כמה בטוח זה מספיק בטוח?

מאמר זה דן בשימוש במתודולוגיית ה-LOPA (Layers Of Protection Analysis), לצורך ניתוח סיכונים מורכבים בדרגת חומרה גבוהה בתעשייה התהליכית

מאת: שי שגב, M.Sc.
מומחה לניתוח סיכונים תהליכיים וסיכוני אש

מתודולוגיית ה-LOPA היא אחת המתודולוגיות הנפוצות והאפקטיביות ביותר לניתוח סיכונים כמותי של תרחישי כשל בתהליכים בעלי מורכבות רבה ובדרגת חומרה גבוהה. זהו אחד הכלים המרכזיים בארגז הכלים של מנתח הסיכונים המקצועי. מתודולוגיית ה-LOPA משלימה את ניתוחי הסיכונים האיכותניים, כגון ה-HAZOP (Hazard and Operability Study) או ה-What If, ומאפשרת לוודא ששכבות ההגנה שהומלצו במהלך ניתוחי ה-HAZOP או ה-What If אכן צפויות להוריד את הסיכון לרמת סיכון קביל. אם רמת הסיכון המתקבלת אינה קבילה, מאפשרת לנו מתודולוגיית ה-LOPA לנתח את האפשרויות השונות, שבהן שכבות ההגנה יספקו רמת סיכון קבילה וכך לבחור את מערך שכבות ההגנה האופטימלי. כמו כן, מתודולוגיית ה-LOPA מאפשרת לזהות את הציוד והמכשור הקריטיים מבחינה בטיחותית, כדי להבטיח את בטיחותם לאורך השנים, ולתת להם עדיפות בתחזוקה ובבדיקות התקופתיות.

הצורך בניתוח סיכונים כמותי

מהו סיכון קביל? סיכון קביל מוגדר בתקנות ארגון הפיקוח על העבודה (תכנית לניהול הבטיחות) התשע"ג- כ"סיכון שהוקטן עד לרמה שהוגדרה כקבילה ביד המחזיק במקום העבודה, בהתחשב בחובותיו לפי דין ובמדיניות הבטיחות של מקום העבודה".

בעת ביצוע ניתוח סיכונים תהליכי, ההחלטה אם הסיכון הקיים בתרחיש מסוים הוא קביל או לא, יכולה להתבצע בשתי גישות: הגישה הראשונה והנפוצה ביותר היא **הערכה איכותנית**, כלומר הערכה סובייקטיבית, המסתמכת על הניסיון והידע המצטבר של חברי הצוות. הערכות אלו הן טובות כאשר לחברי הצוות יש ניסיון וידע עם יחידות ציוד דומות, תהליכים דומים או כאשר קיימים תקנים בינלאומיים מוכרים עבור יחידות הציוד והתהליכים הללו. במקרים אלו ניתוח הסיכונים מתבסס בעיקר על ניתוח הפערים בין התהליך המוצע ובין התהליך הנתפס כרצוי לדעת חברי הצוות (Best Practice), בהתבסס על ניסיונם, על לקחים שנלמדו מאירועים וכשלים, על דרישות התקנים וכד'.

היתרון בגישה זו הוא פשטותה והזמן הקצר - יחסית - הנדרש כדי לקבל באמצעותה החלטה על קבילות הסיכון או על אמצעי הבטיחות שנדרש להטמיע בתכנון כדי להפחית את הסיכון לרמה קבילה. חסרונה הגדול של גישה זו נעוץ בסובייקטיביות ההחלטה: מניסיון שהצטבר בעולם אנו יודעים כי בגישה זו קיימת הסתברות גבוהה להערכת חסר של הסיכון, ככל שהתרחיש המנותח מורכב יותר וככל שההסתברות להתממשות התרחיש נמוכה יותר. הערכת חסר זו מתרחשת כיוון שבמקרים רבים אין בידי הצוות המקבל את ההחלטה על קבילות הסיכון כל המידע הנדרש לצורך קבלת החלטה, ואין שימוש בשיטה המאפשרת לו לזהות את המידע החסר ולנתח את המידע הקיים באופן הגיוני ושיטתי.

