

# קבוצת עבודה ניהול סיכונים ניהול סיכוני תפעול

כתב: אבי הראל – ארגולייט בע"מ,

יו"ר קבוצת העבודה: ד"ר משה ויילר – הטכניון ותע"א

## 1. רקע

במסגרת קבוצת העבודה בנושא "ניהול סיכונים" תחת INCOSE\_IL ואילטם התקיים ב-19 בינואר דיון בנושא סיכוני תפעול והגורם האנושי. בסיכום הדיון התקבלה החלטה לכתוב מסמך "מתכון" למהנדסי מערכות, על מנת לסייע להם בהתמודדות עם סוג סיכונים אלה (שמטבעם "רכים" יותר). לצורך כך, חברי הקבוצה התבקשו להציע סיכוני תפעול בהם נתקלו במהלך עבודתם, ולהציג אותם כדוגמאות לבדיקת איכות המתכון (המסמך נכתב ב-15 לפברואר 2010 ועבר הגהות של חלק מחברי הקבוצה).

## 2. מטרה

מטרת מסמך זה להגדיר את תכולת המתכון ולהציג גרסה ראשונית של המתכון ושל תוכנו.

## 3. שיטה

פרק 4 מציג את 15 דוגמאות שהובאו על ידי חברי הקבוצה ושל כותב מסמך זה.

פרק 5 מגדיר 6 סוגים של סיכוני תפעול, ומשייך אליהן את הדוגמאות של חברי הקבוצה, של כותב המסמך וכן דוגמאות מהספרות של חקר תאונות.

פרק 6, מציג הצעה לניהול הסיכונים, כולל תרופות ספציפיות לסוגים השונים של סיכוני התפעול.

פרק 7 (הדיון), המסכם מסמך זה, מנתח ומעריך את האפקטיביות של השימוש בתרופות המוצעות על סמך הדוגמאות.

## 4. דוגמאות של טעויות תפעול

מקור : חברי קבוצת העבודה

### 4.1 שבירת נעילה

בטילי נ"ט מדורות מתקדמים הנורים ע"י כוון קרקעי, לכוון הטיל קיימת בעיה המשויכת לתחום האמור, מאחר והוא עצמו חלק פיזי מהמערכת. לרוב, מביט הכוון דרך הכוונת האופטית אל המטרה (להלן הציר האופטי), ואז עובר להביט דרך ערוץ נוסף (להלן ציר הטיל). בציר הטיל מתבצעת "נעילה" על המטרה, ואז באם הכוון מטה את המערכת בכיוון מטה (תופעה שקיימת טבעית), עדיין נשמרת הנעילה (למרות התזוזה הקיימת אך האיטית הכוון אינו מרגיש בה כמעט). במצב זה מתפתח סיכון חמור של ירי לעבר הקרקע בעוד הכוון חושב שהוא יורה לעבר המטרה בציר המחבר אותו אליה. הפיתרון לכך בא בדמות מנגנון אוטומטי של שבירת נעילה באם ציר הטיל יורד נמוך מידי (יש להגדיר כמה זה נמוך מידי, על מנת לא לשבור נעילה כל הזמן).

מאפייני (חומרת) הסיכון :

ירי טיל לקרקע לפני הכוון מהווה אירוע חמור בטיחותית, ולכן זו חומרה גבוהה.

הסתברות הסיכון :

ההסתברות לקרות האירוע יחסית גבוהה משני היבטים : האחד, מאחר ולרוב סוג כזה של מערכות כולל יכולת לצודד ו/או להגביה או להנמיך את משגר הטיל, אזי על מנת לשמור את המערכת ביציבות הכוון חייב להשקיע כוח מסוים אם כי קטן, ואז לכיוון מטה בשל כוח הכובד ישנה עדיפות. השני, הכוון נוטה "ליפול" קדימה בייחוד בעת הכנסת העין לכוונת ו"דחיפת" המצח לתוך המערכת, מה שיביא לאותה תוצאה.

### 4.2 אנרגיה מסוכנת בתחזוקה

מכשיר ראית לילה שכולל בתוכו לייזר שמופעל בעזרת מתח גבוה (כמה מאות וולטים) עם אנרגיה מסוכנת. בעת פתיחת קופסה לצורך תחזוקה, עלול להיווצר מצב בו נשאר מתח מסוכן על פני קבל האנרגיה, דבר שעלול לסכן את איש התחזוקה.

