שילוב שיקולי בטיחות המוצר וניהול הבטיחות בתהליך פיתוח טכנולוגי

(חלק שני)

מאת ד"ר מיכאל מהרי"ק וד"ר שמשון ארואטי

בהפעלתם של מוצרים טכנולוגיים כרוכים סיכונים לאדם ולסביבה. כדי להפחית את הסיכונים במידת האפשר, יש לשלב שיקולי בטיחות בפיתוח של מוצרים אלה

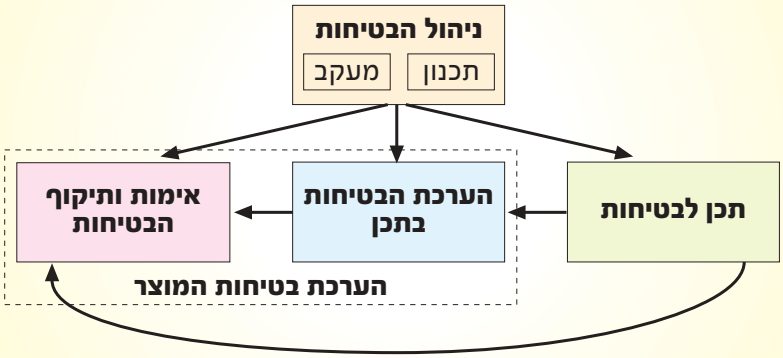
בחלקו הראשון של המאמר (בטיחות, גליון 320) הבהרנו את הזיקה בין "בטיחות הייצור" ו"בטיחות המוצר", הצגנו מקורות ומאפיינים לדרישות לבטיחות המוצר, הגדרנו ארבעה ערוצים המרכיבים את פעילות הבטיחות בתהליך הפיתוח, ופירטנו בנושא ערוץ התכן לבטיחות. במאמר זה נציג את שלושת הערוצים האחרים, ונסכם במספר הערות כוללניות.

הערכת הבטיחות בתכן

הערכת הבטיחות מלווה את התכן עם התקדמותו, בעוד שהמוצר המצוי בפיתוח נמצא "על הנייר" בלבד, או בסטטוס של "דגם פיתוח" (אבטיפוס). ההערכה אמורה להוביל לזיהוי נקודות תורפה בהיבטי בטיחות ולפתרונן, בטרם יעוגנו כמרכיב בלתי הפיך בתכן. בנוסף, ההערכה אמורה לתמוך במעבר לשלב מתקדם יותר של התכן, או למנוע מעבר כזה, על בסיס הידע הניתן למיצוי מן התכן בשלבו הנוכחי.

הערכת הבטיחות כוללת ריכוז מידע רלוונטי ממקורות שונים, ניתוח המידע, הערכת משמעות המימצאים וקביעת יעדים על בסיס המימצאים ומשמעותם. יעדים אלה ימומשו בשני ערוצים: האחד - ערוץ התכן לבטיחות, שבמסגרתו יופחתו הסיכונים במידת האפשר, והשני - ערוץ אימות העמידה בדרישות ותיקוף הבטיחות, שבמסגרתו יינתן מענה לפערי ידע שזוהו ותיבחן בפועל נכונות ההערכות התיאורטיות. לאור העובדה שפרטי התכן הולכים ומתבהרים במהלך הפיתוח, וכן עקב המשוב שמספקת ההערכה לתכן לבטיחות (כאמור לעיל), התהליך כולו הוא איטראטיבי (נערך במספר סבבים, שתפוקת כל אחד מהם משופרת בהשוואה לסבב הקודם). פירוט רב יותר של התהליך ומרכיביו ראו באיור 2. הערכת הבטיחות מסוכמת בניתוחים מתועדים בשלבי התכן השונים; עניין זה יפורט בהמשך, בפרק העוסק בניהול הבטיחות.

איור 1: זיקה בין ערוצי הפעילות לבטיחות בפיתוח פרויקט



כאמור לעיל, הכלים המשמשים להערכת הבטיחות של מוצר הנמצא בתהליך פיתוח הם בעיקר ניתוחי בטיחות לסוגיהם השונים. נושא זה נסקר בהרחבה במאמר שפורסם בעבר בכתב-העת "בטיחות"[1], ולכן נסתפק כאן בסקירה תמציתית של שיטות הניתוח העיקריות ובהצעה למתכונת שימוש אינטגרטיבית בהן בהקשרים טכנולוגיים שונים.

ארבע מן השיטות העיקריות המשמשות בתהליכים של פיתוח טכנולוגי הן FMECA, HAZOP, FTA, ו-ETA[2].

- **FMECA ניתוח אופני כשל, אפקטים וקריטיות** (Failure Modes, Effects and Criticality Analysis)

הניתוח מוחל בנפרד על כל אחד מ**רכיבי המערכת** (לחילופין, ניתוח זה יכול להיערך על פונקציות של המערכת או על תהליכים שונים, כדוגמת תפעול ותחזוקה, במקום על רכיבים פיזיים), ונערך "מן הפרט אל הכלל":

- באיזה אופנים עלול הרכיב להיכשל?
- האם אופני הכשל הם בדיקתיים?
- מה גורם לרכיב להיכשל, בכל אחד מאופני הכשל?

ד"ר מיכאל מהרי"ק הוא מנתח סיכונים ומהנדס בטיחות במגזר הטכנולוגי-תעשייתי.

