

מניעת ירי דו־צדדי: מדרישות בטיחות לדרישות מבצעיות

אבי הראל – מהנדס מערכת, קצין חת"ם בדימוס ergolight@gmail.com

תקציר

המאמר בוחן את התאונות בצאלים ובמשגב־עם באמצעות שאלה מבצעית אחת: כיצד ניתן לבצע את המשימה ביעילות, מבלי להיחשף לסיכון שאינו מזהה או שאינו נשלט. הטענה המרכזית היא כי בשני האירועים הבעיה אינה רק פעולה שגויה, אלא אפשרות לבצע פעולה נכונה מבחינה מקומית על בסיס תרחיש שגוי.

בצאלים, הבעיה הייתה בהתייחסות לשלב הלא נכון בתכנית. במשגב־עם, הבעיה הייתה בבחירת תכנית שלא התאימה לתרחיש ולנתונים שעליהם נשענה. שני המקרים מייצגים, בהיבטים שונים, פער בין התרחיש שעל פיו המסתייע פועל לבין התרחיש שעל פיו המסייע פועל.

מכאן נובעת הבחנה בין בטיחות באימונים לבין בטיחות במבצעים. באימון, שבו התרחיש מתוכנן מראש, הדגש הוא על מניעת סיכון שאינו מוצדק ועל שמירת ביצוע במסגרת התכנית. במבצע, שבו המציאות משתנה והמידע חלקי, הדגש הוא על זיהוי סיכון ועל התאמה מתמשכת של התכנית לתרחיש. המערכת צריכה לזהות ולהציג סיכון, אך לא לקבוע בעצמה אם המשימה מצדיקה את קבלתו.

בטיחות אינה מסתכמת בבדיקה שהפעולה נכונה על פי התכנית. יש לוודא שהפעולה נכונה עבור התרחיש שבו המערכת נמצאת בפועל. המאמר מציע לעבור מדרישות בטיחות כלליות לדרישות מבצעיות הניתנות להגדרה ולבדיקה: זיהוי חריגות, זיהוי אי־התאמות בתמונת המצב, תיאום בין המסייע למסתייע, הערכת רמת הביטחון בתוצאה, מניעת עומס קוגניטיבי, מדרג תגובות בהתאם לרמת הסיכון, ושמירת סמכות ההחלטה המבצעית בידי המפקד.

נספח המאמר מדגים כיצד ניתן לתרגם את דרישות הבטיחות לאפיון מערכת בקרה תומכת בטיחות, ולמבחני קבלה.

1. הבעיה המבצעית: פעולה בטוחה בתרחיש שגוי

מטבע הדברים, סיוע באש כרוך בנטילת סיכון. בלחימה אין משמעות לדרישה לבטל כל סיכון, ולעיתים נטילת סיכון מחושבת היא תנאי להצלחת המשימה. הבעיה מתחילה כאשר הסיכון אינו מוכר למפקד, משום שתמונת המצב שעליה מבוססת ההחלטה אינה תואמת את המציאות.

בסיוע אש בכלל, וארטילרי בפרט, קיים סיכון הנובע מהמורכבות של הממשק שבין המסייע למסתייע. המסייע מחזיק ביכולת האש, ואילו המסתייע מחזיק בחלק מן הידע המבצעי הנדרש להבנת המצב, המטרה והצורך באש. כאשר שני הגורמים פועלים על בסיס הנחות שונות לגבי המשימה, המטרה, השלב או תנאי הביצוע, כל אחד מהם עשוי לפעול באופן סביר מבחינתו, ובכל זאת התוצאה המשותפת תהיה שגויה.

לצורך מאמר זה, ירי דו־צדדי הוא מצב שבו קיים פער בין תמונת המצב שעל פיה פועל המסייע לבין תמונת המצב שעל פיה פועל המסתייע, באופן העלול להביא לפגיעה בכוחות ידידותיים. לכן מוקד הבטיחות אינו רק תקינות החישוב או ביצוע הפקודה, אלא התאמת הפעולה לתרחיש המשותף.