הגישה השנייה לקבלת החלטה בדבר קבילות הסיכון היא **הגישה הכמותית** (כלומר חישוב הסיכון או סדר הגודל שלו). בגישה זו מומלץ להשתמש כאשר מנתחים תרחישים מורכבים או תרחישים ברמת חומרה גבוהה. השימוש בגישה זו מאפשר לוודא ששכבות ההגנה המוצעות אכן אפקטיביות ומורידות את הסיכון לרמה קבילה.

עד לפיתוח מתודולוגיית ה-LOPA היו לגישה זו שני חסרונות מרכזיים: הזמן הרב שנדרש כדי לבצע את חישובי הסיכון, והמורכבות הגבוהה של החישובים. חסרונות אלו גרמו לכך שניתוח סיכונים בגישה זו היה בלתי מעשי עבור מרבית המפעלים.

יתרונות מתודולוגיית ה-LOPA

ניתוח הסיכונים במתודולוגיית ה-LOPA מבוצע בגישה הכמותית. הוא אפקטיבי, פשוט וקצר יותר מאשר ניתוח סיכונים בשיטות כמותיות אחרות, כגון ETA (Event Tree Analysis) וניתוח עצי כשל - FTA (Fault Tree Analysis), בשל שתי סיבות מרכזיות: הסיבה הראשונה היא שניתוח הסיכונים הכמותי מבוצע רק על תרחישים בעלי מורכבות / חומרה גבוהה: במתודולוגיה זו ניתוח הסיכונים מבוצע בכל פעם רק על אחד מהתרחישים שזוהו במהלך ניתוחי ה-HAZOP או ה-What If כתרחישים בעלי מורכבות או חומרה גבוהה, ולא על התהליך כולו (דוגמאות לתרחישים בעלי חומרה גבוהה: פיצוץ ריאקטור בשל עליית טמפרטורה בלתי מבוקרת; גלישת חומר נפיץ ממכל בשל כשל מערכת בקרת הגובה וכד'). במרבית התהליכים בתעשייה רק חלק קטן מהתרחישים (בדרך כלל כ-10%) הם מורכבים או בעלי חומרה גבוהה ודורשים, לפיכך, ניתוח מעמיק יותר בעזרת מתודולוגיית ה-LOPA.

הסיבה השנייה לאפקטיביות הגבוהה יחסית של מתודולוגיית ה-LOPA היא השימוש בסדרי גודל של הסתברויות כשל שכבות

ההגנה שנעשה בהן שימוש (לדוגמה, הסתברות כשל של אחת לעשר שנים, של אחת למאה שנה, של אחת לאלף שנה וכד') במקום שימוש בהסתברויות מדויקות של הכשל. כתוצאה מכך, קל הרבה יותר למצוא בספרות את הסתברות הכשל המתאימה ולבצע את החישובים הנדרשים.

מאחר שרמות הסיכון המתקבלות ב-LOPA הן מספריות, ניתן להשוות באופן אובייקטיבי בעזרת מתודולוגיה זו את רמות הסיכון הקיימות במתקנים שונים באותה חברה ואפשר להשתמש בה לצורך הגדרת האמינות הנדרשת משכבות ההגנה השונות כדי להוריד את הסיכון לסיכון קביל (לדוגמה: הגדרת רמת ה-Safety Integrity Level-SIL הנדרשת ממכשור מסוים שנעשה בו שימוש כשכבת הגנה בטיחותית).

חסרונות מתודולוגיית ה-LOPA

מתודולוגיית ה-LOPA אינה מיועדת לזיהוי תרחישי סיכון חדשים אפשריים, אלא מבוססת על כך שכל תרחישי הסיכון הקיימים בתהליך זוהו ונותחו באופן איכותני בעזרת מתודולוגיות אחרות, כגון HAZOP או What If (הניתוח בעזרת מתודולוגיות אלו מאפשר לזהות את התרחישים הדורשים ניתוח מעמיק יותר בעזרת מתודולוגיית ה-LOPA).

