שילוב שיקולי בטיחות המוצר וניהול הבטיחות בתהליך פיתוח טכנולוגי

(חלק ראשון)

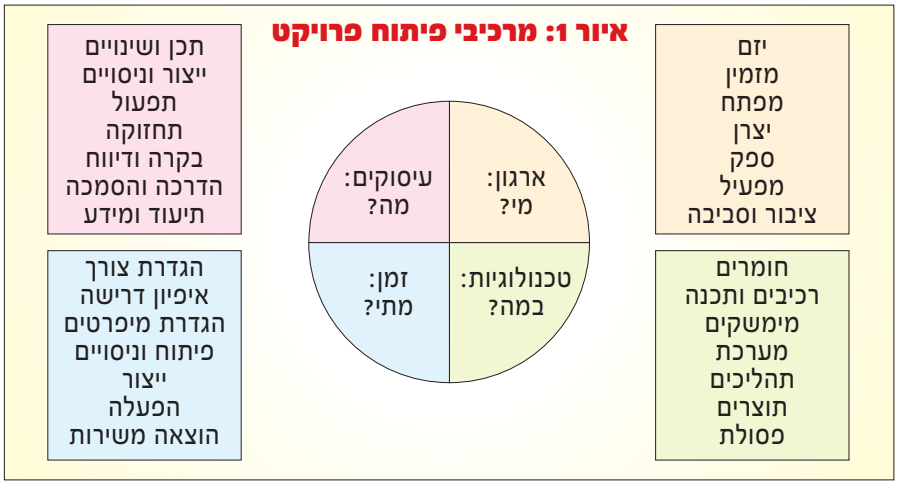
מאת **ד"ר מיכאל מהרי"ק וד"ר שמשון ארואטי**

טכנולוגיות עוסקות בחומרים, במיתקנים, בתהליכים ובמוצרים. בכל אלה כרוכים סיכונים לאדם ולסביבה

כדי להפחית, במידת האפשר, את הסיכונים הכרוכים בחומרים, במיתקנים, בתהליכים ובמוצרים - יש לשלב שיקולי בטיחות בתכן ובהפעלה של הטכנולוגיות. צירוף המלים "תֶכֶן" ו"טכנולוגיות" מעורר אסוציאציה של שולחן- שרטוט (וכיום - של צג המחשב), אבל למעשה מדובר במארג מורכב של פעילויות הנדסיות וניהוליות החורגות מן התכן עצמו וכוללות את תהליך הפיתוח כולו (ראו הגדרות ל"תכן" ול"פיתוח" במסגרת). בתפישה הרחבה המאפיינת בשנים האחרונות את הראייה הבטיחותית, עלינו להתייחס לא רק ל"בטיחות בתכן" של מוצר כלשהו אלא ל"בטיחות בפיתוח המוצר" - כלומר, גם לכל מרכיבי הפיתוח שמעבר לתכן-גופו. בתפישה זו יש לכלול את "בעלי העניין" השונים (החל ביזם ובמפתח וכלה באנשים הנמצאים בסביבת המוצר המופעל), את מיגוון העיסוקים ומיגוון הטכנולוגיות המשמשים בפיתוח, ואת מרחב הזמן המלא של מחזור חיי המוצר (איור 1).

במאמר זה נציג מתכונת שיטתית, המקובלת מזה שנים במספר ארגונים טכנולוגיים מובילים בישראל, לשילוב שיקולי בטיחות וניהול הבטיחות בתהליך פיתוח. למיטב ידיעתנו וניסיוננו, מתכונת זו מספקת תוצאות טובות יותר - במונחים של שילוב הבטיחות במוצר בתפישה מערכתית והתאמתו לקריטריונים מִבְנִים - לעומת גישות שהיו מקובלות בטכנולוגיה בעבר.

איור 1: מרכיבי פיתוח פרויקט



"בטיחות הייצור" ו"בטיחות המוצר"

את שיקולי הבטיחות יש לשלב בפיתוח טכנולוגי-תעשייתי בשני תחומים:

- התחום הראשון הוא הבטיחות ב**תהליכי הפיתוח והייצור** במפעל. תחום זה כולל תכנון והקמה של מבנים ומיתקנים, בחירת ציוד וחומרים ושילובם בעבודה, תכנון תהליכי עבודה, הכנת נהלים לפעולה בשגרה ובמצבי חירום, תכנון וביצוע פעולות תחזוקה, הדרכת עובדים וכו'. בהקשר הזה מדובר, בראש ובראשונה, בבטיחותם של עובדי הפיתוח, הייצור, הניסויים ושאר "פעילויות הליבה", ונוסף לכך גם בבטיחותם של עובדים אחרים במפעל, בבטיחותם של תושבים המתגוררים בשכנות למפעל, וכן בהפחתת סיכונים לנכסי המפעל ולסביבה.
- התחום השני הוא בטיחות ה**מוצרים** שמפתח המפעל. בהקשר הזה מדובר, קודם-כל, בבטיחות המשתמש - עובד, עקרת-בית, ילד, חייל - לאורך מחזור החיים של המוצר, אך גם בבטיחות אנשים הנמצאים בקרבת המשתמש במוצר, בהפחתת סיכונים לנכסים הנמצאים בקרבת המוצר, ובהפחתת סיכונים לסביבת האתר שבו נעשה שימוש במוצר. לעתים בטיחות המוצר מתייחסת גם לסיכונים באתרים הנמצאים הרחק מסביבת השימוש המתוכנן במוצר. לדוגמה: בהפעלת מערכת מוטסת לא מאוישת יש לקחת בחשבון גם את הצורך למנוע פגיעה של המערכת (עקב תקלה בה) באזורים מרוחקים מן האזור שבו היא מופעלת; בבחירת חומרים למערכת קירור יש לקחת בחשבון פגיעה אפשרית בשכבת האוזון.