2. צאלים ומשגב־עם: שני מופעים של אותה בעיה

תאונת האימונים בצאלים בשנת 1990 ואירוע הירי על משגב־עם בשנת 2026 התרחשו בתקופות שונות, במערכות שונות ובנסיבות שונות. לצורך הדיון במאמר, ובהתבסס על התיאור המקובל של האירועים, הם משמשים כשני מקרי מבחן לבעיה מערכתית משותפת.

בצאלים, הכשל הרלוונטי לדיון הוא התייחסות לשלב שגוי בתכנית. פעולה שהייתה יכולה להיות תקינה בשלב אחר של התרגיל הפכה למסוכנת משום שהופעלה בשלב מאוחר יותר של התרגיל, לאחר שהמטרה נכבשה ואוישה על ידי המסתייע.

במשגב-עם, הכשל הרלוונטי לדיון הוא בחירת תכנית ירי שלא התאימה לתרחיש המבצעי ולנתונים שעליהם נשענה. בכך הודגם כי גם כאשר חישוב טכני מבוצע כראוי, התוצאה אינה בהכרח מתאימה למשימה אם התכנית וההנחות אינן תואמות את המצב.

ההבדל בין האירועים חשוב, אך המשותף חשוב יותר: בשניהם נוצר פער בין המצב שעל פיו פעל המסייע לבין המצב שעל פיו המסתייע פעל. לכן הלקח אינו רק מי ביצע את הפעולה השגויה, אלא האם למערכת הייתה יכולת לזהות את אי-ההתאמה לפני שהפעולה בוצעה.

ניתן לסכם את ההבחנה כך:

- צאלים: התייחסות לשלב שגוי בתכנית.
- משגב-עם: בחירת תכנית שאינה מתאימה לתרחיש.
- הבעיה המשותפת: פעולה נכונה מבחינה מקומית, המבוססת על תרחיש שאינו תואם את תפיסת התרחיש של הצד האחר.
- האתגר הבטיחותי: לזהות את התרחיש, לאמת את התאמת התכנית אליו, ולזהות אובדן תיאום בזמן המאפשר תיקון.

3. בטיחות באימונים לעומת בטיחות במבצעים

באימון, בניגוד למבצע, התרחיש מתוכנן מראש. לכן ניתן לבסס את הבטיחות על תכנון מוקדם, תדריכים, תיאום, סימון גבולות, נהלים ואישורים. באימון, הבטיחות היא ערך עליון, ואין הצדקה לקבלת סיכון שאינו נדרש לצורך ההכשרה. כתנאי לכך, המשתתפים באימון חייבים לפעול באופן מתואם לתכנית. תאונת צאלים ממחישה את הסיכון שנוצר כאשר פעולה מבוצעת באופן שאינו תואם את שלב התכנית. לכן באימון אין להסתפק בשאלה 'האם הפעולה בוצעה בהתאם לתכנית?'; יש לשאול גם 'האם כל הגורמים מבינים באיזה שלב ובאיזה תרחיש הם נמצאים?'

במבצע, לעומת זאת, המציאות משתנה, המידע חלקי ותכניות עשויות להשתנות במהלך האירוע. לכן אין די בבדיקה שהפעולה מבוצעת בהתאם לתכנית. הסיכון עלול להיווצר כבר בשלב בחירת התכנית. בטיחות במבצע צריכה לכלול אימות מתמשך שהתכנית מתאימה לתרחיש הנוכחי ושהנתונים שעליהם היא מבוססת עדיין תקפים.

ההבחנה המרכזית היא אפוא:

- באימון: הדגש הוא על מניעת סיכון שאינו מוצדק ועל ביצוע בטוח של תכנית מוכרת.
 - במבצע: הדגש הוא על זיהוי סיכון ועל הבטחת התאמת התכנית למצב המתפתח.
- המערכת צריכה לזהות ולהציג את הסיכון, אך לא להחליט אם המשימה מצדיקה את קבלתו. באימון, חריגה משמעותית יכולה להצדיק עצירת פעולה. בלחימה, אותה חריגה מחייבת התרעה והתנ"ת הביצוע באישור המפקד.

