# ניתוח סיכונים הסתברותי

**מאת ד"ר**

ניתוח סיכונים הסתברותי (ניס"ה) מטפל, בעיקר, באופן שבו מוטמעת הבטיחות בתכנון מוצרים להבטחת פעולה נכונה ובטוחה. הכרת הנושא, הכולל מספר עקרונות שעליהם מושתתת הבטיחות, משמעותית גם לעבודה היומיומית של ממונה הבטיחות - כאשר נדרשים ניתוחי בטיחות של מערכות וקווי ייצור

בתוכנית ימי העיון לממוני בטיחות של המוסד לבטיחות ולגיהות נכלל (החל משנת 2002) יום עיון בנושא "ניתוח סיכונים הסתברותי" (ניס"ה). ניס"ה הוא נושא חריג במקצת במכלול תוכנית ההשתלמות. עיקר עיסוקם של ממוני הבטיחות בעבודה הוא הדאגה לתפעול נכון של מערכות, כדי למנוע חריגות ממצב בטוח שתגרומנה לפגיעה בעובדים ובסביבה. ניס"ה מטפל בעיקר באופן שבו מוטמעת הבטיחות בתכנון הראשוני (תֶכֶן) של מערכות הנדסיות, בשלבי הפיתוח.

**הכותב הוא מהנדס בטיחות בחברת 'רפא"ל'**

**תודה לידידי: ד"ר מיכאל מהר"יק, מר ישי לבנון ובעיקר – מר ראובן גרינברג, אשר הערותיהם תרמו רבות לשיפור תוכנו של המאמר**

**1. כתבה בעתון הארץ, 26.4.03**

**2. ההליך הנכון היה כיבוי הכור. על פי הוראה ממוסקבה המשיכו להפעילו, כדי לחסוך את תהליך ההפעלה מחדש, הנמשך 24 שעות.**

**3. ישנם המייחסים את ליקויי התֶכֶן, עקיפת אמצעי הבטיחות ואת הנוהג הכללי שאיפשר למפעילים לשנות את הוראות הבטיחות הכתובות – עפ"י שיקול דעתם, תוך כדי התהליך – ל"תרבות בטיחות לקויה" כללית, כפי שהיה נהוג בתחנה בצ'רנוביל וכנראה גם בתחנות כוח גרעיניות אחרות בבריה"מ.**

**4. קיימות הערכות שונות: ההערכה הרשמית היא של 3800 הרוגים ו–11,000 נכים; עפ"י הערכה אחרת: 10,000 הרוגים ו–15,000 פצועים; הערכת 'Greenpeace', מ–1999, מדברת על 16,000 הרוגים וכחצי מיליון פצועים**

לכאורה, הנושא מעסיק בעיקר את מי שעוסק בפיתוח של מערכות חדשות ואין לו שימוש רב בתפעול שוטף של מערכות קיימות. אך, כפי שיתברר בהמשך, להכרת הנושא יש תרומה משמעותית בעבודתו היומיומית של ממונה הבטיחות, מכיוון שהוא כולל מספר עקרונות שעליהם מושתתת הבטיחות. ידיעת העקרונות מאפשרת לממונה הבטיחות לראות בעין בוחנת, ומזווית חדשה, מערכות שאת אופן פעולתן הוא מכיר משכבר.

המאמר עוסק ב–3 נושאים עיקריים הכלולים ביום העיון:

- כשלים בבטיחות שאירעו במערכות שונות והגורמים להם;
- מרכיבים חיוניים של תֶכֶן לבטיחות;
- שיטות לניתוח בטיחות של מערכות הנדסיות מורכבות.

## כשלים בבטיחות וגורמיהם

התעשייה המודרנית לא הצליחה, למרות המאמצים שהושקעו, למנוע כשלים בבטיחות בעבודה (תאונות, mishaps, accidents). יתירה מזאת: חומרתן של התאונות המדווחות גדלה בד בבד עם התפתחות התעשייה. לכאורה, סביר להניח שטכנולוגיות חדישות תאפשרנה אימוץ שיטות הגנה יעילות בפני תאונות. אך יישום הטכנולוגיות הללו – המאפשרות פיתוח מוצרים ותהליכים חדשים – מלווה בסיכון מובנה גדול יותר ומורכבות גדולה של המערכות המפותחות, בעוד שהניסיון שנצבר, עד כה, בשימוש בהן – עדיין איננו מספיק.

המצב המאפיין הרבה מאוד תאונות חמורות הוא שלא ניתן ליחס אותן לגורם יחיד, אלא לשילוב של גורמים – שחלקם מעוגן בתֶכֶן וחלקם בתפעול ובתחזוקה לא נכונים.

### אסון צ'רנוביל

התפוצצות הכור הגרעיני בצ'רנוביל (אוקראינה) היתה התאונה החמורה ביותר אי–פעם בתעשייה הגרעינית. ב–26.4.86 התרחש בכור פיצוץ כימי ובעקבותיו שריפת גרפיט, שגרמו לפיזור כמות גדולה של חומרים רדיואקטיביים ברדיוס שחרג מגבולות המדינה. מספר הנפגעים הכולל לא ידוע בבירור. אמנם, רשמית נמסר על 31 הרוגים – מיידית, ובמהלך הטיהור. דו"ח UNSCEAR (ועדה מדעית של האו"ם) משנת 2001, מדבר על כ–600,000 עובדים שנחשפו לרמות קרינה גבוהות, ואשר רובם הועסקו בסילוק אדמה מזוהמת, שטיפת כבישים וכו'; ועל האוכלוסיה באזור שנחשפה לרמות קרינה נמוכות יותר. דיווחים לגבי השפעות על הבריאות מתייחסים לכ–18,000 ילדים שלקו בסרטן בלוטת התריס.

הערכות אחרות, מוסמכות פחות[1], מדברות על כ–15,000–30,000 הרוגים עד היום.

חומרת התוצאות מיוחסת שם לגורמים שונים, בכללם גורמים חברתיים וכאלה הנוגעים למצב הפוליטי בבריה"מ, לאופי המישטר, לחלוקת סמכויות בין משרדים שונים, לחוסר יעילותם של פקידי המימשל וכו'. אנו נתייחס לצדדים הטכניים בלבד.

