פברואר 2024

שילוב הנדסת אמינות ובטיחות בהנדסת מערכות

דווח על ממצאי מחקר במרכז גורדון, 2023

דר' שרון שושני תבורי,טכניון,ערן פלג,מטאפור,דר' אביגדור זוננשיין,מרכז גורדון להנדסת מערכות
ומוסד שמואל נאמן, בשיתוף:אולגב גלפשטיין,מידבר 21,דר' טניה שוירץ,רפאל, אור נדלר,רפאל

רקע

הנדסת אמינות ובטיחות מיושמות באופן מסורתי בפיתוח מערכות מורכבות למשימות בהן פרמטרי האמינות והבטיחות הם בעלי חשיבות חיונית,כמו: מערכות צבאיות וביטחוניות, מערכות חלל, מערכות אויוניקה, מערכות אוטומטיביות, מתקני גרעין, מתקנים בעלי היבטים סביבתיים ועוד. פעילויות הנדסת אמינות ובטיחות מבוצעות על ידי מומחים לכך, וכוללות בין השאר: גיבוש מודל אמינות ובטיחות,ניתוח אופני כשל בעלי משמעויות אמינותיות או בטיחותיות, תכן לאמינות ובטיחות בשיטת שונות, גיבוש ויישום ניסויי הדגמת אמינות (כמו מבחני אוך חיים). פעילויות אלו אמורות להשתלב בפעילויות הנדסת מערכת שמבוצעות בפרויקטי פיתוח מערכות מורכבות שהוזכרו לעיל. למרות חיוניות השילוב של הנדסת אמינות ובטיחות בהנדסת מערכות, במקרים ובארגונים רבים השילוב הזה הוא חלקי ולא אופטימלי. אחת המטרות העיקריות של מחקר זה היא לגבש מתודולוגיה סדורה ואפקטיבית של שילוב הנדסת אמינות ובטיחות בהנדסת מערכות מבוססת מודלים. יישום הנדסת מערכות מבוססת מודלים היא מרכיב חשוב יישום הנדסה דיגיטלית כיוזמה של משרד ההגנה האמריקאי וגם כפועל יוצא מהמהפיכה התעשייתית הרביעית (תעשייה 4.0).

בעבודת מחקר זו גיבשנו לא רק את מתודולוגיית השילוב בהנדסת מערכות מבוססת מודלים,אלא גם זיהינו פערים נוספים ביישום הנדסת אמינות ובטיחות ונתנו לרובם פתרונות מתאימים.

מטרות המחקר

מטרות המחקר גובשו רובן בתחילת המחקר על פי ניסיוננו ,ניסיון אלו העוסקים בהנדסת אמינות ובטיחות והנדסת מערכות,ועל פי סקר ספרות בנושא. במסגרת זו זוהו הפערים הקיימים ביישום הנדסת אמינות ובטיחות בסביבה מבוססת מודלים:

- בחינה וגיבוש מתודולוגיות מבוססת מודלים להנדסת אמינות ובטיחות
- ניתוח וגיבוש מתודולוגיית ניתוח אופני כשל אמינותיים (FMEA-Failure Modes & Effects Analysis) על בסיס פרופיל RAAML (Risk Analysis & Assessment Modelling Languageשגובש לאחרונה על ידי ה OMG (OBJECT MANAGEMENT GROUP)
- ניתוח וגיבוש מתודולוגיית ניתוח בטיחות מבוססת מודלים באמצעות יישום מתאים של מודל STPA - System Theoretic Process Analysis
- זיהוי פערים מוכרים בניתוחי אמינות ובטיחות, ומתן מענה מתאים לפערים אלו באמצעות שיטות מבוססות מודלים
- הדגמה ובחינה של שיטות נבחרות לניתוח אופני כשל וניתוח בטיחות

הנדסה דיגיטלית ו MBSE

הנדסה דיגיטלית גובשה לראשונה במסגרת המהפיכה התעשייתית הרביעית (תעשייה 4.0) שכללה טרנספורמציה דיגיטלית נרחבת. ב 2018 משרד ההגנה האמריקאי על אסטרטגיית הנדסה דיגיטלית

שמשמעותה שתהליכי התכן ימומשו במתודולוגיות ושיטות דיגיטליות מבוססות מודלים כמוצג בתרשים הבא:.

המרכיב העיקרי באסטרטגית הנדסה דיגיטלית הוא קיום מקור מוסמך של האמת-

Authoritative Source of Truth (ASoT) שמשמעותו שזהו מרכז המידע והנתונים הקיימים ,הנכונים ,מקושרים ומתואמים עבור המודלים של ניהול, תכן,יצור,תמיכה ותפעול המערכות בכל הדיסיפלינות. כאמור כל תחום וכל דיסיפלינה מתבטאת ומתנהלת באמצעות מודלים מתואמים.כמובן, זה מסביר את החשיבות של שימוש בהנדסת מערכות מבוססת מודלים MBSE.למרות זאת, יש לציין שבמציאות הנוכחית,גם אם כל דיסיפלינה ותחום משתמשים במודלים,היא עושה זאת בכלי ייעודי בלתי מקושר.