כאשר הלייזר נדרך, אך לא ירה, קבל האנרגיה נשאר טעון ויכול להישאר כך למשך זמן רב. אם המכשיר מגיע בצורה כזו לתחזוקה, ישנה סכנה מוחשית שהטכנאי יקצר בידיו את הקבל לקופסה המוארקת ויסכן בכך את חייו.

פתרון אחד היה להכניס נגד פריקה קבוע שיפרוק את קבל האנרגיה תוך פרק זמן נתון. חסרון של פתרון זה שגורם לבזבוז אנרגיה בזמן הטעינה וההמתנה לירי הלייזר, דבר שמפחית את שימושיות המכשיר שפועל על סוללה.

פתרון שני היה לחבר נגד דרך ממסר שיחבר אותו רק אם פותחים את הקופסה (אינטרלוק נפתח). הבעיה במקרה זה אינה עלות אלא חוסר בנפח פנוי להכנסת ממסר כזה.

הפתרון שנבחר היה לנתק את הקופסה מהארקה (מקטין את הסיכון) ובהנחיות הבטיחות נדרש ומודגש לקצר את הקבל לפני כל טיפול, בדומה לפעולה שעושים במערכות דומות במכ"מים.

מאפייני (חומרת) הסיכון :

קיים סיכון חיי אדם ונזק למכשיר, אם המתחזק משמיט את המכשיר מידי. לאיש התחזוקה שאינו פועל על פי ההנחיות, עלולה להיגרם פגיעה ברמות שונות, החל מהפתעה לא נעימה של מכת חשמל קלה וכלה בסיכון חיים אם הוא גורם לקבל להתפרק דרך שתי ידיו וליבו.

הסתברות הסיכון :

ההסתברות שפעולה כזו תקרה אינה גבוהה ומתייחסת לצירוף של כמה נסיבות (טעינת קבל הלייזר ואי פירוקו).

### 4.3 קרינת לייזר

בד"כ קרינת הלייזר איננה מסוכנת למפעיל (הלייזר בטוח עין החל מטווחים קצרים מאוד). ישנם לייזרים בהם טווח הבטיחות הוא מס' קילומטרים. לזירה אקראית עלולה להיות מסוכנת למפעיל או למשתמש או לאנשים בסביבה התפעולית. במקרים כאלו אנו משתמשים בניצרת חומרה על מנת להקטין את סיכון ההפעלה המקרית. למרות זאת הסיכון להפעלה מקרית (תקלת חומרה או תוכנה) נשאר ברמה שיורית קטנה ואינו יורד ל-0. סיכון דומה קיים כאשר המכשיר אינו מפסיק ללזור כאשר נדרש לכך.

קרינת לייזר בתחומי הנראה ועד 1.5 מיקרו מטר, עוברת דרך עדשת העין והנוזל שבתוכה ועל כן נבלעת ע"י הרשתית. ישנם לייזרים בעלי עוצמת קרינה שמסוכנת לראיה (תוצאות פגיעה יכולות להיות החלק מעיגול נטול יכולת הראיה ברשתית שנראה כאילו ישנו כתם שחור בתמונה הנראית למשתמש שנפגע ועד לעיוורון, אם איזור הפוביאה, נקודת מרכז הראיה, נפגע). מאחר ואחת התכונות של אור הלייזר שהוא כמעט ולא מתבדר, צפיפות האנרגיה הזו עלול להימדד גם במרחקים ניכרים (תלוי באיכות הלייזר ויכול להגיע למספר קילומטרים בלייזרים טובים). אור באורך גל גדול יותר מ-1.5 מיקרומטר נבלע על ידי נוזל העין, לכן אינו מגיע לרשתית. במקרה כזה הסיכון לנזק משמעותי

יכול לקרות במרחקים של עד מספר ס"מ. הבעיה שבאורך גל כזה גלאיי האנרגיה יקרים והרבה פחות מצויים בשוק. כמו כן ישנה בשוק כמות גדולה של חימוש שמונחה על ידי הלייזרים הללו, שפועלים באורך גל מסוכן לעין, לכן החלפת החימוש הזה אינה פרקטית מבחינה כלכלית.

מאפייני (חומרת) הסיכון :

פגיעה ביכולת הראייה של אדם שמסתכל לעבר המכשיר בעת שהוא לוזר. הפגיעה בדרך כלל גורמת לחור (לא גדול אך מטריד מאד) בשדה הראייה, ויכולה להגיע גם לאובדן כולל של הראייה.

הסתברות הסיכון :

נמוכה. מוכרים מספר מקרים כאלה בצבאות המערב במשך עשרות שנות שימוש ותפוצה רחבה. לאחר התיקון, ההסתברות לסיכון אפסית.

