

אפיון הפתרון ומימושו

האפיון המערכתי הוא השלב הסופי של תהליך ייזום והיערכות למימוש הפרויקט. האפיון מתאר את החלופה שנבחרה למימוש לאחר ניתוח הצורך ובחינת מרחב החלופות האפשריות.

הכנת האפיון המערכתי והעבודה מולו הן אחת המשימות המרכזיות של מהנדס המערכות. אפיון מערכתי מגדיר את הביצועים של המערכת, תצורתה ואופן פעולתה, לצד נושאים כמו בטיחות, אחזקה ועוד, שנדרשים להיות משולבים היטב בתהליכי התכנון והנדסת המערכות. באפיון מערכתי יש תחומי ידע רבים שמהנדס המערכות נדרש להתייחס אליהם: אמינות, אבטחת מידע, איכות הסביבה, חיים בצוותא, בטיחות, אחזקה, זמינות ותחומים רבים נוספים.

מהנדס המערכות איננו בהכרח מומחה תוכן או מתמצא בכל אחד מנושאים אלו. אולם נושאים אלו הם חשובים להצלחה של המערכת, לא פחות מהדרישות הפונקציונליות. האתגר הגדול של מהנדס המערכות הוא בשילוב עבודה של מומחים רבים בהתאם לתחומי אחריותם. התוצר הסופי נדרש להיות אפיון מערכתי ברור, תמציתי ועקבי שיאפשר לקבל מוצר המתאים לדרישות ובאיכות גבוהה.

מסמכי הפרויקט

מסמכי הפרויקט, או מסמכי ההתקשרות, שונים במבנה ומתכונת בין תחומים שונים. באופן עקרוני הם כוללים את המסמכים האלה:

1. החוזה או מסמך ההזמנה מגדיר נושאים משפטיים וכספיים, כמו תנאי תשלום, אופן התשלום, ביטחונות, הצמדות וכדומה;
2. האפיון המערכתי מגדיר את ה"איך", כלומר את הדרישות המערכתיות והאופן שבו המערכת תבצע את משימתה: הביצועים הנדרשים של המוצר;
3. מסמך תכולת עבודה - מגדיר את ה"מה" וה"מת": כמויות, מועדי אספקה, תהליך הפיתוח, אבני דרך ועוד.

נהוג שההזמנה או החוזה קובעים את התכולות המרכזיות ומפנים להרחבה למסמכי אפיון. המסמכים מופיעים לעיל על-פי סדר הקדימות הנפוץ למקרה של סתירה ביניהם. בדרך כלל החוזה הוא בעל הקדימות הגבוהה ביותר ומסמך תכולת עבודה - sow - הוא האחרון בסדר הקדימות.

תהליך הכנת האפיון

תהליך של אפיון מערכתי, בוודאי עבור מערכת מורכבת או מערכת של מערכות, הוא משימה מורכבת. נושא מרכזי בהכנת אפיון הוא הבנה של הצורך והדרישות המערכתיות בהתאם לסביבת ההפעלה ולדרישות בעלי עניין. לצד זאת נדרש להגדיר היטב את הביצועים של המערכת ואופן בדיקתם, אך לא פחות חשוב מכך, את כלל הנושאים הנלווים - זמינות, אמינות, אמצעים לאחזקה ולאיוונים ועוד.

לפיכך יש להתייחס לכתיבת האפיון כאל פרויקט בפני עצמו. היעד בפרויקט כתיבת האפיון הוא מסמך מקיף ואיכותי. אבות הטיפוס הם הטיוטות להתייחסות. אבני הדרך על-פי לוחות הזמנים הם, למשל דיוני סטאטוס והצגה לבכירים. מלבד שעות העבודה של מהנדס המערכות לעיתים נדרש גם תקציב ממשי למשימה, בעיקר אם האפיון נעשה בשילוב מומחים חיצוניים.

אפשר להסתכל על מסמך האפיון המערכתי כעל מוצר בפני עצמו. האפיון כולל הגדרה מקיפה של מוצרים

או שירותים לפיתוח או רכש. מכאן שאפיון מובנה, מקיף, ממוקד ואיכותי הוא הכרחי לתכן של מוצר המביא את הערך הדרוש ללקוח. לדוגמה, פעמים רבות משרדי ממשלה, ארגונים ביטחוניים וגם חברות פרטיות מפתחים ומייצרים המערכות נדרשות באמצעות ספקים חיצוניים. אם האפיון לא יתאר היטב את הנדרש מהמערכת - המערכת שמפותחת בחברה חיצונית כנראה לא תתאים לייעודה.

אפשר להמשיך את האנלוגיה של האפיון המערכתי למוצר באמצעות סקירת מחזור החיים שלהם. בתהליך הפיתוח מוצר נהוג להבחין בשלבים של הגדרת דרישות, תכן, ייצור, בחינה ואחזקה. גם באפיון מערכתי מתקיימים שלבים דומים. למשל שלבי התכן והייצור בהקשר למסמך האפיון הם שלבי החשיבה, ההיערכות והכתיבה. שלב הבחינה הוא תהליך אישור המסמך ווידוא עמידה בכל הדרישות של בעלי העניין השונים. שלב האחזקה הוא שלב השינויים וההתאמות של מסמך האפיון לפני הפרויקט ובמהלכו, כתוצאה משינויי דרישות או אילוצים טכניים.

מומלץ להתחיל את האפיון המערכתי מדף חלק או מתבנית ריקה, ולא על בסיס אפיון קודם או חומרי רקע. רק לאחר שמגבשים באופן ראשוני את הדרישות הפונקציונליות המרכזיות ומבנה עקרוני, ניתן לשלב חומר קיים, לרכז נושאי מעטפת ועוד.

הדרך ההפוכה - "דרך הקיצור" שהיא התחלה מאפיון דומה או קודם וביצוע שינויים והתאמות - עשויה להתגלות בסופו של דבר כדרך ארוכה יותר שגם לא תביא לתוצר הרצוי. אפיון מערכתי נעשה הרבה פעמים למערכות השונות מהותית מהקיים, ואלמלא כן לא היה צורך בכתיבת מסמכים חדשים. אם מתחילים ממסמך קיים, רב הפיתוי לשנות מעט ככל האפשר ולהיצמד להגדרות ישנות ולמבנה הישן של המערכת. זאת דרך בטוחה לאבד בסופו של דבר חלק מהיכולות הנדרשות במערכת החדשה. במקרים רבים אם מתחילים מאפיון ישן, מזהים את הבעיה בשלב כלשהו במהלך העבודה, ואז מתחילים מ"דף חלק", אך כבר לאחר שהושקעו זמן ומאמץ לחינם.

הכנת אפיון למערכת שאינה טריוויאלית מחייבת ריכוז של כלל החומר הזמין והתייעצות עם גורמים מקצועיים רבים. כאמור, אפיון המערכת כולל נושאים מגוונים שאינם בהכרח בתחום ההתמחות הספציפי של מהנדס המערכות. לכן חשוב להתייחס לכל ההיבטים במידת האפשר על בסיס חומר מקצועי עדכני ומומחי תוכן לנושא. מלבד נישות מקצועיות ספציפיות בתחומי ביצועים ותכונות, כמו סייבר, חומרים וכדומה, הדבר אמור גם לנושאי "מעטפת", כמו בטיחות, בדיקתיות וכדומה.

אופיון ביצועים מול מפרט טכני

קיימות שתי גישות עקרוניות להגדרת מערכות: אופיון ביצועים מול מפרט טכני (באנגלית: Build to Spec vs. Build to Print).

אופיון ביצועים מגדיר את הביצועים שנדרשים מהמערכת ולא את הפתרון הטכני. במקרה כזה האחריות לפיתוח המערכת ועמידתה במשימות שהוגדרו באופיון, מוטלת על הספק.

מפרט טכני, לעומת זאת, כולל הגדרה מדויקת של השרטוטים והדגמים הנדרשים. במקרה זה כל עוד המוצר עומד במה שהוגדר במפרט, מוטלת האחריות לתקינות ולשמישות של המערכת על הלקוח שפיתח את המוצר והעביר את מפרטי הייצור לספק.

אופיון ביצועים אינו כולל פרטים טכניים שהספק יפתחם ויגדירם בשלב המימוש. בפרויקטי פיתוח נחוץ לרוב שהספק יקבל את האחריות המלאה לתכן ולעמידה של המערכת הסופית במתאר הפעולה הנדרש, ולכן עיקר האופיון הוא על בסיס ביצועים. בה בעת אם לא מגדירים במדויק, למשל את דגם המחשב, אלא מגדירים את הביצועים הנדרשים וממדי המארז - פרטים המתארים את מתאר הפעולה, האחסנה ועוד - מקבלים

דגמים ומידות שונים ממה שהתכוונו. לכן אם נדרש ציוד מסוג מסוים ומפורש, למשל לצורך תאימות עם מערכות קיימות מאותו סוג ודגם, יש להגדירו בצורה מפורשת (מפרט טכני) ולא באמצעות אופיון ביצועים.

מכשולים באפיון - אפיון יתר ואפיון חסר

שתי מכשולות גדולות הקיימות בכתובת האופיון הן אפיון יתר ואפיון חסר. אפיון יתר כולל מספר רב של פרטים טכניים ואינו מאפשר פתרונות שונים ויעילים יותר. אפיון יתר מוביל לאופיון מקיף וסבוכה המתבטא בסופו של דבר גם במוצר יקר ומסורבל. סיכון נוסף בדרישות רבות ומפורטות הוא הצורך בשמירה על עקביות הדרישות מול השינויים באופיון לאורך הזמן. יש לשים לב שאפיון יתר אינו דומה להגדרת דרישות שאפתניות או אתגריות, והוא יכול להופיע גם בדרישות לרכש מוצרים פשוטים ויומיומיים.

אפיון חסר אינו כולל פרטים ואילוצים חיוניים לפעולת המערכת. פשטות היא ערך חשוב שעשוי להוזיל את המוצר, אך לא על חשבון אי מיצוי דרישות ומאפיינים. במונח אפיון חסר אין כוונה לציין שהדרישות הן "חלשות" או נמוכות ממה שאפשר להשיג.

מהי דרישה טובה?

דרישה טובה היא דרישה המובנת היטב לקורא האופיון, והבנתו הולמת באופן מלא את כוונת הכותב. יש כמה מקורות המגדירים את המצופה מדרישה טובה. אחד מהם הוא תקן iso-iec-ieee-29148:2011 שמגדיר בסעיף 5.2.5 מאפיינים של דרישות טובות. בטבלה להלן נביא פירוט לנושא עם התאמות, עדכונים ודוגמאות למערכות באופן כללי:

מס'	מאפייני דרישה טובה	תיאור
1.	מדויקת מול צורך	מתארת מאפיין או גודל שנגזר מהמשימות או התרחישים שהמערכת צריכה לקיים. לדוגמה: "האפליקציה תאפשר קבלת התרעה על אירוע חירום ברדיוס של 300 מטר מהמכשיר".
2.	ברת בדיקה ואימות	הדרישה תהיה מנוסחת כך שניתן יהיה לבדוק האם המערכת עומדת בה או מקיימת את המבוקש בניסוי, הדגמה, אנליזה או בחינה. לדוגמה: "הטיל יפגע באזור בגודל של 1x1 מ' ממרחק 3 ק"מ בהסתברות של 90%".
3.	מוגדרת היטב	<p>הדרישה תוגדר חדמשמעית כאחת מאלה:</p> <ol style="list-style-type: none"> 1. דרישת סף מחייבת; 2. דרישת MUST (חייבת באישור לקוח במקרה של חריגה); 3. דרישה אופציונלית (בקשה בגדר NICE TO HAVE); 4. תיאור, רציונל, הסבר. <p>לדוגמה:</p> <ol style="list-style-type: none"> 1. (תיאור): המארזים מיועדים לאחסון ואיסוף ציוד. 2. (דרישה מחייבת): המארז ייוצר בישראל. 3. (דרישת MUST): מספר המארזים לא יעלה על 4. 4. (דרישה אופציונלית) בעדיפות - מספר המארזים לא יעלה על 3.
4.	מנוסחת היטב	מובעת בניסוח החלטי בגוף שלישי בזמן עתיד. לדוגמה: "המערכת תחשב YYY".
5.	חדערכית	<p>דרישה אחת בכל משפט. לדוגמה:</p> <ol style="list-style-type: none"> 1. "המערכת תורכב משלושה מכלולים. 2. שלושת המכלולים של המערכת יעמדו בגשם לפי מפרט xxx. 3. שלושת המכלולים של המערכת יעמדו בפרופיל נסיעה לפי מפרט YYY".
6.	חדמשמעית	<p>לא ניתנת לפרשנות ולא משתמעת לשתי פנים. לדוגמה:</p> <ol style="list-style-type: none"> 1. "המערכת תעמוד בתקני הנדסת אנוש xxx". 2. "ההסתברות לתקלה קטסטרופלית במערכת תהיה נמוכה מ-1 ל-10⁶".
7.	עקבית	אינה סותרת דרישות אחרות במסמך.
8.	כמותית	כוללת פרמטר מספרי שמולו ניתן לבצע את התכן והאימות. לדוגמה: "המבנה יכיל חדר הרצאות עם 40 כיסאות. הכיסאות יסודרו ב-4 שורות של 10 כיסאות בכל שורה". (בהמשך יופיע פירוט דקדקני לכלל הפרטים הרלוונטיים).
9.	שלמה	כוללת את כל הפרטים הנדרשים. לדוגמה: "הגובה הכולל של המערכת (מבסיס הזחל עד קצה האנטנה) יהיה 1.80 מ'".