4. אחריות המפקד באימונים ובמבצעים

באימונים, אחריות המפקד מתמקדת ביצירת תנאים שבהם כלל המשתתפים מבינים את התכנית, את שלביה, את גבולות הגזרה ואת כללי הבטיחות, ובבקרה, שמטרתה לוודא ביצוע במסגרת התכנית.

במבצעים, אחריות המפקד מורכבת יותר. המפקד אינו יכול להסתפק באישור תכנית שנמצאה מתאימה בעת הכנתה. עליו לוודא שהתכנית מתאימה למצב המבצעי כפי שהוא מתפתח, ולזהות כאשר שינוי במצב, אי-ודאות או מידע חדש מחייבים בחינה מחדש של ההחלטה.

עם זאת, ככל שהמערכת נעשית אוטומטית ומורכבת יותר, אין לצפות מהמפקד לבצע ידנית את כל פעולות המעקב והאימות. יש להעביר למערכת חלק מפונקציות הבקרה והאימות של התאמת התרחיש, תוך שמירת הסמכות והאחריות המבצעית בידי האדם.

מכאן נובעת חלוקת תפקידים ברורה: המערכת מזהה מצב, אי-התאמה ורמת סיכון; המפקד קובע אם הסיכון מוצדק ואם יש להמשיך במשימה.

5. תיאום מסייע-מסתייע

הצלחת הסיוע תלויה לא רק בתקינות כל אחד מהגורמים בנפרד, אלא גם בתיאום ביניהם. פעילות המסייע והמסתייע מתבססת על מידע שונה, תוך שימוש במונחים שונים, תוך התייחסות לשלבים שונים של המשימה ותוך הנחות שונות לגבי פעילות הצד האחר.

כדי לאפשר את התיאום, התפעול צריך להתבסס על תרחיש משותף: המסייע נדרש לזהות באיזו תכנית ובאיזה שלב בתכנית המסתייע פועל, ולפעול בהתאם לכך. התרחיש אינו מתאר את כל מורכבות המציאות. הוא מגדיר את המצבים שבהם המערכת מורשית לבצע פעולה ואת התנאים הנדרשים למעבר ביניהם.

ככל שמערכות התקשוב והשו"ב נעשות מורכבות יותר, כל תוספת של משתתף, ערוץ תקשורת, אישור, מצב ביניים או מעבר בין מצבים מוסיפה אפשרות לפער בין תמונות המצב. לכן דרישה המנוסחת כללית כמו 'המערכת תתאם בין המסייע למסתייע' אינה מספיקה. יש להגדיר מה חייב להיות מתואם, מתי התיאום נחשב תקף, כיצד הוא מתעדכן וכיצד מזהים אובדן תיאום ושינוי משימה.

6. חריגה מתרחיש ובקרת תרחישים

כאשר המצב בשטח חורג מן התרחישים המאומתים, המערכת אינה צריכה להמציא פתרון או להמשיך באופן עיוור. עליה לעבור למצב ברירת מחדל מבוקר ולהציג למפקד את החריגה ואת אובדן התיאום.

נקודת כשל קריטית היא מצב שבו המסתייע עובר למטרה אחרת בעוד המסייע ממשיך לפעול לפי המטרה הקודמת, או כאשר שינוי משימה אינו מגיע לכל המשתתפים בזמן. ככל שתהליך התיאום כולל יותר משתתפים, מצבים, העברות מידע ואישורים, כך גדל הסיכוי לפער בתרחיש.

מעקב אחר שלב בתכנית, זיהוי שינוי תרחיש ואימות התאמה הם משימות קוגניטיביות הרגישות לעומס, לחץ, ריבוי מידע והפרעות. לכן אין להסתמך על הגורם האנושי בלבד. המערכת צריכה לבצע חלק מפונקציות בקרת התרחישים: לזהות את התרחיש הפעיל, לעקוב אחר השינויים בו, להשוות אותו לתרחיש שעל פיו פועל המסתייע ולהתריע כאשר נוצרת אי-התאמה.

אין פירוש הדבר שהמערכת מחליפה את המפקד. תפקידה הוא לשמור רציפות של מודעות תרחישית ולספק למפקד מידע בזמן המאפשר תיקון או קבלת החלטה מודעת.