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".

העקרונות, הגישות ואף הכלים הטכניים המשמשים ליישום שיקולי בטיחות עשויים להיות דומים בשני התחומים. בפועל, לא תמיד הדבר הוא כך. בהיבטים ארגוניים וניהוליים יש הבדלים מהותיים בין הבטיחות המפעלית לבין בטיחות המוצר:

- הבטיחות המפעלית עוסקת בעובדי המפעל, ואילו בטיחות המוצר מתייחסת בעיקרה לאנשים שיעשו שימוש במוצר;
- הבטיחות המפעלית ממוקדת במידה רבה בשגרה, בסיכוני ההווה ובבעיות של יום-יום, ואילו בטיחות המוצר מקדישה את המאמץ העיקרי למתן פתרונות כוללים לסיכונים עתידיים בטווח-זמן ארוך;
- הבטיחות במפעל מאופיינת ע"י רציפות והתמשכות, בעוד שפיתוח מוצר הוא "חבילת עבודה" שיש לה התחלה, משך מוגדר וסוף.

כפועל יוצא מהבדלים אלה - בארגונים רבים נעשה הטיפול ב"בטיחות המפעל" וב"בטיחות המוצר" על ידי גורמים שונים, שלעתים מופרדים זה מזה עד רמות הניהול הבכירות: "בטיחות המפעל" ממומשת ע"י הנהלת המפעל ויחידות הביצוע, ואילו "בטיחות המוצר" מופקדת בידי מינהלות הפרויקטים. הפרדה זו שכיחה בעיקר בארגונים שבהם מיושמת גישת "ניהול מטריצי" ("קווי מוצר" פרויקטיים הפועלים מול יחידות ביצוע מקצועיות). עם זאת, במקרים לא מעטים מתקיימים שיתוף פעולה מקצועי והפריה הדדית בין הגורמים המטפלים בשני ההיבטים, ואף קיימים ארגונים שבהם העיסוק בשניהם נתון בידי מנגנון ניהולי ומקצועי אחד.

מאמר זה עוסק בבטיחות מוצרים טכנולוגיים. הדגש בו הוא על הטמעת בטיחות המוצר כבר בתהליך הפיתוח. כל האמור להלן רלוונטי גם לעניין הבטיחות במפעל; אבל העקרונות, הגישות והפעלת הכלים יוצגו בראיית פיתוח המוצר כפרויקט שיש לו שלבים, לוחות זמנים, יעדים ואבני דרך ובעיקר התחלה וסוף, להבדיל מן הפעילות המתמשכת המאפיינת, כאמור לעיל, את ה"בטיחות המפעלית".

לנוחות הקוראים, להלן הגדרות למספר מונחים שבהם נעשה שימוש במאמר זה (על פי סדר הופעתם):

תֶּכֶן (design): תכנון טכנולוגי-הנדסי ישיר של מיתקן או תהליך.

פיתוח (development): מסגרת רחבה של פעילויות ארגוניות, מקצועיות וניהוליות הכרוכות ביצירת מיתקן או תהליך: הגדרת צורך, אפיון דרישות, הכנת מפרטים, תכן, ייצור והרכבה, בחינה וניסויים, ותמיכה במוצר לאורך כל מחזור חייו עד לגריטתו ועד בכלל.

מוצר: במאמר זה - תוצר, מכל סוג שהוא, של תהליך פיתוח פרויקטי. מוצר יכול להיות, לפיכך, צעצוע, מכונית, מבנה, מפעל כימי או כור גרעיני. במאמר זה נשתמש לעתים גם במונח "מערכת" באותה משמעות.

מכלל: חלק של מוצר, המורכב מפריטים שונים ונועד לבצע תפקיד מוגדר בפעולת המוצר.

מחזור חיים של מוצר: האוסף המלא של שלבי הטיפול במוצר החל באפיון, בפיתוח ובייצור, המשך בקליטה, בהפעלה, בתחזוקה, בהובלה ובאחסון, וכלה בהוצאה מן השירות ובגריטה.

גריטה: תהליך הוצאה של מוצר מן השירות, לרבות פירוק וטיפול במרכיבים ובחומרים הנותרים בתום הפירוק (עצם ההתייחסות לתהליך הגריטה כמרכיב בפיתוח המוצר אינו עניין מובן מאליו. אבל, במקרים לא מעטים, התייחסות כזאת היא הכרחית למניעת סיכוני בטיחות כבדים).

אימות בטיחות (safety verification): הוכחה או הדגמה של עמידה **בדרישות** לבטיחות מוצר.

