון אופטימלי
- הנחיות למניעת כשלים סמויים, כגון, בגין ניתוק מערכות גיבוי לחירום
- הנחיות למניעת טעויות מצב
- הנחיות לתכן לחסינות בתהליכי תחזוקה
- הנחיות להגדרת ערכי ברירת מחדל במפרטים
- הנחיות לפתרון דילמות השליטה-אוטומציה
- הנחיות לפתרון דילמת עומס מסך
- הנחיות לאבטחת תואמות מצב, על ידי תכן מונחה תרחישיים
- הנחיות לגבי התאמה למפעילים ולתנאי התפעול
- פרק על התאמה לתפקידי המפעיל
- הנחיות להקצאת אחריות מונחית בטיחות
- הנחיות לאימון ותרגול להתמודד עם מצבים חריגים ועם אירועים בלתי צפויים.

כמו כן נדרשו שינויים בפורמט המודל והמדריך:

- פותחה גירסה אינטקטיבית, שמקלה על ההתמצאות בסבך ההנחיות
- ההנחיות אורגנו על פי פעילויות הנדסיות במהלך פיתוח, במקום על פי אופייני הכשל.

מגבלות

- בגירסה הנוכחית של המדריך קיימות מספר הנחיות שלכאורה סותרות זו את זו. מיקרים של הנחיות סותרות נקראות במדריך זה "דילמות". המדריך כולל המלצות לפתרון הדילמות, אבל עדיין לא ברור באיזו מידה המלצות אלה ברות תוקף.

- מדריך זה לא ייושם עדיין על פרויקט אמיתי, במלואו. יש לצפות שדילמות נוספות יוצגו לאחר שנקבל נסיון ביישום המדריך על פרויקט אמיתי.
- לא ניתן להגדיר בנקל את אילוצי התפעול במדויק כבר בשלב הגדרת הדרישות. יש לפתח אותם בהדרגה, עם רכישת נסיון בהפעלת המערכת, לרכך אילוצים הגורמים להתרעות שווא, ולהוסיף אילוצים בתגובה לאירועי כשל מפתיעים.
- על מנת שאפשר יהיה ליישם את המדריך ולבדוק אותו על פרויקט אמיתי, יש צורך להגדיר תהליך של שיפור הדרגתי של האילוצים, על בסיס הנסיון שמצטבר במהלך התפעול, וכן את הכלים הדרושים למימוש תהליך כזה: מעקב אחר התפעול, איתור אירועי כשל, דיווח, ניתוח האירועים, הערכה ועידון של החוקים.
- השיטה להערכה ולתיקוף המדריך רגישה להטיות, מכיוון שפעילויות ההערכה התיקוף מנוהלות על ידי מחברי המאמר, המעורבים בפיתוח המדריך. יש להרחיב את מעגל ההערכה והתיקוף לכלול בו מהנדסי מערכות שאינם קשורים אל מחברי המאמר.

סיכום

מודל החסינות והמדריך לאבטחת חסינות הוצגו בפני קבוצת העבודה של אילטם INCOSE_IL. חברי הקבוצה הביעו את הערכתם לגבי הצורך במדריך כזה, והתרומה הפוטנציאלית שלו. בשלב זה אנחנו מחפשים אחר שותפים בתעשייה המעוניינים ליישם את המדריך בפרויקטים שלהם. תכנית העבודה ליישום המדריך בפרויקטים כוללת פיתוח תהליך של כיוון אילוצי התפעול.

מקורות

- Abbott, K., (2010). Presentation made at the Flight Safety Foundation International Aviation Safety Seminar, November, Milan, Italy.
- AlertDriving. 2014. "Human error accounts for 90% of road accidents". Accessed 15 May. <http://www.alertdriving.com/home/fleet-alert-magazine/international/human-error-accounts-90-road-accidents>
- Bainbridge, L. 1983. Increasing levels of automation can increase, rather than decrease, the problems of supporting the human operator. *Automatica*, 19, 775-779. Reprinted in: (1987) Rasmussen, J., Duncan, K. and Leplat, J. (eds.) *New Technology and Human Error*, Wiley, Chichester, pp. 276-283,
- Baker, C.C. & Seah, A.K., 2004. "Maritime Accidents and Human Performance: the Statistical Trail" Paper presented at MARTECH 2004, Singapore, September 22-24, <https://www.eagle.org/eagleExternalPortalWEB/ShowProperty/BEA%20Repository/References/Technical%20Papers/2004/MaritimeAccidentsHumanPerformance> Accessed 15 May. 2014
- Casey, S.M., 1998. *Set Phasers on Stun: And Other True Tales of Design, Technology, and Human Error*. Aegean Pub. Co.