ד"ר שמשון ארואטי הוא מהנדס בטיחות בחברת 'רפאל' בע"מ.

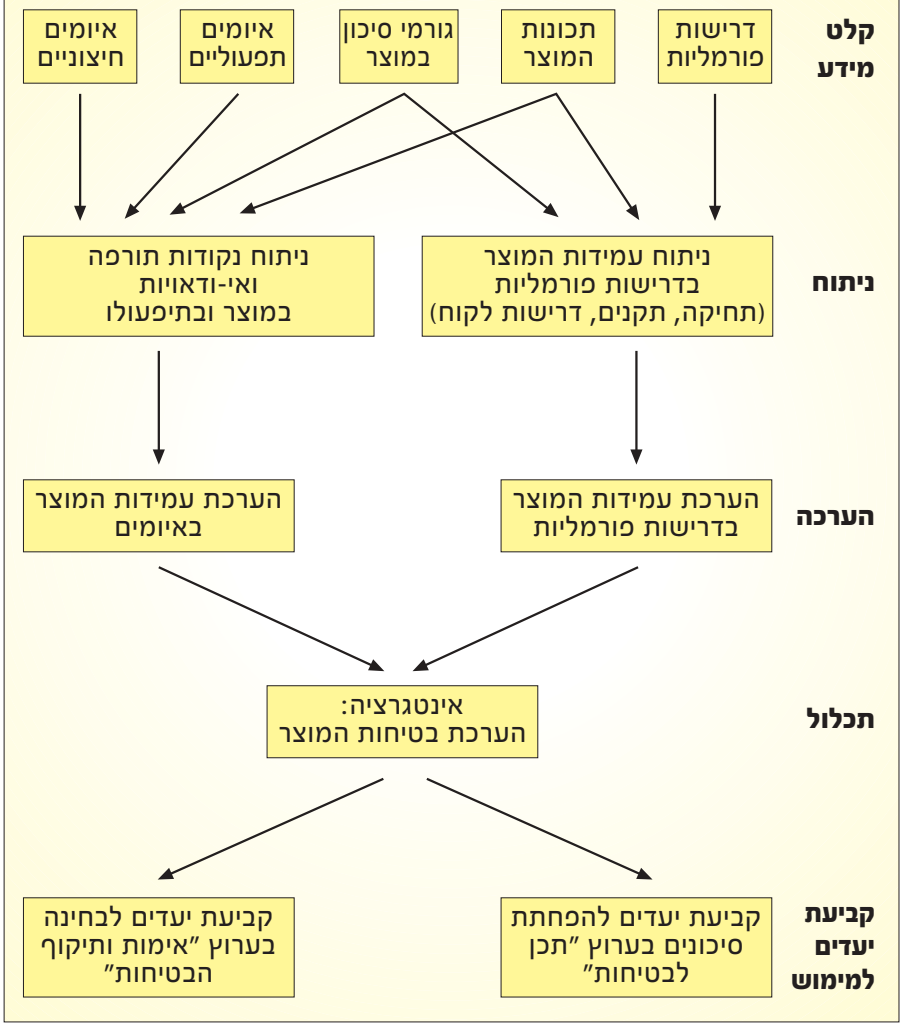
הכותבים מודים לאברהם חסון, לאבי הראל, לראובן גרינברג, לרפי מירון ובמיוחד לישי לבנון על הערותיהם לטיוטת המאמר.

המאמר פורסם לראשונה ב"קול המערכות" - כתב העת של מהנדסי המערכות בישראל (גליון 3, פברואר 2008), ופרסומו כעת ב"בטיחות" נעשה ברשות "קול המערכות".

---

1. ש. ארואטי, ניתוח סיכונים הסתברותי ככלי עזר לממוני בטיחות, בטיחות 290 (יוני-יולי 2004).
2. הפרסום System Safety Analysis Handbook, בהוצאת System Safety Society (ניתן לרכישה גם על גבי CD), מציג ומתאר כמאה שיטות שונות לניתוח סיכונים.

איור 2: הערכת הבטיחות בתכן



- מהי תוצאת הכשל - בסביבה המיידית של הרכיב, במעגלים רחבים יותר, במערכת כולה?
- מהי ההסתברות להתרחשותו של אופן כשל מסוים בחומרה מסוימת?
- אם התוצאה היא קריטית למערכת כולה - כיצד נמנע את הכשל, או את השפעתו?

דוגמה לרכיב ולכשלים אופייניים בו: נגד חשמלי - נתק או קצר.

דוגמאות לשיפורי-תכן שניתן להפיק מניתוח FMECA: החלפת רכיבים, תכן שונה של התקנות וזיווד, שיפור התכן לבדיקתיות, הוספת ניסויים, מעקב התיישנות, הוספת נוהלי בדיקות, הפעלה או תחזוקה.

השיטה איננה נותנת ביטוי לתרחישים מורכבים (מספר תקלות במקביל, תפעול שגוי או תזמון שגוי).

● **HAZOP - ניתוח גורמי סיכון ותפעוליות** (Hazard and Operability Study)

הניתוח עוקב אחר **תהליך הזרימה** במערכת המנותחת:

- מה יקרה אם הזרימה בנקודה X תופסק, תוגבר, תתהפך, תתחמם, ...?
- אם התוצאה קריטית למערכת - מה עלול לגרום לכך?
- אם התוצאה קריטית למערכת - כיצד נמנע את האירוע, או את תוצאותיו?