התעמולה הסובייטית הגדירה את תעשיית הגרעין כ–"נקייה מתאונות". לכן לא סופקו לעובדים אמצעי מיגון מספקים. החקירה שנערכה בעקבות התאונה העלתה גם כי תכנון היבטי הבטיחות של התחנה היה לקוי.

התאונה התרחשה במהלך ניסוי שנועד (כמה אירוני) לבחינת נושאי בטיחות: נבחנה אפשרות להשתמש בגנרטור הראשי להספקת מתח במשך כ–2 דקות לאחר הפסקת חשמל (החשמל נחוץ להפעלת משאבות הקירור בשעת חירום), עד להכנסתם לפעולה מלאה של גנרטורים מונעים בדיזל. כדי לבצע את הבדיקה הנדרשת עברו המפעילים מספר עבירות בטיחות, ביניהן: הפעלת הכור בהספק נמוך תוך כדי הניסוי[2], ניטרול מנגנוני בטיחות (כגון מערכת קירור החירום) והפעלת משאבות קירור נוספות, שגרמו לירידת רמת המים במפריד הקיטור.

פרט לעבירות הבטיחות הללו, ניתן לייחס לתֶכֶן הלקוי של תחנת הכוח[3] תרומה מרכזית לעצם האירוע ולחומרתו.

**הליקוי המרכזי:** המערכת לא היתה מתוכננת כ–fail-safe, כלומר: להיכשל באופן שאיננו גורם לסיכון בטיחותי. במרבית הכורים המודרניים (הכורים המערביים וכן כורים רוסיים מודרניים יותר) הקירור והאטת הנויטרונים נעשים ע"י מים. בכורים מטיפוס הכור בצ'רנוביל המים משמשים רק לקירור, ואילו האטת הנויטרונים נעשית באמצעות גרפיט. לפיכך, בכורים המודרניים גורם חימום המים, עד לרתיחה, להפסקת פעולת הכור (בגלל הפגיעה בתכונת האטת הנויטרונים), מה שלא יתרחש בכורים שבהם נעשה שימוש בגרפיט.

# ככלי עזר לממוני הבטיחות

**שמשון ארואטי**

הכור התחמם עקב התאונה והמצב בתחנה הוחמר עקב עלייה פתאומית ברמת הקריטיות הגרעינית. נגרם נזק פיזי למוטות הדלק – חדירת מים לתוכם גרמה לתגובה כימית ובסופו של דבר לפריצת קיטור ואחריה – לפיצוץ כימי, לשריפת גרפיט, ולפיזור כמות גדולה מאוד של חומר רדיואקטיבי.

**ליקויי תֶכֶן נוספים:** מערכת הבקרה ואמצעי הבטיחות היו משותפים ל-4 היחידות בתחנה. במאמצים שנעשו כדי למנוע את התפשטות האש לעבר היחידות הנוספות באתר קופחו חיים רבים.

**ליקויי תפעול:** הניסוי נערך בשעות הלילה. הצוות לא כלל את המפעילים המומחים ביותר.

בשנת 1981 התרחשה תאונה בתחנת הכוח האמריקאית ב-'Three Mile Island' (TMI). גם כאן גרמה שורה של טעויות אנוש לפגיעה ביכולת הקירור ולפגיעה בשלימותם הפיזית של מוטות הדלק. אך תכן שונה לחלוטין, הכולל "הגנה לעומק" ו-"fail safe", מנע את התפשטות האירוע אל מחוץ לתחנה. כמו כן, לא היו פגיעות בנפש (אם כי נרשמה פליטת כמות מסוימת של חומרים רדיואקטיביים לאטמוספירה).

## בוהפל (Bhopal)

תאונה חמורה נוספת התרחשה בשנת 1984 במפעל 'Union Carbide' בעיר בוהפל שבהודו. התאונה גרמה לחשיפתם של מאות אלפי בני אדם לחומרים כימיים מסוכנים. אין מידע מדויק לגבי מספר הנפגעים, אך על פי ההערכות שונות – אלפים מתו עד כה[4] ומאות אלפים חלו. רבים מתים מהשפעות התאונה עד היום.

התאונה נגרמה עקב כשל בשסתום. הכשל גרם לזרימת מים אל תוך מיכל שהכיל 40 טונות של חומרים כימיים, המהווים תוצר ביניים בתהליכי הייצור של 'סֶוויִן' (Sevin – קוטל חרקים). התגובה הכימית היתה בלתי נשלטת והובילה לפליטת גזים רעילים לסביבה.

חומרת התוצאה נובעת משילוב של גורמים שונים:

**ליקויי תכן:** פליטת גזים במפעלים דומים במערב (בכללם מפעלי 'Union Carbide' בארה"ב) חייבת להגיע לתוך "מיכל איסוף" וממנו להתקן-להבה (flare), שבו החומרים בוערים ומתכלים. כמו כן, נהוג להתקין התקני להבה בכמות גדולה מהנדרש לשימוש השוטף ("יתירות" של התקני-להבה).

במפעל ההודי לא היה מיכל איסוף, אך אפקט דומה היה אמור להתקבל ע"י חיבור מספר מיכלים, והשארת נפח התפשטות ריק בכל מיכל. יכולת זו לא מומשה כיוון שהברזים בין המיכלים הושארו סגורים. בנוסף, עוד לפני מועד התאונה הוצאו משימוש לצורך שיפוץ ה-flare היחיד והמסנן (scrubber) היחיד (שתפוקתו ממילא לא היתה מספיקה בתאונה בסדר גודל שכזה).

**ליקויי תחזוקה ותפעול:** רמת התחזוקה במפעל ורמת ההדרכה של העובדים היו נמוכות מאלה המקובלת במפעלי 'Union Carbide' בארה"ב. רמה זו הידרדרה בשנים האחרונות לפני התאונה בגלל קשיים תקציביים. גם המשך ההפעלה למרות השבתת התקן הלהבה, הוא ליקוי תפעולי חמור.

**קירבת המפעל לריכוזי אוכלוסייה:** רבים מתושבי בוהפל התיישבו במקום בעקבות הקמת המפעל.

## התרסקות המעבורת 'צ'לנג'ר'

תאונת החלל המפורסמת ביותר (עד לאבידה האחרונה של המעבורת 'קולומביה') היתה התרסקות ה'צ'לנג'ר' ('Challenger') בשנת 1986. כמו תאונות חמורות אחרות – גם זאת התרחשה כתוצאה משילוב גורמים שהובילו לכשל הבטיחותי. הגורמים הטכניים העיקריים היו:

- תכן **"לא רוּבָסטי"** – תכן שאיננו מביא בחשבון תנאי תפעול קיצוניים ולכן מאפשר הגעה למצבי כשל בתנאים כאלה.