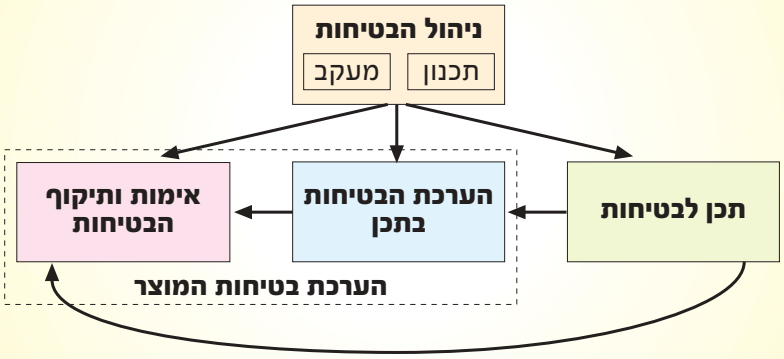
תיקוף בטיחות (safety validation): הוכחה או הדגמה של התאמת מוצר **לצורך** בהיבט הבטיחות, כלומר עמידתו באיומים העלולים להתממש במחזור החיים התקני שלו ובמצבי תאונה גם אם לא הוזכרו בדרישות, כדוגמת תרחישי שריפה, הצפה או שבירה. ל"תיקוף" יש משמעות רחבה יותר מאשר ל"אימות", והוא עשוי לכלול יסוד גדול יותר של שיפוט.

הערכת בטיחות המוצר (product safety assessment): תהליך שבו מפתח או מפעיל בוחן, מאמת, מתקף ומציג את העמידה בדרישות הבטיחות ובצרכים הבטיחותיים, במהלך התכן ולאחר השלמתו. תהליך זה מתועד ומסוכם ב"דוח בטיחות".

סינרגיה: צירוף של מרכיבים היוצר תפוקה שהיא גדולה מן הסכום הישיר של תפוקות המרכיבים הבודדים, כלומר לעצם הצירוף ביניהם יש תרומה נוספת משלו בנוסף לתרומת המרכיבים כשלעצמם.

סיכונים שיוריים (residual risks): סיכונים שנותרים בתום תהליך של הפחתת סיכונים, מכיוון שלא ניתן לבטלם או להפחיתם יותר.

איור 2: זיקה בין ערוצי הפעילות לבטיחות בפיתוח פרויקט



"בטיחות המוצר" - ערוצי הפעילות

המוצר שאותו מפתחים צריך לעמוד במכלול של דרישות, ובהן, כמובן, גם דרישות בטיחות. פעילות הבטיחות נערכת בתהליך הפיתוח, כדי להבטיח מענה מלא לדרישות אלה. ניתן לחלק את הפעילות הזאת לארבעה ערוצים: תכן, הערכה, אימות ותיקוף, וניהול. בכל אחד מן הערוצים מתקבלות במהלך הפיתוח תפוקות שונות (האבחנה והחלוקה הפורמליות בין הערוצים אינן חיוניות לגופו של עניין; במאמר זה נשתמש בהן ככלי להצגת מרכיבי הפעילות ולהסבר הזיקות בין המרכיבים האלה). העבודה בערוצים אלה נעשית, במרבית שלבי הפיתוח, במקביל, וקיימות ביניהם זיקות של העברת מידע ושל ניהול ובקרה (איור 2, למעלה):

א. תכן לבטיחות

הפעילות בערוץ זה מספקת את המענה לדרישות הבטיחות שהוצבו למוצר. מרכיביה העיקריים הם הכנת מיפרטים ומימושם. המענה עשוי להיות, לדוגמה, פיתוח מנגנונים ייעודיים לבטיחות (כגון: תמונה 1), יתירות של מנגנוני בטיחות (לדוגמה, התקנת מספר גלאי אש במקביל) ואף שונות בין המנגנונים היתירים (בדוגמה האחרונה - התקנת גלאי להבה, חום ועשן). פתרונות התכן לבטיחות צריכים להשתלב בתכן התפקודי ובתכן לאמינות. התכן לבטיחות הוא, כמובן, הערוץ העיקרי בפעילות הבטיחותית, אבל הוא בהחלט אינו היחיד.

ב. הערכת הבטיחות בתכן

מפתח המוצר זקוק להערכה על מידת העמידה של התכן בדרישות הבטיחות. הערכה זו נדרשת כאשר המוצר שבפיתוח נמצא, רובו ככולו, עדיין "על הנייר": אם היא מבוצעת מספיק מוקדם, היא עשויה לאתר פערים ולזהות איומים על הבטיחות במועד שבו תיקונם עדיין אפשרי, במאמץ קטן ובעלות נמוכה. הכלים העיקריים המשמשים להערכת הבטיחות של מוצר הנמצא בתהליך פיתוח הם ניתוחי בטיחות לסוגיהם השונים. כאשר מזוהים פערים בדרך זו - מידעים את אנשי התכן לגבי הפערים שהתגלו ונותנים להם פתרונות בערוץ ה"תכן לבטיחות", ובו ניתנים להם פתרונות.

תמונה 1: דוגמה למנגנון ייעודי לבטיחות - כסא-מפלט במטוס קרב

ג. אימות העמידה בדרישות הבטיחות ותיקוף הבטיחות

כאשר המוצר - או לפחות חלקים ממנו - כבר קיימים בפועל, יש להוכיח (או לפחות להדגים) כי הוא עונה לצורך, כלומר: עומד בדרישות הבטיחות ובאיומים נוספים המזוהים במהלך הפיתוח. האימות והתיקוף של הבטיחות נעשים בעיקר באמצעות כלים של ניתוח, סימולציה, בדיקה וניסוי.

הערה: המונח "הערכת בטיחות המוצר" משמש, בדרך כלל, כשם משולב לערוץ הערכת הבטיחות בתכן ולערוץ אימות ותיקוף הבטיחות בסיומו. ההפרדה בין השניים במאמר זה מסייעת באבחנה בין מועדי פעילויות ובהתאמתם לשלבי הפיתוח, כמובהר בהמשך.