#### 4.4 תצוגה עלית מסנוורת

אירוע אחר נוגע לתקלה שעלולה לקרות בתצוגה עילית במטוס, שם התצוגה מופעלת בבהירות מירבית על כל המסך וגורמת לכך שהטייס מסנוור ואינו יכול לראות את הנוף בקדמת המטוס. מסוכן בעיקר בעת הסעה (Taxiing) או בנחיתה במצב של עננות נמוכה מאד (פחות מ- 300' רגל, שאז אין לו זמן לכבות את התצוגה).

במהלך ניתוח בטיחות של תצוגה עילית לטייס (תע"ל) נמצאו שני סיכונים מסכני חיי אדם עיקריים: הפחות חשוב שבהם, אך קריטי מבחינת חיי אדם הוא Misleading Information, בו התע"ל מציג נתונים לא נכונים (בעיקר נתון גובה שגוי). הבעיה יכולה לנבוע מתקלת מדידה, תקשורת, תוכנת תצוגה או חיווט פנימי בתע"ל. הפתרון למצב זה הוא לנטר לפחות שני ערוצי מידע בלתי תלויים לחלוטין (רצוי גם בשיטת המימוש), החל משני סנסורי מדידה וכלה בחיבורים אל הצג. במקרה של שונות בנתונים, לכבות את הנתונים או את התע"ל. אגב, אם מנטרים 3 סנסורים, ניתן להשתמש במעגל Majority, שיבחר את שני הנתונים הזהים. הבעיה במקרה כזה, שהמעגל הזה עצמו הוא Single point of failure, לכן אין נטייה להשתמש בפתרון כזה.

הבעיה היותר קשה הינה המצב בו מסיבה כלשהי התע"ל עובר למצב של בהירות מירבית על כל המסך. במקרה כזה, הטייס אינו רואה מאומה במרכז איזור העניין שלו, מצב שהוא מסוכן בזמן ההסעה על המסלול בהמראה או בנחיתה, או בזמן נחיתה במצב של עננות נמוכה מאד, כאשר הטייס משתמש בתע"ל ככלי הנחתה עיקרי. פתרון למצב זה הוא חיבור מספר (לא גדול) של מדידי עוצמת תאורה המפוזרים על המסך במקומות בהם לא יכולה להיות תמונה. במקרה שמספר סנסורים כאלה מגלים עוצמת תאורה גבוהה מהנדרש, מכבים את התע"ל על ידי ניתוקו ממקור האספקה. אם הטייס

אינו מורשה במצב כזה לנחות, הוא מונחה, בהוראה מראש, לבטל את מצב הנחיתה ולחפש אתר חלופי לנחיתה (בתלות במצב הדלק שלו).

מאפייני הסיכון :

הסיכון הוא באובדן חיי אדם של הנוסעים והצוות וכן אובדן המטוס.

ההסתברות לסיכון :

נמוכה. לאחר התיקון-אפסית (פחות מפעם אחת בכל המטוסים ושנות התעופה האזרחית).

#### 4.5 מערכת טלויזיה ביתית

המשתמש בשלט-רחוק של הטלויזיה הביתית טועה לפעמים בהתמצאות במצב המערכת. כתוצאה מכך הוא עלול לכבות את הממיר הדיגיטלי במקום להדליק את הטלויזיה, והוא עלול להעביר תחנה בטלויזיה במקום בממיר. משתמשים שאינם בעלי חוש טכני מתקשים לאבחן את מצב המערכת, ונוזקים לעזרה.

הסתברות הסיכון :

גבוהה, תופעה יומיומית בתפעול המערכות הנפוצות.

חומרת (מחיר) הסיכון :

- המחיר למשתמש : במקרה הטוב, המשתמשים מקבלים את העזרה, אבל נותרים בתחושה של תסכול ואי שביעות רצון.
- המחיר לספק השירות : עלות אנשי התמיכה הטכנית ללקוחות.

#### 4.6 נורית חום מנוע במכונית

בדגמי המכוניות העממיות, התרעת חום המנוע מבוססת על מדידת טמפרטורת מי הקירור. התרעה זו בלתי אמינה משתי סיבות עיקריות :

(1) במקרה של התחממות כתוצאה מאובדן מי קירור, המדידה אינה משקפת את מצב החום במנוע.

2) המשתמש שאינו מודע למצב הבעייתי במכונית עלול לא להבחין בהתרעה. בעיה זו חמורה בעיקר במכוניות בהן ההתרעה מבוססת על חוגה שמגיעה לאזור "אדום".