**מאפייני התכן:** קירבה פיזית בין מנועי ההאצה (הבוסטֶרים) שהם טילים המונעים בדלק מוצק, לבין המיכל העיקרי המכיל חמצן ומימן להנעת המנוע הראשי. הבוסטרים בנויים ממיקטעים, שאזור החיבור ביניהם מוגן מפני דליפת גזים חמים באמצעות אטם, מסוג שהיה רגיש במיוחד לטמפרטורה נמוכה.

- החלטה שגויה (למרות ההנחיות הטכניות) לשגר את המעבורת בתנאי מזג אוויר לא תקניים. הטמפרטורה הנמוכה גרמה להתקשות האטם ולפליטת גזים חמים מתוך אחד הבוסטרים, אשר גרמו לפיצוץ מיכל הדלק.

גם בתאונה הזאת לא קשה להתחקות אחרי סיבות-על פוליטיות וניהוליות, אשר הביאו לשגיאות הטכניות ולתאונה.

## תאונות אוויריות שנבעו מכשלי תכן מכשלי תוכנה ומטעויות אנוש (דוגמאות)

■ טיל 'Ariane 5' צרפתי התרסק (ב-4.6.96) 37 שניות לאחר המראתו. הסיבה: כשל תוכנה. המתכננים אימצו את תוכנת הבקרה של הגירסה הקודמת, 'Ariane 4', מבלי לבדוק ביסודיות, לאור תנאי התפעול השונים, שהדבר אומנם אפשרי. במקרה זה – לטיל 'Ariane 5' יש מאפייני מסלול שונים מאלה של 'Ariane 4'. שינוי זה גרם לאחד הפרמטרים של מעוף הטיל להציג נתוני שגיאה ולהוציא את אחד ממרכיבי מערכת הבקרה מכלל פעולה. כתוצאה מכך הפכה טיסת הטיל לבלתי יציבה וגרמה להתפרקותו.

■ בין השנים 1988-1997 התרסקו במהלך ניסיונות נחיתה 4 מטוסי 'Airbus A-300', 'Airbus A-320' ומטוס 'A-330' (שהיה בניסוי טיסה). מקורות שונים העלו השערות שלפיהן מקור התקלות הוא בתכן המערכת האוטומטית של המטוס. מערכת זו מאופיינת בתחכום רב, המאפשר נוחות בהטסה וחיפוי על מרבית השגיאות האפשריות של הצוות.

מחקירות התאונות הללו עולה שהגורם העיקרי, ברובן, היה שגיאות של צוות המטוס. בכל המקרים היו גם גורמים תורמים נוספים, אשר חלקם קשור לתיחכום הרב של מערכות המטוס. בין השאר מדובר בהדרכה לא מספקת של הטייסים, שבעטיה לא זוהו נכון מאפייני הטיסה (mode) שאליו נקלעו; הבנה לא מספיקה של אופן תגובת הטייס האוטומטי למצבים קיצוניים; ולפחות באחד המקרים – בטחון מופרז בפעולת המיכשור האוטומטי, שהוביל את הצוות לביצוע תימרונים במצבים קיצוניים של המערכת.

■ שני מטוסי 'Boeing 737', הנחשבים כבטוחים מאוד, התרסקו בשנים 1991 ו-1994 מסיבה דומה, הקשורה לתזכזן המטוס: מערכת הבקרה ההידראולית (PCU) של ההגאים הותקנה באזור לא מחומם. ההפרש בין טמפרטורת האוויר הנמוכה שבחוץ, לשמן החם שזרם אל תוך המערכת ההידראולית, גרם להיתקעות של חלקים נעים בתוך הבקר, ולתנועות הגה בלתי מבוקרות – אשר גרמו להתרסקויות.

## תאונות שנבעו מפיגור בפיתוח מערכות בטיחות

אירועי בטיחות רבים הם תוצאה מהתפתחות טכנולוגית מואצת, שאין בעקבותיה התפתחות מקבילה של אמצעי בטיחות. לדוגמה:

### ספינה מהירה במסע הרס

בתאונה בספינה מהירה מסוג: Catamaran, שהתרחשה בהונג-קונג (ב-1991) נהרגו 4 בני אדם. התפוסה בספינה היתה גדולה במיוחד - באותה עת החלו בתכנון תפוסות גדולות יותר לספינות מסוג זה, ודובר על תכן לתפוסה של 1400 נוסעים ו-200 כלי רכב. הטכנולוגיה של הספינות החדשות התבססה, במידה רבה, על זו של תעשיית התעופה, בעיקר בכל מה שקשור למערכות הבקרה. הספינה התנגשה במספר ספינות אחרות, לאחר שהשליטה על מערכות ההיגוי וההינע שלה אבדו בו זמנית, גרמה למותם של 4 אנשים ונעצרה על החוף.

חקירת התאונה העלתה שסיבת האירוע היתה כשל יחיד של מפסק (24 וולט) על לוח הבקרה, אשר דרכו עברו 6 מקורות מתח שונים. המתח הזה (24 וולט) חיוני לשליטה על ההיגוי והבקרה של הספינה, ובלעדיו - אין שליטה. החקירה מיחסת חלק מהאשמה לניסיון לאמץ מערכות בקרה משוכללות, כמו במטוסים, מבלי להתחשב בכך שבמערכות אלה אין בטיחות מובנית, באופן מלא, כמקובל במערכות ימיות מסורתיות.