קבוצת ה OMG שהוזכרה לעיל היא קונסורציום וקהילה האחראים על התקנים לשפות המידול השונות לתעשיות ולשימושים השונים, כמו UML עבור עולם התוכנה ו SYSML לעולם המערכות. בשפות מידול אלו יש אפשרות להתאמה (הרחבה או צמצום) לתחומים שונים באמצעות פרופילים. פרופיל ה RAAML התווסף לאחרונה למידול בעולמות האמינות ובטיחות.פרופיל זה מאפשר לנו את השילוב של הנדסת אמינות ובטיחות בהנדסת המערכות.

פערים עיקריים בשילוב הנדסת אמינות ובטיחות בהנדסת מערכות

פערים אלו מזוהים מהניסיון בתעשייה ומדווחים בספרות הרלוונטית:

- אין בסיס מידע משותף ASoT

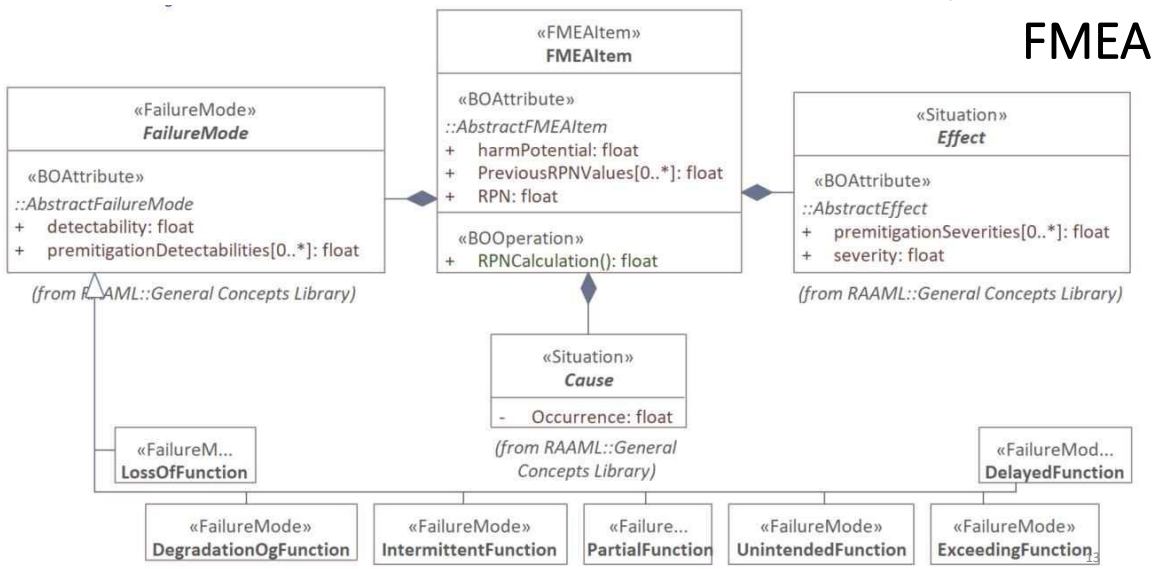
- הגדרת המערכת שונה בהנדסת מערכות ובניתוחי אמינות ובטיחות,כלומר חישובי וניתוחי האמינות והבטיחות אינם מתייחסים למערכת הקיימת בפועל,פער זה גורם לחלק מניתוחי אמינות לא להיות רלוונטיים לתכן המערכת
- הנדסת אמינות ובטיחות לא משולבת מספיק בהחלטות המערכתיות,מצב זה נובע הן מאי הרלוונטיות המצויינת בסעיף הקודם והן מהאי ההכרות של חלק מקבלי ההחלטות עם משמעויות ניתוחי האמינות
- הממשקים בין המערכות והאינטראקציות עם הארגונים בהם מופעלת המערכת ועם המתפעלים והמשתמשים אינה נלקחת בחשבון בניתוחי האמינות והבטיחות.מניתוח תקלות ואסונות משמעותיים מסתבר שבמקרים רבים היבטים אלו הם גורמי השורש לתקלות ולאסונות
- תרבות ניתוחי האמינות והבטיחות שונה בין ארגונים ותעשיות, ומקשה להפיק תובנות משותפות מממצאי ניתוחים אלו
- יש צורך לא ממומש במידה מספקת של סימולציות בניתוחי אמינות ובטיחות

בעבודת מחקר זו פעלנו לתת פתרונות ראויים לפערים אלו על ידי יישום והדגמת שימוש בניתוחי אמינות ובטיחות מבוססי מודלים.