הסתברות הסיכון :

תופעה שכיחה במצבים של תקלה במערכת הקירור.

חומרת (מחיר) הסיכון :

- המחיר למשתמש : מחיר שיפוץ המנוע.
- המחיר לספק השירות : מחיר שלילי, ספק השירות זוכה להכנסות מהשיפוצים, מכיוון שהתקלה מיוחסת למשתמש, ולא למערכת.

#### 4.7 התרעות טורדניות במערכות רפואיות

במקרה של החמרה במצב החולה הנמצא במעקב, המערכת צריכה להתריע בקול. לצורך הטיפול, הצוות הרפואי צריך להשתיק את המערכת. בתום הטיפול, הפרמטרים של החולה עדיין במצב התרעה, ולכן הצוות הרפואי אינו יכול לוותר על מצב השתקת המערכת. במקרה של החמרה נוספת במצב החולה, הצוות הרפואי לא מקבל התרעה, והחולה נמצא בסכנה.

מאפייני הסיכון :

ההערכה היא שבארה"ב מתים בכל שנה 100,000 איש כתוצאה מטעות אנוש. אין נתון לגבי הסיכון של התרעות טורדניות.

מקור : אירועי בטיחות בספרות

#### 4.8 קריסת מערכת החשמל ב-NYC

בשנת 1977 העיר ניו-יורק שקעה באפילה לאחר פגיעת ברקים בשתי תחנות טרנספורמטורים. קריסת המערכת העירונית נבעה מכך שמפעיל חדר הבקרה של תחנת Con Edison לא מצא את הפקד שנדרש להתאוששות מהפגיעה בטרנספורמטורים.

[http://en.wikipedia.org/wiki/New\\_York\\_City\\_blackout\\_of\\_1977](http://en.wikipedia.org/wiki/New_York_City_blackout_of_1977)

מאפייני הסיכון :

המערכת הייתה מותאמת למפעילים מיומנים בלבד, ונכשלה כאשר המפעיל היה בלתי מיומן.

#### 4.9 המיכלית Torrey Canyon

בשנת 1967 המיכלית Torrey Canyon עלתה על שרטון לאחר ניתוק בטעות של מערכת ההיגוי.

[http://en.wikipedia.org/wiki/Torrey\\_Canyon](http://en.wikipedia.org/wiki/Torrey_Canyon)

מאפייני הסיכון :

הניתוק היה בלתי צפוי ובלתי מתואם למצב שיוט, והמערכת לא סיפקה התרעה לגבי המצב החרוג.

#### 4.10 תקלה במטוס Airbus 320

בשנת 1978 מטוס A-320 בטיסת AF-296 נכשל בתמרון של נסיקה, לאחר שהטייס לא היה מודע לשינוי באופן התנהגות מערכת הבקרה במצב הילוך סרק.

[http://en.wikipedia.org/wiki/Air\\_France\\_Flight\\_296](http://en.wikipedia.org/wiki/Air_France_Flight_296)

לקחי התאונה לא נלמדו, ובשנת 1990 טיסה 605 של Indian Airlines הסתיימה באסון לאחר שהמטוס הגיע קרוב מדי, והמטוס לא נשמע לפיקוד הטייסים.

[http://en.wikipedia.org/wiki/Indian\\_Airlines\\_Flight\\_605](http://en.wikipedia.org/wiki/Indian_Airlines_Flight_605)

מאפייני הסיכון :

שינוי באופן התנהגות המטוס במצבים חריגים, בניגוד להרגלי הטייסים.

#### 4.11 תקלה בכור הגרעיני ב-TMI

בשנת 1979 הייתה תקלה באחד הרכיבים של מערכת הקירור של תחנת הכוח הגרעינית TMI בפנסילבניה. התקלה גרמה למפולת של התרעות, והמפעילים הצליחו לאתר אותה רק לאחר חמישה

ימי חיפושים. [http://en.wikipedia.org/wiki/Three\\_Mile\\_Island\\_accident](http://en.wikipedia.org/wiki/Three_Mile_Island_accident)

מאפייני (חומרת) הסיכון :

חיי אדם רבים וזיהום, התקלה גרמה למעשה להקפאה של תהליך המעבר לאנרגיה גרעינית בארה"ב.

ההסתברות לסיכון :

הסתברות של תקלה ברכיבים של מערכת קירור היא גבוהה יחסית.