כדי להבין טוב יותר כיצד לנסח דרישות טובות, חשוב ללמוד לזהות ולנתח דרישות שאינן מתאימות לקריטריונים. להלן דוגמאות לדרישות בניסוח טעון שיפור עם הסברים לטעויות בהגדרת הדרישה:

מס'	דוגמאות לדרישות לקויות	הסבר לטעויות בהגדרת הדרישה
1.	"על החברה לעמוד בתקני איכות פנימיים"	מיותר מול חברה שממילא אמורה לעמוד בתקנים של עצמה, גם בלי שהלקוח יכתוב לה זאת. מיותר עוד יותר בשלב המכרז, כאשר לא ברור מה תהיה החברה ומהם הנהלים בה.
2.	"המערכת תהיה בטיחותית לשימוש"	לא ניתן לבדיקה. האם הכוונה לשימוש על-ידי מפעיל מיומן או אולי על-ידי כל עובר אורח? מה זמן ההכשרה? מה קריטריון הבטיחות?
3.	"המערכת תתוכנן למינימום סיבוכיות"	כנראה שאין הרבה מערכות שמתוכננות בכוונה תחילה להיות מורכבות או מסובכות. מאחר שהסיבוכיות אינה מוגדרת, הספק יוכל לטעון שלשיטתו המערכת פשוטה ביותר ולהתעלם מהדרישה.
4.	"המכלול יהיה תואם לתקני הנדסת אנוש מקובלים"	כותב האופיון כנראה אינו בקי בתקני הנדסת אנוש ומנסה להעביר את הטיפול בנושא לספק. לאיזה חלק במערכת מתייחסים? מהם התקנים האמורים?
5.	"למוצר נדרש אישור לבטיחות פעולה באתר הרס"	בטיחות באתר הרס אינה מוגדרת היטב, ובין היתר לא ידוע על מעבדה המוסמכת באופן ייעודי לנושא. האם הסכנה היא נפילה, התחשמלות או סכנה אחרת?
6.	"יש להשתמש בפרוטוקול סטנדרטי".	חברות רבות משתמשות בפרוטוקולים סטנדרטיים או מקובלים מבחינתן שהם פנימיים או חסויים, כלומר אינם מפורטים ואינם נגישים. מהם הפרוטוקולים הסטנדרטיים מבחינת כותב האופיון?
7.	"המערכת תופעל בצורה פשוטה וקלה"	קשה למצוא ספק שמתכנן מערכת להפעלה מסובכת וקשה. ניסוח חליפי לדוגמה: "ההפעלה תהיה באמצעות 2 פעולות לכל היותר", "המערכת תופעל באמצעות מסך מגע", "התפריטים יהיו בעברית".

לאחר סיום כתיבת האופיון, יש כמה שאלות מנחות שיעזרו להעריך את איכות המסמך ובהירותו. אם התשובה לאחת השאלות היא חיובית, נדרש לעדכן את המסמך ובמידת הצורך חלקים נוספים הקשורים לאותה דרישה. השאלות הן אלה:

1. האם המערכת שאופיינה מתאימה לדרישות הלקוח?
2. האם האפיון מכיל את כל המידע הנדרש לספק?
3. האם ניתן לבדוק את כל הדרישות?
4. האם יש דרישות המגבילות את מרחב הפתרונות?

5. האם כל הדרישות הן הכרחיות?
6. האם יש דרישות הפוגעות באמינות או באחזקת המערכת? האם דרישות אלו נחוצות?
7. האם יש סתירות בדרישות?

אפיון מערכתי - מבנה ותכנים

קיימות כמה תצורות לאפיון מערכתי. בפרויקטים קטנים או בשוק הפרטי אפשר לפגוש אפיונים מינימליים, אפילו של 3 עד 5 עמודים. לעיתים מסמכים אלו כוללים בתוכם גם את החוזה ואת ה-SOW. באותה מידה במסמכי אפיון של מערכות מורכבות רק תוכן העניינים, הקדמות, תיאורים ותקצירים יכולים להתפרס על עשרות עמודים והאופיון בפני עצמו יכול להיות מחולק למסמכים רבים. המבנה הכללי של האופיון שאנו מציגים כאן מבוסס בין היתר על תקן MIL-STD 961E ומתודולוגיית החטיבה הטכנולוגית ליבשה בצה"ל (חט"ל). המבנה העיקרי כולל שישה פרקים ראשיים, ואלה הם:

1. פרק כללי;
2. הגדרות ומסמכים ישימים;
3. דרישות טכניות;
4. דרישות אימות ביצועים;
5. דרישות למסירת המערכת;
6. הערות.

הנושאים המרכזיים המטופלים באפיון המערכתי הם נושאי דרישות ביצועים ואימות של המערכת (פרקים 3 ו-4). לפני פרקים אלו מופיעים נושאי רקע והקשרים נדרשים לצורך הדיון במערכת (פרקים 1 ו-2). לאחר הפרקים המרכזיים מצויים נושאי מסירה של המערכת והערות כלליות (פרקים 5 ו-6). להלן נביא תיאור קצר של נושאים מרכזיים בפרקים השונים. בתיאור להלן אין כוונה לנתח לעומק את כלל ההיבטים הרלוונטיים לכל סוג מערכת. קרוב לוודאי שאפיון של מערכת מורכבת ידרוש הרחבה בהיבטים רבים שלא התייחסנו אליהם. בנוסף, כל תחום או סעיף הוא מקום לידע וניסיון ארוך שנים ואין הכוונה למצות כאן את הדיון על הנושאים השונים. מטרת ההצגה היא סקירת עיקרי התחומים המדוברים בהקשר לשאר סעיפי האופיון ומתן הנחיות מעשיות לדרישות רלוונטיות.

פרק כללי

בפרק זה מובא תקציר מנהלים המציג את המידע הנדרש להבנת הצורך בפרויקט ועקרונות המוצר הנדרש. זהו פרק חשוב להגדרה ולמיקוד המערכת. לעיתים זהו פרק שמגיע לבעלי עניין בכירים, ולכן והתיאור בו נדרש להיות תמציתי וממוקד.

התיאור מתחיל בדרך כלל בהצגת רקע, מצב קיים, ניתוח הבעיה והפער המערכתי שבגיננו נדרש הפיתוח או הרכש. לאחר מכן מוצג ייעוד המערכת ואופן פעולתה בסביבה המבצעית או מול תרחישים עיקריים. לאחר מכן מגיע שלב של תמצית פרטים מערכתיים מרכזיים ותתי-מערכות על-פי הצורך. לבסוף מוצגים פרטים או שיקולים נוספים היכולים להיות רלוונטיים עבור המערכת ומקבלי החלטות. למילים יש כוח רב, ולכן התיאור צריך להיות ממוקד ומובחן. לדוגמה, להלן שני קטעים מתוך תקצירים

העוסקים בנושא תחבורה עתידית הכוללים תיאור רקע, התייחסות למצב קיים והפער המערכתי שהמערכת מיועדת למלא.

1. נפח התחבורה העולה בשנים האחרונות אינו מאפשר עוד שימוש ברכב מאויש בתצורה המוכרת. המערכת מהווה אמצעי נידות אוטונומי, אישי, קומפקטי ובטיחותי בעלות שתאפשר תפוצה רחבה.
2. מערך התחבורה הקיים הוא בלתי יעיל - רוב הזמן הרכבים אינם בשימוש וחונים ליד הבית או בעבודה. המערכת מאפשרת אוטומציה גלובאלית של מערך התחבורה והקטנה של שטח החנייה הנדרש על בסיס אפליקציית שיתוף רכבים, ללא צורך בשינוי כלשהו ברכבים הקיימים.

כפי שנראה משתי הפסקאות מעלה, משפט או שניים מספיקים כדי להציג בצורה מובנת ותכליתית את המערכת. אולם התיחום הניתן לפרויקט הוא שונה לגמרי בשני התיאורים. בסך הכול כמה עשרות מילים מכוונות את המערכת למקומות שונים מאוד: בפסקה הראשונה מדובר על אמצעי פיזי לניוד מתקדם ובפסקה השנייה מדובר על אפליקציה.

תיאור ממצה וקצר של המערכת ניתן לעשות בשלושה חלקים בדומה למודלים לכתובה מדעית.²⁸ כל חלק עשוי לכלול משפט או שניים בהתאם לצורך:

1. **תיאור הרקע או המצב הקיים** תוך הדגשת חשיבות הנושא או פרטים על המערכות והשיטות הקיימות;
 2. **תיאור הפער או הצורך במערכת לעיתים תוך השוואה למצב הקיים**;
 3. **הגדרת תפקיד המערכת והמצב החדש** - אופן מילוי הפער או יכולות מרכזיות. דוגמה לתיאור מערכת מידע לטכנאים לפי מודל זה:
1. ביצוע פעולות אחזקה מחייב דיווח על בסיס טופס מובנה, עבודה בהתאם לנהלי בדיקה ושימוש במידע טכני, ספרות וקטלוגים;
 2. הדיווחים כיום מבוצעים באופן ידני ואינם מאפשרים בקרה יעילה; המידע הטכני אינו זמין כיום לאנשי האחזקה בתנאי שדה, דבר המוביל, בין היתר, להחלפות שווא של מכלולים;
 3. נדרש לפתח מערכת תמיכת ביצועים באחזקה שתאפשר מילוי ממוחשב של טפסי טיפול בסמוך לכלי ויסייעו לטכנאים באיתור תקלות לצד מימוש המעקב אחר זמינות אמצעי הלחימה.

הגדרות ומסמכים ישימים

הגדרות וקיצורים

בפרק זה מובאות הגדרות למונחים וראשי תיבות שמשמשים בהם במסמך. למרות מיקומו בתחילת מסמך האופיון, זה פרק שמוסיפים אותו לקראת סיום הכתיבה (בדומה לתוכן העניינים). הפרק אמור לסייע למקבל האופיון (כלומר, ספק או יצרן), להבין מושגים וקיצורים שייתכן שהם מובנים מאליהם בחברה או בארגון האחראי על האופיון.

בפרק זה יש להגדיר רק קיצורים ומונחים המופיעים במסמך. יש להימנע מהגדרה של מושגים מובנים מאליהם. כמו בכל המסמך, גם בהגדרות ראוי להימנע במידת האפשר משימוש בראשי תיבות. למעט מקרים חריגים, חלק זה אינו אמור להיות ארוך מעמוד אחד. יש לסדר את המונחים והקיצורים על-פי סדר הא"ב.

²⁸ John M. Swales, *Genre Analysis: English in Academic and Research Settings*, Cambridge UP, 1990

על-פי הצורך ניתן להפריד את הפירוט לשתי רשימות - באנגלית ובעברית.

מסמכים ישימים - מסמכים קיימים שהאופיון המערכתי מפנה אליהם, אך הם אינם נכללים בו. נהוג לחלק את הרשימה למסמכים פנימיים, מסמכים חיצוניים ותקנים.

מסמכים פנימיים - מקורם במפעל, בחברה או במשרד של כותב האופיון. דוגמאות למסמכים רלוונטיים הם נהלי הבטחת איכות ותהליכי בחינה, אופיונים משלימים של מכלולים, תתי-מערכות ועוד.

מסמכים חיצוניים - מקורם הוא מחוץ לארגון שאליו משתייך האחראי על כתיבת האופיון ואינם מוכרים כתקן.

תקנים ("סטנדרטים") - מפרטים או שיטות מקובלים שמסתמכים עליהם לצורך אחידות, נוחות או מכורח תקנה או חוק. דוגמאות לתקנים ידועים בתחומי מערכות צבאיות הם MIL-STD 810E (תקן לבדיקות תנאי סביבה) ו-MIL-STD 461C (תקן לתאימות אלקטרו מגנטית). כמובן שקיימים תקנים טכניים רבים כמעט בכל תחום, הנכתבים על-ידי ארגונים כמו ISO, IEEE ואחרים.

אומנם פרק המסמכים הישימים נראה פשוט מאוד, אך קל מאוד גם לטעות בו, והטעות תהיה בולטת מאוד לעין. להלן נפרט כמה שגיאות אופייניות בנושא מסמכים ישימים וההפניה אליהם מהאופיון:

חוסר היכרות עם המסמכים: לפעמים קיימת נטייה לבצע העתקה של החומר ממסמכי אפיון קודמים והדבקה ללא בדיקה. לעיתים מציינים בתחילת הכתיבה מספר רב של מסמכים ישימים כדי לא לשכוח חומר היכול להיות רלוונטי, ואין חוזרים לאחור מכן כדי לוודא סגירות מול תוכן המסמך העדכני. לפעמים רושמים את כל המסמכים הידועים כדי "שהמסמך יראה מקצועי" או "שהספק יחשוב שאנחנו מקצועיים".

