

יישום המדריך להנדסת מערכות מכוונת חסינות למצבי הירום: ניתוח אירוע השריפות נובמבר 2016

אבי הראל – ארגולייט

תקציר

המדריך הורחב להנדסת מערכות מכוונת חסינות כולל המלצות למפתחי מערכות הנדסיות כיצד למנוע תאונות בעלות אפיונים מסויימים. בנובמבר 2016 התנאים האקלימיים הקיצוניים גרמו לשריפות ברחבי הארץ, שגרמו לנזקים כבדים לבתי תושבים ולתכסית. מאמר זה מציג את האירוע של נובמבר 2016 כאירוע עם סיכון, שמאופיין ככשל מערכתי, ומתאר כיצד המדריך הנ"ל יכול לסייע למנוע או לנהל בהצלחה אירועים כאלו. האירוע של שריפות 2016, כמייצג של אסונות טבע, שונה מהאירועים הקודמים ששימשו לפיתוח המדריך, בכך שהוא מתייחס אל מערך המורכב ממספר מערכות, שהקישורים ביניהם דינאמיים.

מבוא

המדריך לאבטחת חסינות מערכות פותח בין השנים 2010-2015, בשיתוף מרכז גורדון להנדסת מערכות ואילתם (זוננשיין והראל, 2015). המדריך כולל המלצות למפתחי מערכות הנדסיות כיצד למנוע תאונות בעלות אפיונים מסויימים. בהמשך, המדריך הורחב להנדסת מערכות מכוונת חסינות בכך שנוספו לו פרק הכולל הצעה לדרך לשילוב ההנחיות בתהליכי פיתוח מערכת הנדסית, וכן פרק המיועד למהנדסים שמתנסים בשימוש בו בפעם הראשונה (זוננשיין והראל, 2016).

בנובמבר 2016 התנאים האקלימיים הקיצוניים גרמו לשריפות ברחבי הארץ, שגרמו לנזקים כבדים לבתי תושבים ולתכסית (הראל, 2016). שריפות אלה עוררו את השאלה האם ניתן להגדיר תהליכים לתפעול מערכות עם אתגרים ברמה הלאומית, כגון, פגעי טבע. שיטה להתמודד עם אתגרים ברמה הלאומית נדונה בהרחבה במודל STAMP (Leveson, 2004) והשאלה שמתבקשת היא האם המדריך הנדון כולל המלצות שיכולות לסייע גם לאירועים כאלו.

האירוע של שריפות 2016, כמייצג של אסונות טבע, שונה מהאירועים הקודמים ששימשו לפיתוח המדריך, בכך שהוא מתייחס אל מערך המורכב ממספר מערכות, שהקישורים ביניהם דינאמיים (מערכת של מערכות SoS). מאמר זה מציג את האירוע של נובמבר 2016 כאירוע עם סיכון, שמאופיין ככשל מערכתי, ומתאר כיצד המדריך הנ"ל יכול לסייע למנוע או לנהל בהצלחה אירועים כאלו.

שכבות ההגנה

המדריך בגירסתו החדשה כולל שבע שכבות הגנה (במדריך). בהקשר של שריפה, יש לתרגם אותן להנחיות והמלצות במונחים של תכניות למניעה ולכיבושי שריפות. הטבלה להלן מתארת תרגום כזה, וכן את ההתנהלות בפועל, תוך הדגשה של התנהלות שאינה תואמת את ההמלצות שבמדריך. שכבות ההגנה מסומנות על ידי $PL_n, n = 1..7$ (קיזור ל- Protection Layer)