השיטה מתאימה במיוחד לניתוח תהליכים במיתקנים כימיים מורכבים, או במערכות אחרות שבהן ניתן לזהות זרימה של תהליך ולעקוב אחריה.

דוגמה: המשמעויות התפעוליות וההשלכות הבטיחותיות של הפסקה בכניסת חומר קירור לתהליך הכולל ריאקציה אקזותרמית.

● **FTA - ניתוח עצי תקלות** (Fault Tree Analysis):

הניתוח מתחיל מ**אירועים סופיים** קריטיים ונערך מהכלל אל הפרט:

- איך (בניתוח לוגי לאחור) יכול להתרחש אירוע קריטי Y?
- מהם צירופי הגורמים לאירוע קריטי זה?
- מהי ההסתברות להתרחשות כל אחד מן הגורמים לאירוע קריטי זה?
- איך (על בסיס הניתוח הלוגי) ניתן למנוע את האירוע הקריטי?

השיטה מתאימה במיוחד לניתוח מערכות מורכבות ומערכות אדם-מכונה.

דוגמה: הגורמים ל"אירוע סופי" של פיצוץ קטלני במפעל העוסק בחומרי נפץ.

● **ETA - ניתוח עצי אירועים** (Event Tree Analysis):

הניתוח מתחיל **מהתרחשות בודדת**, כדוגמת כשל טכני או פעולה שגויה ("אירוע מתחיל"):

- איזה מנגנונים במערכת עשויים למנוע או להפחית את חומרת התוצאה הנובעת מההתרחשות?
- איזה תקלות או פעולות נוספות עלולות להחמיר את תוצאת ההתרחשות המקורית?
- מהם התרחישים האפשריים בעקבות התרחשות התקלות הנוספות?
- מהן ההסתברויות לתרחישים אלה, אם נתונות ההסתברויות לתקלות הבסיסיות?

השיטה מתאימה במיוחד לאפיון צירופי כשלים בתפקודים העקריים של המערכת, שיגרמו לתקלה בטיחותית, וכן למיצוי המיגוון האפשרי של אירועים סופיים.

דוגמה: התוצאות של רשרת אירועים, שהראשון בה הוא נפילת הֶסְפֵּק מרשת החשמל החיצונית במפעל שבו ההספק החשמלי הוא חיוני.

טרם פותחה שיטת ניתוח שהיא מספקת למיצוי שיטתי מלא של כל הכשלים והתרחישים האפשריים במערכת טכנולוגית מורכבת. לפיכך, כדאי להפעיל יותר משיטת ניתוח אחת לבחינת מערכת. במערכות אלקטרומכניות מורכבות מקובל לפתוח בניתוח ETA כדי למפות את כל האירועים הסופיים האפשריים; מן הרשימה המתקבלת ממוצים אירועים קריטיים, שכל אחד מהם מחייב הכנת ניתוח FTA נפרד. כדי לפרט את עצי התקלות עד לרמת רכיבים, חיוני להכיר היטב את מאפייני הכשלים של הרכיבים האלה. מכאן נובע צורך בביצוע FMECA למערכת הנבחנת לפני עריכת ניתוח FTA בה.

בניתוח תהליכים כימיים מורכבים מקובל להפעיל את שיטת HAZOP. בניתוח מיתקנים כימיים כדאי לפתוח בניתוח FMECA כדי להבין את מאפייני הכשלים של הרכיבים, לפני המעבר לניתוח תהליכי הזרימה במערכת. לעתים כדאי לנתח תת-מערכות מסוימות במיתקן הכימי גם בשיטת FTA.

רצוי לקשור בין ניתוחי הבטיחות לניתוחי האמינות, כדי "להציף" מוקדם ככל האפשר ניגודים בין שני מאפיינים חשובים אלה של המוצר (לדוגמה: השפעת מורכבות של מערכת, הנובעת מצורכי בטיחות, על האמינות).

אימות העמידה בדרישות הבטיחות ותיקוף הבטיחות

אימות ותיקוף הבטיחות נועדו לבסס את תחושת הביטחון במוצר עם התקדמות הייצור, ולאשש (או להפריך) את המסקנות שהופקו בשלב הערכת הבטיחות. בשלב זה ניתן גם מענה לפערי ידע שזוהו בשלב ההערכה, ואשר מחייבים ביצוע ניסויים והפעלת סימולציות. ערוץ-פעילות זה כולל, כאמור, הן אימות עמידתו של המוצר בדרישות בטיחות פורמליות, והן מתן תוקף לבטיחות המוצר - באמצעות הוכחה או הדגמה של עמידתו בתרחישים בטיחותיים ("איומים"), אשר זוהו במהלך התכן, ואשר המפתח רואה

מחובתו לתכנן את המוצר כך שיישאר בטוח דיו גם אם יתרחשו (למרות שהעמידה בהם לא נדרשה פורמלית).

על אף ההבדל העקרוני בין המושגים "אימות" ו"תיקוף" - במישור המעשי קיימת חפיפה חלקית בין הפעולות הנדרשות למימוש האימות והתיקוף. לפיכך מקובל לאחדם לערוץ פעולה משותף[3].