אין זה נדיר למצוא אופיונים לרכב ממוגן שמפנים לפרופיל נסיעה של טנקים ושיטות בדיקה של מזגנים ביתיים... קורא המסמך אינו יכול להיות מודע לכוונות הכותב ולגלגולים שעבר המסמך. הקורא מניח שלכאורה המסמך נכתב ונבדק היטב, וכולל מסמכים ישימים משמעותיים ורבי ערך. הכלל הוא פשוט מאוד: אם לא קראת את המסמך הישים - אל תשלבם באופיון. אופיון הכולל שגיאה גסה במסמכים ישימים הוא לכל הפחות מביך ובוודאי אינו נראה מקצועי.

ציון מסמכים שאין אליהם הפניה מהאופיון: אם אין הפניה למסמך בגוף האופיון - המסמך אינו נכלל בדרישות, ולכן הוא מיותר. הדבר מעיד על חוסר תשומת לב של כותב האופיון או על שימוש בתבנית לא רלוונטית.

הפניה שאינה מפורטת למסמכים ישימים: ההפניה למסמך בגוף האופיון נדרשת להיות ממוקדת לסעיף מסוים. דוגמה להפניה ממוקדת: "בדיקת אטימות תבוצע על-פי MIL-STD 810E Method XXX, משך הבדיקה - YYY". במקרים נדירים יכולה להיות הפניה כללית למסמך, כמו עמידה בתקן איכות על-פי ISO 9000:2008. במקרים אלו המסמך הישים עצמו נדרש לכלול פירוט של קריטריונים לתאימות, כלומר אופני האימות והבדיקה לוודא שהמערכת, המכלול או הרכיב תואמים למסמך או התקן. בהיעדר קריטריון תאימות במסמך הישים נדרשת הפניה מפורטת.

מסמך ישים שלא ניתן להעביר לספקים: מסמכים ישימים הם חלק בלתי נפרד מהאופיון ונדרשים להיות מועברים לספקים יחד איתו. לפיכך, אין לציין או להסתמך על מסמכים פנימיים, מסווגים, שאינם זמינים או שלא ניתן להעביר לספקים מסיבה אחרת.

אם מציינים מסמך ברשימת המסמכים הישימים, יש להקפיד לציין את המספר המזהה, המהדורה המחייבת ותאריך הפצת המסמך. כאמור, יש לשלב מסמכים נדרשים בלבד, אשר כותב האופיון מודע היטב לתוכנם ונושא אחריות על הרלוונטיות שלהם לשימוש הספציפי במערכת.

אם נדרשת התייחסות לחלק מהמסמך בלבד, מומלץ לפרטו ולהפנות אליו. אם נדרשת התייחסות לכמות מזערית של מידע מתוך המסמך, מומלץ פשוט לגזור את הדרישות הספציפיות לתוך האופיון ולחסוך מהספק נבירה מיותרת בערימות מסמכים שאין כוונה או צורך להשתמש בהם.

דרישות טכניות

הנדסת דרישות

חלק מרכזי בעבודת מהנדס המערכות הוא יצירת אופיונים ומפרטים טכניים. עריכה של מסמך דרישות נראית פשוטה במבט ראשון. לכאורה נדרש בסך הכול ליצור תיאור ברור של הפונקציה והמאפיינים הנדרשים מהמערכת, המוצר או השירות מבוקש. עם זאת, בתהליך האפיון מגיעים מהר מאוד לתיאור של עשרות ומאות פרטים טכניים ואחרים, מצבי הפעלה, ממשקים ועוד. תיאור תפקיד המערכת והרכיבים מתברר עד מהרה כמורכב ביותר, באופן ששמירה על ראייה מערכתית ברורה לצד הימנעות מסתירות הופכת להיות אתגר אמיתי.

עם התקדמות העבודה, בעקבות הערות מעמיתים, מנהלים או לקוחות, השינויים נכנסים באופן בלתי נמנע למסמך ברמות שונות, החל מתצורה ורכיבים ברמה גבוהה וכלה ביחידות מדידה, משקלים ועוד. שינויים אלה משפיעים על תנאי הקבלה ותוכנית הבדיקה, מחייבים הוספה של דרישות חדשות או הסרה של כמה תיאורים ישנים. לפעמים יש מצבים שהפרויקט מוקפא זמנית, ולאחר מכן העבודה עליו מתחדשת. מסמך יכול להיבדק על-ידי עמית עם סגנון אישי וראייה שונה שיבואו לידי ביטוי בשינויים ובהערות. שינויים בלתי נמנעים אלה בטקסט משאירים מעט סיכוי למסמך להישאר עקבי ומדויק.

כתיבה של מסמכים טכניים ועריכתם באופן שיטתי ומובנה מחייבת התייחסות כאילו המסמך עצמו היה מוצר או מערכת. כשמתחילים לעבוד על מערכת, נדרש לציין תחילה את "סיבת הקיום" שלה - המטרה העיקרית של בנייתה. אם מדובר על מסמך, נדרש להגדיר עבורו את ההיקף, המטרה, היעדים, בעלי העניין ואת התועלת הצפויה או הערך עבור כל בעל עניין, לעיתים בהתייחס לחומר קודם רלוונטי.

לאחר סיום שלב הגדרת המסמך, התהליך הבא הוא תכנון המסמך, המקדים את שלב הביצוע - כלומר שלב הכתיבה עצמה. בעולם של מסמכים טכניים התוצאה של שלב זה היא טיוטת המסמך הטכני. האם הטיוטה ערוכה היטב, מתאימה ורלוונטית? זה המקום שבו בדיקת המסמך ממלאת תפקיד חשוב. הבדיקה מאפשרת לבדוק את הטיוטה מול התכנון הראשוני.

בשלבם מאוחרים יותר אחזקה של מסמך טכני לאורך זמן דומה לאחזקה של מערכת. המסמך הטכני צריך לכלול עדכונים הנובעים מדרישות משתנות, יכולות חדשות נדרשות וטכנולוגיות חדשות. אלו דורשים שינוי מתמיד של המוצר (המסמך), וכתוצאה מכך שינוי של התכנון.

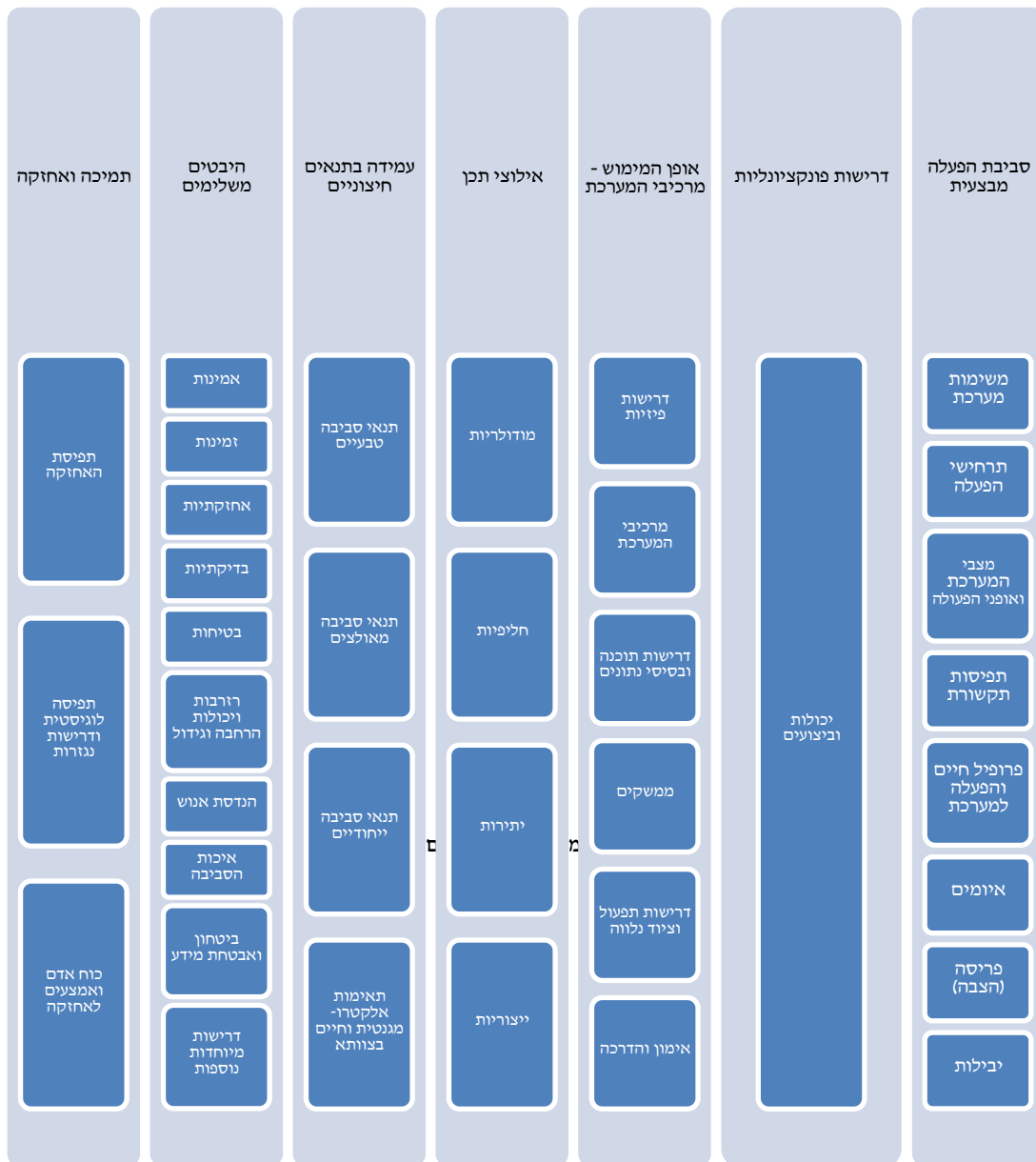
היכר סעיפי הדרישות

הגדרה של כל מערכת, ובוודאי של מערכת מורכבת, דורשת פירוט של מספר רב של דרישות, מאפיינים ונושאים. בדרך כלל בוחרים להתחיל את הצגת הדרישות בנושאים הנוגעים לסביבה המבצעית ולצורך. לאחר מכן ממשיכים אל הפתרון והמאפיינים השונים שלו. לבסוף מוצגים נושאי מעטפת שמשלימים את האפיון. בהמשך לרציונל לעיל וכדי להקל על המיקוד, הדרישות חולקו לשבע קבוצות עיקריות. סעיפי הדרישות הטכניות מובאים בהתאם לסעיפים מתוך התקן MIL-STD 961E ומתודולוגיית החטיבה הטכנולוגית ליבשה בצה"ל (חט"ל), עם התאמות והרחבות על-פי הצורך.

להלן שבע הקבוצות העיקריות של הדרישות:

1. סביבת הפעלה מבצעית;
2. דרישות פונקציונליות;
3. אופן המימוש - מרכיבי המערכת;
4. אילוצי תכן;
5. עמידה בתנאים חיצוניים;
6. היבטים משלימים;
7. תמיכה ואחזקה.

הקבוצות העיקריות של הדרישות הן קבועות יחסית ומופיעות באפיונים רבים, אם כי לעיתים בסדר שונה. באיור הבא נביא מיפוי של נושאים מרכזיים הקשורים לדרישות אלו. לאחר מכן נתאר באופן פרטני את הנושאים הנדרשים בכל אחד מתחומי האפיון הספציפיים.



סביבת הפעלה מבצעית

משימות המערכת

משימות המערכת הם המענה של המערכת לצרכים של המשתמש, כלומר פעולות ויעדים שהמערכת מכוונת לעמוד בהם ולשם מילויים היא נוצרה. מלבד הייעוד המרכזי, משימות המערכת כוללות בדרך כלל מגוון רחב של נושאים קשורים המרחיבים את התיאור שמהם ניתן לגזור דרישות לתכנן. לדוגמה, המשימה המרכזית עבור מערכת תצפית עשויה להיות העברת חוזי איכותי לטווח מסוים ביום ובלילה. משימות משלימות של מערכת תצפית יכולות לכלול הכוונת ציון לייזר של מטרות, גילוי תנועה או מיפוי שטח.

תרחישי הפעלה

תרחישי הפעלה נגזרים מתפיסת ההפעלה (Concept of operations). תפיסת ההפעלה היא תכנון ברמת-על של האופן שבו המוצר או המערכת יפעלו בסביבתם המיועדת למילוי הצרכים של הקוחות. תפיסת ההפעלה מתוארת בדרך כלל כרצף של תהליכים לאורך זמן.

תרחישי הפעלה הם רצף של פעולות או מצבים שבהם מתרחשת אינטראקציה בין המערכת לסביבתה, בדרך כלל בשילוב המפעיל או המשתמש ובהקשר ליעד או המשימה של המערכת. תרחישי הפעלה מאפשרים להציג את הפונקציונליות של המערכת כולה בסביבה המיועדת לה. מכאן נובעת חשיבות תרחישי השימוש ככלי מרכזי לתקשורת בין לקוחות, משתמשים ומתכננים. במידה וקיימות תצורות מערכת שונות או שימושים שונים למערכת, יש לספק תרחישי הפעלה המבוססים על כל התצורות או השימושים.