### חומרים כימיים ללא איפיון רעילות

מיפגע בטיחות מסוג אחר תואר במאמר בכתב העת 'Scientific American' (יולי 1995). במאמר נטען כי מאז התאונה בבוהפל גדל, בהתמדה, מספר התאונות במפעלים כימיים שבהן התפזרו חומרים מסוכנים. הגידול התבטא הן בכמות החומרים והן ברעילותם. המאמר מצביע על בעיה מרכזית: לא מושקעים משאבים רציניים ברישום טוקסיקולוגי מפורט לחומרים כימיים שאינם מיועדים למאכל. כתוצאה מההזנחה הזאת - רק לחלק קטן מאוד מ-70.000 חומרי ביניים המשמשים בתעשייה הכימית יש רישום טוקסיקולוגי מסודר. בעבר אמנם נעשה ניסיון ליצור בסיס מידע שלם יותר, אך הוא נכשל בגלל מימדיה של המשימה. כך - עובדי המפעלים הכימיים משמשים, לעתים, כ"עכברי מעבדה" לגבי השפעותיהם של חומרים שתכונותיהם אינן ידועות.

## אמצעים למניעת כשלי בטיחות

קיימות כמובן, עשרות רבות של דוגמאות נוספות על לקחיהן, אך ריכוז מקיף של כל התאונות החמורות במאמר יחיד הוא משימה בלתי אפשרית. מה שניתן, בכל זאת, לעשות הוא לציין מספר גורמים מרכזיים, אשר הטיפול בהם יפחית את הסיכוי להתרחשות תאונות כאלה, ועשוי להפחית את חומרת התוצאה - אם תתרחשנה, למרות זאת.

רשימת האמצעים שלהלן מתייחסת לגורמים טכניים בלבד. ניתן, כמובן, ליחס חלק גדול מהאירועים ומחומרתם לסיבות-על, כגון: סיבות ניהוליות (אופן הניהול והפיקוח); סיבות חברתיות ופוליטיות (התארגנות השלטונות והציבור להתמודדות עם תאונות); סיבות כלכליות (מידת ההשקעה באמצעי בטיחות ובניתוח הבטיחות) ואחרות.

> ככל שהמערכת מורכבת ומתקדמת יותר - לתחזוקה יש תפקיד מרכזי יותר בשמירה על רמת הבטיחות

אמצעים רבים מבין אלה הכלולים ברשימה צריכים להיות חלק מתכן המערכת. אמצעים אחרים מתייחסים לתפעול ולתחזוקה נכונים של מערכת קיימת. מובן שהרשימה שלפניכם איננה מלאה.

**הגנה לעומק:** שילוב של שכבות הגנה שונות, בצורת מנגנונים מונעי תאונה ומערכות המפחיתות נזקי תאונות. לדוגמה: אמצעים לקירור במקרי חירום; אספקת חשמל ממקורות יתירים (אשר מסוגלים לספק יותר מהנדרש); מבנים/ מיתקנים אטומים ומאצרות - לכליאת שפך של חומרים מסוכנים; מערכות כיבוי אש; תכן "מוגן פיצוץ" וכו';

**תכן הכולל תכונות של בטיחות מובנית (inherently safe) ו-מוגנת כשלי בטיחות (fail safe):** מערכות שבהן נכללות תכונות בטיחות כאלה הן מערכות רגישות מהיבט הבטיחות ומתוכננות כך שכאשר מתרחש כשל - תוצאותיו תהיינה מתונות, והוא לא יוביל לפגיעה בבטיחות. לדוגמה: הכשל יגרום לכיבוי המערכת אך ימנע את "בריחת" התהליך, כלומר: יציאתו ממהלך מתוכנן עד כדי אבדן שליטה, ו/או דליפה/פליטה של תוצרי התהליך;

**יתירות ושונות:** ריבוי מנגנוני הגנה בטיחותיים שונים במערכת, והקפדה על אי-תלות בין המנגנונים - כך שגורם כשל יחיד לא יוציא יותר ממנגנון אחד מכלל פעולה (דוגמאות לתלות בין מנגנונים יכולות להיות הכשל בספינת ה-Catamaran והתרסקויות מטוסי ה-Airbus שתוארו לעיל);

**תכן רובסטי:** תכנון המביא בחשבון תנאי תפעול קיצוניים, כך שגם בתנאים כאלה המערכת לא תגיע למצבים המסכנים את הבטיחות;

**שמירה על רמת תחזוקה נאותה:** ככל שהמערכת מורכבת ומתקדמת יותר - לתחזוקה יש תפקיד מרכזי יותר בשמירה על רמת הבטיחות;

**הדרכת עובדים:** גם כאן החיוניות גדלה עם הגידול במורכבות המערכת. חיוני שכל עובד יכיר גם מערכות שיש להן נגיעה עקיפה בלבד לתהליכים שעליהם הוא אחראי;

**לימוד לקחי עבר ומעקב אחרי שינויים:** קיום בסיס נתונים על תקלות בעבר הוא מידע חיוני. לא פחות חשובה היא ההתייחסות להיבטי הבטיחות של שינויים הנעשים במערכת - מכיוון שעלול להתקיים מצב שבו נעשים שיפורים, אשר חלקם מכוון להגברת רמת הבטיחות, אך הם יכולים להוביל, מתוך חוסר תשומת לב, לתקלות במקומות אחרים. לפיכך, נדרש ניתוח רציני - לעומק ולרוחב - של כל שינוי המתבצע במערכת.

## שיטות ניתוח

ניתוח בטיחות של מערכת הוא כלי אופייני לשלבי התכן. עם זאת, ישנם מצבים שונים גם במהלך תקופת פעילותה של מערכת שבהם יש צורך בניתוחי בטיחות. להלן, מצבים אופייניים המחייבים ניתוח בטיחות:

- שלבים שונים של תכן ופיתוח מערכת חדשה;
- לקראת/במהלך שינויים הנעשים במערכת קיימת: שינויים מבניים, שינויים באופן התפעול, הוספה או שינוי של אמצעי בטיחות, הוספת מערכת בקרה חדשה וכו';
- לקראת שינוי תהליכים או הכנסת תהליכים חדשים במערכת קיימת;
- לקראת הפעלה מחדש של מערכת, לאחר השבתה ארוכה לצורכי שיפוץ או תחזוקה יסודית (לדוגמה: החלפת צנרת ושסתומים);
- לקראת הוצאת המערכת משירות (decommissioning) - לזיהוי סיכונים ומניעתם בעת הפירוק, וסיכונים שיוריים לסביבה - לאחר סילוק המיתקן מהמקום;
- לקראת ניסוי. במקרה כזה חשוב במיוחד לבחון את המערכת - לאור ההבדלים האפשריים בין תצורת הניסוי לתצורת התפעול השוטף, וגם לאור העובדה שמתוכננת הפעלה של מערכת אשר לא עברה עדיין את הניסויים, אשר אמורים לקבוע את אמינותה ואת בטיחות פעולתה.