קיימות מספר שיטות לאמת את בטיחות המוצר:

- **ניתוח:** חישובים הנדסיים תוך שימוש במודלים ובנוסחאות והסתמכות על טבלאות נתונים ועל שיקולי דמיות (by similarity). לדוגמה: חישוב מקדם-בטחון למיכל-לחץ.
- **סימולציה:** מודל ממוחשב של המוצר או של חלקים ממנו, עם או בלי דגם חלקי או מוקטן של המוצר, והרצות של המודל המדמות את אופן הפעולה הצפוי של המוצר בפעולה תקנית, בתנאי קיצון או במצב תאונה.
- **בדיקה:** הפעלת תהליכי בחינה על המוצר הנבדק בתנאי סביבה מוגדרים. נבדקים מרכיבים תקניים של המוצר, והבדיקה נערכת באופן שיוכלו לתפקד באופן תקין גם לאחר ביצועה. במהלך הבדיקה נמדדים תכונות ופרמטרים תפקודיים של המוצר על פי תכניות בדיקה מוכנות מראש.
- **ניסוי:** הפעלה של המוצר, שבו מורכבים ומשולבים גם פריטים שהוכנו במיוחד לצורך הניסוי ושאינם אמורים לתפקד כמרכיבים במערכת תקנית. במהלך הניסוי נהרסים לעתים המוצר כולו, או חלקים ממנו, (לדוגמה - כאשר נבחנת בטיחות המוצר בתרחישי תאונה, תמונה 1).

3. בהמשך הפרק נשתמש לעתים במונח "אימות הבטיחות" במשמעות של אימות ותיקוף.

תמונה 1: ניסוי לאימות בטיחות - התנגשות רכב

דרכים נוספות לאימות הבטיחות הן תצפית-עין וביקורת חזותית.

אימות תכונה בטיחותית מסוימת נעשה, במרבית המקרים, בשילוב של מספר שיטות. לדוגמה: נעשה שימוש במודל לצורך זיהוי תרחישים. בעזרת תרחישים אלה מזוהים תנאי סביבה אופייניים, ובהם נערכים ניסויים חלקיים למרכיבי המערכת או בדיקות וניסויים במערכת השלמה.

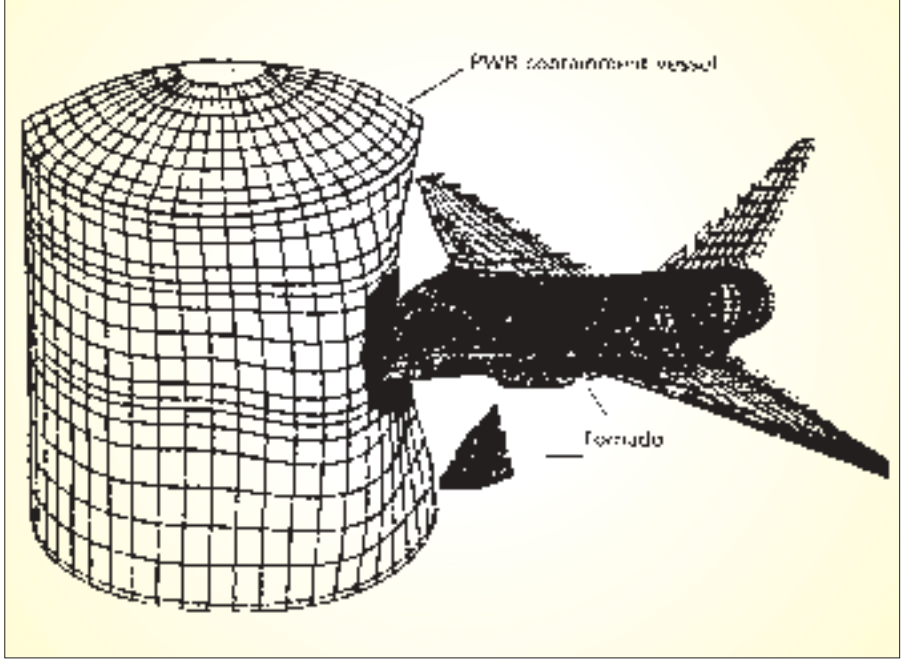
בפרויקט מורכב רצוי להכין "תכנית לאימות ולתיקוף הבטיחות". התכנית בנויה כטבלה (מטריצה), המציגה את אופן האימות מול דרישות הבטיחות שנקבעו ע"י המזמין ומול האיומים הרלוונטיים, כאשר אופן האימות הוא ניתוח - התכנית מפרטת את אופי הניתוח ואת הפרמטרים הנבדקים; כאשר אופן האימות הוא סימולציה - מתוארת הסימולציה וניתנים תחומי הערכים של הפרמטרים שיהוו קלט להרצתה; כאשר אופן האימות הוא בדיקה או ניסוי - מפורטים מטרות הפעולה, מערכת הניסוי, אופן השילוב בתכנית הכוללת של הניסויים ותחומים של המשתנים הרלוונטיים לניסוי. תכנית אימות ותיקוף הבטיחות היא מסמך מתעדכן, על פי רמת הידע הקיימת בפרויקט וה"איומים" הנוספים המזוהים בכל שלב של הפיתוח. קיומה של תכנית פורמלית לאימות הבטיחות המוסכמת, בין בעלי עניין שונים ובעיקר בין המזמין לבין המפתח, מפשט בסוף הפיתוח, את הכנת ההנמקה ע"י המפתח כי המוצר בטוח, ולאור זאת - את הליכי אישור הקבלה ע"י המזמין.

