

לקראת משפחות של מערכות חסינות

מאמר ביום עיון לזכר ד"ר יוסי לויין, 9 בינואר, 2013

אבי הראל

ד"ר אביגדור זוננשיין

ארגולייט

רפא"ל

שימוש חוזר ברכיבים

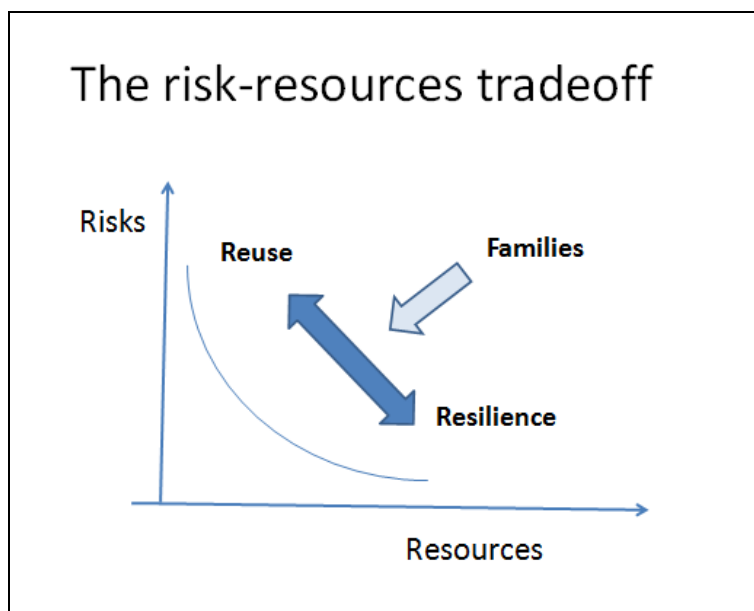
אחת הדרכים לצמצם את עלויות הפיתוח של מערכת חדשה היא על ידי שימוש חוזר ברכיבים ובתת מערכות של גירסאות קודמות. בתכנון מראש, ניתן להגדיר משפחות של מערכות, כאשר ההגדרה כוללת מודולים המשותפים לבנות המשפחה. ניתן לפתח מראש את המודולים הללו כך שיהיו ישימים לכל בנות המשפחה, כאשר עיקר ההשקעה הוא במודול הגנרי, ולפיכך ההשקעות הנדרשות לכל ישום ספציפי פוחתות באופן משמעותי.

מגבלות

הגישה של שימוש חוזר ברכיבים הוכיחה את עצמה בעבר, אבל התבררה כבעייתית כשמדובר במערכות עתירות סיכוני תפעול. כך, למשל, בגלל הבדלים באופן השימוש ברכיבים בהשוואה לגירסאות הקודמות, מערכת הריפוי על ידי הקרנות Therac-25 שפותחה בגישה זו גרמה בשנים 1985-1987 למותם של שלשה חולים ולכוויות חמורות בשלשה חולים נוספים ([קישור לויקי](#)). קיים אם כן צורך למצוא דרך חסכונית להגדיר ולפתח מערכות עבור ישומים עתירי סיכון.

אבטחת בטיחות באילוצי תקציב

התרשים הבא ממחיש את הדילמה של בטיחות באילוצי תקציב:



התרשים מראה שלצורך צמצום הסיכונים, יש להקצות משאבים. השימוש בפתרונות קיימים, כגון, בדרך של הגדרת משפחות מוצרים, מביא לחסכון בהוצאות, אבל לעליה בסיכון. האתגר שלנו הוא להביא לצמצום סיכוני תפעול, מבלי לפרוץ את מסגרת התקציב. הדרך המוצעת כאן היא על ידי משפחות של מערכות חסינות.

פיתוח מערכות חסינות

מרכז גורדון בטכניון, בשיתוף אילטם ו- INCOSE-IL מקיים בשנים האחרונות פעילות מחקר בתחום של תכן ופיתוח מערכות שהן חסינות בפני טעויות תפעול. הפעילות עד כה כללה:

- סיווג ראשוני של טעויות תפעול והצעות להתמודדות עימן, (לדו"ח)
- הגדרת עקרונות בהתמודדות עם אירועים בלתי צפויים (למאמר)
- פיתוח מודל של טעויות תפעול וישומו בתפקיד של נהיגה בכלי רכב (למאמר)
- פיתוח מודל לחסינות מערכות ומדריך לתכן מערכות חסינות.