קיים מיגוון רחב של שיטות, שהמשותף לכולן הוא שימוש בכלים המאפשרים ניתוח שיטתי. ניתוח כזה מגדיל את הסיכוי שכל מאפייני הסיכון וכל המרכיבים בעלי ההשפעה על הבטיחות יילקחו בחשבון. בחירת שיטת הניתוח – ולעתים שילוב של מספר שיטות – תיעשה בהתאם לאופי המערכת המנותחת, מורכבותה, הניסיון שנצבר במוסד המבצע את הניתוח, אופי המידע שהצטבר לגבי המערכת ועוד.

**אירועי בטיחות רבים הם תוצאה מהתפתחות טכנולוגית מואצת, שאין בעקבותיה התפתחות מקבילה של אמצעי בטיחות**

**(HAZOP) Hazard and Operability Study**

זוהי שיטה המקובלת בתעשייה התהליכית. מאפייניה העיקריים הם:

- לימוד התהליך וניתוח המערכת המיישמת את התהליך באמצעות עקיבה, צעד אחר צעד, אחר מרכיבי התהליך ומרכיבי החומרה (צנרת, מיכלים, שסתומים וכו');
- הניתוח נעשה בשיטת "סיעור מוחות", שבו משתתפת קבוצת מומחים מתחומים שונים הקשורים לתהליך (כימאים, מומחים לבקרה, מהנדסי חשמל, מנהלים וכו'); הניתוח מנוהל ע"י אדם מנוסה בניהול HAZOP אשר למד באופן יסודי את אופן פעולת המערכת;
- הניתוח הוא איטרטיבי (כלומר: חזרה על אותן פעולות בכל מרכיבי המערכת), ונעשה בו שימוש עקבי (קונסיסטנטי) במילות מפתח, המציינות אופני כשל אפשריים שונים. בניתוח כזה נשאלות שאלות קבועות לגבי שינויים בתהליך (יותר, פחות וכו'), ונבחנות השפעותיהם. בכך נמנע דילוג על כשלים פוטנציאליים. הטיפול נעשה בו זמנית לכל סוגי הכשל: הבטיחותיים והתפעוליים.

## ניתוח סיכונים הסתברותי (ניס"ה, PSA, PRA[5])

ראשיתה של השיטה בתעשייה האווירית, וממנה התפתחה בצורה נרחבת בתעשייה הגרעינית האמריקאית ואח"כ בתעשיית החלל ובתעשיות נוספות. השיטה מבוססת על יצירת תבנית לוגית של המערכת המפותחת מן הכלל אל הפרט (top down), ועל הערכה הסתברותית של כשלי בטיחות שונים, אשר עלולים להתרחש בה. לצורכי הניתוח נעשה שימוש מושכל במיגוון כלים, בהתאם למורכבות המערכת ולאופי המידע הקיים לגביה.

הבסיס המתודי להפעלת גישת ניס"ה הוא הגדרת הסיכון. על פי הגדרה זו – סיכון ממערכת הנדסית כולל 3 מרכיבים עיקריים:

- תרחישים אשר עלולים להוביל ל"תוצאה בטיחותית";
- הסיכוי להתרחשותו של כל תרחיש כזה;
- רמת הנזק הצפוי – אם התרחיש אכן יתרחש.

בשפה מתמטית ההגדרה נרשמת כך:

$$R=\{S_j, P_j, D_j\}, \quad j=1, n$$

(כאשר: $R$ הוא הסיכון הכולל מ-$n$ תרחישים שונים; $S_j$ מסמן תרחיש מס' $j$; $P_j$ מסמן את ההסתברות לתרחיש $S_j$; ו-$D_j$ מסמן את הנזק הצפוי מתרחיש $S_j$).

הניתוח נעשה בשלבים. בשלב הראשון נבנה מודל לוגי להתפתחות כשלי בטיחות במערכת ומזוהים התרחישים $S_j$. בשלבים האחרים נאספים מידע סטטיסטי והיסטורי, וכן תוצאות של חישובים וניסויים, אשר מאפשרים – עם שילובם במודל הלוגי – את הערכת ההסתברות ($P_j$) ואת הנזק ($D_j$), לכל תרחיש ולמערכת כולה.

התוצאות העיקריות שאותן ניתן לקבל בניתוח סיכונים הסתברותי (ניס"ה) הן הערכת הסיכון, השוואת הסיכון המחושב לקריטריונים ולדרישות בטיחות, השוואת רמות הסיכון הנובעות מחלופות תכן וזיהוי מרכיבי המערכת אשר ראוי כי יהוו יעד לשיפור הבטיחות.

הטכניקות המשמשות לניס"ה רבות ומגוונות, ולא ניתן לתאר את כולן במאמר יחיד. לכן, נזכיר את העיקריות מביניהן ואת השימוש שנעשה בהן:

- **עצי אירועים (event trees):** משמשים לניתוח "רמת העל" (הרמה העליונה) של מערכת מורכבת ולזיהוי תרחישי בטיחות אשר עלולים להתרחש בה.
- **עצי תקלות (fault trees):** משמשים לניתוח לוגי של מרכיבי מערכת או תת-מערכת נתונה. הניתוח נעשה מהכלל אל הפרט: תחילתו – זיהוי כשל בטיחות אשר עלול להתרחש, וסיומו – זיהוי צירופים של כשלי מרכיבים במערכת, טעויות אנוש, אירועים חיצוניים וכו' אשר מביאים להתרחשות כשל הבטיחות.
- **שיטות לאיסוף וניתוח מידע סטטיסטי והסתברותי:** מקורו של המידע הנאסף בשיטות הללו, לגבי מרכיבים שונים של המערכת, הוא בבסיסי מידע כלליים, בנתוני כשל מהעבר של המערכת המנותחת ושל מערכות דומות לה, ובהערכות סובייקטיביות של מומחים. המידע "נשתל" ב"עצי תקלות" ומשמש לחישוב ההסתברויות של התרחישים השונים ושל כשלי בטיחות במערכת.