- Casey, S., 2006. Death on Call; in S. Casey: *The Atomic Chef, And Other True Tales of Design, Technology and Human Error*, Aegean Publishing.
- Dekker, S., 2006. *The Field Guide to Understanding Human Error*, Ashgate.
- Dekker, S., 2007. *Just Culture: Balancing Safety and Accountability*. Ashgate.
- Doc 9859, 2009. *Safety Management Manual (SMM)*. International Civil Aviation Organization (ICAO)
(http://www.icao.int/anb/safetymanagement/DOC_9859_FULL_EN.pdf).
- Eurpcontrol, 2006. "[Revisiting the Swiss cheese model of accidents](#)". October 2006
- Firesmith, D.G., 2005. "Are Your Requirements Complete?", in *Journal of Object Technology*, vol. 4, no. 1, January-February pp. 27-43.
http://www.jot.fm/issues/issue_2005_01/column3
- Harel, A. & Weiss, M., 2011. "Mitigating the Risks of Unexpected Events by Systems Engineering". Paper presented at The Sixth Conference of INCOSE-IL, Hertzelia, Israel
<http://www.ergolight-sw.com/CHI/Company/Articles/Weiss-Harel-Managing%20Unexpected%20Events.pdf> Accessed 15 May. 2014
- Hollnagel, E. (1983). "Human error". Position Paper for NATO Conference on Human Error, August 1983, Bellagio, Italy
- Hollnagel, E., Woods, D. and Leveson, N. 2006. *Resilience Engineering: Concepts and Precepts*. Aldershot, UK: Ashgate Publishing Limited.
- Jackson, S. 2010. *Architecting Resilient Systems: Accident Avoidance and Survival and Recovery from Disruptions*. Hoboken, NJ, USA: John Wiley & Sons.
- 2013. "Resilience principles for engineered systems". *Systems Engineering* 16(2):152-164.
http://www.researchgate.net/publication/255992165_Resilience_Principles_for_Engineered_Systems Accessed 15 May. 2014
- Kariuki, G. & Löwe, K., 2004. "Prism: incorporation of human factors in the design process". Accessed 15 May. <http://www.epsc.org/data/files/PRISM/Background.pdf>
- Landauer, T.K., 1996. *The Trouble with Computers: Usefulness, Usability, and Productivity*. A Bradford Book.
- Leveson, N., 2004. "A New Accident Model for Engineering Safer Systems". *Safety Science*, Vol. 42, No. 4.
- Leveson, N., 2012. "Engineering a Safer World: Applying Systems Thinking to Safety". *MIT Press*. <http://mitpress.mit.edu/catalog/item/default.asp?tttype=2&tid=12662> Accessed 15 May. 2014
- Meister, D., 1999. *The History of Human Factors and Ergonomics*, CRC Press
- Nielsen, J., 1993. *Usability Engineering*, Academic Press, Boston

- Norman, D.A. 1983. Design rules based on analyses of human error. *Communications of the ACM*, 4, 254-258.
- Norman, D.A., 1990. "Commentary: Human Error and the Design of Computer Systems". Editorial published in *Communications of the ACM*, 33, 4-7.
- Perrow, C., 1984. *Normal Accidents*, Princeton University Press
- PlaneCrashInfo. 2014. "Causes of Fatal Accidents by Decade (percentage)". Accessed 15 May <http://planecrashinfo.com/cause.htm>
- Reason, J., 1997. *Managing the Risks of Organizational Accidents*, Ashgate.
- Robert, D., Berry, D., mullaly, J. and Insensee, S., 1998, *Designing for the User with OVID*. Macmillan Technical Pub
- RSWG. 2014. "Resilient Systems Working Group". Accessed 15 May. <http://www.incose.org/practice/techactivities/wg/rswg/>
- SEBK. 2014. "Systems Engineering Body of Knowledge" Accessed 15 May. 2014 http://www.sebokwiki.org/wiki/Resilience_Engineering
- Segal, G. 2014, "The validation of templates for designing resilient systems", M.Sc. Dissertation, Technion, Haifa.
- Silvianita, M., Faris, K. and Kurian, V. J., 2011, Critical Review of a Risk Assessment Method and its Applications, Int. Conference on Financial Management and Economics, Singapore. <http://www.ipedr.com/vol11/16-R10014.pdf> Accessed 23 Oct. 2014.
- Taleb, N., 2007. *The Black Swan: The Impact of the Highly Improbable*, Random House Trade Paperbacks.
- Weinberg, G., 1971. *The Psychology of Computer Programming*. Dorset House.
- Wikipedia. 2014. "Bhopal disaster". Accessed 15 May. http://en.wikipedia.org/wiki/Bhopal_disaster,
- . 2014a. "Three Miles Island accident". Accessed 15 May. http://en.wikipedia.org/wiki/Three_Mile_Island_accident
- . 2014b. "Torrey Canyon oil spill". Accessed 15 May. http://en.wikipedia.org/wiki/Torrey_Canyon_oil_spill
- Weiler, M. & Harel, A., 2011. "Managing the Risks of Use Errors: The ITS Warning Systems Case Study". Paper presented at The Sixth Conference of INCOSE-IL, Hertzelia, Israel. <http://www.ergolight-sw.com/CHI/Company/Articles/ITS-Alarms-Apr2011.pdf> Accessed 15 May. 2014
- Zonnenshain, A. and Harel, A., 2009. "Task-oriented System Engineering". Paper presented at the INCOSE International Symposium, Singapore. <http://www.ergolight-sw.com/CHI/Company/Articles/Task-Oriented-SE.pdf> Accessed 15 May. 2014

- Zonnenshain, A. and Harel, A., 2013. "Resilience-oriented design". Paper presented at The Seventh Conference of INCOSE-IL, Hertzelia, Israel. <http://ergolight-sw.com/CHI/Company/Articles/Resilience-oriented-design.pdf> Accessed 15 May. 2014
- , 2013a, "Towards families of resilient systems". Paper presented at The Yossi Levin Conference, Technion, Haifa, Jan. 9th, <http://ergolight-sw.com/CHI/Company/Articles/TowardFamiliesArticle-eng.pdf> Accessed 15 May. 2014