## 4.12 התאונה במפעל ה-MIC ב-Bhopal

בשנת 1984 חדרו מים למיכל של מפעל ה-MIC בחברת Bhopal בהודו. הריאקציה גרמה לבקיעה של

המיכל ולפגיעה המונית על ידי הגז הרעיל. [http://en.wikipedia.org/wiki/Bhopal\\_disaster](http://en.wikipedia.org/wiki/Bhopal_disaster)

מאפייני הסיכון :

המערכת לא סיפקה מידע מתאים לגבי המצב, והמפעילים לא ידעו מה קורה ומה עליהם לעשות.

מחיר הסיכון :

הגז הרעיל דלף וגרם למותם של אלפים ולפגיעה של חצי מליון התושבים של העיר.

## 4.13 מכשיר הרדיותרפיה Therac-25

שש תאונות מתועדות במהלך ההפעלה של מכשיר הרדיותרפיה בין השנים 7-1985. המפעילים המיומנים להפעיל במוד רנטגן, העבירו אוטומטית למוד זה גם כשנדרש מוד טיפול בקרן אלקטרוניים, אבל הבחינו בטעות בעוד מועד, ותיקנו במהירות. המערכת הגיבה לאט מדי לתיקון, והופעלה במצב כלאיים. כתוצאה מכך המטופלים ספגו קרינה בעוצמה בסדרי גודל יותר מהמתוכנן.

<http://en.wikipedia.org/wiki/Therac-25>

מאפייני הסיכון : הפעלה במצב מערכת חריג, בלתי צפוי.



#### 4.14 אש ידידותית – צאלים א' ו- ב'

באימון אוגדה בשנת 1990 בצאלים, קצין הקישור הארטילרי פקד מילת הפעלה שגויה לסוללה הארטילרית. כתוצאה מכך הסוללה ירתה פגז על הכוח המסתייע.

<http://www.ynet.co.il/yaan/0,7340,L-1120082-PreYaan,00.html>

לקחי התאונה לא נלמדו. בהמשך, בשנת 1992, ירה חייל של סיירת מטכ"ל טיל חי במצב של תרגיל יבש. [http://he.wikipedia.org/wiki/אסון\\_צאלים\\_ב'](http://he.wikipedia.org/wiki/אסון_צאלים_ב')

מאפייני הסיכון:

הסיכוי לטעות באבחון מצב התרגיל, או בזיהוי עמית-טורף (זע"ט) הוא גבוה, והמחיר גבוה.

#### 4.15 אש ידידותית – אפגניסטן 2001

כח של הממשל האפגני תקף את מורדי הטאליבאן ליד קאנדהאר בסיוע מטוסי B52 של ארה"ב. ציון המטרה נעשה בעזרת מכשיר GPS שהופעל על ידי צוות אמריקאי. לפני שהמטוסים הגיעו, נדלקה במכשיר ה-GPS נורית אינדיקציה לצורך להחליף סוללה. הסוללה הוחלפה בהתאם להנחיות, וכתוצאה מכך ניצ המטרה התאפסה, והוחלפה בניצ בו נמצא מכשיר ה-GPS.

<http://www.cdi.org/terrorism/killing-pr.cfm>

מאפייני הסיכון:

ההסתברות לטעות כזו היא נמוכה, אבל המחיר גבוה.

## 5. סיווג סיכוני תפעול (הדוגמאות סווגו לקטגוריות)

### 5.1 תקלות צפויות שתוצאותיהן צפויות (ומסוכנות)

#### דוגמאות

##### *דוגמה: אנרגיה גבוהה בתחזוקה*

זוהי תקלה צפויה, שעלולה לפגוע באיש התחזוקה אם אינו נוקט באמצעי זהירות. ניתן להיערך למניעת הפגיעה באיש התחזוקה על ידי תכנון מתאים.

##### *דוגמה: קרינה מסוכנת*

זוהי תקלה צפויה, שניתן להיערך לה בתכנון המערכת, אם כי הסיבות לה יכולות להיות מגוונות. במקרה של תקלה, הקרינה עלולה לגרום נזק לראיה של אנשים שנפגעים ממנה.

### 5.2 תקלות צפויות שתוצאותיהן בלתי צפויות

#### דוגמאות

##### *דוגמה: תצוגה עילית מסנוורת*

מדובר בתקלה צפויה, שניתן להיערך אליה על ידי צמצום העוצמה המרבית בהתאם לתאורת הרקע ולשיקולים של יכולת המפעיל להבחין בין האות לבין הרקע. הסיבה בגללה המפתח לא נערך להתמודד עם תקלה זו היא, שהצורך להיערך לתקלה לא היה ברור בשלב התכנון.