בשל הדרישות הנוקשות משכבות הגנה, הניתוח המבוצע באמצעות מתודולוגיית ה-LOPA נחשב כשמרני יחסית למתודולוגיות כמותיות אחרות (כלומר, תרחישים שהסיכון עבורם חושב כבלתי קביל בעזרת מתודולוגיית ה-LOPA יכולים להימצא לפעמים קבילים, אם ייעשה עבורם חישוב כמותי מדויק יותר בעזרת מתודולוגיות כמותיות אחרות).

שלבי הניתוח במתודולוגיית ה-LOPA

שלב 1 - סינון וקביעת התרחישים שינותחו בעזרת מתודולוגיית ה-LOPA: שלב זה מתבצע לאחר שנבחנו כל התרחישים האפשריים על פי מתודולוגיית HAZOP / What If. בשלב זה, מסומנים תרחישים מורכבים ותרחישים בעלי חומרה גבוהה. כמו כן, נבחנים תרחישים באותם נושאים שעדיין לא פורסמו בהם תקנים או הנחיות מקצועיות מקובלות, המגדירות אילו שכבות הגנה נדרשות כדי למזער את ההסתברות להתממשותם (לדוגמה: תקני NFPA, API, FM, Chlorine Institute וכו').

כל אחד מהתרחישים הללו נרשם כצמד המורכב **מכשל התחלתי** (הסטייה מתפעול תקין, Deviation, שזוהתה ב-HAZOP) **ומההשלכות** של תרחיש זה (Consequences).

דוגמה לרישום תרחיש: **כשל התחלתי:** עליית הלחץ בריאקטור, מעבר ללחץ המרבי המותר. **השלכות:** פיצוץ שכתוצאה ממנו ייהרגו עובדים.

שלב 2 - מציאת התדירות הקבילה להתממשות התרחיש / הסיכון

בשלב זה מוצאים מתוך מטריצת הסיכון של המפעל את השכיחות שעבורה התרחיש יהיה ברמת סיכון קבילה. לדוגמה:

איור מס' 1 : דוגמה למטריצת סיכונים. לפי מטריצה זו התדירות הקבילה לתרחיש של פיצוץ ריאקטור (אירוע רב נפגעים) היא 10^{-7} שנים (אחד ל-10 מיליון שנה).

שכיחות			חומרה						
			2	3	4	5	6	7	8
			עזרה ראשונה	טיפול במרפאה Recordable Injury	תאונה עם היעדרות Lost Time Injury	פציעה עם אשפוז או תאונה עם מספר נפגעים	נכות או תאונה עם מספר מאושפזים	1-2 הרוגים	אירוע רב נפגעים (מספר רב של הרוגים)
עליה	0	פעם בשנה							
	10^{-1}	פעם בעשור							
	10^{-2}	1/100 שנה							
	10^{-3}	1/1,000 שנה							
	10^{-4}	1/10,000 שנה							
	10^{-5}	1/100,000 שנה							
	10^{-6}	1/1,000,000 שנה							
	10^{-7}	1/10,000,000 שנה							
	10^{-8}	1/100,000,000 שנה							

סיכון לא קביל | סיכון קביל גבולי - נדרש המשך פעילות עד להורדה לסיכון קביל | סיכון קביל

במטריצה המובאת באיור מס' 1 התדירות הקבילה לתרחיש של פיצוץ ריאקטור (אירוע רב נפגעים) היא אחת ל-10^{-7} שנים.

שלב 3 - זיהוי שכבות ההגנה הבלתי תלויות (IPL- Independent Protection Layers)

שלב זה הוא השלב החשוב ביותר בניתוח הסיכונים במתודולוגיית ה-LOPA.