מצבי המערכת ואופני הפעולה

מצבי המערכת הם הגדרות לתפקודים מובחנים של המערכת והאינטראקציה שלה עם סביבתה לצורך ביצוע המשימה ולאורך מחזור החיים. מצבי היסוד של מערכת אופיינית הם: אחסנה, אחזקה, אימונים, הובלה, הכנה לפעולה, הפעלה (כולל התארגנות, נסיעה, הפעלה, חזרה לאחסנה). דוגמאות נוספות למצבי פעולה הן: אוטומטי, ידני, ביצועים מלאים וביצועים מופחתים בעת תקלה.

אחד ממצבי המערכת הנפוצים שקל "לפספס" הוא מצב סרק - IDLE. במצב זה המערכת נמצאת בהיכון וממתנה לאות הפעלה. אם ניקח כדוגמה מערכת גדר התרעה אלקטרונית, נראה כי המערכת נמצאת בשלב זה רוב זמן החיים. התרעה בעת אירוע חדירה, שהיא ייעודה המרכזי, מופעלת רק לעיתים נדירות. מכאן נובעת החשיבות של אפיון פעולת המערכת בתרחיש שימוש זה ובחינתה. בהקשר לגדר התרעה - למשל עמידות בתנאי סביבה של גשם ורוח, אמינות, בדיקות ועוד.

דוגמה למערכת נוספת עם מרכיב מהותי של מצב IDLE היא מערכת "מעיל רוח". "מעיל רוח" היא מערכת הגנה אקטיבית לרק"ם המיירטת איומים הנורים לעברה. בעבר דווח לפחות על מקרה אחד²⁹ שבו המערכת יצאה ממצב IDLE באופן שגוי ו"..." זיהתה נגמ"ש של גולני כגורם עוין - וחומר נפץ נפלט מהטנק והתפוצץ בשטח פתוח".

אופני הפעולה מתארים את התהליכים המרכיבים את התפקוד של המערכת, ובדרך כלל התיאור מופיע בחלוקה למצבי המערכת השונים. החלוקה בין מצב מערכת ואופן הפעולה אינה חד-משמעית וניתנת להגדרה על-פי התפיסה של מאפיין המערכת. לדוגמה, אופני הפעולה עבור מערכת הגנה מפני טילים במצב מבצעי עשויים להיות גילוי, עקיבה, שיערוך, העברת מידע למכלול היירוט ועוד. אולם חלק מאופני פעולה אלו עשויים להיות מוגדרים כמצבי מערכת בפני עצמם, ואז עומק הפירוט יגדל בהתאם.

²⁹ <http://www.ynet.co.il/articles/0,7340,L-4439221,00.html>. אוחר ב-11/10/13.

בסעיף מצבי המערכת ואופני הפעולה חשוב להגדיר את התנאים למעברים בין המצבים ואופני הפעולה. מומלץ לחזור מעת לעת לסעיף זה במהלך כתיבת האופיון ולוודא שכלל הדרישות שנגזרות ממצבים ואופני הפעולה שולבו במסמך. כל צמד של מצב ואופן פעולה יכול לייצר דרישות פונקציונאליות ייחודיות, ויש להתייחס לכך במידת הצורך בהגדרת הדרישות בסעיפים הבאים.

נוח לערוך טבלה מסכמת עם תיאור כלל המצבים ואופני הפעולה של המערכת, על השלכותיהם על הדרישות מהמערכת. דוגמה לטבלת מצבים ואופני פעולה עבור מערכת תצפית המותקנת בשטח ולא מחוברת לאנרגייה חיצונית מובאת להלן:

שידור לאחור	מערכות צילום	צריכת אנרגייה	אופן פעולה / מצב
אין	לא עובדות	נמוכה	המתנה
יש	עובדות	גבוהה	צילום

תפיסות תקשורת

תקשורת ומערכות שליטה ובקרה ממלאים בימינו תפקיד מרכזי במערכות רבות. בסעיף זה נדרש לציין דרישות מיוחדות לנושא. חשוב לציין מערכות ומכשירים הנדרשים להתממשק למערכת תוך הצגת תפיסת הקישוריות השלמה. אפשר שהסעיף לא יכלול דרישות מחייבות כלל, אך נדרש להציג את תמונת הקישוריות שתאפשר הצגה של המענה המתאים ביותר על־ידי המפתח.

פרופיל חיים והפעלה למערכת

פרופיל חיים והפעלה הוא תיאור של הסביבה שבה אמורה לפעול המערכת, וציון משכי הזמן הרלוונטיים. מערכות מסוימות, כדוגמת טילים, מיועדות לתקופת אחסנה ממושכת, ולאחריה לשימוש מבצעי רגעי. מערכות אחרות, כמו מערכות ניטור וידיאו או גדר חכמה, מיועדות לפעול באופן מלא לכל אורך חייהן. מכאן נובעת החשיבות של הנתונים בסעיף זה, והם משמשים בסיס לחישובי זמינות ואמינות בהמשך האופיון.

דוגמה לפרופיל חיים של משקפת:

1. שינוע באריזה על כבישים סטנדרטיים מהמפעל למחסן הלקוח (צה"ל).
2. אחסנה לוגיסטית במחסן מרכזי עד 20 שנה.
3. במהלך תקופת האחסנה הלוגיסטית - ניפוק למחסן גדודי לאחסנה מבצעית למשך ממוצע של כשנה והחזרה למחסן מרכזי לאחר מכן.
4. במהלך אחסנה מבצעית - ניפוק לחייל להפעלה מבצעית בתנאי שטח הרריים.
5. החזרה לבדיקה, אחזקה ואחסנה מבצעית לגדוד.

איומים

איומים על המערכת הם גורמים שעשויים לפעול או מצבים העשויים להתרחש ולהביא לשיבוש פעולתה התקינה. אין הכוונה לגורמים שמולם המערכת מיועדת לפעול: טיל שמערכת יירוט אמורה ליירט איננו איום עליה אלא איום ייחוס שהמערכת מתוכננת לפעול מולו. איום על המערכת עשוי להיות למשל חסימת GPS שתפגע בדיוק המיקום העצמי וכתוצאה מכך תשבש את הנתונים המופקים ממנה.

פריסה (הצבה)

סעיף זה מתאר את אופן הפיזור של המערכות בשטח, למשל בחלוקה גיאוגרפית או שיוך ארגוני. פריסה של

מכשירי קשר טקטיים, למשל, יכולה לכלול עשרות יחידות ברמת הגדוד, בחלוקה למסגרות השונות ולסוגים (נישא, מותקן ברכב ועוד). הפריסה משפיעה בין היתר על ההיערכות לאחזקה, יכולת עמידה ביעדי זמינות ועוד.

יבילות

יבילות בהקשר של אפיון מערכת היא אופן ההתאמה של המערכת להובלה, והמתקנים הרלוונטיים הכלולים במערכת. מכיוון שהובלה לעיתים קרובות משלבת אמצעים חיצוניים, כמו מנופים או משטחים, יש לתת את הדעת בסעיף זה על הגדרת ממשקים לאמצעים אלו.

דרישות פונקציונליות

הגדרת פונקציונליות במונחי יכולות וביצועים היא לבליבו של האפיון. יחד עם זאת, השונות בין אופנים שונים של הגדרת הדרישות היא גבוהה ותלויה במידה רבה במערכת המפותחת. חשוב להימנע מהגדרות שאינן תואמות את התכונות המצופות מדרישה טובה. "מינימום זמן", "ידידותי למשתמש" ושאר ניסוחים עמומים אינם מתאימים לסעיף זה.

הפורמט להגדרת הדרישות הפונקציונליות אינו קבוע. יש המגדירים דרישות פונקציונליות בפורמט של טבלה עם סעיפים וערכים, ויש העורכים רשימת דרישות ממוספרת. כך או כך, חשוב לוודא ציון מדויק לכל דרישה כדי שתהיה אפשרות להתייחס אליה בפרק האימות (פרק 4).

אופן המימוש - מרכיבי המערכת

דרישות פיזיות ותיאור פיזי

בסעיף זה יש לציין מידות, משקלים ופרמטרים אחרים הנדרשים מהמערכת. חשוב לזכור שבאפיון ביצועים יש לציין רק את הדרישות שהן הכרחיות, למשל עקב ממשק למערכת אחרת או מגבלת משקל נשיאה של חייל.

מרכיבי המערכת

בסעיף זה מובאת החלוקה של המערכת לתתי-מערכות עם תיאור תתי-מערכות ותכונותיהם. נהוג לשאוף שהחלוקה לתתי-מערכות תתאים ככל האפשר לחלוקה פונקציונלית. ריבוי תתי-מערכות יוצר בלבול ופוטנציאל לבעיות אינטגרציה. מיעוט מכלולים מקשה על מודולריות של המערכת ויכולת גידול עתידית. עבור כל מרכיב יש לצרף הגדרה תמציתית הכוללת בין השאר ייעוד, תיאור כללי (ארכיטקטורה, תצורה), פונקציונאליות או תפקוד למימוש היעד המערכתי, ציון האם הם חלק מהמערכת או מרכיב חיצוני, ואילוצים רלוונטיים אחרים.

מומלץ לדרוש שהצימוד בין מרכיבי המערכת השונים, בוודאי עם מערכות אחרות, יהיה רופף. אומנם עלות הפיתוח הראשונית עשויה להיות גבוהה יותר, אך תתאפשר גמישות ויכולת גידול עצמאית לכל אחד מהמרכיבים, ובנוסף עלויות האחזקה צפויות להיות נמוכות יותר.

בבחירת המרכיבים ומכלולי המערכת יש לתת משקל משמעותי להיות המרכיב או המכלול בשימוש במשק. לרכיב או מכלול הנמצא כבר בשימוש נרחב יהיה יתרון גדול על רכיב או מכלול מקביל בעל תכונות דומות.

דרישות תוכנה ובסיסי נתונים

רוב המערכות בימינו הן משולבות תוכנה, והתוכנה מציבה לעיתים דרישות ייחודיות. כדי לאפשר יכולת שינוי עתידית נהוג להקפיד על הגדרת שכבות תוכנה - נתונים, לוגיקה ותצוגה, באופן ששינוי תצוגה, למשל, לא ידרוש שינוי אורכי בכל המערכת אלא התאמה של המודולים הגרפיים בלבד.

במידת האפשר נהוג להגדיר מערכת פתוחה וארכיטקטורה פתוחה ולעיתים גם קוד פתוח. במערכת פתוחה מימוש דרישות נוספות יהיה נדבך נוסף מעל לפיתוח הקיים ולא יהיה צורך לפתח מחדש או לשנות מרכיבים שפותחו בגרסאות קודמות.

מערכת פתוחה היא מערכת התומכת בסטנדרטים שיאפשרו לה לעבוד בשיתוף עם מערכות אחרות, והמאפשרת הגירה קלה של מערכות ממנה ואליה. המשמעויות של עבודה בשיתוף והגירה ממדדים על-פי שני מאפיינים:

1. תמיכה ב־Interoperability - היכולת להחליף מידע ולעשות שימוש במידע שהוחלף;
2. ביצוע Porting של מערכות מהמערכת הפתוחה למערכת אחרת ולהפך - התאמת קוד תוכנה מסביבת העבודה שבה הוא נכתב לסביבה חדשה; לדוגמה, הרצה על מערכת הפעלה חלונות של מערכת שיועדה ללינוקס.

ארכיטקטורה פתוחה היא תכנון המאפשר שינוי, שדרוג והחלפת מכלולים בקלות. לדוגמה, מחשב שמאפשר החלפה של כרטיסי הרחבה. ארכיטקטורה פתוחה מתאפשרת באמצעות שימוש בממשקים סטנדרטיים. להשוואה, שינוי של מערכת הבנויה בארכיטקטורה סגורה לרוב אינו אפשרי, ואם הוא אפשרי, נדרש שינוי משמעותי באמצעות טכנאי של החברה, תשלום דמי רישיון ועוד. לדוגמה, רוב מחשבי השולחן בנויים ברמת החומרה ארכיטקטורה פתוחה, ורוב מחשבי המחברת, מחשבי הלוח והטלפונים החכמים בנויים ברמת החומרה בארכיטקטורה סגורה.

קוד פתוח הוא קוד המקור המפורסם עם רישיון לשנות ולהפיץ את התוכנה לכל אחד ולכל מטרה. קוד פתוח אינו מחייב שהמערכת או הארכיטקטורה תהיה פתוחה: יכולה להיות מערכת סגורה עם קוד פתוח. בהגדרת דרישות התוכנה במערכות משובצות-מחשב יש לשלב דרישות למערכות הניהול של המערכת. יש לאפיין כיצד תתבצע הקונפיגורציה למערכת, ומה סוג המידע שאותו ירצה המפעיל או המשתמש לקבל בזמן ריצה, למשל מידע על התראות, תקלות או סטטיסטיקות. אם הדבר רלוונטי, יש להוסיף דרישות לגבי בסיסי הנתונים. יש להתייחס בדרישות, ככל הניתן, להיבטים המבצעיים, כמו היקפי המידע המבצעי הנדרשים לאגירה, יכולות שליפה ואחסון, קצבי טיפול במידע, יכולות מיון וסינון מידע מבסיס הנתונים, רגישויות לטיב המידע, משכי הזמן הנדרשים לאגירה ודרישות גיבויים ושמירת המידע.