במידת האפשר, רצוי לשלב את הניסויים והבדיקות המיועדים לאימות הבטיחות, בתכנית הניסויים והבדיקות להוכחת ביצועי המוצר ולאימות אמינותו. יחד עם זאת, יש לעמוד על ביצוע ניסויים נפרדים כאשר לא ניתן לענות במידה מספקת באמצעות השילוב על צורכי אימות הבטיחות.

קיימות מספר בעיות המקשות מאד על אימות הבטיחות של המוצר. נציג כאן אחדות מהן:

- כאמור לעיל, מעטפת התנאים הנדרשים **לבטיחות** המוצר היא נרחבת בהרבה ממעטפת התנאים הנדרשים **לתקינותו**. כפועל יוצא מכך, גם אימות העמידה במעטפת הבטיחות קשה בהרבה מאימות העמידה בדרישות התקינות הטכנית במעטפת הביצועים התקנית.
- השאיפה העקרונית היא **להוכיח** בעזרת ניסויים את עמידת המוצר בדרישות הבטיחות. "הוכחה" - משמע אמון מלא ומוחלט בבטיחות המוצר. אבל, במקרים רבים, הוכחה ניסויית אינה אפשרית: בעוד שניתן להוכיח בעזרת ניסויים אמינות בסדר גודל של 99% ואף למעלה מכך, אין דרך ניסויית להוכיח רמת בטיחות של אחד למיליון ברמת מהימנות סבירה. בלית ברירה מדברים על **אימות** - ביטוי "רך" יותר מאשר הוכחה - ולעתים אפילו על "**הדגמה**" בלבד.
- עקב הקושי באימות ניסויי על פני כל מעטפת הבטיחות הנדרשת, מנסים לעתים לאמת את הבטיחות בעזרת ניתוח תגובת המוצר לסדרה של תרחישים חזויים, כלומר: נעשה אימות בנקודות "מייצגות" (לכאורה) ומכך מקישים על המעטפת כולה.

איור 3: סימולציה של פגיעת מטוס במבנה כור גרעיני



גישה זו היא ציורית ומשכנעת, אבל חולשותיה בחוסר השיטתיות שלה (התרחישים הנבחרים הם, מדרך הטבע, כאלה הצצים בקלות רבה בדמיון, ולא בהכרח אלה המייצגים את הנקודות החשובות באמת במעטפת), וכן באי-התייחסותה ל"תרחיש שלא חשבנו עליו", אשר עלול להתגלות בעתיד ולשמוט את הקרקע מתחת לטענת הבטיחות המאומתת.

- גישה חלופית להפחתת מספר הניסויים היא "שיטת קנס", שבה מוחלפים מספר ניסויים בנקודות שונות של מעטפת התנאים הנדרשים, בניסוי אחד הנערך בתנאים מחמירים. חסרונה של הגישה הוא בכך שבמקרה של כישלון בניסוי, קשה להסביר אם הוא נבע מתכן לקוי המחייב תיקון, או מתנאי הניסוי החריגים שכלל אינם רלוונטיים לפעולת המערכת.
- העלות של ניסויים במערכת שלמה עלולה להיות גבוהה מאוד. לפיכך נערכים לעתים ניסויים חלקיים, והשלמת המידע לרמת המערכת מבוצעת בסיוע ניתוחים וסימולציות. גישה זו היא שימושית יותר, אבל מחירה הוא תוקף (validity) נמוך יותר של המסקנות המופקות ממנה.

ניהול הבטיחות

ניהול הבטיחות נדרש לתת מענה לשני צרכים חשובים:

- האחד - צורך בניהול מובנה של הפעילויות בתחום הבטיחות כשלעצמו, הנובע מריבוין של הפעילויות האלה וממורכבותן. הניהול המובנה נועד להשיג, בין השאר, **אפקטיביות מרבית של החשיבה הבטיחותית**, כלומר מעבר ישיר וטבעי מזיהוי פערים וחולשות לאיתור פתרונות וליישומם ההנדסי הנכון. כדי לענות על צורך זה יש ליצור מסגרת פורמלית לפעילות הבטיחות בפיתוח, להכין תכניות שעל פיהן תבוצע העבודה, ולהפעיל כלים למעקב אחר ביצוע התכניות.
- השני - צורך להבטיח היזון חוזר בין האנשים העוסקים בקביעת עקרונות הבטיחות לבין מנהלי הפרויקט ומפתחיו, וההכרח לתאם את פעילויות הבטיחות עם שאר הפעילויות בפרויקט. ההיזון החוזר והתיאום נועדים להשיג **השפעה של שיקולי הבטיחות על התכן במועד מוקדם ככל האפשר**, כך שיהיה מוטבע מלכתחילה באיפיון המערכתי, באיפיון המיכללים ובתפישת ההפעלה. שילוב מוקדם זה מונע צורך בשינויים ובשיפורים של תכן ונהלים במועד מאוחר, כאשר מתגלים פערים וחולשות בתחום הבטיחות ונוצר צורך לגשר עליהם. מענה הניתן בתפיסה העקרונית (concept) של המוצר ושל אופן הפעלתו הוא תמיד יעיל, חסכוני ומשולב יותר מאשר מענה המוצמד כ"טלאי" על גבי מוצר מוגמר. כלי ניהולי מרכזי בחשיבותו להשגת יעד זה הוא מעקב מתמיד, החל בשלבים הראשונים של הפיתוח וכלה בסיומו, על מצב העמידה בדרישות הבטיחות ("סטטוס הבטיחות").