7. מה ניתן ללמוד מתאונות צאלים ומשגב'עם

בשני האירועים קיימת אותה שאלה מערכתית: האם המסייע מודע לתרחיש שעל פיו המסתייע פועל, והאם המערכת יכולה לזהות כאשר תרחיש זה אינו תואם עוד את התרחיש שעל פיו המסייע פועל?

מכאן נובעת הבחנה קריטית: יכולת חישוב טכנית של פתרון אינה שקולה ליכולת להבטיח שהפתרון מתאים לתנאי ההפעלה המבצעיים. מערכת יכולה להיות מדויקת מבחינה חישובית ועדיין להפיק פעולה שאינה מתאימה למשימה, אם התרחיש, התכנית או ההנחות אינם נכונים.

לכן הדרישה למערכת בקרה אינה רק לספק נתוני פעולה, אלא גם לספק אינדיקציה לכך שהנתונים, ההנחות והתיאום בין הגורמים נמצאים בתחום המאפשר להסתמך עליהם.

8. מה צריכה לכלול הגדרת הדרישות המבצעיות

- מסמך הדרישה המבצעית הוא המקום שבו נקבע מה המערכת נדרשת לעשות, כיצד תיבחן ומה יהיה בסיס לקבלתה מהתעשייה. פרק הבטיחות במסמך זה אינו נספח חיצוני - הוא חלק בסיסי של הגדרת התנהגות המערכת, כולל:
- זיהוי חריגה מתנאי הפעלה: המערכת תזהה מצבים מוגדרים שבהם אחד התנאים הנדרשים לביצוע בטוח אינו מתקיים.
 - זיהוי אי-התאמות בתמונת המצב: המערכת תזהה פערים בעלי משמעות מבצעית בין נתונים, פקודה, מטרה, מצב המשימה ותמונת המצב של המסייע ושל המסתייע.
 - הצגת רמת הביטחון בתוצאה: כאשר התוצאה רגישה לנתון מסוים, כאשר אי-הוודאות חורגת מן התחום שהוגדר או כאשר קיימת סתירה בין מקורות מידע, המערכת תציג זאת באופן ברור למפקד.
 - מנגנון תיאום מוגדר: יוגדר המידע המשותף הנדרש, מתי הוא מתעדכן, כיצד מאשרים שינוי במשימה וכיצד המערכת מזהה שהצדדים אינם מסונכרנים.
 - מניעת הסחת דעת והתראות סרק: ההתראות יהיו תמציתיות, חד-משמעיות וממוקדות, כדי שלא להפריע לתהליך בקרת הפעולה או לגרום להתעלמות מהתרעות משמעותיות.
 - מדרג תגובות מערכתי: יוגדר מראש מהי תגובת המערכת לרמות סיכון שונות, כגון מניעה, השהיה ודרישת אישור, או התרעה בלבד. הגבולות אינם מושארים למימוש התוכנה.
 - שמירת סמכות ההחלטה המבצעית: המערכת אינה מחליטה אם הסיכון מוצדק. כאשר עקיפה מותרת, המפקד צריך להבין על מה התריע המנגנון ומדוע, ולבחור באופן מודע אם לקבל את הסיכון.
 - גבולות מורכבות ותסריטי מצב בטוח: תוגדר קבוצת תרחישים מאושרים. מצב שאינו מתאים לתרחיש מוכר או אובדן תיאום יוביל למצב עבודה מבוקר ומוגדר מראש.
 - בחינות קבלה מבצעיות: כל דרישה תהיה ניתנת למדידה ולבדיקה, באמצעות תרחישים הכוללים טעות מפעיל, נתונים סותרים, אובדן סנכרון ושינוי פתאומי במצב המשימה.