### 5.3 טעויות צפויות בהתמצאות המפעיל במצבי תקלה

#### דוגמאות

##### *דוגמה: שבירת נעילה*

התופעה מוכרת בתחום הפסיכולוגיה הקוגניטיבית בשם Tunnel Vision כמטפורה לתופעה בתחום הרפואה [http://en.wikipedia.org/wiki/Tunnel\\_vision](http://en.wikipedia.org/wiki/Tunnel_vision) וההסבר התיאורטי שלה הוא מגבלת הקיבולת של זיכרון העיבוד האנושי. טעויות כגון אלה צפויות במצבים של פעולה תחת לחץ. במצבים בהם ניתן להגדיר ולצפות טעויות אלה, ניתן לספק התרעה למפעיל, להביא את המצב הבעייתי למודעות.

#### **דוגמא: נורית חוס מנוע במכונית**

תופעה זו צפויה, בעיקר במכוניות בהן אין חיווי בולט לעליה חריגה בחוס המנוע.

#### **תקלה בכור הגרעיני ב-TMI**

באופן בסיסי, מדובר בתקלה צפויה, שניתן להיערך אליה בעוד מועד. הקושי באיתור התקלה נגרם כתוצאה מהצפת מידע בלתי רלבנטי, מעבר לקיבולת העיבוד של המפעילים.

#### **התאונה במפעל ה-MIC ב-Bhopal**

באופן בסיסי, מדובר בתקלה צפויה, שניתן להיערך אליה בעוד מועד. הקושי באיתור התקלה נגרם כתוצאה מחוסר מידע חיוני למפעילים.

### **5.4 טעויות תפעול בהתמודדות עם תקלות צפויות**

#### **דוגמאות**

#### **דוגמא: קריסת מערכת החשמל ב-NYC**

תקלות במערכות חשמל קורות בתכיפות גבוהה יחסית, ומפעיל מיומן יודע להתמודד עמן. טעות התפעול נבעה מחוסר ניסיון של המפעיל הספציפי בהתמודדות עם תקלות אלו.

### **5.5 טעויות צפויות בבחירת פונקציית התפעול**

גירסה של חוק מרפי המותאמת לשלב התפעול היא :

*אם מאפשרים למפעיל לטעות – בסופו של דבר הוא יטעה.*

הכוונה היא שהמפעיל בחר בפונקציה שמיועדת להפעלה במצבים אחרים, אך לא במצב הנוכחי של המערכת.

## **דוגמאות**

### **דוגמא: מערכת טלוויזיה ביתית**

השלט-רחוק של מערכת הטלוויזיה הביתית מאפשרת למשתמש בה לטעות ולכבות את הממיר במקום את הטלוויזיה, ולהעביר ערוצים בטלוויזיה במקום בממיר. ההסתברות לטעויות אלו היא גבוהה ביותר, והמחיר הוא תחושת תסכול אצל המשתמשים, ועלויות גבוהות של התמיכה הטכנית.

### **דוגמא: התרעות טורדניות במערכות רפואיות**

במצבי לחץ, המפעיל בוחר באופציה שנוחה ביותר לפתרון הבעיה לטווח הקצר. אם המערכת מאפשרת למפעיל לבחור בקלות באופציה בלתי בטוחה, ההסתברות לכך שיבחר באופציה זו היא גבוהה.

### **דוגמאות: אש ידידותית – צאליס א' ו- ב'**

בדוגמא זו קצין הקישור פקד פקודה שהיא בלתי סבירה, בהתחשב במיקום היחידה שהתאמנה, והיא בלתי צפויה מנקודת מבט המתכנן. ההסתברות לטעות מסוג זה היא נמוכה ביותר, והמחיר הוא בחיי אדם.

### **דוגמא: המיכלית Torrey Canyon**

בדוגמא זו המערכת איפשרה ניתוק בטעות של מערכת ההיגוי. ההסתברות לטעות מסוג זה אינה זניחה, אבל בדרך כלל למפעילים יש מספיק זמן לזהות את המצב החריג בעוד מועד. ההסתברות לתאונה כתוצאה מטעות זו היא נמוכה ביותר, אבל המחיר גבוה, כפי שארע במקרה הנדון.

## **5.6 תקלות כתוצאה מתפעול במצב חריג**

הכוונה לאירוע רגיל במצב תפעול רגיל, שכתוצאה ממנו המערכת עוברת למצב חריג.