כדי לעמוד ביעדי העל האלה, ניהול הבטיחות בפרויקט צריך לכלול שני סוגים של כלים: כלי **תכנון** וכלי **מעקב**. כלי התכנון העיקריים הם תכנית הבטיחות של הפרויקט ותכנית אימות ותיקוף הבטיחות; תכניות אלה נכתבות כבר בשלבים הראשונים של הפרויקט (לקראת סקר התכן הראשוני), ומעודכנות במהלך התכן והפיתוח על פי הצרכים המתפתחים. הנושאים העיקריים למעקב הם סטטוס תכנית הבטיחות, סטטוס העמידה בדרישות, סטטוס אימות הבטיחות, והסיכונים השיוריים.

א. כלי תכנון: תכנית בטיחות של הפרויקט

תכנית הבטיחות, שיש להכינה בצמוד להתארגנות הראשונית של הפרויקט, כוללת:

- הצגת ארגון הפרויקט בתחום הבטיחות: הבהרת אחריותו של ראש הפרויקט לבטיחות, מינוי "מהנדס מערכת לבטיחות", והגדרת הזיקה של בעלי התפקידים השונים במינהלת הפרויקט למימוש דרישות הבטיחות (עוד על האחריות הניהולית לבטיחות - בהמשך).
- זיהוי מקורות לדרישות הבטיחות (חוקים ותקנות, תקנים, נוהלי הארגון, דרישות המזמין).
- זיהוי תהליכים שבאמצעותם ישולבו שיקולי הבטיחות בפרויקט (הכנת דרישות ומיפרטים, תהליכי תכן, הערכה ואימות).
- זיהוי מימשקים רלוונטיים לשיקולי בטיחות (עם מערכות אחרות, עם הסביבה, עם המשתמש וכו').
- הצגת עקרונות המעקב שיבוצע על מידת העמידה בדרישות ועל סטטוס המימוש של התכניות עצמן.
- הצגת המנגנונים שבהם תושג בטיחות העובדים בפרויקט הפיתוח.

ב. כלי תכנון: תכנית אימות ותיקוף הבטיחות

תכנית מפורטת לאימות ולתיקוף הבטיחות, שתכניה תואמים לאמור בפרק הדן בנושא זה לעיל. נדרשת תכנית ממוקדת בעניין זה עקב ההשפעה ההדדית של מרכיביה עם ניסויים, בדיקות ופעילויות נוספות של הפרויקט, הנערכים כחלק מתהליך הפיתוח, כרוכים בהשקעת משאבים רבה ומחייבים תיאום מדויק.

ג. כלי מעקב: סטטוס תכנית הבטיחות, אימות העמידה בדרישות הבטיחות ותיקוף הבטיחות

המעקב בנושאים אלה נועד לוודא כי ביצוע התכניות אינו "דועך" עם התקדמות הפיתוח, אלא נותר חי, פעיל ואף "בועט" כאשר הדבר נדרש. המעקב מבוצע לאורך כל חיי הפרויקט, ונתוניו מתעדכנים במקביל להתקדמות התכן, ההערכה והייצור. דיווחי סטטוס מוצגים באופן תקופתי ובמתכונת שיטתית לביקורת הנהלת הפרויקט, המזמין וגורמים רלוונטיים נוספים. הצגת סטטוס הבטיחות משולבת ב"אבני דרך" חוזיות כדוגמת סקרי תכן (ראו בהמשך).

ד. כלי מעקב: "פנקס סיכונים שיוריים"

רשימת סיכונים מזוהים בפרויקט, שתחילתה ב"רשימה ראשונית של גורמי סיכון" המוכנה במקביל לאיפיון המערכתי הראשוני של המוצר, והיא מתעדכנת באופן שוטף. הרשימה משתנה, עם התקדמות הפיתוח, בשתי מגמות: האחת - מחיקה של סיכונים שהתכן נותן להם פתרון מספק, והשניה - פירוט רב יותר של הסיכונים הנותרים. בסיום הפרויקט מקבל המזמין את הרשימה הסופית של ה"סיכונים השיוריים" - אלה שנותרו בתום תהליכי הפחתת הסיכונים, מכיוון שלא ניתן לבטלם או להפחיתם יותר - והנחיות כיצד לנהוג ולהשתמש במוצר כך שהסיכונים הבלתי-נמנעים האלה יישארו בשליטה ולא יובילו לתאונות ולפגיעות.

הדרך הנכונה לוודא ניהול רצוף ומעקב "חי" בתחום הבטיחות היא לשלב את הניהול והמעקב האלה במנגנוני הניהול והמעקב הכלליים של הפרויקט: פעולות הבטיחות מהוות אז מרכיבים אינטגרליים בתכנית העבודה של הפרויקט ובמעקב שעורכת ההנהלה. בשום פנים אין לנהל את פעולות הבטיחות במסגרת תכנית עבודה המנותקת מתכנית הניהול הכוללת של הפרויקט!