ממשקים

נהוג לציין שני סוגים של ממשקים: ממשקים חיצוניים וממשקים פנימיים. ממשקים חיצוניים הם ממשקים מכניים ואלקטרוניים של המערכת מול סביבתה ומול מכלולים חיצוניים. הגדרה מקיפה של ממשקים חיצוניים חשובה להתאמה טובה של המערכת לסביבתה וליכולת עתידית לשדרוג ללא צורך בשינוי פנימי אלא בהתאמה להגדרת הממשק בלבד. הגדרה מדויקת של ממשקים חשובה גם בנושאים שהם לכאורה מתואמים, ושלא צפוי שהם יוחלפו. לדוגמה, הגדרת הממשק לכלי הרק"ם בתכן של מערכת הגנה אקטיבית לטנקים יכולה לאפשר בעתיד הסבה פשוטה יותר לכלים אחרים, כמו רכבים ממוגנים, דחפורים ועוד.

ממשקים פנימיים הם ממשקים בין מכלולים במערכת. הגדרה מפורטת של ממשקים פנימיים יכולה לשחרר

מתלות ברכיב מסוים ולהקל על מעבר לספקים אחרים, לטכנולוגיה חדשה ועוד. תכונה הקושרת בין ממשקים פנימיים למכלולים היא מודולריות - גישת תכן שבה המערכת מורכבת מכמה מכלולים המתאימים לפונקציות השונות של המערכת. שמירה על מודולריות מאפשרת שינוי במכלול אחד ללא צורך בעדכון שאר המכלולים, ושימוש במכלולים קיימים או עתידיים ללא צורך בשינויים החורגים מהממשק. חשוב להשקיע מאמץ ולהקפיד על הגדרה של ממשקים באופן כללי, וממשקים פנימיים באופן מיוחד. עם זאת, מכיוון שמדובר באופיון ביצועים ולא במפרט, יש להיצמד להגדרה של ממשקים סטנדרטיים ככל הניתן ולא להיכנס עמוק מדי להגדרות פנימיות שאינן רלוונטיות ברמה של מערכת או תתי-מערכות.

דרישות תפעול וציוד נלווה

תפיסת התפעול (Operations Concept) הוא האופן שבו המערכת מממשת את תפיסת ההפעלה (Concept of Operations). תפיסת התפעול עשויה לכלול תיאור של אופן ביצוע משימות, צורת שמירת המידע ואבטחתו ועוד.

כוח-אדם לתפעול הוא חלק מהנושאים שנדרש לתת עליהם את הדעת ביציאה לפרויקט. דוגמה למערכת שבפיתוחה נדרשת התחשבות בנושא, היא אפליקציה לדיווחי אזרחים. בחלק מהרשויות המקומיות קיימות אפליקציות, וחלקן מאפשרות תקשורת ודיווח בין האזרח למוקד העירוני, כלומר משלוח הודעות על מפגעים ומענה של המוקד.

רשויות שאין ברשותן אפליקציות, מבינות היטב שמערכת כזו צפויה לשפר במידה גדולה מאוד את המענה לתושבים. ברור גם שלא קיימת מניעה טכנית לביצוע הפרויקט, שהרי יש מערכות דומות ברשויות מקומיות אחרות.

יחד עם זאת, נושא התפעול הוא הגורם המרכזי לכך שברשויות רבות טרם מוסדו אפליקציות לדיווחי אזרחים. לצורך תפעול ולמענה באמצעות האפליקציה נדרש כוח-אדם רב. אם כוח-אדם זה אינו זמין - אין ערך רב למערכת, ומוטב מלכתחילה שלא להיכנס לפיתוח.

עבור כוח האדם המתוכנן להפעיל את המערכת יש להגדיר: מקצועות נדרשים, מיומנות נדרשת ומספר המפעילים על-פי מקצוע.

ציוד נלווה לתפעול המערכת כולל אמצעים הנדרשים לצורך הפעלת המערכת, אך הם אינם מהווים חלק ממנה. בדרך כלל הכוונה היא לפריטים כמו כפפות, אביזרי שמע, אנטנות, מנשאים ועוד. חשוב לכלול התייחסות מפורשת לאמצעים אלו כחלק מהפרויקט - אם לא תתאפשר הפעלה תקינה של המערכת מהיום הראשון, סיכויי ההצלחה של המערכת ייפגעו.

אימון והדרכה

האמצעים הטכניים הנדרשים לצורך האימון וההדרכה הם מכלולים, רכיבים ופונקציונליות מיוחדת המאפשרת תרגול בסיטואציות הדומות למשימה המבצעית אך מדמות או מבצעות סימולציה עבור חלקים שלא הגיוני, כלכלי או אפשרי לבצעם למטרות אימון והדרכה בלבד. למשל אפשרות לשימוש בכדורים חסרי קליע למטרות אימון או סימולציה למטוס המתגלה במכ"ם ללא צורך להזניק מטוס לאוויר בפועל.

מערכות רבות מיועדות לפעול בתרחישי חירום שלשמתנו אינם מתרחש לעיתים קרובות. הדבר מציב אתגר הדרכתי בהכשרה של המפעילים, ובמקרים רבים אין יכולת להתאמן באמצעי אלא בסביבה סימולטיבית. במקרים כאלו הסימולטורים וסביבת ההדרכה באופן כללי הם חלק מהפרויקט, והם משפיעים רבות על ההצלחה שלו. גם בפרויקטים פשוטים יותר יש להקפיד על אופן ההסמכה וההדרכה של המפעילים כדי

למצות את מלוא הפוטנציאל של הפרויקט.

מערכות הגנה אקטיבית - "חץ דורבן", "מעיל רוח" ואחרות - מתוכננות להתמודד עם תרחיש של ירי טילים על הרכב המשוריין שעליו הן מותקנות. הפעם הראשונה שבה המפעיל ייתקל בתרחיש כזה הוא בקרב, ולכן מערכות אלו הן דוגמאות למערכות שמציבות אתגר באימון ובהדרכה. דוגמה מעניינת נוספת בנושא אימון והדרכה היא מערכת "אלומה" - מערכת מתקדמת לאיתור לכודים במתארי הרס, אסון וכדומה. המערכת מבצעת איכון של טלפונים סלולריים על בסיס ההנחה שהמצאות טלפון סלולרי באזור אסון, למשל מתחת להריסות, מעידה בסבירות גבוהה על הימצאות לכוד בסביבתו. מערכת "אלומה", כמו מערכות דומות המיועדות לשימוש בתרחיש קיצון בלבד, מציבה אתגרים בתחום הבדיקות והאימון. במערכות נשק, למשל, אפשר להתאמן ולירות במטווח לפני היציאה למשימה מול האויב. לעומת זאת, במערכת "אלומה" אין יכולת לבצע אימון ואפילו בדיקת ביצועים בצורה סדורה. לכן במסגרת פרויקט "אלומה" נרכשו אמצעים מיוחדים לצורך אימון ובדיקת הביצועים. אמצעים אלו הם... צינורות ביוב. הצינורות הונחו במבנה שיועד לאימונים בטרם הריסתו. זה אפשר הכנסה של טלפונים סלולריים פנימה אל תוך אתר ההרס והוצאה החוצה ממנו באמצעות חבלים. במצב כזה ניתן להתאמן בהפעלת המערכת וגם לבדוק את ביצועי האיכון של המערכת מול מכשירים אמיתיים במיקומים ידועים. האימון מתבצע בתנאים של בניין שקרס בפועל, בין השאר בהיבטי ניחות אות סלולרי, והדבר מגדיל את הרלוונטיות לתרחיש הצפוי במציאות.

אילוצי תכן

מודולריות

מודולריות היא גישת תכן שבה המערכת מורכבת מכמה מכלולים המתאימים לפונקציות השונות של המערכת (במקום להיות במבנה אחד או עם צימוד הדוק). שמירה על מודולריות מאפשרת שינוי במכלול אחד ללא צורך בעדכון שאר המכלולים ושימוש במכלולים קיימים או עתידיים ללא צורך בשינויים החורגים מהממשק. לדוגמה, מערכת גילוי מודולרית המורכבת ממכלולי מכ"ם, עיבוד מידע, תצוגת נתונים, ממשקי תקשורת ועוד. זאת לעומת מערכת שבה, למשל אין הפרדה מודולרית בין מרכיבי החישוב, התצוגה והתקשורת, וכל אלו ממומשים במחשב יחיד.

הגדרת מודולריות מיועדת לאפשר שימוש במרכיבי המערכת כיחידות נפרדות במערכות אחרות, שילוב בעתיד של מודולים שאינם מפותחים בשלב זה ללא שינויים משמעותיים במערכת הנוכחית, שימוש במודולים קיימים ומעל הכול - יכולת הכנסת שינויים במרכיב מסוים בלי לשנות מרכיבים אחרים במערכת. חשוב לדרוש שהחלוקה למודולים מבחינת חומרה וזיוד תהיה זהה ככל האפשר לחלוקה הפונקציונלית.

חליפיות

חליפיות היא גישת תכן שבה ניתן להחליף מכלולים זהים בין מערכות (לעומת גישה שבה המכלולים של המערכת מתאימים אך ורק למכלולים של אותה המערכת, ולא ניתן להחליף בין מכלול השייך מערכת מסוימת למכלול זהה השייך למערכת אחרת). לדוגמה, במערכת גילוי ניתן לדרוש יכולת להחליף שני מכלולי מכ"ם בין שתי מערכות שונות. אם אין מגדירים חליפיות - ייתכן שמערכת מכ"ם של ערכה מסוימת תהיה מתוכננת לעבור אך ורק עם מערכת מחשב מאותה ערכה. במידת האפשר יש לדרוש כי החלפת פריטים לא תצריך כיוונים וכיולים (חשמליים או מכניים). חליפיות אמורה לא להיות תלויה ביצרן, כלומר חלקים עם אותו מספר קטלוגי יהיו חליפיים זה לזה פיזית ותפקודית (בתוכנה ובחומרה) ללא קשר לגורם שייצר אותם.

יתירות

יתירות היא הכללה של אמצעים במערכת שאינם בשימוש באופן רגיל, וייעודם הוא גיבוי מכלולים אחרים להגדלת החסינות והאמינות של המערכת. מערכת ניווט שנייה במטוס שאינה מופעלת, אלא מהווה גיבוי למערכת הראשית (הזהה לה) ונכנסת לפעולה רק בשעת תקלה, היא דוגמה למערכת שמיועדת להעניק יתירות למכלול קריטי.

יש להגדיר האם נדרשת יתירות למערכת, ובאיזה אופן. האם היתירות אמורה להיות אקטיבית - המערכות מחוברות ופועלות במקביל או לחילופין יתרות פסיבית - חלק מהמערכות פועלות, והאחרות נמצאות בהמתנה. בדרישות היתירות יש להגדיר את פרק הזמן הנדרש למעבר למערכת האלטרנטיבית. אם היתירות היא פסיבית, יש להגדיר כי כל הנתונים הנדרשים צריכים להופיע בכל המערכות ולאפיין מהם אותם נתונים נדרשים.

ייצוריות (יכולת ייצור)

דרישות ייצור מתייחסות להתאמה של המערכת לתהליכי ייצור וחומרים רלוונטיים. דרישות ייצור באופיון ביצועים נכללות רק במקרה שיש תהליך ייצור מוגדר שיידרש בוודאות, או אם המערכת נדרשת לעיבוד נוסף שאינו חלק מההגדרה באופיון.

עמידה בתנאים חיצוניים

נושאי התאמה לתנאים חיצוניים נדרשים להגדרה עבור כלל פרופיל המשימה של המערכת, כולל שינוע, התקנה, הפעלה, אחסנה ועוד.

תנאי סביבה טבעיים

תנאי סביבה טבעיים כוללים תנאי מזג אוויר, כמו טמפרטורה, שמש, גשם, רוח ועוד. חשוב לא להפריז בהגדרה של תנאי סביבה ולדרוש רק את מה שרלוונטי באופן ספציפי למערכת. למשל עבור מערכות שמיועדות להתקנה חיצונית בארץ בלבד, אין הגיון לדרוש עמידה בטמפרטורות נמוכות מ-20°C, אפילו אם בארצות אחרות דורשים עמידה גם ב-40°C. הגדרות חופשיות מדי של תנאי סביבה מייקרות את המערכת שלא לצורך ופוגעת בכושר התחרות שלה.

חשוב להתאים את תנאי הסביבה לייעוד של המערכת. עבור מחשב נייד המיועד לשימוש בטנק נדרשת עמידה בהלמים וברעידות המתפתחים בזמן הנסיעה. עבור מחשב נייד זהה המיועד לשימוש במוצב או בחמ"ל - דרישות אלו מיותרות ומייקרות את המערכת שלא לצורך.

תנאי סביבה מאולצים

תנאי סביבה מאולצים כוללים גורמים מלאכותיים המצויים בקרבת המערכת או המשפיעים עליה, למשל כתוצאה מהניוד בשטח, מעצם הפעלה (בתלות במערכת עצמה) ומהשפעת מערכות נוספות היכולות להיות בסביבת הפעלה. דוגמאות לגורמים כאלו הם חום וקרינה ממערכות סמוכות, תאוצות ורעידות בשינוע, רעש, קרינה מכל הסוגים ועוד.