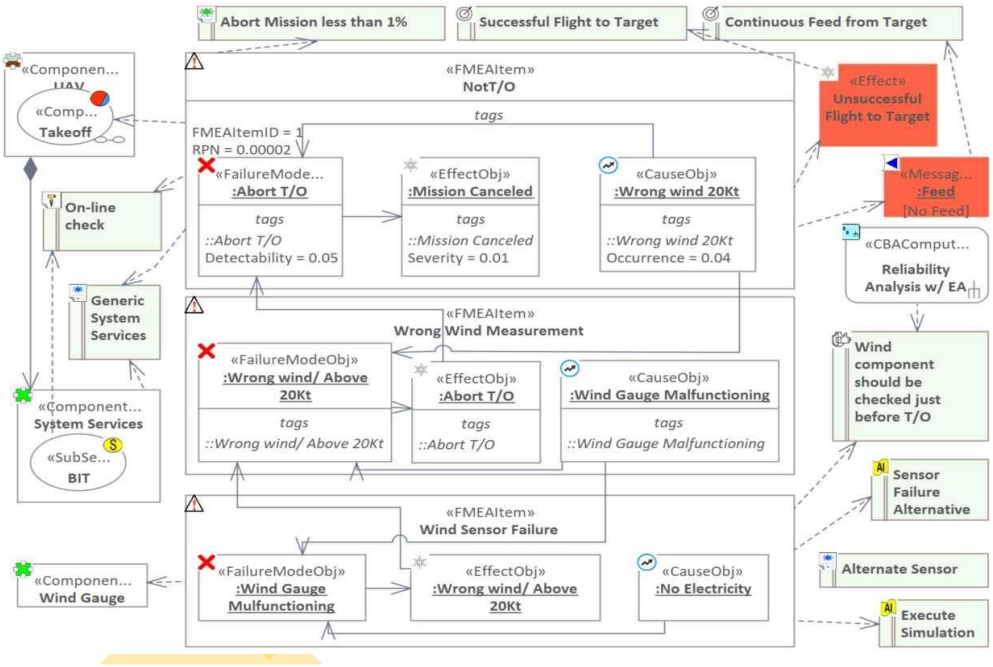
ניתוח אופני כשל אמינותיים FMEA מבוססי מודלים

כאמור פרופיל ה RAAML מאפשר לבצע ניתוח אופני כשל במערכות המפותחות באמצעות MBSE. יישמנו והדגמנו שימוש בפרופיל ה RAAML וקיבלנו ניתוח מתאים. היישום וההדגמה מוצגים בשני התרשימים הבאים. בניתוח זה הוספנו גם את הממשקים בין המערכות,ואת האינטראקציות עם הארגונים ועם גורמי האנוש המתפעלים והמשתמשים. בכך סגרנו למעשה את רוב הפערים שצויינו לעיל.

RAAML עבור FMEA



דוגמת שימוש



ממצאים מיישום FMEA מבוסס מודלים

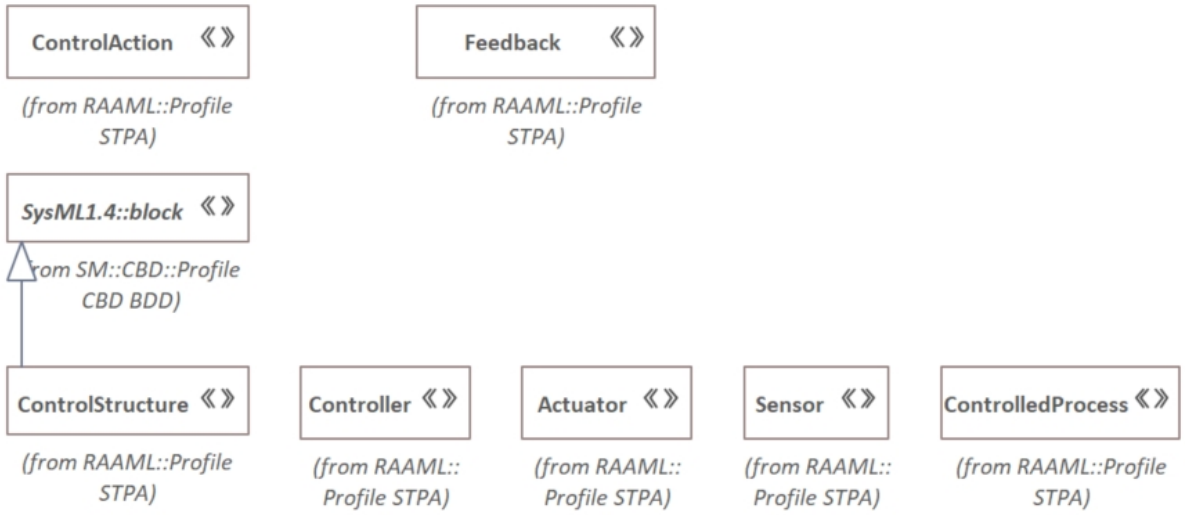
בהתאם לפערים שזוהו לעיל ובמהלך הניתוח בפועל בעבודת המחקר גובשה מתכונת עבודה משותפת בין מהנדסי המערכות ומהנדסי האמינות, וגובשו אסטרטגיות עבודה משותפת מותאמת שלב. זוהו והוצגו ערכים מוספים למהנדסי אמינות,כמו:

- מודל אמת מערכתי אחוד
- קישוריות למודל המערכת מאפשרת ניתוח שיטתי ועדכני וכיסוי מלא
- שילוב הממשקים (ארגוניים ואנושיים) השונים בניתוחי האמינות הרחיב והעמיק את אפקטיביות ניתוי האמינות
- הכנסת תוצאות ניתוחי האמינות למודל מביא לשילובן במעגל הדרישות, ומהווה תשתית למעקב טיפול ויישום המלצות לשיפור
- שיפור ביכולת הבנת של אימפקט שינויים במערכת ובמודל
- הקטלוג הקיים בכלי המידול מאפשר שימוש חוזר לפריטי ניתוח וגם לתבניות שלהם

ניתוחי בטיחות מבוססי מודלים

בפרופיל RAAML בחרו את מתודולוגיית STPA מבית מדרשה של פרופ' ננסי לווסון כמתודולוגיה לניתוחי בטיחות. להערכתנו זו בחירה נכונה, כיוון שה STPA נוקט גישה מערכתית להנדסת בטיחות וניתוח בטיחות. בניתוח זה מתייחסים לכל מרכיביה כולל הממשקים,גורמי האנוש והארגונים המעורבים במערכת. ניתוח הבטיחות מאתר את הגורמים לתקלות באמצעות מודלי בקרה סיבתיים. לעומת זאת תקני הבטיחות הבינלאומיים שמנחים ניתוח בטיחות ליניארי המתייחס רק לתקלות ברכיבים כגורמי כשל שעלולים להביא לתקלות בטיחות. לכן מתודולוגיית STPA מתאימה להיות פרופיל לניתוחי בטיחות מערכתיים.

בעבודת מחקר זו ניתחנו והדגמנו את פרופיל ה STPA ב RAAML לניתוחי בטיחות ולהנדסת בטיחות,שהמבנה שלו מתואר בתרשים הבא:



מהניתוח שלנו נראה שנדרשת עוד עבודה התאמה כדי שפרופיל ה STPA כפי שממומש ב RAAML יתאים לניתוחי בטיחות מערכתיים.

סיכום ומחשבות קדימה

עבודת מחקר זו שבוצעה על ידי צוות משולב של 3 חוקרים ממרכז גורדון בטכניון, ו 3 מומחי אמינות ובטיחות מהתעשייה הניבה תוצאות ותובנות מעניינות. פרופיל ניתוח אופני כשל עובד יפה במסגרת RAAML ומממש את הציפיה לניתוח מערכתי שלם ועדכני במערכות המפותחות בעזרת MBSE. גם פרופיל ניתוחי בטיחות במודל STPA עושה את העבודה,אבל צריך עדיין לסגור פערים.

יש צורך בשילוב אוטומציה ביישום הפרופילים של ניתוחי אמינות ובטיחות, כדי להקל ולהנגיש פרופילים אלו למהנדסי אמינות ובטיחות.

העבודה האינטגרטיבית בין מהנדסי המערכות ומהנדסי אמינות ובטיחות הוכחה כאפשרית ומאפשרת ניתוחי אמינות ובטיחות מערכתיים נכונים ושלמים יותר, על המערכת המפותחת בסביבת MBSE.

פרטים מלאים על המחקר וממצאיו מוצגים במאמר להלן שהכנו לסיכום מחקר זה וכולל גם את המאמרים והספרות התומכת.שילבנו מאמר זה גם באתר מרכז גורדון. הציפיה היא שארגונים יאמצו MBSE ושמהנדסי אמינות ובטיחות יחד עם הארגון שלהם יאמצו את פרופיל RAAML לניתוחי אמינות ובטיחות. נשמח לסייע לארגונים ומומחים המעוניינים בכך.

INTEGRATING REIABILITY & SAFETY ENGINEERING in the MODEL BASED SYSTEMS ENGINEERING- a critical implementation review

Dr. Sharon Shoshany Tavory, Technion, Eran Peleg, Metaphor, Dr. Avigdor Zonnenshain, The Gordon Center for Systems Engineering, Technion, Olga Gelfestein-Westfried, Midbar 21 Ltd, Dr. Tanja Schwierz, Or Nadler, RAFAEL Ltd