### **דוגמא: שיגור טיל בטעות**

בדוגמא זו האירוע הרגיל הוא הפסקת מתח רגעית, ומצב התפעול הרגיל הוא מוד תרגול. הבעיה היא כאשר כתוצאה מהאירוע, המשגר עובר ממוד תרגול למוד מבצעי, כאשר יחידת הבקרה נשארת במוד תרגול.

### **דוגמא: אש ידידותית – אפגניסטן 2001**

בדוגמא זו האירוע הרגיל הוא החלפת סוללה ומצב התפעול הרגיל הוא ציון מטרה. הבעיה היא כאשר כתוצאה מהאירוע, מכשיר ה-GPS עובר ממוד ציון מטרות למוד ציון מיקום המכשיר.

### **דוגמא: מכשיר הרדיותרפיה Therac 25**

בדוגמא זו האירוע הרגיל הוא פקודה של המפעיל להחלפת מוד קרינה, ומצב התפעול הרגיל הוא מוד הקרנת רנטגן. כתוצאה מהאירוע, מצב המערכת משתנה באופן זמני למצב כלאיים, והבעיה היא כאשר מתבצעת הקרנה במצב הכלאיים.

### **דוגמא: תקלה במטוס Airbus 320**

בדוגמא זו המערכת הגיע למצב שהוא בלתי צפוי מנקודת מבט המתכננים. ההסתברות להגיע למצב זה הייתה נמוכה ביותר, והראיה לכך היא שהמטוס פעל כשורה במשך מספר רב של חודשים, אבל המחיר של טעות זו היה בחיי אדם.

## **6. הצעה לניהול סיכונים סיכוני תפעול**

### **6.1 תקלות צפויות שתוצאותיהן צפויות (ומסוכנות)**

ניהול הסיכונים מתבצע בהתאם לשלבים הבאים:

- שלב א: ניתוח הסיכונים – FMEA – HAZOP ;
- שלב ב: פתרונות – על ידי מיטב המהנדסים ;
- שלב ג: תקצוב – הערכת העלות של מניעת הנוקים באמינות של X אחוזים ;
- שלב ד: ישום הפתרון הנבחר ;
- שלב ה: הוכחת אפקטיביות התרופה. יזום תקלות ובדיקת ההתנהגות.

### **6.2 תקלות צפויות שתוצאותיהן בלתי צפויות**

תהליך ניהול הסיכונים דומה לזה של סעיף 6.1. בעיית התכן היא לזהות שהתוצאה של תקלה רגילה עלולה להיות חמורה, למרות שמראש נראה שהתקלה אינה כרוכה בסיכונים. להתמודד עם אתגר זה אנו נדרשים לניתוח סיכונים (שלב א' לעיל) קפדני, בגישה הפרנואידיית.

### 6.3 טעויות צפויות בהתמצאות המפעיל במצבי תקלה

בעיית התפעול במצבי תקלה נובעת מכך שלמפעיל לא היו הזדמנויות להכיר את המצבים הללו בתהליך תפעול שוטף. בעיית התכן היא לספק למפעילים הזדמנויות להכיר את המצבים הללו.

דרך מקובלת להתמודד עם הבעיות הללו היא על ידי תכן ממוקד משתמש (UCD). בשיטת תכן זו המפתחים נדרשים לתכנן את האינטראקציה על פי הערכה של יכולת המפעילים לתפוס את מצב המערכת בתנאי הפעלה אמיתיים. זאת, בניגוד לשיטת התכן הנוחה יותר, על פי יכולת המפתחים לתפוס את מצב המערכת בתנאי מעבדה.

הערכת כשר התפיסה של המפעילים צריכה להתבסס על המחקר בתחום מגבלות התפיסה האנושית ועל הערכה של עומס התפקיד בתנאי הפעלה סבירים, ובתנאי הפעלה קיצוניים. הערכת כושר התפיסה של המפעילים יכולה להיות סבירה אם היא מבוססת על תצפיות של אופן פעולתם בביצוע משימות. בשלב בדיקות האלפא ניתן ללמוד את כושר התפיסה של המפעילים בבדיקות במעבדת שימושיות, על ידי סימולציה של תרחישי שימוש אמיתיים. ניתן לשפר את איכות הערכת ציפיות המפעילים על ידי תצפית בבדיקות בטא באתר הלקוח.

דרך אפשרית ללמד את המפעילים להכיר את המצבים הבעייתיים ולאמן אותם להגיב נכון היא על ידי הפעלה במוד תרגול, המבוסס על סימולציה של תקלות.