תנאי סביבה ייחודיים

תנאי סביבה ייחודיים הם תנאים חיצוניים שלא פורטו בשני הסעיפים הקודמים. למשל במערכות צבאיות יש להתייחס לתנאי הסביבה שהאויב גורם להם, או מצבים ותנאים שעלולים לקרות, ולמערכת צריכה להיות

יכולת להמשיך ולתפקד באופן תקין תוך כדי עמידה בכל הדרישות, גם אם יתרחשו. דוגמאות לתנאי סביבה הנגזרים מפעולות האויב הם אווירת שדה קרב (פיצוץ, ירי וכדומה), חסימות תקשורת GPS, חומרי לחימה בלתי קונבנציונליים ועוד.

תאימות אלקטרומגנטית וחיים בצוותא

בסעיף זה מוגדרות דרישות שעל־פיהן המערכת נדרשת לא להפריע למערכות אחרות, ושהמערכות הנוספות בסביבה לא תפרענה לפעולת המערכת, כל עוד קרינתן נמצאת בטווח שהוגדר.

כדי לא להפריע למערכות בסביבתה, הפליטה האלקטרומגנטית של המערכת תוגדר להיות נמוכה מסף מסוים בטווח תדרים כלשהו. על־מנת שמערכות נוספות בסביבה לא יפריעו לפעולת המערכת, המערכת נדרשת לתפקד באופן תקין מול הגדרה של עוצמות ותדרי שידור RF שנמדד או חזוי בסביבה המבצעית שלה.

תאימות אלקטרומגנטית שונה מממשק RF, שהיא דרישה הנכללת במסגרת דרישות ממכלולי המערכת. דרישות מממשק RF יכולות לכלול, לדוגמה, הגדרת פרוטוקול שהמערכת נדרשת לממש או לקיים.

היבטים משלימים

אמינות

אמינות היא ההסתברות שהמערכת תפעל באופן תקין במשך זמן מסוים. האמינות היא מונח סטטיסטי במהותו, וניתן להגדיר אותה במונחי זמן ממוצע בין תקלות - זמב"ת (MTBF - Mean Time Between Failures). עבור רכבים ניתן לדרוש ממוצע של קילומטרים בין תקלות (MKBF) ולהגדיר פרמטרים רלוונטיים בהתאם לאופי המערכת ומשימתה. לצד האמינות החזויה המוגדרת בשלב התכנון, יש להתייחס למדידת נתוני האמינות בפועל לאחר תקופת הפעלה מבצעית משמעותית ועדכוני תכנון נדרשים אם ערך זה נמוך מהדרוש. נהוג להגדיר תוכנית אמינות שמפרטת את הפעילויות המבוצעות כדי להבטיח עמידה בכל דרישות האמינות המוגדרות. במסגרת התוכנית מבצעים באופן חלקי או מלא פעולות אלה:

1. קביעת קריטריוני תיכון לאמינות: בחירת רכיבים, רכש רכיבים, תיאום בין רכיבים, תחום טמפרטורה של רכיבים, הפחתת מאמצים חשמליים ומכניים, תיכון תרמי והפחתת מאמצים תרמיים, יתירות, אפיצויות (טולרנסים), התעייפות ואורך חיים, שיקולי זיוד, ריכוזי מאמצים, סדקים, קורוזיה, התאמה לתנאי סביבה, בחירת חומרים.
2. פיתוח מודלים לאמינות; הקצאת אמינות - בהתאם למרכיבי המערכת השונים; חיזוי אמינות - הגדרת יכולת המערכת לעמוד בדרישות אמינות בהתאם להתקדמות התכנון; ניתוחי מאמצים - חשמליים ותרמיים.
3. ניתוח אופני כשל (FMECA - Failure Modes Effects and Criticality Analysis).
4. תהליך הוכחת אמינות - על־פי MIL-HDBK-781 או בגישה אחרת;
5. תוכנית גידול אמינות; הערכת אמינות באמצעות השוואת תהליך התקדמות האמינות עם מודל מתוכנן של גידול אמינות.
5. איסוף נתוני תקלות, אירועים וכשלים שיארכו במהלך הניסויים המתבצעים לפי תורת הניסויים.

זמינות

זמינות היא חלק הזמן שבו המערכת תקינה ומוכנה לפעולה או פועלת באופן תקין. פרקי זמן הפוגעים בזמינות הם זמני תיקון תקלות, אחזקה מונעת ועוד.

אחזקתיות (יכולת אחזקה)

מידת ההתאמה של המערכת לביצוע משימות אחזקה. היכולת להחליף חטיבת כוח בטנק בשטח בעת תקלה היא יכולת שהוגדרה כדי להעלות את האחזקתיות של המערכת. עם זאת, אם כדי לבצע משימה נפוצה ברכב, כמו להחליף מצבר, נדרש לפרק את רצועת התזמון (טיימינג) - האחזקתיות היא כנראה נמוכה.

מונח הקשור לנושא האחזקתיות הוא הזמן הממוצע לתיקון - MTTR - Mean Time to Repair. כמובן שיש לשקול נתון זה מול דרג התיקון הנדרש. מערכת עם MTTR נמוך יחסית עשויה להיות אטרקטיבית יותר מבחינת המשתמש מאשר מערכת עם MTTR גבוה בתנאי שהתיקון יכול להתבצע ברמת המפעיל שדורש פעולת טכנאי או מסירת המערכת למעבדה.

חלק מנושא האחזקתיות הוא תפיסת האחזקה ואופן התמיכה והתיקון של המערכות. לדוגמה, תפיסת האחזקה של צבא ארה"ב שונה מאוד מתפיסת צה"ל, מכיוון שדרגי האחזקה שלהם מרוחקים מאוד משדה הקרב, ונדרשת יכולת עצמאית לתיקון מירב התקלות.

כמו כן, יש הבדל גדול בין מערכות לשימוש כללי ובתפוצה רחבה (כמו טלפונים חכמים, שעונים ועוד) לבין מערכות ייעודיות שמשמשות כוח-אדם מיומן ומוכשר (כמו תוכנה להפעלת ציוד בדיקה אלקטרוני). לדוגמה, ההבדלים בפריסה של המערכות והמיומנות הייעודית של המפעילים גוזרים דרישות שונות ליכולות האחזקה המתאפשרות בדרג המפעיל ולדרישות לוגיסטיות הרלוונטיות למערך התמיכה במערכות. במערכות צבאיות יש אפשרות להגדיר שיטת אחזקה שונה בהתאם למערכת ולדמינה למערכות אזרחיות רלוונטיות. למשל רכב סופה שהוא נפוץ מאוד, דומה לרכב אזרחי, אינו אמצעי עיקרי בלחימה וקל לשנעו, מתאים לאחזקה אזרחית יותר מטנק שכנראה אין אפשרות לאחזקו מלבד אחזקה צבאית.

חשוב להגדיר בסעיף זה דרישות שתאפשרנה גמישות ונוחות בהתקנה בשטח. דוגמאות: פרק זמן סביר להתקנה, משקל המתאים להרמה באמצעות אמצעים בשטח, היעדר תשתיות ייעודיות להתקנה כמו מתח של 110v, נגישות - מרווחי אחזקה, פתחי גישה וחיפויים, יכולת פירוק מכללים, גישה לנקודות בדיקה, מהירות ביצוע כיוונים וכיולים, הנחיות לצמצום כוח-אדם נדרש לאחזקה, ידיות ואזורי אחיזה, התחשבות במשקל מותר להרמה על-ידי אדם, תכנון המערכת כך ששינוי או עדכון נתונים ייעשה ללא צורך בפרוק כרטיסים ורכיבים ועוד.

אם הדבר רלוונטי, יש לפרט בסעיף זה גם את הדרישות להתקנת התוכנה ואחזקתה. ניתן להתייחס בין השאר לנקודות האלה:

1. יכולת לשכפל, להפיץ ולהתקין את גרסאות התוכנה, כולל יכולת שכפול והתקנה על מספר יחידות מחשוב; יכולת להגדיר ולהתקין מערכת אחת ולהעתיק בקלות לאחרות;
2. מנגנון הפצה אוטומטי של טעינה מרחוק למערכות עם יחידות קצה מרוחקות;
3. שדרוג אוטומטי של הנתונים במעבר לגרסה מתקדמת;
4. אפשרות נסיגה עבור כל שדרוג גרסה.

בדיקתיות (יכולת בדיקה) - היכולת לבצע גילוי יעיל של מצב המערכת ובידוד מקורות הכשל והתקלה במקרה הצורך. נהוג להגדיר רמות בדיקה מובנית (BIT - Built-in test) במערכת: בדיקה עצמית מחזורית (CBIT - Continuous

(BIT), בדיקה עצמית התחלתית (IBIT - Initial BIT), בדיקה עצמית יזומה על-ידי מפעיל או טכנאי ועוד. לכל אחת מבדיקות BIT נהוג להגדיר את הסתברות הגילוי של התקלה הרלוונטית וסיכוי לדיווחי שווא. חשוב לזכור שבדיקות קשורה לאמינות - ריבוי מכלולים מוספים לצורך מימוש מנגנוני BIT פוגעת באמינות הכוללת של המערכת.

דרישות בדיקות כלליות עשויות לכלול התייחסות לצידוד בדיקה נדרש, פירוט המצבים שבהם נדרשת בדיקה, הגדרת תנאים מיוחדים הנדרשים לצורך ביצוע הבדיקה, קיום נקודות בדיקה וכניסות לצידוד בדיקה והתוצאות המבוקשות בבדיקות, אופן הניתוח והצגת התוצאות.

מומלץ לדרוש שביצוע בדיקות ה-BIT לא יפגע בפעילות השוטפת של המערכת. יש לוודא תאימות בין הגדרת הבדיקה ליכולות ציוד הבדיקה. מומלץ להגדיר את משך הזמן שבו תשמר היסטורית התקלות, באיזה פורמט, ועל איזו מדיה.

נגישות להיסטוריה צריכה להיות זמינה ואפשרית גם לאחר שדרוג גרסאות. בתכנון אמצעי הבדיקה והסימולטורים יש לתכנן אפשרות ליצירת מצבי כשל ולא רק אופציה לבדיקת הנתיבים המתוכננים ללא תקלות.

בטיחות

מערכות רבות מיועדות להגדיל את הבטיחות בביצוע המשימה או לאפשר ביצוע סביר במקומות שביצוע המשימה אינו אפשרי ללא המערכת. גם בהפעלת המערכות יש לרוב אלמנט של בטיחות עבור המפעיל, המאחזק והאנשים הנמצאים בסביבה.

הגדרות בטיחות כוללות לעיתים קרובות דרישות הארקה, אמצעים המונעים הפעלה בשוגג או הפעלה בזמן שאדם נמצא באזור סכנה ועוד. הבטיחות תלויה בתרחישי השימוש, ויש להגדירה בהתאם לגורמי הסיכון הספציפיים בכל אופן הפעלה.

התחומים הנדרשים להתייחסות הם לפחות אלה:

1. בטיחות מפעילים בכל מצבי המערכת;
2. בטיחות גורמים חיצוניים למערכת - הן למערכות הפעלה מבצעיות שכנות והן לסביבה אחרת (אזרחית למשל) - העלולים להיות מאוימים עקב הפעלת המערכת ומרכיביה;
3. בטיחות גורמי האחזקה והלוגיסטיקה בכל הרמות ובכל מצבי האחזקה;
4. בטיחות המערכת במקרה שהתרחשו כשלים טכניים או פגיעה במרכיבי המערכת במהלך תפקודם המבצעי או בכל מצב אחר במהלך חיי המערכת;
5. בטיחות בהיבטי שימוש בחומרים מסוכנים;
6. בטיחות של מקורות אנרגיה.

זרבות ויכולות הרחבה וגידול

יכולות גידול הן משאבים והכנות במערכת שאינם בשימוש כיום, אך צפוי כי ייעשה בהם שימוש בעתיד כחלק מרצף שדרוגים מתוכנן, עקב התפתחות טכנולוגית או מסיבה אחרת. בתכן של מערכות מחשב נהוג להגדיר יתירות זיכרון מסוימת כדי להימנע מהצורך בשדרוג חומרה בעת הוספת תוכנות או משימות חדשות, שלעיתים אינן מוגדרות בשלבי האפיון של המערכת.

מצד אחד אין ודאות שהרזרבות תנוצלנה בעתיד, ויכול להיות מצב ששדרוג עתידי יהיה זול יותר מהכנה

מראש של רזרבות. מצד שני אי התייחסות לצרכים עתידיים יכולים להשבית את המערכת עם כל גרסת תוכנה או מערכת הפעלה חדשה שדורשת זיכרון נוסף.