9. מהדרישה המבצעית למימוש ולהוכחה

- המעבר מדרישות בטיחות כלליות לדרישות מבצעיות מחייב להגדיר לא רק מה המערכת עושה במצב תקין, אלא כיצד היא מתנהגת כאשר התנאים משתבשים. המטרה אינה להכתיב את הארכיטקטורה הטכנולוגית, אלא להגדיר התנהגות נדרשת ותנאים שבהם ניתן להסתמך עליה.
- השרשרת המומלצת היא:
- תרחיש: מהו המצב המבצעי ומהם התנאים המגדירים אותו.
 - דרישה: מה המערכת נדרשת לזהות או לאמת.
 - התנהגות: מה המערכת עושה כאשר התנאי מתקיים או כאשר נוצרת אי-התאמה.
 - תגובה: האם נדרשת מניעה, השהיה ואישור, או התרעה.
 - מבחן קבלה: כיצד מוכיחים בתרחיש מבצעי שהמערכת אכן מתנהגת כנדרש.
- ניסוח כללי כמו 'המערכת תהיה בטוחה מפני ירי דו-צדדי' אינו ניתן לאימות. לעומת זאת, דרישה המגדירה שינוי בתכנית או בשלב המשימה, זיהוי השינוי, עדכון התרחיש, בדיקת התאמה והפעלת תגובה מוגדרת, זוהי דרישה שניתן לבחון.

10. מבחני קבלה מבצעיים

במבחני הקבלה של מערכת בקרה ארטילרית נדרש לבחון את ההתנהגות המשותפת של המסייע והמסתייע ולא רק את תקינות הרכיבים. סדרת המבחנים צריכה לכלול לפחות:

- תרחיש תקין: זרימת מידע וביצוע פעולה בסנכרון מלא.
- תרחיש טעות מפעיל: הזנת נתון שגוי באופן יזום ובחינת יכולת המערכת לזהות את החרیגה.
- תרחיש שינוי משימה: שינוי במטרה או בשלב המשימה במהלך רצף הפעולה ובחינת עדכון התרחיש.
- תרחיש אובדן תיאום או תקשורת: ניתוק הקשר בין הגורמים ובחינת המעבר למצב שהוגדר מראש.
- תרחיש מידע סותר: הופעת מידע שאינו תואם בין מקורות ובחינת הצגת אי-הוודאות.
- תרחיש עקיפה מבצעית: בחינת יכולת המפקד לקבל החלטה מודעת כאשר המערכת מתריעה.
- תרחיש סיכון גבולי נסתר: בחינת יכולת המערכת להציג מדרג סיכון כאשר הנתונים נמצאים בקרבת גבול מעטפת הבטיחות.

11. סיכום

תאונות הירי בצאלים ובמשגב-עם אינם מייצגים בהכרח את אותו מנגנון כשל, אך הם מאפשרים לזהות בעיה מערכתית משותפת: האפשרות שהמסייע יפעל באופן תקין מבחינה מקומית על בסיס תרחיש שאינו תואם את התרחיש שעל פיו המסתייע פועל.

באימון, הפתרון הוא בעיקר מניעת סיכון שאינו מוצדק ושמירה על סנכרון עם תכנית מוכרת. במבצעים, הפתרון דורש יכולת לזהות שינויים, אי-ודאות ואי-התאמה בין התכנית לבין המצב, ולהציג אותם למפקד באופן המאפשר החלטה מודעת.

מכאן נובעת הדרישה המרכזית למערכות האש העתידיות: לא רק לבצע את הפעולה שנבחרה, אלא לספק בקרה על התאמת הפעולה לתרחיש. המערכת צריכה לזהות את התרחיש, לעקוב אחר שינויו, לזהות אובדן תיאום ולהפעיל תגובה שהוגדרה מראש. המפקד נשאר בעל הסמכות לקבוע אם הסיכון מוצדק ואם המשימה מחייבת את קבלתו.

המעבר מדרישות בטיחות דקלרטיביות לדרישות מבצעיות הניתנות לבדיקה מאפשר לדרוש מיצרן מערכת הבקרה התנהגות מערכתית מוגדרת ולהוכיח אותה במבחני קבלה. בכך ניתן לבנות מערכות שאינן רק מדויקות ומהירות יותר, אלא גם מסוגלות לנהל באופן מוכח את הסיכון הנובע ממצבים חריגים, שינויי תרחיש ואובדן תיאום.