שכבת הגנה בלתי תלויה מוגדרת כהתקן, מערכת או פעולה המיועדים למנוע את התקדמות התרחיש לעבר מימוש התאונה / האירוע (במקרה של התממשות גורם הכשל).

כדי ששכבת הגנה תיחשב כבלתי תלויה, עליה לקיים את כל התנאים הבאים:

א. עצמאות/אי-תלות (Independence) - התפקוד של שכבת ההגנה חייב להיות בלתי תלוי ובלתי מושפע מגורם הכשל או מפעולה של שכבת הגנה אחרת.

דוגמאות:

1. מערכת ספרינקלרים אינה נחשבת כשכבת הגנה בלתי תלויה בתרחיש של אש כתוצאה מרעידת אדמה, כיוון שרעידת אדמה גורמת במקרים רבים גם לכשל של מערכת הספרינקלרים, למעט מקרים שבהם במערכת הספרינקלרים הותקנו תמיכות מתאימות.

במקרים רבים עצמאות שכבת ההגנה נפגעת בשל תופעה המכונה בספרות Common Cause Failure, לדוגמה:

2. הפסקת חשמל גורמת לכשל ההתחלתי, אך גם גורמת לכשל של שכבת ההגנה.
3. אותו מד טמפרטורה משמש גם להתרעה וגם להשמטה - הפסקת התהליך (הפסקת פעילות מד הטמפרטורה גורמת לכשל, וגם פוגעת בתפקוד שכבת ההגנה).
4. הצטברות מוצקים בחלקו העליון של הריאקטור גורמת לכשל בו-זמנית של דיסקת הפיצוץ ופורק הלחץ (במקרה זה דיסקת הפיצוץ ופורק הלחץ אינן שכבות הגנה בלתי תלויות, ולכן יש להתייחס אליהן כאל אותה שכבת הגנה).

ב. פונקציונליות - שכבת ההגנה צריכה להיות מסוגלת למנוע את התרחשות התאונה / אירוע, ולכן יש צורך לוודא ששכבת ההגנה תוכננה בהתאם לתקנים המקובלים ושקיים זמן מספיק לשכבת ההגנה לזהות את הסטייה ממצב התפעול הבטוח ולהחזיר את התהליך למצב בטוח.

דוגמאות:

1. כדי למנוע תרחיש של פיצוץ מחמצן תרמי (RTO - Regenerative Thermal Oxidizer), כתוצאה מכניסת גזים בתחום הנפיצות, מותקן בדרך כלל גלאי נפיצות בקו כניסת הגזים אליו. בכמה תאונות שאירעו בעולם, התברר כי פיצוצים של מחמצנים תרמיים התרחשו אף שלא היה כל כשל בגלאי הנפיצות ובמערכות הבקרה (הפיצוצים התרחשו לפני שהברזים על קו כניסת הגזים נסגרו). פיצוצים אלו התרחשו מאחר שבמסגרת התכנון וניתוח הסיכונים לא נלקח בחשבון זמן התגובה של מערכת ההגנה, ולכן לשכבת ההגנה (גלאי הנפיצות, מערכות הבקרה וברזי הניתוק על קו כניסת הגזים) לא היה מספיק זמן לזהות את הסטייה ממצב התפעול הבטוח ולהחזיר את התהליך למצב בטוח.
2. כדי לוודא שדיסקת פריצה המותקנת על ריאקטור תוכל לפרוק את כל עודפי הלחץ ולמנוע פיצוץ של הריאקטור, גם במקרה של תגובה הגורמת לאיבוד השליטה על התהליך (Run Away Reaction), יש לוודא שגודל דיסקת הפריצה ולחץ הפריצה המיועד (Set Pressure) חושבו בהתאם למתודולוגיית DIERS - Design Institute for Emergency Relief Systems.