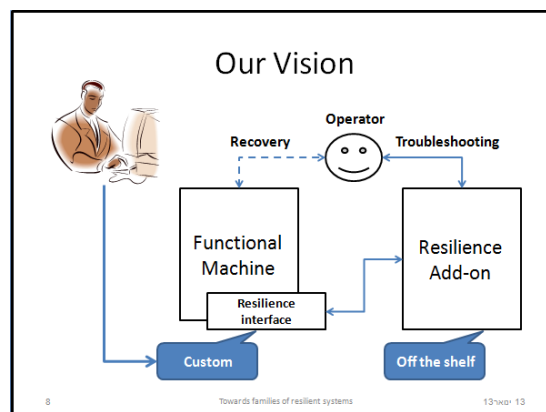
יישומים

המודל והמדריך לאבטחת חסינות ישימים למערכות בהיבטים הבאים:

- בטיחות בתפעול: תחבורה, צבא, תעשייה תהליכית
- תפוקת המשתמשים: מערכות מידע, בקרת ייצור, עמדות לרשות הציבור
- שימושיות של מוצרי צריכה: מוצרי חשמל ביתיים, מכשירי תקשורת, טלביזיה ביתית.

ארכיטקטורה

בהקשר של משפחות של מערכות חסינות, האתגר הוא להגדיר מודולים תיקניים שמאפשרים להתמודד עם אופני כשל מוכרים. התרשים הבא ממחיש דרך לשילוב מודול תיקני במערכת השייכת למשפחת מערכות המשתמשות בו.



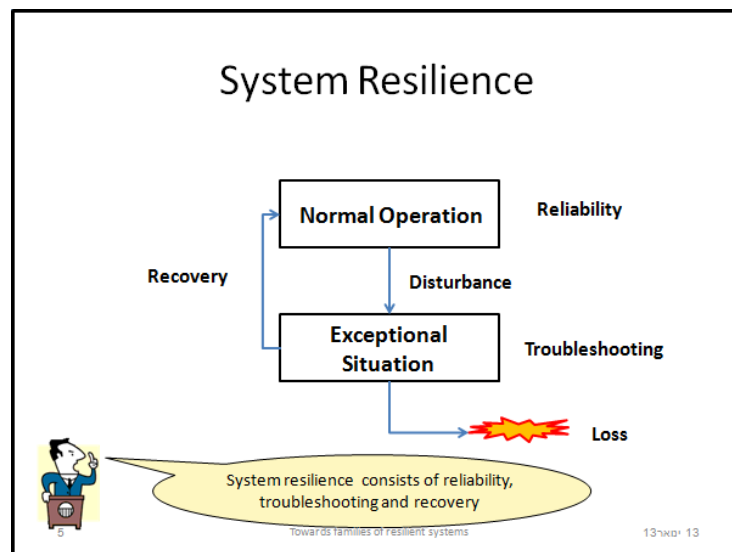
דוגמא של מודול תקני כזה היא מודול בקרה פשוט, שצריך לאפשר אמינות תפעולית בכיבוי והדלקה של תכונה מסוימת במערכת כלשהי (כגון, מנוע). מודול כזה צריך להתמודד עם מצבי התקלה הבאים:

- תקלה במיתוג: המיתוג במנוע או במפסק ההפעלה עלול להיות תקוע במצב נתק או במצב קצר
- תקלה במנוע: המנוע עלול לעבוד בתפוקה חלקית, או בתפוקת יתר
- מגעים רופפים. לדוגמא, מגעים רופפים במנוע או במפסק ההפעלה עלולים להביא לשינויים אקראיים במצב ההפעלה

בכדי למנוע טעויות תפעול במצבי תקלה, המודול צריך לכלול אינדיקציות לגבי מצב הפעולה של המנוע, למשל על ידי נוריות. האינדיקציה צריכה לאפשר למפעיל לזהות במהירות את מצב הפעולה, לאחר הפעלה בטעות, החמצה, או שכחה. כמו כן, המודול צריך לאפשר איתור מהיר של גורמי תקלה במפסק ההפעלה. בנוסף, המודול צריך לאפשר זיהוי מהיר של תקלות מהדרגה השניה, דהיינו, תקלות באמצעי החסינות שנוספו למודול (למשל, תקלה בנורית אינדיקציה).

מודל החסינות

תכונת החסינות מוגדרת כתכונה הנובעת משלשה מאפייני חסינות: אמינות, איתור תקלות והתאוששות. התרשים הבא מדגים את היחס בין מאפיינים אלו לבין תכונת החסינות.