הנדסת אנוש

דרישות הנדסת אנוש הן נושאים המגדירים את אופן ההתאמה של המערכת להפעלה על-ידי אדם ואת נוחות ההפעלה ויעילותה. למרות שדרישות הנדסת אנוש הן לרוב מובנות מאליהן ומוגדרות היטב בתקנים הרלוונטיים, יש להתייחס לנושא בהתאם לפרויקט הספציפי. לדוגמה, הדרישה לתפריט בעברית, ממשק אינטואיטיבי ועוד היא דרישה סטנדרטית בכל אפיון לפיתוח מערכת חדשה, במיוחד במערכת המיועדת לשימוש כוחות הביטחון. לעומת זאת, מערכת "אלומה" לאיתור טלפונים סלולריים מתחת להריסות, שכבר פגשנו, היא מערכת מסוג שונה. נוחות ההפעלה במערכת "אלומה" היא פרמטר משני מאחר שהמערכת היא יחידנית ואינה מיועדת למערך רחב, ולכן ממשק המשתמש יכול להיות מורכב מאוד ובשפה האנגלית. המערכת מיועדת ממילא להיות מופעלת על-ידי מומחים ואף מהנדסים שיעברו את ההדרכה המתאימה בחברה. לכן אין צורך לפתח תפריטים מיוחדים ומפושטים, בייחוד אם ברור שהמפעילים יצטרכו לעבוד חלק גדול מהזמן עם המידע הגולמי.

בדרישות להנדסת אנוש יש להתייחס, בין השאר, לגורמים האלה:

1. אינדיקציות למשתמש לגבי מצב המערכת, סטאטוס הפעולות והתראות על תקלות;
 2. הכוונה לשימוש נכון בכל הפונקציונאליות של המערכת;
 3. הגנה מביצוע טעויות קריטיות, כלומר מניעת אפשרות לבצע פעולות שיגרמו נזק;
 4. נוחות בתפעול ובגישה, למשל מנשא נוח לנשיאת הציוד על גב החייל;
 5. יכולת לבצע את המשימה לאורך זמן;
 6. אילוצים על יכולות ומגבלות האדם דוגמת עומסי הפעלה;
 7. קריטריונים להשפעתה של הסביבה על האדם כמו: תאורה, חום, תאוצות, רעש וכדומה;
- הניסיון ההנדסי מלמד שנושאי הנדסת אנוש הם מרכיבים מהותיים בהצלחת המערכת ופעולתה התקינה.

איכות הסביבה

דרישות לשמירה על איכות הסביבה נועדו למנוע פגיעה בסביבה באמצעות המערכת או עקב הפעלתה. לעיתים דרישות איכות הסביבה רלוונטיות דווקא לשלבי הגריטה של המערכת ואופן המחזור. כמובן שחשוב לוודא שאין בשימוש חומרים רעילים או מסוכנים בצורה שתהיה מסוכנת לא רק למפעילים וסובבים, אלא גם לסביבה. דרישות איכות הסביבה עשויות לכלול הנחיות להימנע מלהשתמש בחומרים רעילים ובחומרים הפוגעים באוזן, דרישה להשתמש בחומרים ממוחזרים וידידותיים לסביבה ככל שניתן, ולתכנן את הגריטה בהתחשב באספקטים של איכות הסביבה.

ביטחון ואבטחת מידע

במערכות צבאיות הדרישות לביטחון ואבטחת מידע מובנות היטב. גם במערכות אזרחיות יש לא מעט היבטים רלוונטיים, למשל רמה אבטחת מידע באתר או באפליקציה נדרשת למנוע חשיפה של פרטים אישיים. הבסיס להגדרת הדרישות יהיה ניתוח סיכוני אבטחת המידע. ניתוח זה יכלול פרטים כדוגמת אלה:

1. מי הגורמים העשויים לנסות לפרוץ למערכת;

2. סוג פריצה או איום רלוונטי על הנתונים במערכת: קריאה, הריסה, שינוי (עדכון), איסוף;

3. מידת הנזק הצפוי לכל צירוף גורם או סוג פריצה;

4. יכולת השיפוי (תיקון, התאוששות) מנזק זה.

הדרישות הכרוכות בהיבטי ביטחון מידע של המערכת, מרכיביה וביצועיה יכללו היבטים במהלך הפעלתה המבצעית והפעלה בשגרה לצד דרישות הכרוכות במערכות הבאות עם המערכת במגע או שהמערכת כלולה בהן.

דרישות מיוחדות נוספות

כאן המקום לציין דרישות מיוחדות, כמו רכיבים, חומרים מיוחדים או כל נושא רלוונטי למערכת שלא נכלל בסעיפים הקבועים של פורמט האופיון.

תמיכה ואחזקה

תפיסת האחזקה

תפיסת האחזקה כוללת את הדרישות הטכניות לתמיכה בסבבי האחזקה, טיפול בתקלות והתמיכה הטכנית הנדרשת. הדרישות יכללו את הסעיפים האלה:

1. **דרישות למנהלות אחזקה:** דרגי האחזקה ומיקומם, מדיניות האחזקה והאחריות המוטלת על כל דרג

בתחום האחזקה, דרישות לאחזקה מונעת, כולל קריטריונים מה עושים ומתי ושירותים נדרשים מגוף התפעול כמו גיבויים, ניטורים ועוד;

2. **דרישות אחזקה פרטניות:** אילוצי המתקן או השטח שבו נמצאת המערכת, והאילוצים הנובעים

מהציוד הנוסף הקיים שם, יכולת תמיכה מרחוק של הספק (היכן שרלוונטי), טיפול בשינויים ושיפורים ועדכון גרסאות ואופן הפצת התוכנה.

מומלץ להוסיף למכלולי המערכת דרישה לשני שעוני פעילות. שעון אחד יציג את מספר שעות העבודה שצבר המכלול החל מהאיפוס האחרון, והשעון השני יצבור את סך השעות הכולל של המכלול. קריאת השעונים תיעשה באמצעות בקרה חיצונית ולא תחייב פתיחה או פירוק המערכת, והיא תשמש לביצוע חישובי אמינות, אחזקתיות וזמינות המערכת.

תפיסה לוגיסטית ודרישות נגזרות

התפיסה תכלול דרישות לתכן הנובעות משיקולי עיתוד מלאים ואופני אספקה על-פי פרופיל החיים הטכני והלוגיסטי שנבנה לה. יוגדרו המרכיבים הנדרשים לאספקה במהלך חיי המערכת ובתנאי הפעלתה המבצעית. יצינו גורמים ואמצעי אספקה קיימים ומידת יכולתם לענות לדרישות האספקה למערכת. תוגדר שיטת האספקה, מיקום מערומי האספקה ומרכיבי המערכת (החלפים) שיימצאו באותם מערומים.

כוח-אדם ואמצעים לאחזקה

הלקוח הסופי בדרך כלל אינו רואה את בעלי המקצוע בתחומי האחזקה, והוא נתקל בהם לעיתים רחוקות. יחד עם זאת, כוח-אדם בתחומי התמיכה, האחזקה והשירות, כמו גם אמצעים לאחזקה, הם רלוונטיים לכל פרויקט. גם טלפון סלולרי שבמרבית הזמן עובד היטב, ומעט התקלות נפתרות בדרך כלל באמצעות הפעלה מחדש, לעיתים נדרש לאחזקה של בעל מקצוע. אם בעל המקצוע לא יוכשר מראש ויצויד באמצעי בדיקה וחלקי חילוף, כנראה ששביעות הרצון של המשתמש תיפגע מאוד.

עבור כוח-אדם מאחזק יש להגדיר מיומנות נדרשת, מספר אנשי האחזקה והתמיכה הטכנית הנדרשים במצבי המערכת השונים, כולל אחסנה, פריסה, הפעלה מבצעית, אחזקה וכדומה. בתכנון הציוד יילקחו בחשבון כלי הבדיקה והאחזקה. בנוגע לציוד תמיכה תחזוקתית (צת"ת) יש לשלב דרישות כלליות ודרישות לצת"ת ייעודי דוגמת עריסות, עגלות שינוע וכדומה. יש להימנע מתכנון ציוד המצריך כלים מיוחדים לאחזקה. יש לאפיין גם את ציוד הבדיקה שימש בכל דרג, ובמידת הידוע בשלב זה את הדרישות הספציפיות מהציוד (סביבת הפעלתו, ניידות, מה נדרש לבדוק).

דרישות אימות ביצועים

דרישה טובה מחויבת להיות, בין היתר, בת אימות. אם האימות לא יבוצע, גדול הסיכוי שהתכונה שהוגדרה בדרישה לא תתקיים או לא תתפקד כנדרש. אופן הבדיקה של הדרישות מוצג בפרק אימות הביצועים המגיע לאחר פרק הדרישות הטכניות.

תהליך האימות של מערכת

אימות המערכת נדרש להיעשות לכל אורך הדרך, "ויפה שעה אחת קודם": אם איהוודאות היא משמעותית, עדיף לבדוק אותה מוקדם ככל האפשר, כדי שתהיה אפשרות סבירה לעדכן את התכן במידת הצורך. לעומת זאת, בשלבים המוקדמים של הפרויקט התכן אינו שלם, ולכן יש דברים שקשה לבדוק בתחילת הפיתוח, וגם אם בודקים - התוצאות אולי לא תהיינה רלוונטיות לביצועים הסופיים. נהוג לחלק את תהליך האימות לשלושה חלקים: בדיקות מפתח, בדיקות דגם ובדיקה סדרתית. להלן נציג בקצרה כל אחד מאלו.

בדיקות מפתח הן בדיקות שמבצע היצרן (לרוב ביידוע הלקוח ובשיתופו), ומטרתן להוכיח ולהדגים פעולה תקינה בשלבים מוקדמים של הפרויקט וכך להוריד סיכונים פיתוח. למרות היתרונות הברורים של בדיקות מפתח, כאמור, לעיתים אי-אפשר לבצע אותן עד שהמערכת בשלה מספיק או משולבת עם מערכות נוספות, וזה יכול להתרחש רק לקראת סוף הפיתוח.

בדיקות דגם מתבצעות על דגם המערכת, כלומר המערכת הראשונה שיוצרה בתצורה סופית. בדיקות הדגם מחולקות בדרך כלל לשני שלבים המכונים בהקשר של מערכות ביטחוניות "אישור בטיחות" ו"אישור דגם". המטרה של האישור הבטיחותי היא לוודא שהשימוש במערכת לא יזיק למשתמשים, למערכות אחרות או לסביבה. לצורך האישור הבטיחותי המערכת הנבדקת אינה נדרשת לביצועים כלשהם, ובלבד שהיא אינה מסכנת את המפעילים והסובבים. כלומר, מערכת שאינה עושה שום דבר מועיל, עשויה לקבל אישור בטיחותי, בתנאי שהיא אינה פוגעת או מזיקה.

אישור דגם הוא אישור של עמידת המערכת בביצועים הנדרשים. בדרך כלל תהליך של אישור בטיחותי הוא קודם או משולב באישור דגם. יש הנוהגים לכוונת תהליך של אישור דגם בשם "בדיקת קבלה מורחבת". **בדיקה סדרתית** היא בדיקה של מערכות בשלבי ייצור סדרתי. מטרת הבדיקה היא לוודא עמידה של פריטים המיוצרים בייצור סדרתי לדרישות האופיון ונתוני אישור הדגם וכך לתקף את שרשרת הייצור.

שיטות האימות

קיימות חמש שיטות אימות עיקריות: הצהרת יצרן, הדגמה, אנליזה, בחינה וניסוי. סדר השיטות הוא "מהקל אל הכבד": הצהרת היצרן היא השיטה הזולה והקלה ביותר לביצוע מבחינת הספק, אך היכולת של הלקוח לוודא ולבדוק את ההצהרות היא נמוכה או לא קיימת. ניסוי הוא תהליך הדורש את מירב האמצעים, אך

בניסוי המערכת עצמה מופעלת בתנאים הקרובים למצב האמת, ולכן תוקף התוצאות אמור להיות הרב ביותר. להלן נביא תיאור קצר של כל שיטת אימות.

הצהרת יצרן - מסמכי יצרן או כל הכרזה של הספק שלא עברה אימות על-ידי הלקוח, ושאינה מסתמכת על נתונים או אנליזות. במסמכי יצרן יכולים להיכלל גם דוחות מעבדה של הספק או אישורים של בעלי מקצוע מוסמכים (למשל אישור חשמלאי מוסמך). נהוג לבקש ולהסתמך על הצהרה של היצרן לעמידה בדרישות מסוימות.

הדגמה - הצגה או הפעלה של המערכת על-ידי היצרן כדי להראות עמידה בדרישות מסוימות. בדרך כלל בהדגמה מוצגת המערכת בסביבה מבוקרת, וההפעלה נעשית על-ידי מפעיל מיומן של הספק. השימוש בהדגמה נפוץ בתצוגת ממשקי משתמש, תכונות חיצוניות ועוד. בהדגמה נבדק שהמוצר מתאים לנדרש ממנו ללא מדידות כמותיות אלא על סמך התרשמות בלבד.

אנליזה וסימולציה - הצגת נתונים ותוצאות של חישוב תיאורטי שיכולים להעיד או לנבא עמידה של המערכת בתנאים מסוימים. משתמשים באנליזה אם נדרש לבחון ביצועים בתרחישי קיצון שאינם ניתנים לשחזור באופן מעשי. לעיתים המערכת נדרשת לעמוד בתרחישים רבים מאוד, אך ניתן לעשות רק מעט ניסויים חיים. במקרה כזה משתמשים בסימולציה כדי לקבל מעטפת ביצועים עקרונית והערכה להתנהגות בכל הסביבות המבצעיות, ובמקביל מבצעים כמה ניסויים כדי לתקף את תוצאות הסימולציה.