ג. שלמות (Integrity) - התכנון של שכבת הגנה צריך להתייחס הן לכשלים השיטתיים האפשריים בשכבת ההגנה והן לכשלים האקראיים. כדי שיהיה אפשר לתת קרדיט לשכבת ההגנה, הפחתת הסיכון הצפויה צריכה להיות בסדר גודל אחד לפחות (הפחתת סיכון של פי 10 לפחות).

ההערכה של הפחתת הסיכון הצפויה חייבת לקחת בחשבון גם את התכנון והניהול של שכבת ההגנה (לדוגמה: תדירות הבדיקות, איכות הבדיקות, הרמה המקצועית של הגוף המבצע את הבדיקה וכד'). אם לדוגמה, פורקי הלחץ אינם נבדקים תקופתית בהתאם לתקן בינלאומי מקובל כגון API 576, אזי קיים סיכוי גבוה שפורקים אלו לא יתפקדו בעת הצורך ולכן אינם יכולים להיחשב כשכבת הגנה.

ד. אמינות (Reliability) - אמינות שכבת ההגנה מוגדרת כהסתברות שההגנה תפעל כמתוכנן, בתנאים המוגדרים ולמשך הזמן הנדרש. כדי שיהיה אפשר לתת קרדיט לשכבת הגנה מסוימת, יש צורך במסמכים או באינפורמציה המאשרת את אמינות שכבת ההגנה, לדוגמה: אישור מעבדה מוסמכת, ניסיון תפעולי וכד'. אמינות שכבת ההגנה מבוטאת בדרך כלל באמצעות ההסתברות לכשל במקרה של דרישה (PFD - Probability of Failure on Demand). ככל שערך ה-PFD נמוך יותר, שכבת ההגנה אמינה יותר. ערכי PFD אופייניים למגוון שכבות הגנה, ציוד ואביזרים תהליכיים אפשר למצוא בספרות המקצועית.

ה. בחינות (Audiability) - כדי שיהיה אפשר לתת קרדיט לשכבת הגנה, חייבת להיות שיטה שבעזרתה נוכל לוודא תקופתית את אמינותה. שכבת ההגנה חייבת תמיד לשמור על האמינות שנקבעה - כלומר, לתפקד כחדשה. כל שכבות ההגנה חייבות להיות כלולות בתכנית האחזקה והבדיקות התקופתיות. שכבות הגנה שתלויות בפעולות של אנשי תפעול צריכות להיות מגובות בנהלים כתובים. עובדים שיש להם אחריות לתפעול שכבת האחזקה, לבדיקתה או לתחזוקתה, חייבים לקבל הדרכה והסמכה לתפקידם ולהיבחן על הנהלים.

ו. הגבלת גישה - שכבת ההגנה צריכה לכלול שימוש באמצעים אדמיניסטרטיביים ופיזיים המיועדים למזער את ההסתברות של ביצוע שינויים בלתי מאושרים ושל ביצוע שינויים בשוגג (ללא כוונה).

ז. ניהול שינויים - מאחר שחלק נכבד מהכשלים של שכבות ההגנה נגרם כתוצאה מביצוע שינויים ללא ניתוח סיכונים מתאים, חובה לבצע ניתוח סיכונים לפני ביצוע שינוי כלשהו בשכבת ההגנה.

שלב 4 - חישוב תדירות התרחיש

תדירות ההתממשות של השלכות התרחיש שווה למכפלת תדירות הכשל הראשוני בהסתברות הכשל של כל אחת משכבות ההגנה הקיימות:

$$f=IF* PFD_1* PFD_2* ...*PFD_n$$

$\hat{f}$=תדירות התממשות התרחיש

IF= תדירות הכשל הראשוני

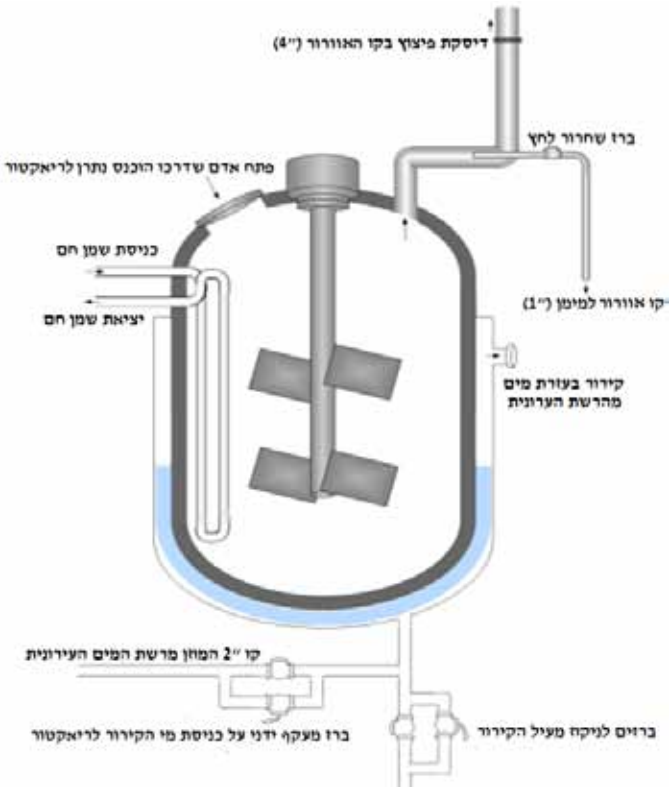
PFD_1= תדירות הכשל הצפוייה של שכבת הגנה מס' 1

סוף בעמוד 16

כמה בטוח זה מספיק בטוח?

המשך מעמוד 7

PFD_2= תדירות הכשל הצפוייה של שכבת הגנה מס' 2
PFD_n= תדירות הכשל הצפויה של שכבת ההגנה האחרונה בתרחיש (מס' n)



דוגמה (על בסיס תחקיר התאונה ב-T2 Laboratories, שבה נהרגו ארבעה עובדים ונפצעו 14): בריאקטור זה בוצעה תגובה אקסותרמית (תגובה הפולטת חום). כדי למנוע הצטברות לחץ והיווצרות תגובות בלתי רצויות היוצרות גם הן חום ולחץ, התבצע קירור של מעטפת הריאקטור בעזרת מים שהגיעו מהרשת העירונית. לו היה מבוצע ניתוח סיכונים במתודולוגיית HAZOP לתרחיש זה, סביר להניח שהוא היה מגלה את האפשרות הבאה לסטייה מתפעול בטוח (כשל ראשוני):

- שסתום כניסת מי הקירור נכשל במצב סגור (בספרות המקצועית אפשר לראות כי ההסתברות לכשל זה היא 10^{-1} לשנה).
- המפעיל בחדר הבקרה לא מזהה את הכשל ולא פותח את הברז הידני בקו המעקף (בספרות המקצועית אפשר לראות כי ההסתברות לכשל זה היא 10^{-1} למקרה). לפיכך, החישוב הוא שההסתברות להיווצרות לחץ יתר בריאקטור היא 10^{-2} לשנה ($IF = 10^{-2}$).

חישוב תדירות הכשל:

במקרה זה הייתה רק שכבת הגנה אחת. בתאונה הזו שכבת ההגנה לא עמדה בתנאי הפונקציונליות, מאחר שדיסקת הפיצוץ לא תוכננה בהתאם למתודולוגיית DIERS (Design Institute for Emergency Relief Systems). אילו דיסקת הפיצוץ הייתה מתוכננת כנדרש לפי DIERS, היה אפשר למצוא בספרות המקצועית כי פקטור הפחתת הסיכון הוא 10^{-2} ($PFD_1 = 10^{-2}$). לפיכך, תדירות התרחיש הצפויה הייתה $f=IF*PFD_1$, כלומר עדיין היה צורך להוסיף שכבות הגנה נוספות שמורידות את הסיכון ב-3 סדרי גודל (פי 1,000) עד להסתברות התרחשות של אחת ל-10 מיליון. ■