יחידת החסינות

התכונות של יחידת החסינות צריכות להגזר מדרישות התפעול. כך, למשל, המודול שצריך לתמוך בשליטה במכונה מרחוק צריך לכלול אמצעים שיבטיחו שהמפעיל יזהה נכונה את מצב המכונה. כמו כן, אמצעי בקרה שמיועד לשלוט במספר מערכות חסינות צריך לכלול אמצעים שימנעו מהמפעיל הפעלה בטעות של מערכת אליה לא התכוון. המודול שמאפשר שליטה במכונה אחת בעזרת מספר אמצעי בקרה צריך לכלול אף הוא תכונות בקרה יחודיות. בנוסף, המודול שמאפשר איתור מצבים של תת-תפוקה או של תפוקת יתר צריך לכלול

אמצעים מיוחדים למדידה ולזיהוי חריגות בפרמטרים של ביצוע, דוגמת שיטות לבקרת תהליכים סטטיסטית (SPC).

גורמי אנוש

בשאיפה, הטיפול בהפרעות כגון הפעלה בטעות של פונקציה שאינה תואמת את מצב המכונה, צריך להיעשות אוטומטית. בפועל, טיפול אוטומטי אפשרי רק בחלק מהמקרים. לפיכך, עיקר הדיון במודל החסינות הוא במצבים בהם נדרשת התערבות המפעיל, כגון, לאיתור ולתיקון תקלות בחומרה. בכדי להבטיח ששילוב המפעיל יהיה יעיל, התכן צריך להניח את הפרדיגמה של **גירסת גורמי אנוש של חוק מרפי**:

אם המערכת מאפשרת למשתמשים להכשל, יש לצפות לכך שהם אכן ייכשלו.

לפיכך, המניעה של אופני הכשל הצפויים היא באחריות המתכנן. בעיקר, התכן צריך להבטיח שהמכונה תספק למפעיל מידע לגבי מצבה, תוך התחשבות במגבלות התפיסה של המפעיל. במיוחד, המודל עוסק בנושא של התרעות לגבי מצבים חריגים ולגבי שינויים במצב המערכת המחייבים טיפול.

מערכות התרעה

המשמעות של חסינות בנושא ההתרעות היא שקיים צורך להגדיר ולתכנן את התרעות כך שהן יעוררו אצל המפעיל את התגובה נכונה. בנושא זה הוגדרו העקרונות של אמינות ההתרעות, כולל שיטות להבטיח שהן תישמענה, ושהמשתמש בהן יבין את משמעותן ואת דרגת חומרתן ([קישור למאמר](#)). דוגמאות של מודולים בנושא ההתרעות כוללות:

- התרעות במערכות רפואיות, כגון, במוניטורים רפואיים
- התרעות בחדרי בקרה, כגון אלו שבתעשייה התהליכית
- התרעות בנהיגה בכלי רכב
- התרעות לציבור במצבי חירום, כגון, בפני אסון טבע, מפגע סביבתי או מתקפת אויב.

לגבי כל אחד מהמודולים הללו, יש להגדיר את הדרישות והתכונות המיוחדות, שמבדילות אותו מהמודולים האחרים. כך, למשל, מודול ההתרעות במערכות רפואיות צריך לכלול פתרונות לרצף התרעות גם במקרים בהם הצוות הרפואי נדרש להתייעץ בסביבה שקטה במצב חירום. בנהיגה, יש צורך לשלב את ההתרעה הקולית עם אופנויות חישה פיסית, על מנת להבטיח זיהוי מהיר של גורם ההתרעה, ולהבטיח תגובה נכונה תוך חלקיק שנייה. בהתרעות במצבי חירום, יש להגדיר שיטה שתבטיח שהציבור יבין את משמעות ההתרעה ברמת הפרט, ואת הנדרש ממנו לעשות על מנת להציל את חייו.

דוגמת יישום

המודל של התרעות לציבור במצבי חירום מבוסס על לקחים ממלחמת לבנון השנייה ([קישור למכתב לעתונן](#)). עד למלחמה זו ההתרעה התבססה על צופרים ששימשו בעצרות של ימי הזכרון להתייחדות עם החללים, על ידי צפירות בתדר קבוע. בעתות מלחמה, צופרים אלו סיפקו התרעות בתדר משתנה סינכרוניזציה. בכל

המלחמות עד למלחמת לבנון השנייה, בלטה לעין העובדה שחלקים נכבדים מהציבור אינם מצייתים להתרעות שנעשות בדרך זו, ואילו חלקים אחרים מהאוכלוסיה מגיבים בהיסטריה. אחת המסקנות ממלחמת לבנון השנייה היתה שקיים צורך לשנות את שיטת ההתרעות.