ד. ניהול הבטיחות

בפרויקט רחב היקף, העשייה בתחום הבטיחות היא מארג מורכב של פעילויות רבות. תחילתן של פעילויות אלה - בזיהוי הצורך במוצר ובקביעת הדרישות ממנו, וסיומן - עם פירוקו בסוף השימוש בו או בתום "משך חייו". יש לתכנן פעילויות אלה כהלכה, לבצען במועדים המתאימים (לא מוקדם מדי וכמובן לא מאוחר מדי), לעקוב אחר מימוש הדרישות ואחר הביצוע, לתעד לקחים ו"סיכונים שיוריים" ולהציג את סטטוס הבטיחות במסגרת המעקב על התקדמות הפרויקט כולו. ערוץ ניהול הבטיחות עוסק בשילוב הנכון של פעילות התכן, ההערכה והאימות בתכנית הפרויקט, ובפרט בסקרי התכן ובניסויים.

בפרקים הבאים נציג עקרונות, גישות וכלים המשמשים לביצוע כל אחד מארבעת ערוצי הפעילות הנזכרים לעיל. נקדים לכך סקירה קצרה בעניין דרישות הבטיחות: חשיבותן הרבה של דרישות הבטיחות למוצר כשלעצמו היא מובנת מאליה, אבל הן חשובות לא פחות מכך להערכת הבטיחות של המוצר: לא די בכך שהמוצר **יהיה** בטוח, אלא יש גם **להראות** שהוא בטוח!

דרישות לבטיחות המוצר

ברמה הגבוהה ביותר של סדר העדיפות - דרישות הבטיחות מתקבלות או נגזרות מן התחיקה (חוקים ותקנות) ומן התקנים העוסקים במשפחת המוצרים המדוברת. בתחיקה העוסקת בתכנון מבנים, לדוגמה, מוקדש מקום רב לעניין הבטיחות. ברמה "מקומית" יותר, נוהלי הבטיחות במפעל הפיתוח עוסקים (כאשר מדובר במפעל רציני ואחראי) גם בבטיחות בתהליכי ייצור, הרכבה וניסויים, ופרויקט הפיתוח כפוף לנהלים אלה של המפעל, כשאר הגופים הפועלים בו. בנוסף לכך, כאשר יוזמת הפיתוח אינה של המפתח עצמו, דרישות לבטיחות המוצר מוצגות לעתים קרובות באורח מפורש ופורמלי גם על ידי הגורם המזמין. לעומת זאת, במקרים אחרים אין מוצבות בפני המפתח דרישות בטיחות מפורשות, וקביעתן נתונה לשיקול דעתו ולמידת האחריות המאפיינת אותו; כך, לדוגמה, בתחומים שבהם מפתח המוצר הוא גם היזם ("המזמין"), כדוגמת יצרני רכב המפתחים דגמי מכוניות חדשים, או יצרנים של צעצועים חדשים המופצים בשוק.

דרישות בטיחות עשויות להיות דטרמיניסטיות ("צריך שיהיה..." או הסתברותיות ("ההסתברות לכשל מסוג ... לא תעלה על ..."). הדרישות עשויות להיות פונקציונליות (כיצד צריך המוצר להגיב ל"אירוע מעורר" בטיחותי) או טכניות (מה צריך לתכנן במוצר כדי שיגיב כנדרש). ובנוסף, דרישות בטיחות עשויות להיות כלליות (לדוגמה: מהו מספר מנגנוני הבטיחות שנדרש על מנת למנוע כשל בטיחותי קטסטרופלי) או ייחודיות (לדוגמה: איך להפריד בין המוצרים באחסון).

משיקולים של שוק, תחרות, היצע וביקוש, וגם משיקולים ציבוריים ואתיים - רמת הבטיחות הנדרשת צריכה להיות תואמת למאפייני המוצר והמשתמש, לסיכונים הכרוכים בשימוש בו ולתועלת המופקת ממנו (לדוגמה: דרישות הבטיחות מצעצועי ילדים מחמירות בהרבה מדרישות הבטיחות מ"צעצועי מנהלים"). מימוש דרישות הבטיחות משליך על העלות, הנפח, המשקל, ההספק, המורכבות, האמינות והתפעוליות של המוצר. דרישות בטיחות יש לקבוע בחכמה: אין קל מלדרוש מן המוצר רמות בטיחות גבוהות מאד, עד כדי "בטיחות מוחלטת", אבל המחיר עלול להתגלות כגבוה, עד כדי אי הצדקת הפיתוח או עד כדי חוסר יכולת למתן פתרון תפעולי. אכן, ישנם מקרים שבהם מוצדק לבטל פיתוח אם המימוש האפשרי היחיד אינו בטוח דיו! לדוגמה: לדעת רבים אסור לעסוק בפיתוח בתחום "הנדסה גנטית" עקב הסיכונים הכרוכים בכך. דוגמה נוספת: פרויקטים של נחיתת אדם על הירח ועל פלנטות רחוקות אינם "ממריאים" בעשורים האחרונים עקב חוסר יכולת להבטיח את בטיחות האסטרונאוטים.

דרישת בטיחות צריכה להיקבע ולהיות מנוסחת כך שהעמידה בה תהיה ניתנת לאימות. מכאן, שבעת הכנת דרישות הבטיחות יש להפעיל לגבי כל דרישה "מבחן" של קיום מתכונת, או שיטה, שתאפשר לאמת את העמידה בה, ורצוי אף להזכיר מתכונת זו כהערה במסמך הדרישות. דרישת בטיחות שהעמידה בה אינה ניתנת לאימות צפויה לעורר אי הסכמות ומחלוקות, ולהקשות מאד על הליכי אישור המוצר וקבלתו.