**ניתוח סיכונים הסתברותי מאפשר הפקת לקחים ושימוש בשיטות שונות כמעט לכל תחום טכני ותעשייתי הכרוך בסיכוני בטיחות**

## ניתוח אופני כשל וקריטיקליות (FMECA)

זוהי טכניקה שבה ניתן להשתמש בנפרד או בשילוב עם ניס"ה. בשיטה זו מזהים, באופן פרטני, את אופני הכשל האפשריים של כל אחד ממרכיבי המערכת. לאחר מכן, מרכיבים טבלה שבה מפורטים גורמיו והשפעותיו של כל אופן כשל על המערכת, והערכת ההסתברות להתרחשותו[6].

ניתוח זה יכול להיעשות למרכיבי חומרה (מיכללים ורכיבים) וגם לפונקציות או לתהליכים (כגון תהליכי ייצור והרכבה במפעל ייצור).

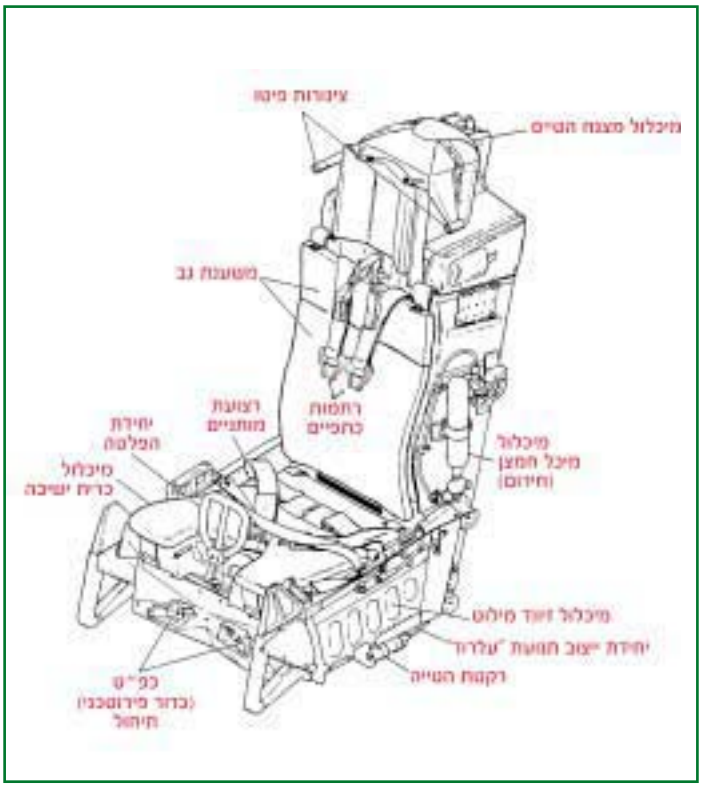
'FMECA' משמשת לניתוחי אמינות, בטיחות ותחזוקתיות. במערכות מורכבות במיוחד היא מהווה נדבך אחד, שבו נאסף מידע פרטני על המערכת. המידע הזה משולב, אחר כך, בעצי התקלות במסגרת ניס"ה – לצורך ניתוח כולל של המערכת. בניתוח תת-מערכות ומערכות פשוטות יותר (לדוגמה: מערכות שאין בהן יתירויות) מסתפקים ב-FMECA מבלי לשלב אותה בניתוחים אחרים.

אחד מהמימצאים העיקריים של הצוות אשר בדק את תאונת ספינת ה-Catamaran (New Scientist, 6 july 1991) הוא כי אי-ביצועו של ניתוח אופני כשל לתכן הספינות מדגם זה היה שגיאה חמורה.

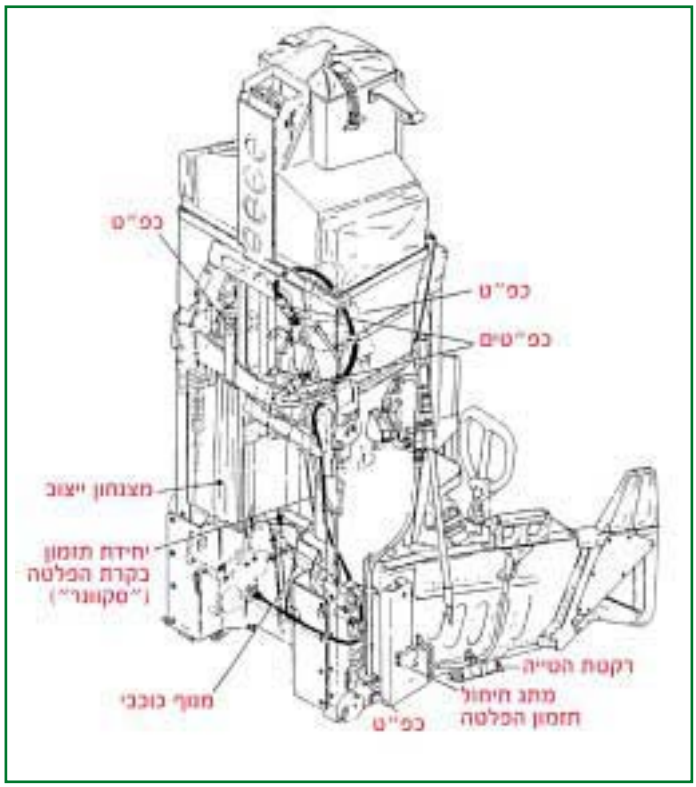
---

5. PRA = Probabilistic Risk Analysis, PSA = Probabilistic Safety Analysis

6. ניתוח אופני כשל (FMEA) היא שיטה דומה, שבה נעשים אותם תהליכי ניתוח פרט לחישובי ההסתברות