פיתוח מודול חסינות

הפיתוח של מודול חסינות נערך בחמישה שלבים:

1. הכרה בכך שיש בעיה
2. ניתוח הבעיה
3. הגדרת דרישות
4. הצעת פתרונות והוכחת היתכנות
5. תיכון ומימוש.

להלן הדגמה של תהליך הפיתוח עבור המודול של התרעות לציבור במצבי חירום.

הכרה בכך שיש בעיה

אחת המסקנות ממבצע עופרת יצוקה היתה שקיים צורך ליישם את העקרונות של אקלים בטיחות ([קישור לויקיפדיה](#)). במקום להטיל את האחריות על הקורבנות ([קישור לדוגמא](#)), הארגון האחראי על הבטיחות צריך לדאוג לכך שהמערכת תמנע את התאונה, בהתחשב בפרדיגמה של גירסת גורמי אנוש של חוק מרפי ([קישור למאמר](#)).

ניתוח הבעיה

בניתוח היעילות של ההתרעות התברר שהציבור תופס את רוב ההתרעות כבלתי רלבנטיות, מכיוון שהפיצוץ שבא בעקבות ההתרעה נשמע מרוחק. לעומת זאת, התרעות שמתבררות כרלבנטיות, אינן מובחנות מהתרעות שהן בלתי רלבנטיות, והתגובה לפיצוץ קרוב היא לעתים היסטרית. כמו כן, ההתרעה אינה כוללת מידע לגבי הזמן שנותר עד לרגע הפיצוץ, שהוא חיוני לצורך ההחלטה לגבי אופן התגובה הנכון ([קישור למאמר](#)).

הגדרת דרישות

הדרישות ממערכת ההתרעות צריכות לכלול דרישות להבטחת אימון הציבור במערכת, ודרישות להפקת המידע הנחוץ למפעיל לצורך בחירת אופן ההתנהגות הבטיחותית במצב הנתון ([לפירוט נוסף](#)).

- בכדי להבטיח את אימון הציבור במערכת ההתרעות, התרעה צריכה להיות באמינות גבוהה, ולהשמע בכל מצב בו סביר להניח שיישמע בעקבותיה קול פיצוץ.

- בכדי להבטיח שהציבור מבין את משמעות ההתרעות לידיעה (שאינן בגדר סיכון עבורו), ובכדי למנוע תגובה היסטורית של הציבור, ההתרעה צריכה לכלול אינדיקציה של רמת הסיכון.
- בכדי להבטיח התנהגות בטיחותית של הציבור, ההתרעה צריכה לכלול הערכה של הזמן שנותר עד לרגע הפיצוץ.

הצעת פתרונות והוכחת היתכנות

פתרונות המאפשרים השמעת מידע לגבי הרלבנטיות, רמת הסיכון והזמן שנותר עד לרגע המפגע קיימים בתצורות שונות, כמו, בכריזה בערוצי רדיו, בתקשורת סלולרית, באמצעות ביחידות כריזה בבתים (כגון, במקומות המועדים לסופת טורנדו) ועוד. את הערכת הזמן עד לרגע המפגע ואת רמת הסיכון ניתן לקדד להבטחת תפיסה נכונה, על ידי שינוי תדר ועוצמת הקול, והמרווח בין האותות (דוגמת השיטה הנהוגה בהתרעות בנהיגה לאחור).

תיכון ומימוש

בעקבות הלקחים, פיתח פיקוד העורף מערכת חדשה, המסננת את ההתרעות על פי תחזית של מקום של מקום נפילת הטילים ([קישור למאמר](#)). כמו כן, במערכת החדשה, פיקוד העורף פירסם מידע לציבור לגבי הזמן הממוצע מרגע ההתרעה ועד לפיצוץ ([מפה](#)).

ככל הנראה, רמת הדיוק בהערכת הזמן בשיטה זו אינה מספקת. אצל מרבית האנשים, קיים קושי להעריך את הזמן שעבר מתחילת ההתרעה, כאשר הם נמצאים בסכנה. כפי הנראה, במבצע "עמוד ענן" היו נפגעים בציבור כתוצאה מישום שיטה זו ([קישור למקרה כזה](#)). יש לקוות שבעתיד פיקוד העורף ימצא דרך למימוש התרעת הזמן הנותר בזמןאמת, באופן שיאפשר לציבור לדעת כיצד עליו לנהוג ([קישור למאמר](#)).