שכבת הגנה	הפעילות המשתמעת מההמלצות במדריך	ההתנהלות בפועל
PL1 - תכן למניעת טריגרים	תכניות להדרכה והסברה למניעת רשלנות במדורות, בכיבוי סיגריות ... מניעת הסתה להצתה	יש התקדמות בנושא הדרכה והסברה למניעת רשלנות באש אבל תהליך ההטמעה ממושך.
PL2 - תכן להסימת האיום (ריבאונד)	תכניות מתאר תכסית שטח: מניעת תנאים שמאפשרים התפשטות אש (דילול עצים, ביעור קוצים, שיחים ...),	הרשויות עודדו גינון. תושבי חיפה שביקשו לדלל עצים נדרשו לקבל אישור מיוחד, ו-או לשלם כופר.
PL3 - תכן להתמודדות עם האיום	תכן איתור מוקדי דליקה: אמצעים, תכנית איסוף, תרגול תכניות של ברזי כיבוי, אספקת מים, פיזור חומר מונע בעירה תכניות להפעלת אמצעי כיבוי	יש טכנולוגיה לאיתור מוקדי דליקה, המבוססת על מצלמות אבטחה, על צילומי לוויין ועל מצלמות תרמיות. נראה יש בעיה בתפעול של האמצעים, ושהמערכת אינה מתרגלת את עצמה באופן סדיר. בפועל חסרים ברזי כיבוי לעומת התקן, אין בדיקות סדורות של תקינות ותפקוד הברזים. חומר מונע בעירה פוזר רק לאחר התפשטות הדליקה.
PL4 - תכן למניעת הסלמה	תכניות גיבוי אמצעי איכון מוקדי שריפה, אמצעי כיבוי או אמצעי שליטה תכניות לפינוי תושבים, תרגול	לא ידוע על תכניות או תרגול של פעולה במצב כשל של האמצעים. לא בוצעו תרגילי פינוי תושבים. בפועל הצירים היו סתומים והתושבים נתקעו שעות בפקקים. ככל הנראה, פינוי התושבים נעשה בהחלטה של תגובה למצב, ולא על פי תכנית.
PL5 - תכן להחלצות ממצבי חירום	תרגול לחילוץ אנשים הלכודים במבנים שעלולים לעלות באש.	במהלך השריפה חולצו אנשים עם מוגבלויות מבתיים ומבתי אבות, במועד, וללא פגע.
PL6 - בדיקות פרואקטיביות	תכנית בדיקות של תפעול מערך הכיבוי ושל פינוי תושבים.	אין בידנו מידע על תהליך הבדיקות
PL7 - תכן לתחקור אירועי כשל	פרוצדורות של הפקת לקחים מאירועים של שריפה מקומית.	שירותי הכיבוי מטפלים ב-100-50 שריפות ברחבי הארץ ביום. אין בידנו מידע על תהליך הפקת הלקחים.

PL1 - תכן למניעת הצתות

המדריך כולל הגדרה ואיפיון של טריגרים (במדריך) וכן פרק שדן במניעתם (במדריך). הצתות נגרמות משילוב של רשלנות ותנאי מזג אוויר קיצוניים. הישום למניעת הצתות כולל טיפול מניעת תכסית (עקירה ודילול שיחי בר ועצים), הסברה ואכיפה של התנהגות אחראית של הציבור, כולל עוברי אורח ומטיילים.

PL2 – תכן להסימת התלקחויות

המדריך כולל הגדרה ואיפיון של איומים (במדריך) וכן פרק שדן במניעתם, על ידי חסימת הטריגרים (במדריך). החסימה היא על ידי שימוש באמצעי תצפית לאיתור מוקדי שריפה, ואמצעי כיבוי. הישום כולל פריסת אמצעי איסוף, תפעול מערכת שליטה ובקרה, הכנת תכניות של ברזי כיבוי, אספקת מים, פיזור חומר מונע בעירה, בדיקות ותרגול.

PL3 – תכן להתמודדות עם השריפה

המדריך כולל הגדרה ואיפיון של אירועי כשל (במדריך) וכן פרק שדן בתהליכים של התמודדות עם האיומים (במדריך). ההתמודדות היא על ידי תכן איתור מוקדי דליקה: אמצעים, תכנית איסוף, תרגול וכן תכניות להפעלת אמצעי כיבוי, מחסומי אש, שריפה מונעת, וכיו"ב.

PL4 – תכן למניעת הסלמה

המדריך כולל הגדרה ואיפיון של סיכונים משניים (במדריך) וכן פרק שדן במניעת הסלמה (במדריך).

אחד המאפיינים של שריפות ענק הוא אובדן שליטה. סיבה עיקרית למצבים כאלו היא בעיית זמינות של אמצעים לאיתור מוקדים ולכיבוי. הסיכונים המשניים בתהליך הכיבוי מתייחסים אל כשל של אמצעי איכון מוקדי שריפה, אמצעי כיבוי או אמצעי שליטה ואל קשיים בפינוי התושבים. את ההסלמה ניתן למנוע על ידי תכנון ותרגול לפעולה במצבים כשל, כולל פינוי תושבים.

PL5 – תכן להיחלצות ממצבי חירום

המדריך כולל הגדרה ואיפיון של מצבי חירום (במדריך) וכן פרק שדן בתפעול ובהיחלצות ממצבי חירום (במדריך). הישום הוא ספציפי לאופי של הסיכון. המדריך אינו מתייחס למצבים מיוחדים, כגון, חילוץ מתוך מבנה בסיכון.

PL6 – בדיקות פרואקטיביות

המדריך כולל פרק שדן בבדיקות חסינות המתבצעות במהלך הפיתוח (במדריך). הישום הוא על ידי יזום של אירועי כשל. בישום של שריפות, יש ליזום שריפות ולתרגל מצבים שמדמים אובדן שליטה.

PL7 – תכן לתחקור אירועי כשל

המדריך כולל פרק הגדרה ואיפיון של תכן ריאקטיבי (במדריך), וכן פרק שדן בתכן לצרכי תחקור אירועי כשל (במדריך). הישום הוא על ידי אמצעים לתיעוד אירועי כשל והפצת דו"חות. העקרון רלבנטי גם לתחום של שריפות, אם כי הפתרונות על ידי אוטומציה הם מורכבים יותר מאשר במערכת הנדסית.