נספח: מדרישה מבצעית לתכן ולמבחן

1. מטרת הנספח

הנספח מדגים כיצד דרישה מבצעית יכולה להתורגם למנגנוני תכן ולמבחני קבלה, מבלי להכתיב מראש את הפתרון הטכנולוגי. המאפיין מגדיר התנהגות נדרשת, גבולות תרחיש ותנאים שבהם ניתן להסתמך על התוצאה.

2. ייצוג תרחיש משותף

המערכת תייצג באופן חד-משמעי את המידע המבצעי הנדרש כדי לזהות את התרחיש שעל פיו המסתייע פועל ולשמור על התאמת הסיוע אליו. הייצוג יכול לכלול, בהתאם לצורך המבצעי:

- זהות המשימה והשלב המבצעי הנוכחי.
- זהות המטרה ומידע מבצעי רלוונטי הנדרש לתיאום.
- זהות המסייע והמסתייע והגורמים המוסמכים לאשר שינוי.

- תנאי ההפעלה הנדרשים ותוקף המידע הקריטי.

- רמת הביטחון הנדרשת בתוצאה.

3. תהליך התיאום

- אירוע המחייב תיאום: שינוי בתכנית, במטרה, בשלב המשימה או בתנאי ההפעלה יוצר אירוע המחייב בחינה מחדש.

- זיהוי פער: מערכת הבקרה משווה את התרחיש שעל פיו עומדת להתבצע הפעולה לתרחיש שעל פיו המסתייע פועל ומזהה אי-התאמה.

- תגובה: כאשר מזוהה פער, המערכת מתריעה או משהה/מונעת את הפעולה בהתאם לרמת התגובה שהוגדרה.

- אישור מחדש: לפני חידוש הפעולה נדרש אימות לכך שהתרחיש זוהה מחדש ושקיימת התאמה בין הגורמים.

4. הגבלת מורכבות ומצב ברירת מחדל

במקום לאפשר סדרת פעולות בלתי מוגבלת, יש להגדיר קבוצת תרחישים מאושרים. כאשר האירועים אינם תואמים תרחיש מוכר, או כאשר נפגע הקשר בין המסייע למסתייע, המערכת תעבור למצב ברירת מחדל מבוקר, תציג את אובדן התיאום ותדרוש את החלטה שהוגדרה מראש.

5. שלוש רמות תגובה

- מניעה (Interlock): חסימת הפעולה במצבים שהוגדרו מראש, למשל באימון או בחריגה קשיחה.

- השהיה ואישור (Confirm & Hold): עצירת הרצף ודרישת אישור מפורש מהמפקד.

- התרעה (Warning): אפשרות להמשך פעולה תוך הצגת הסיכון או אי-הוודאות באופן בולט.

6. דוגמה לדרישה הניתנת לבדיקה

ניסוח לא תקין: 'המערכת תהיה בטוחה מפני ירי דו-צדדי'.

ניסוח מבצעי: 'כאשר חל שינוי בתכנית או בשלב המשימה, מערכת הבקרה תזהה את השינוי, תעדכן את התרחיש הפעיל ותבדוק את התאמת הפעולה לתרחיש שעל פיו המסתייע פועל. במקרה של אי-התאמה, המערכת תציג את הפער ותפעיל את רמת התגובה שהוגדרה לחריגה'.

7. עקרון מבחן הקבלה

מבחן קבלה תקף צריך להוכיח התנהגות מערכתית בתרחיש, ולא רק תקינות רכיב. לכן יש לבחון את רצף האירועים, את זיהוי השינוי, את גילוי אי-ההתאמה, את התגובה ואת יכולת המפקד להבין את המצב ולקבל החלטה בהתאם לסמכותו, כמפורט בסעיף 10 בגוף המאמר.

8. סיכום הנספח

המאפיין אינו נדרש להיות מהנדס מערכת או מהנדס תוכנה. הוא נדרש להגדיר גבולות, תרחישים, התנהגות ומבחני קבלה חד-משמעיים. בכך ניתן להפוך עקרון בטיחות כללי לדרישה מבצעית שהמימוש שלה ניתן לבחינה ולהוכחה.