### 6.4 טעויות תפעול בהתמודדות עם תקלות צפויות

בעיית התפעול במצבי תקלה נובעת מכך שלמפעיל לא היו הזדמנויות ללמוד כיצד להתמודד עם המצבים הללו. בעיית התכן היא להדריך את המפעיל אינטראקטיבית בזמן תקלה.

הדרך להתמודד עם הבעיות הללו היא על ידי תכן ממוקד משתמש (UCD), כמתואר לעיל. בשיטת תכן זו המפתחים נדרשים לתכנן את האינטראקציה על פי הערכה של ציפיות המפעילים ויכולתם להפעיל את המערכת בתנאי הפעלה אמיתיים. זאת, בניגוד לשיטת התכן הנוחה יותר, על פי יכולת המפתחים להפעיל את המערכת בתנאי מעבדה.

הערכת התנהגות המפעילים יכולה להיות סבירה אם היא מבוססת על תצפיות של אופן פעולתם בביצוע משימות. בשלב בדיקות האלפא ניתן ללמוד על התנהגויות שונות ומשונות של המפעילים בבדיקות במעבדת שימושיות, על ידי סימולציה של תרחישים הפעלה. ניתן לשפר את איכות הערכת התנהגות המפעילים על ידי תצפית בבדיקות בטא באתר הלקוח.

## 6.5 טעויות צפויות בבחירת פונקציית התפעול

טעויות בבחירת פונקציית התפעול ניתן למנוע אך ורק על ידי מניעת חופש הבחירה מהמפעיל. בשאיפה, יש לתכנן את המערכת כך שתופעל על פי תרחישי הפעלה, באופן שהמפעיל יוכל להפעיל אך ורק את הפונקציות הרלבנטיות לשלב התפעולי בתרחיש.

דוגמת הפיתרון של שבירת נעילה למניעת טעויות תפעול; במערכות טלוויזיה מתקדמות פונקציות השלט-רחוק הן חד משמעיות כך שמקש הכיבוי וההדלקה פועל על הטלוויזיה בלבד, ומקשי הסריקה פועלים על הממיר בלבד.

## 6.6 תקלות כתוצאה מתפעול במצב חריג

במקרה שהמערכת נמצאת במצב חריג, התגובה לפעילות המפעיל היא בלתי צפויה. זאת, מכיוון שמרבית המצבים האפשריים של המערכת הינם חריגים, אבל פעולת המערכת נבדקת רק במספר מצומצם של מצבים חריגים. לפיכך, על מנת למנוע הפתעות לא נעימות יש הכרח למנוע את הפעלת המערכת במצבים החריגים.

לצורך המניעה, יש להגדיר מהו מצב חריג, וליישם במערכת תוכנה שעוקבת אחר מעברי המצבים, מזהה את המצבים החריגים ומתריעה על המעבר אל מצב כזה. דרך מעשית להגדיר מצב חריג היא דרך השליחה, על ידי הגדרת המצבים התפעוליים הנורמאליים: מצב תפעולי נורמאלי הינו מצב שמוגדר בתהליכי התפעול המתוכננים. כל מצב אחר של המערכת מוגדר כמצב חריג. החלק הקשה הוא להגדיר כיצד המערכת צריכה להגיב במצבים החריגים. דרך התגובה הרצויה תלויה באופי היישום, ובעיקר בסיכון למפעילים ולציבור. במצבים מסוימים, כגון בתפעול מוניטורים רפואיים, בסבירות גבוהה, דרך התגובה הבטוחה היא הפסקת הפעילות. במצבים אחרים, כגון בתא הטייס, הדרך הבטוחה יותר היא להעביר את השליטה לטייס.

## 7. דיון

במסמך זה הצגנו מספר מצבי תפעול בעייתיים, על בסיס מגוון של כ-15 דוגמאות. עבור המצבים הללו, הצגנו עקרונות ושיטות להתמודדות עם מצבי תפעול בעייתיים, על ידי מניעה ועל ידי אבטחת שימושיות בתפעול.

השאלה המרכזית כאן היא האם ההמלצות במסמך זה הן תקפות, לאור המגוון הקטן יחסית של דוגמאות במצבי תפעול בעייתיים? האם העקרונות והשיטות המוצעים במסמך זה מספיקים על מנת למנוע תקלות תפעול במערכות עתידיות?

על מנת לבדוק שאלה זו, יש להגדיל עוד יותר את מגוון הדוגמאות של מצבים בעייתיים. ניתן לעשות זאת על ידי סקר ספרות, או על ידי תרומה מניסיונם האישי של חברי הקבוצה.

שאלה נוספת היא כיצד להגיש את ההמלצות הללו כמתכונת למהנדסי מערכות?