אין ניהול ללא תיעוד, וגם ניהול הבטיחות בפרויקט כרוך בהכנת תיעוד מגוון: מיפרט דרישות הבטיחות, מיפרט דרישות התכן לבטיחות ("תרגום" דרישות הבטיחות הנוגעות לתכן למונחים הנדסיים), מיפרט מימשקי בטיחות, מיפרטי מערכת ומכללים ראשיים ודוחות בטיחות. שליטה ניהולית על ההכנה וההפצה של התיעוד הבטיחותי מושגת באמצעות קביעת "אבני דרך" פורמליות בתחום הבטיחות, שבהן, בין השאר, נכללת ההפצה של מסמכים שנקבעו מראש. אבני הדרך משולבות בסקרי התכן המערכתיים שעורך המפתח מול המזמין, בהתאם לחוזה הפיתוח. קיימת מתכונת מקובלת לשרשרת של סקרי תכן כאלה (ראו טבלה). בכל סקר יש לכלול נושאי בטיחות ספציפיים, המתאימים למועד שבו נערך הסקר.

להלן - סקירת הפעילויות בתחום הבטיחות, שיש לבצע בכל שלב של הפיתוח ולהציג במועד הסקר המסיים את השלב:

1. גיבוש צורך והכנת דרישות עד SRR - סקר דרישות מערכת (System Requirements Review):

- מיפרט דרישות בטיחות (על פי כל המקורות).

2. תכן מערכתי עד SDR - סקר תכן מערכתי (System Design Review):

- תכנית בטיחות פרויקטית;
- מיפרט דרישות תכן לבטיחות;
- רשימה ראשונית של גורמי סיכון (PHL - Preliminary Hazard List)
- מיפרט מימשקי בטיחות בין מרכיבי המוצר, ובינו לבין הסביבה;
- הערכת עמידת עקרונות התכן בדרישות הבטיחות.

3. תכן-על עד PDR - סקר תכן ראשוני (Preliminary Design Review):

- עדכון מיפרט דרישות התכן לבטיחות (אם נדרש לאור לקחי התכן הראשוני);
- תכן מערכתי לבטיחות (אם רלוונטי למוצר);
- הערכת בטיחות ראשונית (עצם היכולת לעמוד בדרישות, ומידת העמידה בהן) (PHA - Preliminary Hazard Analysis);
- תכנית כללית לאימות הבטיחות (דגש על צורך בניסויים);
- פרקי בטיחות למיפרטי מערכת ומיכללים ראשיים;
- הערכת סטטוס הבטיחות במחזור החיים.

טבלה 1: שלבים וסקרי תכן בפרויקט פיתוח אופייני

שלב בחיי המוצר	סקר	פעילות הפיתוח	מידע ומסמכים
אפיון הדרישות		בדיקת היתכנות, לימוד תקנות ותקנים, ניתוח דרישות המזמין	
	SRR - סקר דרישות מערכת	סקר דרישות המזמין	מיפרטי דרישות למוצר
תכן מערכתי		בחינת קונספטים וחלופות, הגדרת מימשקים חיצוניים	סקר חלופות, סקר טכנולוגיות וניתוח סיכונים בפיתוח, הגדרת מימשקים
	SDR - סקר תכן מערכתי	אישור הקונספט הנבחר	סיכום הסקר
תכן ראשוני		קביעת ארכיטקטורה ומימשקים פנימיים; בניית עץ-מוצר שלדי	הגדרת הארכיטקטורה, תכניות אינטגרציה וניסויים תכניות לו"ז ומשאבים
	PDR - סקר תכן ראשוני	אישור הארכיטקטורה	סיכום הסקר
תכן מפורט		תכן מפורט למכללים תכן פרמטרי לביסוס נקודת העבודה	מיפרטי תכן מלאים שרטוטים, אנליזות, חישובים
	CDR - סקר תכן מפורט	אישור התכן המפורט	סיכום הסקר
ייצור אבי-טיפוס וניסויי פיתוח		בניית מכללים ניסויי פיתוח ומבחנים מפורטים	מיפרט ניסויי פיתוח תוצאות ניסויי פיתוח רישום תקלות
	TRR - סקר מוכנות לניסוי	אישור תכנית ניסויי קבלה	סיכום הסקר
ייצור וביצוע מבחני אישור		מבחנים מערכתיים מבחני אישור פורמליים	תוצאות מבחני אישור תיק תכ"מ תיעוד תפעולי
	PRR - סקר מוכנות לייצור	אישור קווי ייצור אישור מיתקנים	סיכום הסקר
ייצור סדרתי		ייצור סדרתי	הוראות תחזוקה
תמיכה במוצר		תמיכה, שידרוגים	
גריטה		תכנית הוצאה משירות תכנית פירוק וטיפול בפסולת	

4. תכן מפורט עד CDR - סקר תכן מפורט (Critical Design Review):

- הערכה מסכמת לבטיחות התכן (הנמקה מפורטת לעמידה בדרישות);
- עדכון מפורט של התכנית לאימות הבטיחות;
- הערכות בטיחות מפורטות למיכללים (SSHA - Sub-System Hazard Analysis);
- אימות הבטיחות - ביצוע (חלקי) ותיעוד; עדכון תכנית האימות;
- עדכון להערכת סטטוס הבטיחות במחזור החיים.

5. פיתוח והרכבה עד TRR - סקר מוכנות לניסוי (Test Readiness Review):

- הערכות בטיחות לתהליכי ייצור והרכבה;
- המשך אימות הבטיחות;
- הערכות בטיחות לניסויי פיתוח וקבלה;
- עדכון להערכת סטטוס הבטיחות במחזור החיים.