ככלל, הדרישות לבטיחות המוצר נבדלות מדרישות לביצועי המוצר במספר מאפיינים:

- אי-האמינות התפעולית המותרת לרוב המוצרים הטכנולוגיים היא, בדרך כלל, ברמה של אחוזים או פרומילים בודדים; אמינות גבוהה יותר נדרשת רק ממערכות נדירות, והשגתה כרוכה בהשקעה רבה מאד של משאבים. בניגוד בולט לכך, סיכונים לחיי אדם הם "עולם של הסתברויות נמוכות" (אחד למיליון ואף למטה מזה): לא היינו מסכימים לחיות בעולם שבו השימוש בטכנולוגיה מטיל על המשתמשים סיכוני מוות ברמות של אחוזים, או אף פרומילים, לאדם לשנה. תכן לרמה גבוהה כזאת של אמינות בטיחותית צפוי להיות יקר בהרבה מתכן לרמה הנקובה לעיל של אמינות תפעולית.
- אנו "מתירים" למוצר להתקלקל כאשר תנאי הסביבה חורגים ממעטפת הביצועים שנקבעה באפיון שלו; אבל איננו מסכימים שבתנאים חריגים אלה יגרום המוצר לפגיעה באדם. במלים אחרות: מעטפת התנאים הנדרשת ל"אי פגיעה בטיחותית" היא נרחבת בהרבה מן המעטפת שבה על המוצר לפעול כהלכה. גם ההבדל הזה הוא תובעני בראיית המתכנן.
- דרישות בטיחות, להבדיל מדרישות אחרות, מתייחסות להשפעות החורגות מתחומי המוצר עצמו, הן במקום והן בזמן. כדוגמה, מפעל צריך להיות בטוח לא רק למפעיליו אלא גם לאוכלוסייה שבסביבתו הקרובה והרחוקה, לאטמוספירה, למקורות המים ולבעלי החיים אשר עלולים להיות מושפעים מפעילותו, וזאת לא רק במשך השימוש בו אלא גם זמן רב לאחר גריטתו (כגון, בהקשר של פסולת רדיואקטיבית מכורים גרעיניים ופסולת רעילה ממיתקנים כימיים).
- במשולש המקובל של הדרישות מן המוצר לביצועים, לעלות כספית וללוח זמנים, ניתן - ואף מקובל - לעשות פשרות לאור אילוצים שונים. בניגוד לכך, אנו הרבה פחות ותרנים כאשר מדובר בפשרות במאפיינים בטיחותיים של המוצר.

תכן לבטיחות

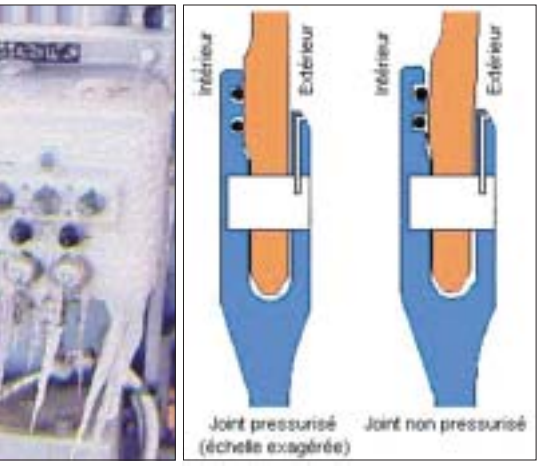
יעדו של התכן לבטיחות הוא הפחתת סיכונים. סיכונים ניתן להפחית בשתי מגמות: מגמה אחת היא הפחתת ההסתברות לתאונה, או השכיחות של תאונות ותקריות (בלשון הדיבור - "מניעת תאונות", אבל אי-אפשר, כמובן, למנוע תאונות לחלוטין). המגמה השניה היא הפחתת החומרה של תאונה, במקרה שתתרחש. את זאת ניתן להשיג באמצעות מניעת נזק במקרה שהסיכון אכן יתממש, או ע"י "מיתון" (mitigation) של הנזק, במקרים שבהם לא ניתן למנעו לחלוטין כאשר הסיכון מתממש.

באיור 1 הצגנו את רב-הממדיות של תהליך הפיתוח. בהתאמה, התכן לבטיחות צריך לעסוק גם הוא בהיבטים רבים ושונים של המוצר, שחלקם מובנים מאליהם וחלקם אינם בהכרח מובנים מאליהם. נושא שאיננו בגדר מובן מאליו הוא, לדוגמה, הוצאת המוצר מן השירות בתום מחזור החיים שלו: תהליכי הפירוק יכולים לכלול השמדה של חומרים מסוכנים (חומ"ס), אחסון חומ"ס שאינם מיועדים (בינתיים) להשמדה, אחסון חומ"ס שאינם ניתנים להשמדה (כדוגמת חומרים רדיואקטיביים), טיהור תשתית והכשרתה לשימושים עתידיים, ובמקרים קיצוניים - אף טיהור קרקע. ישנם מקרים שבהם היבטי הבטיחות של שלב זה במחזור החיים הם חמורים ממש, ונמצאים ברמה הגבוהה ביותר של הסיכונים הכרוכים בהפעלת המוצר.