איור מס. 1: כסא מפלט – מבט מלפנים




איור מס. 2: כסא מפלט – מבט מאחור

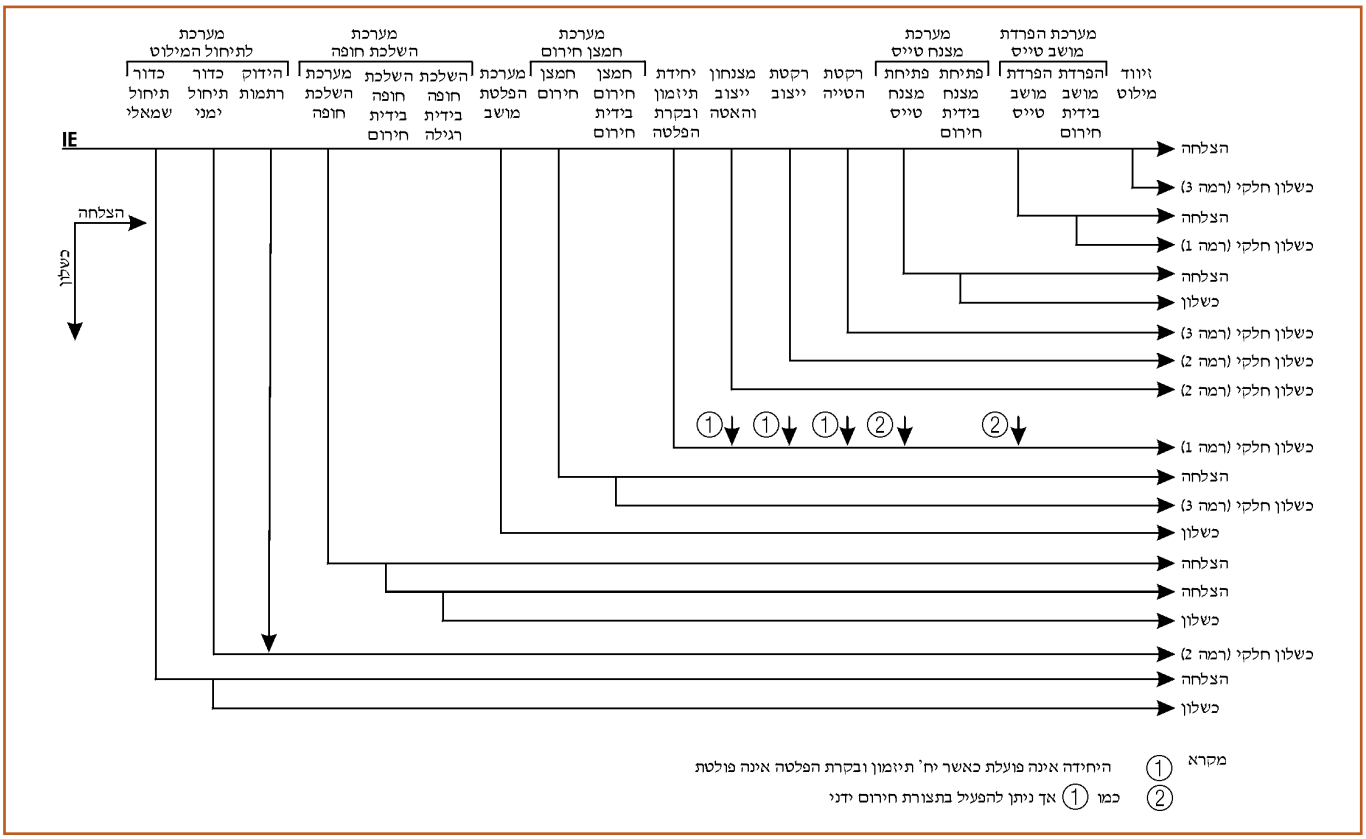
## דוגמה לשימוש בעצי אירועים ועצי תקלות

הדוגמה הבאה, מתוך עבודת מחקר לתואר שני, מדגימה את השימוש בעצי אירועים ובעצי תקלות (בעבודה עצמה נעשה שימוש גם ב–FMECA ובטכניקות נוספות שלא נסקרו במאמר הזה).

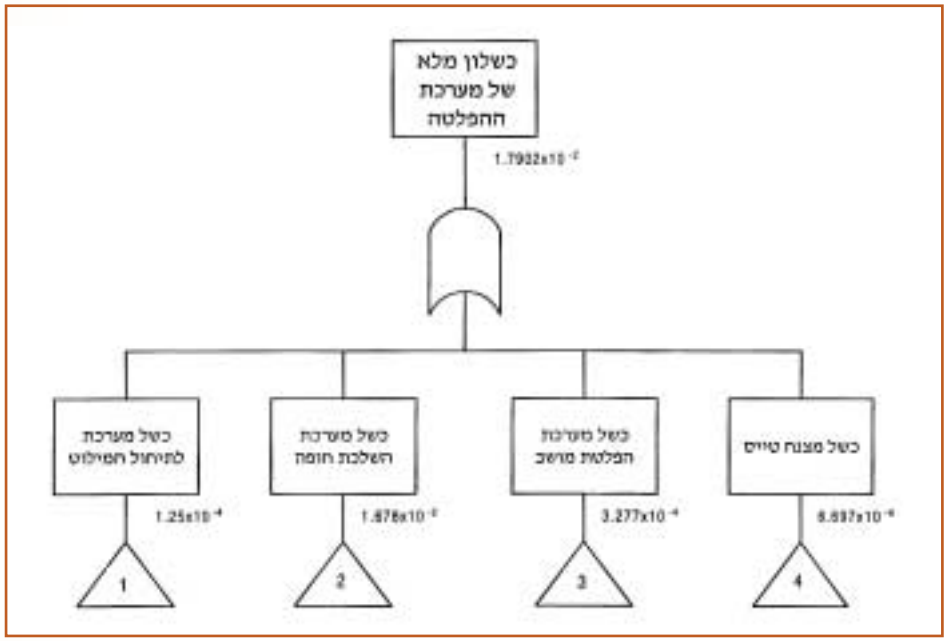
בעבודת המחקר נערך ניתוח סיכונים למערכת ההפלטה במטוס קרב. כסא המפלט, הכולל את מערכת ההפלטה, מוצג באיורים 1 ו–2 במבט מלפנים ומאחור.

● **אופן פעולת המערכת**

**תיחול והשלכת חופה:** משיכת ידית ההפלטה ע"י הטייס מציתה את שני תחלי ההפלטה (מיטעני הנפץ). הגז הנוצר ע"י כל אחד מהתחלים זורם בצינורות ב–2 נתיבים שונים: הגז מובל תחילה אל תָּחֶל מהדק




איור מס. 3: עץ האירועים




**איור מס. 4: עץ התקלות**

הרתמות, מצית אותו ומ**פעיל את מערכת** הידוק רתמות הכתפיים (אשר מצמידה את הטייס אל גב המושב ונועלת אותו בתנוחה זו). בהמשך, הגז זורם אל מנתקי מושב המטוס ודרכם לתוך המערכת המתזמנת את השלכת החופה והמושב.