6. ניסויים ומבחני-אישור עד PRR - סקר מוכנות לייצור (Production Readiness Review):

- השלמת הניסויים ואימות הבטיחות;
- תיעוד מסכם של הערכת הבטיחות עם השלמת הפיתוח;
- הערכת בטיחות להפעלה ולתחזוקה (O&SHA - Operation and Service Hazard Analysis);
- הערכה מסכמת של סטטוס הבטיחות במחזור החיים.

7. בטיחות בייצור ובהפעלה שוטפת - "תמיכה במוצר" לאורך מחזור החיים עד הוצאה משירות

- התעדכנות מתמדת על מצב הבטיחות;
- ניהול והערכת הבטיחות בתהליכי שדרוגים ("ש"וש" - שינויים ושיפורים);
- ניהול והערכת הבטיחות בהוצאת המוצר משירות.

מימוש האחריות לבטיחות בהנהלת הפרויקט

בעמודים הקודמים תוארה מסכת ענפה ומורכבת של פעילויות. לצורך ביצוע פעילויות אלה דרוש צוות מקצועי ומאורגן, שבראשו עומד מנהל ממוקד ובעל תחושת מחויבות עמוקה. **האחריות לבטיחות המוצר חלה על מפתח המוצר, ובראש-ובראשונה - על ראש הפרויקט**: הוא האחראי לעמידה בדרישות הבטיחות באמצעות השגת יעדי הבטיחות הנכללים במיפרטים, לביצועה של תכנית הבטיחות, להטמעתן של המסקנות וההמלצות הנגזרות מהערכות הבטיחות (במהלך הפיתוח) ומן הפעולות לאימות הבטיחות (בשלביו הסופיים של הפיתוח), ומעל לכל - ליצירת תרבות של מחויבות לבטיחות בצוות הפיתוח. לצידו של ראש הפרויקט עומד "מהנדס מערכת לבטיחות" או "מהנדס בקרת סיכונים" (המינוח משתנה בארגונים שונים, אבל המשמעות נשארת בעינה). הוא האחראי להובלה המקצועית והניהולית של כלל פעילויות הבטיחות בפרויקט, להכנת תכניות עבודה בתחום הבטיחות ולמעקב אחר ביצוען, לביצוע ניתוחי בטיחות (או לבקרה על ביצועם בידי גורמים אחרים), ולשילוב (אינטגרציה) של כלל הפעילויות והחשיבה בהיבטי הבטיחות ע"י אנשי התכן, הייצור, ההרכבה, הניסויים והתמיכה במוצר.

מהנדס המערכת לבטיחות איננו פועל ב"חלל ריק": יש לראות את כל בעלי התפקידים בפרויקט כממלאי משימות בתחום הבטיחות, וזאת כמרכיב משולב ובלתי נפרד (אינטגרלי) בעבודת הפיתוח. הבטיחות אינה נחלתם של אנשי הבטיחות המקצועיים בלבד: בצד המימד המקצועי שלה, היא אמורה להיות קו מנחה ובסיס למחשבה של כל צוות הפיתוח. ההטמעה של תפישה זו בקרב אנשי הצוות כולם היא, כאמור, אחת ממשימותיו החשובות של ראש הפרויקט, בסיועו המקצועי של מהנדס המערכת לבטיחות.

סיכום

במאמר זה הצגנו מתכונת שיטתית לשילוב שיקולי בטיחות המוצר וניהול הבטיחות בתהליך פיתוח טכנולוגי, מתכונת המשמשת מזה שנים, במידה רבה של הצלחה, גורמים העוסקים בפיתוח מערכות ומוצרים מורכבים בחזית הטכנולוגיה.

מהי הזיקה בין בטיחות המוצר לבין הביצועים והאמינות התפעולית של המוצר? יש הטוענים כי התכן לבטיחות תומך, מעצם טבעו, באמינות התפעולית (או המבצעית), שכן תנאי למוצר אמין הוא היותו בטוח. אחרים טוענים בתוקף כי הבטיחות כרוכה בהוספת מערכות יתירות ובסרבול לוגיקת ההפעלה, ולפיכך מימוש דרישות הבטיחות יוצר סיבוך הפוגע בביצועים ובאמינות התפעולית. ההנחה העומדת בבסיס טענה זו הוא כי ככל שמערכת היא פשוטה יותר - כך היא אמינה יותר.

לשאלה זו אין, ככל הנראה, תשובה יחידה. לפעמים הטמעת שיקולי הבטיחות במוצר משפרת גם את אמינותו, ובמקרים אחרים היא מפחיתה אותה. הבטיחות והאמינות הן מרכיבים של איכות המוצר. כדרכם של מרכיבים במיכלול, הצירוף שלהם הוא לפעמים סינרגטי ולפעמים - יוצר ניגודים. בשילוב של שיקולי הבטיחות בתכניות הפיתוח של הפרויקט וביישומם במימוש הפיתוח הלכה למעשה יש להפעיל הרבה שיקול דעת, תפישה מאוזנת של צרכים ואילוצים, ובראש-ובראשונה - שכל ישר. בטיחות המוצר חיונית לאיכותו ולשימוש בו; אבל אסור לנתק אותה ממערך השיקולים השוטף של הפיתוח, אלא להיפך - יש לשלבה במערך השיקולים הזה במועד מוקדם ככל האפשר ובמידה המירבית האפשרית. ■