השינויים במדריך

המדריך כולל מספר ניתוחי מקרה, המדגימים את התועלת שבישום ההמלצות. בעקבות הלקחים מהשריפה, נוסף ניתוח אירועי השריפה לרשימת ניתוחי המקרה (במדריך). בנוסף, נוספו המלצות בעניין ההתמודדות עם התרעות שווא ובעניין זמינות אמצעים קריטיים.

הזמינות של אמצעים קריטיים

ניתוח הכשלים בשריפה הביא לתובנה לגבי הצורך באבטחת זמינות גבוהה לרכיבים קריטיים במערכת. מאחר שאמצעי הכיבוי הקרקעיים לא הספיקו, היה צורך לתגבר אותם באמצעים אוויריים. הבעיה היתה שמערך הכיבוי התבסס על אמצעים מארצות שונות. זמן ההגעה מהארצות השונות היה מספר שעות, בהן השריפה עשתה שמות בשכונות שלמות בעיר. תובנה זו באה לידי ביטוי בהמלצה שנוספה למדריך (להמלצה).

דיווח מפעיל על איומים

באוקטובר 2010 השתוללה שריפה במורדות המערביים של הכרמל. שריפה זו גבתה את חייהם של 44 תושבים, וגרמה לנזקים כבדים לבתי תושבים, ולפארק הלאומי. אחד הלקחים מאירוע זה קשור להשהיות בדיווחים של תצפיתנים בשלבים הראשונים של האירוע. ההשהיות נובעות מקושי בקבלת החלטות, בדילמת צל"ש או טר"ש, ברבדים שונים של תפקידים הקשורים בכיבוי: היערכות למניעת שריפות, דיווח על מוקדי שריפות, ניהול כוחות כיבוי וכיו"ב. (הראל, 2011). דילמה זו קשורה לתופעה של דיפוניה של אחריות: בבחירה בין חלופות, אנשים משווים בין הסיכון של התרעת שווא, שזוהי טעות ברמה האישית לבין הסיכון של החמצה, שזוהי טעות משותפת לכלל בעלי התפקידים שאמונים על ההתרעות (Darley & Latané, 1968). בבירור, קושי זה בקבלת החלטות הוא במוקד הכשל בהפקת לקחים מאירוע זה, שהתבטאה להתלבטות בהצטיידות ובהתארגנות למלחמה בשריפות. ככל הנראה, קושי זה התבטא גם באיטיות התגובה של כוחות הכיבוי בשטח בתחילת האירוע האחרון.

הגירסא הקודמת של המדריך דנה בהתרעות שנוצרות על ידי המכונה, אבל לא בדיווחי המפעילים. בעקבות האירוע, הגירסא הנוכחית של המדריך כוללת דיון בנושא ההשהיות בדיווחי מפעיל, והמלצה לצמצם את הסיכון ברמה האישית. ההמלצה שנוספה היא ישום עקרון האוטומציה כברירת מחדל גם לנושא ההתרעות ([להמלצה](#))

סיכום

האירוע של שריפות 2016, כמייצג של אסונות טבע, שונה מהאירועים הקודמים ששימשו לפיתוח המדריך, בכך שהוא מתייחס אל מערך המורכב ממספר מערכות, שהקישורים ביניהם דינאמיים (מערכת של מערכות SoS). במרבית המאפיינים, המדריך להנדסת מערכות מכוונת חסינות עונה על המאפיינים של אירועים כאלו. הדיון באירוע זה סייע לשיפור המדריך, ולהתאים אותו גם למגוון של אירועים ברמת המערך.

מקורות

Darley, J. M. & Latané, B. (1968). Bystander intervention in emergencies: diffusion of responsibility. *Journal of Personality and Social Psychology*, 8, 377-383.

Leveson, N., [A New Accident Model for Engineering Safer Systems](#) by Nancy Leveson. *Safety Science*, Vol. 42, No. 4, April 2004.

הראל, א. 2011 - [ניהול סיכונים תפעול בראי השריפה בהר הכרמל](#) – קבוצת העבודה לניהול סיכונים במסגרת אילטם, הרצליה

הראל, א. 2016 - [רשמים מיום העיון במרכז מינרבה למצבים קיצוניים בנושא השריפות של נובמבר 2016](#)

זוננשיין, א. והראל, א. 2015 - [מדריך לאבטחת חסינות בפני טעויות תפעול](#) - הכנס השמיני של IL-INCOSE

זוננשיין, א. והראל, א. 2016 - מדריך להנדסת מערכות מכוונת חסינות – הצעה למאמר לכנס התשיעי של

IL-INCOSE