**הפלטת המושב וחמצן חירום:** ההפלטה מתבצעת ע"י מנוע רקֶטי, אשר מרים את המושב ומסיעו קדימה. לפני כן מופעל "מָעוֹט" (מיתקן קפיצי), הדוחף את המושב על שתי מסילות המותקנות בגב המושב, אל מחוץ לתא הטייס. כל הפעולות מתבצעות ע"י גזים הנוצרים בתוך יחידות פירוטכניות, אשר מוצתות בצורה מתוזמנת.

בשלב שבו הכיסא עומד לעזוב את תא הטייס מופעלת גם מערכת אספקת החמצן לחירום.

**צניחה, רחיפה ונחיתה:** הגזים (שנוצרו ע"י היחידות הפירוטכניות) מפעילים, בהמשך, יחידת תיזמון ובקרת הפלטה. הבקרה מבטיחה את ביצוע הפעולות הבאות בסדר הנכון: פתיחת מיצנחון ייצוב והאטה; הפעלת רקטת האטה – למניעת התנגשות הכיסא במטוס; הפרדת הטייס מהמושב ופרישת מיצנח הטייס.

**7. אירועי כשל הם מקרים שבהם מרכיבים במערכת מגיעים למצב שאיננו מאפשר ביצוע תיפקודי שלהן באופן בטיחותי, כתוצאה מתקלה או עקב אירוע מחוץ למערכת.**

**8. מצבי כשל בטיחותיים – מצבים של המערכת השלמה, החורגים מהגדרת "מצב בטוח". בכסא המפלט אלה הם מצבים שבהם נגרם סיכון לחיי הטייס או לבריאותו. בין האירועים: אי–פתיחת החופה, אי פתיחת המצנח, אי–פעולת מערכת הידוק הרתמות, אי פעולת מערכת החמצן.**

● **ניתוח הבטיחות**

הניתוח התחיל בהכרת מערכת ההפלטה ואופן פעולתה, פרופיל המשימה (הגדרת הפעולות לפי סידרן) והיבטי התיישנות ותחזוקה (שלבי חייה של המערכת). כמו כן נלמדה בפרוטרוט מעטפת הביצועים והמיגבלות שהיא משיתה על פעולת מערכת ההפלטה.

בשלב הבא הוגדרו מצבי התחלה אפשריים של תהליך ההפלטה וזוהו **אירועי הכשל**[7] האפשריים במיכללי המערכת, בעקבות כל אחד מהאירועים.

המשכו של ניתוח הבטיחות הוא ניתוח מערכתי, שנועד לזיהוי **מצבי כשל בטיחותיים**[8] מנקודת מבטו של המשתמש (במקרה שלנו: הטייס הנזקק להפעלת כסא המפלט) ולזיהוי תרחישים עיקריים המובילים למצבי הכשל השונים. מצבי הכשל חולקו לשתי משפחות עיקריות:

■ כישלון מלא – כזה שיוביל למות הטייס);

■ כישלון חלקי.

עץ האירועים (event tree) באיור 3 הוא הכלי העיקרי ששימש לזיהוי מצבי הכשל והתרחישים העיקריים הגורמים לכל אחד מהם.

בשלב העיקרי של הניתוח מוצגת הלוגיקה של כל אחד ממצבי הכשל באמצעות עץ תקלות, מחושבים צירופים של אירועי הכשל המובילים לכל אחד מהם ומחושבות הסתברויותיהם. באיור 4 מובא, להדגמה, חלקו העליון של עץ התקלות באירוע "כשל מלא".

הדוגמאות של כשלי הבטיחות ודוגמת הניתוח מדגימות כי ניתוח הסיכונים ההסתברותי הוא נושא רב תחומי, המאפשר הפקת לקחים ושימוש בשיטות השונות שתיארנו כמעט לכל תחום טכני ותעשייתי הכרוך בסיכוני בטיחות. ■


**מקורות**

(המקורות, מן העיתונות ומהאינטרנט, מופיעים בסדר כרונולוגי שאיננו חופף את סדר הופעתם במאמר).

**דוחות**

**ניתוח סיכונים למערכת הפלטה ממטוס קרב;** יצחק גרוסמן, חיבור על מחקר לתואר מגיסטר למדעים באבטחת איכות ואמינות, הטכניון, ספטמבר 1994

**ARIANE 5 Flight 501 Failure;** Report by the Inquiry Board chaired by Prof. J.L.Lions, 19 July 1996

**Bhopal, Lessons for Technological Decision–Makers;** R.U.Ayres & P.K.Rohatgi, Technology In Society, Vol. 9 pp. 19–45 (1987)

**Investigation of Large Magnitude Incidents: Bhopal as Case Study;** A.S.Kalelkar, The Institute of Chemical Engineers Conference on Preventing Major Accidents, London, May 1988.

**Report of the United Nations Scientific Committee on the Effects of Atomic Radiation to the General Assembly;** 2000

**מתוך העיתונות**

**Key test is missing as catamarans take to sea;** New Scientist, 6 july 1991

**Toxins Abounding;** Scientific American, 6 July 1995

**An outsider's inside view of the Challenger inquiry;** Physics Today, February 1988

**Out of a clear blue sky;** New Scientist, 4 march 2000

**תנועות ההגה המוזרות של הבואינג;** הארץ, 17.4.00

**131 ניספו באסון התעופה הכבד ביותר בפיליפינים;** מעריב, 21.4.01

**Fresh evidence on Bhopal disaster;** New Scientist, 7 December 2002

**מהאינטרנט**

– www.cnn.com/world/9802/16/airbus.300.safety
Taiwan crash raises questions about Airbus A–300

**– דיווחים ותחקירים של תאונות מטוסים**

– www.esa.int/export/esaCP/Pr_33_1996_p_EN.html
Ariane 501 – Presentation of inquiry board report

– http://www.british–energy.com/media/factfiles/index.html
Fact files: Chernobyl

– ww.tech.plym.ac.uk/sme//FailureCases/Failure.htm
Failure as a design criterion

– www.unscear.org
Chernobyl: Assessment of Radiological and Health Impacts

**מקורות נוספים**

**שקפים של הרצאות (של כותב המאמר)** שניתנו במוסד לבטיחות, בטכניון ובחברת 'רפאל'