בהתאמה לרב הממדיות של הפיתוח ושל התכן לבטיחות, גם הצוות העוסק בכך צריך להיות רב תחומי. במישור המושגי - "צוות תכן לבטיחות" מורכב ממנהלי הפרויקט, מאנשי תכן, מאנשי בטיחות ומנציגי המפעילים והמשתמשים. לכל אחד מאלה יש משימות הנובעות מסמכותו, מכישוריו או מניסיונו: מנהלי הפרויקט נושאים באחריות העליונה לעמידת המוצר בדרישות הבטיחות, מרכזים את תהליכי הניהול, הארגון וקבלת ההחלטות, מקצים משימות ועוקבים אחר ביצוען, אחראים לשילוב בין מרכיבי הצוות, ומאזנים בין דרישות הבטיחות לבין דרישות אחרות לתכן; אנשי התכן תורמים את הידע המקצועי הנדרש בנושאי הפיתוח, מכינים מיפרטים טכניים, ובעיקר - מספקים את פתרונות התכן לדרישות, מתכננים את הניסויים הנדרשים ומבצעים אותם; אנשי הבטיחות מרכזים את בקרת הסיכונים: מכינים את תכנית הבטיחות, מזהים את גורמי הסיכון ומפעילים שיטות ניתוח להערכת הבטיחות ולהפקת מסקנות והמלצות להפחתת סיכונים; נציגי המפעילים והמשתמשים תורמים מניסיונם התפעולי בהגדרת הצרכים, בהערכת הפתרונות התפעוליים ובהכנת נוהלי ההפעלה (איור 3, למטה). בשילוב יעיל בין מרכיבי הצוות ניתן להשיג השפעה סינרגטית משמעותית. התמונה בפועל שונה מן האבחנה העקרונית המתוארת לעיל, כי למעשה לא קיימת בפרויקט קבוצה של "אנשי בטיחות". החשיבה ברוח הבטיחות אינה נחלתה של קבוצה מסוימת, אלא צריכה להיות משותפת לכל העוסקים בפרויקט. כל אנשי הפרויקט הם רב תחומיים: המנהלים החלו את דרכם במקרים רבים כאנשי תכן, חלק מאנשי התכן שימשו בעבר כמפעילים, ואנשי הבטיחות החלו דרכם אם כמפעילים ואם כאנשי תכן. "מהנדס המערכת לבטיחות" בהנהלת הפרויקט (המינוח אינו אחיד ועשוי להיות שונה בארגונים שונים) הוא חבר בצוות הפיתוח ומשתלב בהכללת שיקולי הבטיחות בתכן, ויחד עם זאת מהווה גם חלק מצוות ניהול הפרויקט.

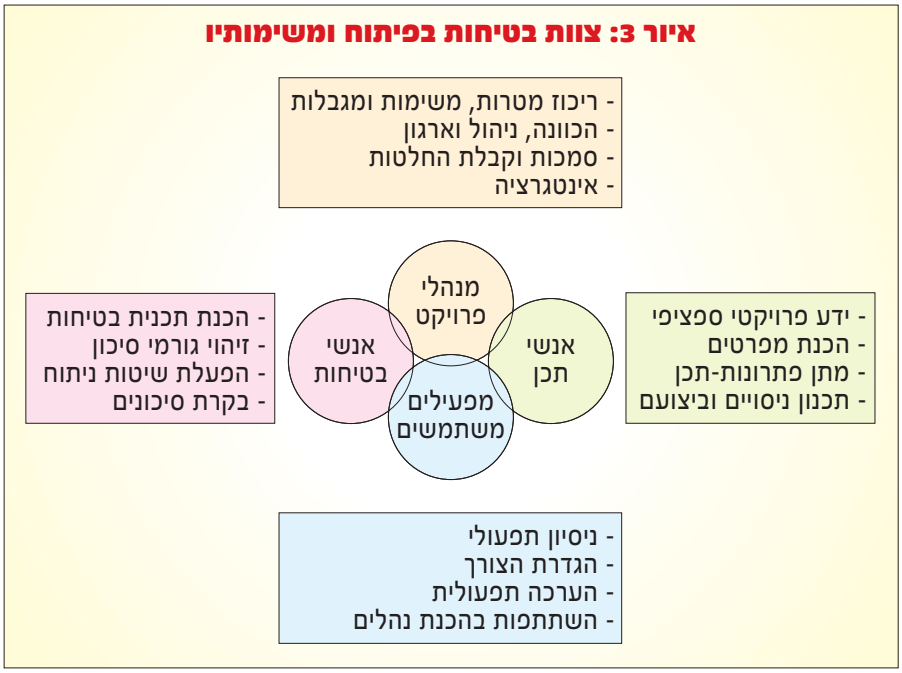
נזכיר כעת מספר עקרונות מקובלים בתכן לבטיחות. עקרונות אלה הם מוכרים וידועים, אבל ראוי לרעננם מעת לעת:

- **"תכן בטוח ביסודו"** - Inherently safe design - הוא תכן שהחשיבה הבטיחותית מוטמעת בו מלכתחילה. תכן כזה, לדוגמה, לא יאפשר הפעלה לא בטוחה או טעות. לפני זמן לא רב הזדעזע הציבור בישראל ממקרה של חיבור צינורית מזון לווריד של פגה בבית חולים; חייה של הפגה ניצלו רק בזכות טיפול מסור ואינטנסיבי. בתהליך המדובר ננקטו לא מעט מנגנונים למניעת טעויות: צבעים שונים לצינורות ההזנה והעירוי הווריידי, נוהל ביצוע מפורט הכולל חתימה על פתקית לאחר החיבור, ניסיון רב (12 שנים) של האחות המבצעת, וביקורת כפל ע"י אחות אחראית. התקיים כאן "רק" מנגנון כשל אחד: מַחְבֵּרים זהים לצינוריות ההזנה והעירוי. לאחר האירוע צוטטו תגובות נוגדות זו לזו באופן קיצוני של רופא בכיר במחלקה ("זו טעות איומה ונוראה... אי אפשר לטעות כך"), ושל אחיות העובדות בה ("זו טעות אנוש... תמיד חששנו מטעות כזאת"). אנשי התעשייה מכירים היטב את השגיאה הפוטנציאלית של חיבור שגוי של צנרת, והנהיגו מזה זמן רב פתרון שהוא "בטוח ביסודו": מַחְבֵּרים בעלי הברגות שונות לצנרת של גזים שונים. עם מחברים כאלה, הטעות היא פשוט בלתי אפשרית.
- **"תכן חסון"** - Robust design - הוא תכן העומד גם בתנאי תפעול החורגים במידה רבה מתנאי התפעול הנומינליים. תכן שאינו חסון במידה מספקת הוא שהביא בשעתו לאבדן מעבורת החלל "צ'לנג'ר" במהלך שיגורה, בשנת 1986 (תמונות 2 למעלה).
- **תכן בגישת "הגנה לעומק"** (או: "הגנה בשכבות") - Defense in depth - הוא תכן המשלב מספר שכבות הגנה שונות ובלתי תלויות. הצורך בכך מבוסס על ההנחה שאין שיכבת הגנה יחידה שהיא בטוחה לחלוטין. מקורה של גישה זו של תכן לבטיחות הוא בתעשייה הגרעינית, אבל כיום היא משמשת גם במספר רב של תחומים אחרים. דוגמאות ל"הגנה לעומק": התקנת מערכות לקירור בחירום בכור גרעיני, כגיבוי למערכת הקירור הראשית; הכנת גנרטור ומערך מצברים כגיבויים מקומיים למתח רשת החשמל; בניית מאצרות סביב מיכלי חומ"ס



תמונה 2: אסון המעבורת צ'לנג'ר - תוצאה של תכן לא חסון. מימין: טבעות-האטימה שנכשלו; באמצע: עדות לטמפרטורה הנמוכה בבוקר השיגור; משמאל: תוצאה

איור 3: צוות בטיחות בפיתוח ומשימותיו



בנוסף למערכות איטום בצנרת; הרחקת חומרים דליקים, הצבת ציוד לכיבוי אש ולבישת ביגוד חסין אש בתהליכי עבודה מסוימים.

● **תכן לבטיחות בהפעלה** מביא בחשבון את יכולותיו ואת חולשותיו של המשתמש במוצר: הוא כולל, לדוגמה, התייחסות למימשק אדם-מכונה בתצוגות ובחיווים, תכנון מערכות בקרה ברורות ו"ידידותיות", ואמצעי הפעלה המוגנים מפני "טעויות אצבע". בנוסף לתרומתו לבטיחות, תכן כזה מונע הפעלה בדרך המנוגדת לכוונת המפתח, ובכך הוא תורם לשימושיות (usability) של המוצר. ראוי להזכיר כאן כי המפעיל חייב להכיר היטב את המוצר, את יכולותיו ומגבלותיו ואת אופן הפעלתו ותחזוקתו, וחובה על המפתח לתת בידי המפעיל את כל המידע והכלים הנדרשים לצורך היכרות זו.

● **תכן ל"בטיחות בכשל"** - Fail-safe design - הוא תכן המביא לכך שאם מערכת נכשלת כאשר היתה במצב בטוח - היא תישאר במצב זה, ואם היא נכשלת כאשר היתה במצב מסוכן - היא תעבור אוטומטית, כתוצאה ישירה מן הכשל, למצב בטוח. הדוגמה הנפוצה ביותר לרכיב הגורם למערכת להיות "fail-safe" היא הנתיך החשמלי. דוגמאות אחרות: ברזים אלקטרומגנטיים (במצב 'normally open' או 'normally closed', כתלות בלוגיקה של חיבורם במערכת), ומוטות הבטיחות בכור גרעיני (התלויים על אלקטרומגנט, ונפילתם בכוח הגרוויטציה במקרה של נפילת מתח מפסיקה את פעולת הכור). במקרים מסוימים ניתן אף להשיג בטיחות בכשל בעזרת חשיבה נכונה בלבד, ללא צורך בהוספת מנגנונים מיוחדים. דוגמה אופיינית: במערכות בקרה שבהן קצר יגרום לאירוע בטיחותי - ניתן לבחור סוג נגדים שאופן הכשל האופייני שלהם הוא נתק ולא קצר.

● **תכן למחזור החיים המלא** הוא תכן המביא בחשבון את כל שלבי "מחזור החיים" של המוצר ולא רק את שלב ההפעלה שלו. התכן צריך לתת את הדעת במיוחד למצבים שבהם המערכת הקיימת בפועל שונה מזו שבתפעול השוטף, לעתים תוך הוספת סיכונים חדשים. דוגמה טיפוסית: מערכת הנמצאת בניסוי שבו הוספו לה מרכיבים חדשים שטרם נוסו בעבר. דוגמה נוספת: בדיקות תחזוקה שבמהלכן חייבים לנטרל או לעקוף חלק מאמצעי הבטיחות כדי לאפשר את הבדיקות.

● **תכן לתחזוקה** הוא תכן שבו משולבים שיקולי תחזוקה בתכנון המוצר למשך כל מחזור חייו, במטרה למנוע הידרדרות ברמת הבטיחות בעת פעילות תחזוקה. הידרדרות כזאת אירעה, לדוגמה, במפעל "יוניון קארבייד" בבופאל שבהודו, שבו נמשכה פעילות הייצור גם כאשר מערכות בטיחות הושבתו לצורך תחזוקתן; כתוצאה מכך התרחש אחד האסונות הכבדים בהיסטוריה של התעשייה הכימית.

● במקביל קיימת גם גישה של **תכן לבדיקתיות**: זהו תכן הכולל תהליכי בדיקה אופטימליים של המוצר במחזור חייו המלא, ואמצעי בדיקה התואמים תהליכים אלה. לדוגמה, כאשר נעשה שימוש בשני מפסקים לצורך יתירות (מחוברים בטור או במקביל, תלוי במבנה המערכת), יש הבדל מהותי אם בביקורות התקופתיות נבדקת התקינות הפונקציונאלית של המכלל בלבד, או שנבדקת התקינות של כל מפסק בנפרד. במקרה הראשון יתכן שאחד המפסקים תקוע במצב לא בטוח מזה זמן רב, היתירות קיימת רק "על הנייר" והבדיקות אינן מגלות זאת, לעומת זאת במקרה השני (שמידת הסיבוך בביצועו תלויה בחשיבה שהוקדשה לכך בתכן) נגלה תקלה בכל מפסק בנפרד ולא רק בתפקוד המכלל, ולכן נבחן ונוודא את קיומה של יתירות של ממש. דוגמה נוספת: התכן המביא להידלקות רגעית של נוריות התרעה במכונית בעת התנעתה, כבדיקה יומית לתקינותן.

מעבר לרמת העיקרון, קיימות מספר גישות יישומיות לתכן לבטיחות:

א. החלפה של גורם סיכון במרכיב שאינו מסוכן: לדוגמה, ההחלפה (שנערכה לפני כ-30 שנה) של גז המימן בבלונים מטאורולוגיים בגז הליום. ההליום יקר יותר וביצועיו פחותים מאלה של המימן, אבל הוא אינו דליק. אילו היתה החלפה זו מבוצעת ב"ספינות האוויר הצפידות" (ה"צפלינים") בשנות השלושים של המאה העשרים, לא היתה מתרחשת התאונה המפורסמת של ספינת האוויר "הינדנבורג" בשנת 1937, והשימוש בטכנולוגיה זו לצרכי תחבורה אולי לא היה נפסק באחת. לעתים מיושמת גישה זו בדרך של החלפת גורם סיכון מסוכן בגורם סיכון מסוכן פחות (תמונה 3, למטה).

תמונה 3: תכן לבטיחות בגישת החלפה - מעבר מגלשני רוח למצנחי רחיפה

ב. הפחתה של כמות גורם הסיכון או של הנזק הפוטנציאלי שלו: לדוגמה, ייצור חומרים כימיים מסוכנים בתהליך של זרימה (שבו נמצאת במערכת בכל רגע כמות קטנה מאד של החומר המסוכן) במקום בתהליך מנתי (שבו נמצאת בתוך ריאקטור כמות גדולה של החומר המסוכן), או הגבלת הכמות של חומרי גלם מסוכנים בנקודת העבודה לכמות הנדרשת למשמרת או ליום העבודה בלבד.

ג. הרחקה של עובדים, ובמקרים מסוכנים במיוחד - אף של המפעיל, ממוקד הפעילות. דוגמאות: הפעלת מיתקנים כימיים וכורים גרעיניים מחדר בקרה מרוחק, והטסת כלי טייס בלתי מאוישים (כטב"מים). ברוח דומה - הרחקה מאזור העבודה, או אף מחצר המפעל, של חומרים מסוכנים שאינם נחוצים מיידית לייצור או לתפעול.

ד. הפרדה בין פעילויות שונות או בין אזורים שונים, למניעת אפשרות של התנגשות מסוכנת או התפשטות של אירוע תאונתי. דוגמאות: הפרדה מיפלסית בין כביש לבין מסילת ברזל, בניית מחלף במקום צומת מרומזר, הפרדה בין אזורים במבנה גדול באמצעות "דלתות-אש".

ה. התניה של קיום פעולה מסוכנת בקיום תנאי בטיחות. דוגמאות: התניית פעולה של מקרן לייזר בסגירת דלת המעבדה, התניית קיום מתח גבוה בסגירת המכסה של מיתקן שבו קיים המתח, התניית הפעלתה של מכונת כביסה בסגירת דלת המכונה והתניית הפיצוץ של ראש קרבי של טיל בהתרחקות מן המטוס המשגר או מאתר השיגור המאויש.

ו. מניעה של מצבים מסוכנים שאינם חיוניים. לדוגמה, הפעלת מכבש בעזרת שתי ידיות מרוחקות זו מזו, כדי למנוע מצב שבו המפעיל משתמש ביד אחת כדי להפעיל את המכבש וביד השניה כדי "לסדר" את מיקום החומר באזור התנועה המסוכן של המיתקן.

ז. הגנה מפני סיכונים במקרים שבהם לא ניתן ליישם את גישות ההחלפה, ההפחתה, ההרחקה, ההפרדה, ההתניה והמניעה. לדוגמה: תכנון אטימות, מאצרות, ריפודים, ציוד מגן אישי לעובדים וכו'.

עד כאן - באשר לערוץ התכן לבטיחות. בחלק הבא של המאמר נציג את שלושת הערוצים האחרים של הפעילות לבטיחות בפיתוח פרויקט ונסכם במספר הערות כלליות. ■