בחינה - בדיקה של המערכת על-ידי נציגי הלקוח, בדרך כלל חזותית או משלבת בדיקות התרשמות ובסיסיות בלבד, כמו מימדים פיזיים, נוחות שימוש, סימונים, צבע ועוד. בחינה עשויה לכלול מדידות פיזיקאליות, חשמליות ומכניות כמותיות פשוטות.

ניסוי - הפעלה של המערכת בתנאים הקרובים לסביבה האמיתית. כאמור לעיל, הניסוי הוא שיטת האימות היקרה ביותר מבחינת התשומות, אך היא אמורה להיות המקורבת ביותר לתנאים במציאות. ניסויים יכולים להתבצע במעבדה או בשדה.

ניסויי מעבדה: ניסויים מבוקרים בתנאי מעבדה שבהם נבדקים מרכיבי המערכת לעמידה בדרישות. המערכת נבדקת מול ציוד בדיקה או סימולטורים פיזיקאליים החל מבדיקת פרמטרים בדידים ועד פעולה שלמה של מערכת מול סימולציה מייצגת של העולם החיצון.

ניסויי שדה: ניסויים עם הציוד המפותח בתנאים הדומים לתנאים השוררים בסביבה המבצעית שבהם מתוכנן הציוד לפעול. ניסויים אלה יכללו ניסויים של מרכיבי המערכת וניסויים מערכתיים.

טבלת אימות

טבלת האימות מפרטת עבור כל דרישה מפרק הדרישות באופן את מיקום הבדיקה בתהליך האימות, שיטת האימות והאופן הפרטני של ביצוע הבדיקה. נהוג לחלק את אימות הדרישות בין השיטות השונות, ואף לאמת דרישה אחת בכמה שיטות לאורך הפרויקט כדי להביא למקסימום את הוודאות בביצועי המערכת בהשקעה של מינימום אמצעים.

3.5.1.1		3.4.4.3	3.2.4.1		סעיף הדרישה	דרישה (פרק 3)
עמידה בתנאי גשם		דיוקי ייצור	טווח ירי		מהות הדרישה	
			✓		בדיקות מפתח	תהליך האימות
✓		✓	✓		בדיקות דגם	
		✓			בדיקה סדרתית	
					הצהרה	שיטת האימות
✓					הדגמה	
			✓		אנליזה	
		✓			בחינה	
✓			✓		ניסוי	
4.3.2	4.4.15.7	4.2.2	4.3.1	4.5.1	סעיף הבדיקה	פירוט הבדיקה (פרק 4)
ניסוי מבצעי בשטח למשך חודש	הדגמה במעבדה	מדידת דיוקים באמצעות פלס אלקטרוני	ניסוי ירי של תחמושת חיה	אנליזה מול מטרות אדם ושריון	מהות הבדיקה	

פירוט הבדיקות

בכל מקרה שבו הבדיקה איננה טריוויאלית, נדרש לפרט את אופן ביצועה. דוגמאות: עבור ניסוי ירי טילים נדרשת הגדרה של כמות הטיילים, תרחישים, תנאים חיצוניים ועוד; עבור אנליזת חוזק נדרש לפרט את המכלולים הנבדקים, תקנים רלוונטיים ועוד. לרוב מידע זה חורג מהמקום הקיים בטבלה, ולכן דורש פירוט בסעיף נפרד.

דרישות למסירת המערכת

אריזה

הסעיף כולל הגדרות לשאלות האלה: כיצד ייארז המוצר? כמה מערכות באריזה? האם האריזה תהיה כבדה, יקרה ועמידה, או אולי לא נדרשת אריזה כלל, למשל אם המוצר יותקן וייכנס לשימוש מיידי? האם נדרשת אריזה נוספת לנשיאה, אחסנה או שינוע אחזקתי לאורך חיי המערכת?

יש לתכנן את דרישת המארזים בהתאם לאופן האחסון וההובלה. המארזים אמורים להגן על התכולה מפני פגיעות מכניות ומפני תנאי אחסון שאינם מתאימים. בדרישות האריזה יש להתחשב גם באמצעי ההובלה והשפעתם על אופן האריזה ובנוחות בהעמסה. יש מצבים שבהם נדרשת אריזה שונה בהתאם לפרופילי הפעלה שונים, כמו מערכת שיש לארוז אותה באופן מסוים להובלה ולאחסנה ובאופן אחר לנשיאה על גב החייל.

אם הדבר רלוונטי, ניתן לדרוש שהאריזה תתאים לשימוש רב-פעמי. יש להגדיר את אופן האריזה גם לחלקי החילוף. בנושאים הרלוונטיים ניתן לדרוש שמכלולים סגורים יוגנו מפתיחה שאינה מורשית, באמצעות מדבקות אבטחה או כל דרך הגנה אחרת.

סימון

סימון המערכת נדרש לצורכי זיהוי, תפעול או אזהרה. נהוג להגדיר את החומרים, המידות והמיקומים של השלטים בשילוב עם הגורמים הרלוונטיים לתמחור (גרפיקה או טקסט, צבע או שחור-לבן ועוד). את התוכן המדויק נהוג להשאיר להגדרה מאוחרת יותר. חשוב להגדיר אמצעי סימון מתקדמים, במידה ורלוונטי (לדוגמה, ברקוד, קוד QR, RFID ועוד).

הערות

פרק ההערות כולל תיאורים משלימים ומידע להבהרה שלא שולב בשאר סעיפי האופיון. למשל מידע זה יכול לכלול הפניות לסעיפים ב-SOW שרלוונטיים לנושא ההגדרות של המערכת. ניתן לכלול בסעיף ההערות הסברים הנוגעים לחלופה שנבחרה או לחלופות שנפסלו והסיבות לפסילתן - אם הוא לא נכלל בסעיפים קודמים, ואם הוא רלוונטי לאופיון המערכת. בדרך כלל פרק ההערות אינו כולל דרישות פורמליות.

סקרים בתהליך הפיתוח

סקר (Review) הוא כלי פורמאלי לבקרה ולאישור איכות המוצר ותוצרי ביניים ולאישור המוכנות להמשך הפיתוח לאורך השלבים במחזור חיי הפרויקט. סקרים משולבים אינטגרלית בתהליכי הנדסת מערכות, והם משמשים אמצעים חשובים ביותר לאימות שלמות המערכת, איכותה והוכחת תקפותה. סקר מהווה גם אבן דרך לבקרה על התקדמות הפרויקט ועמידתו בלוחות הזמנים ובמשאבים. מהות הסקר היא הצגת תוצרי ביניים ודיון בנקודות פתוחות וסיכונים אפשריים לקראת אישור אבן דרך בפיתוח והתארגנות לקראת המשך הפיתוח. סקרים כוללים בדרך כלל שני היבטים, אשר נהוג לשלב ביניהם:

1. היבטי מערכת (סטטוס הפיתוח עצמו): סטטוס רכיבי מערכת וממשקים, איכות, התאמה לדרישות וכדומה;
 2. היבטי ניהול: לוחות הזמנים של הפרויקט, משאבים (כוח-אדם ותקציב), השלכות ארגוניות, סיכונים שעלולים להפריע למימוש הפרויקט וכדומה.
- SRR (System Requirements Review) - סקר דרישות מערכת - יבוצע לאחר חתימת החוזה, עם השלמת ניתוח הדרישות עלידי הספק ולפני הכניסה לתהליך הפיתוח. מטרת הסקר הן אלה:
1. לוודא שהספק מבין היטב את הדרישות ואת אופני הבדיקה, את סדרי העדיפויות ואת המגבלות הקיימות;
 2. לוודא שהספק מתחייב לממש את הדרישות במהלך הפרויקט בהתאם לאבני הדרך ולתוצרים שהוגדרו;
 3. לוודא שהספק הוא בעל היכולת והמשאבים לעמוד בכל דרישות החוזה.
- SDR (System Design Review) - סקר תכנון מערכתי - יבוצע עם השלמת התכנון המערכתי (קונספטואלי). מטרת הסקר היא לבחון ולהעריך את התפיסה המערכתית (קונספט) שנבחרה למערכת ביחס לדרישות המערכת ולהציג באופן מפורט את השלבים השונים הקשורים בתכנון המערכת או המוצר ובפיתוחם לאור תיחום הפרויקט, דרישות הלקוח, סדרי העדיפויות, המגבלות והאילוצים הטכנולוגיים.
- PDR (Preliminary Design Review) - סקר תיכון ראשוני - יבוצע עם סיום שלב התכנון הראשוני ולפני הכניסה לשלב התכנון המפורט. מטרת הסקר היא להציג את חלופות התכנון ותהליך הבחירה של החלופה המועדפת ולהציג לאישור תיכון ראשוני של החלופה שנבחרה.
- CDR (Critical Design Review) - סקר תיכון קריטי - יבוצע עם סיום מלא של שלב התכנון ולפני כניסה לשלב

המימוש. מטרת הסקר הן אלה:

1. לאשר את תוצרי התכנן המפורט, ולוודא שהתכנן מספק מענה שלם לכל דרישות המערכת והתקנים הנדרשים תוך שמירת העקיבות בין האופיון לבין התכנן;
 2. לאשר הקפאת תצורת המערכת או המוצר והממשקים למימוש בשלב הייצור והבדיקות.
- TRR (Test Readiness Review) - סקר מוכנות לבדיקות, לבחינה ולניסויים - יבוצע לקראת כל בדיקה או ניסוי במערכת. מטרת הסקר הן לאשר מוכנות לתחילת בדיקות בהתאם לתוכנית ניסוי ובחינה, לוודא הורדת כל הסיכונים וביצוע כל הבדיקות המקדימות ולאשר תוכנית ניסוי, לוחות זמנים ומשאבים לביצוע הניסוי.
- FTR (Final Test Review) - סקר סיכום בדיקות מערכת - יבוצע לאחר סיום שלב הבדיקות והניסויים. מטרת הסקר הן אלה:

1. להציג את תהליך הבדיקות ואת כל ממצאי הבדיקות שנערכו ברמת המערכת ותת-המערכות, לצד פירוט הרכיבים שלא נבדקו;
 2. להעריך את משמעות הבעיות והתקלות שאותרו במהלך הבדיקות ולקבל החלטה בהתאם באשר למוכנות המערכת והמעבר לשלב הייצור בהיבט הטכני.
- FQR (Formal Qualification Review) - סקר בדיקת התאמה פורמאלי - יבוצע עם השלמת כל מטלות הפיתוח ולקראת ההעברה לייצור. מטרת הסקר היא לאשר שמטלות הפיתוח, ייצור הדגמים וביצוע הבדיקות של אימות התכנן הושלמו בהצלחה, ולאשר את התצורה הסופית של המערכת, כולל ציוד תמיכה.
- PCA (Physical Configuration Audit) - סקר ביקורת קונפיגורציה פיזית - יבוצע לפני הכניסה לייצור וייתחם למוצר כפי שמועד לצאת מקו הייצור. מטרת הסקר היא לוודא את תאימות הפריטים השונים למסמכי התכנן השונים (מפרטים, שרטוטים) ולאשר שתקני הבחינה אכן מאמתים את דרישות התכנן.
- PRR (Production Readiness Review) - סקר מוכנות לייצור - יבוצע לפני שלב הייצור. מטרתו לבחון ולהעריך את סטאטוס המוכנות לייצור ולאשר את תיק הייצור של הדגם וכן את מוכנות קו הייצור לייצור סדרתי.
- SPRR (System Production Readiness Review) - סקר מוכנות למבצוע - יבוצע לאחר סיום הפיתוח, ביצוע בדיקות והניסויים ואישור דגם ולקראת תחילת פעילות שוטפת של המערכת (בהיקף מלא או בהיקף חלקי). מטרת הסקר הן אלה:

1. לוודא מוכנות לקליטת המערכת ולהטמעתה בקרב המשתמשים;
 2. לוודא מוכנות של גורמי הפיתוח, התפעול, אחזקה והתשתיות לקליטת רכיבי המערכת או המוצר, התקנתם והפעלתם בסביבה המבצעית.
- סקרים נוספים שנערכים באופן מחזורי או בעת הצורך הם PMR (סקר ניהולי - Program Management Review) - QAR (סקר הבטחת איכות - Quality Assurance Review). מטרת סקרים אלו היא הצגת תמונה רוחבית בהיבטי ניהול או הבטחת איכות וקבלת החלטות בהתאם.
- בפרויקטים קטנים מקובל לשלב יחד חלק מהסקרים. שילוב מקובל הוא חיבור SDR עם SRR או איחוד בין FTR לסקר ה-FQR. אך בכל פרויקט חשוב לקיים CDR מפורט כנקודת בקרה להצגת כלל המאפיינים שישולבו במערכת וכתנאי להמשך מימוש המשימה.

הרחבה: בטיחות מערכות/משה יצחקי³⁰

פרק זה מתמקד בניתוח בטיחות של מערכת בגישה המכונה בטיחות מערכת (system safety). התחום העוסק בבטיחות מערכת נקרא הנדסת בטיחות מערכת (system safety engineering), ובדרך כלל מבצעים אותו מהנדסים אשר התמחו בניתוח סיכונים של מערכות. בטיחות מערכת נדרשת בעיקר בארגונים המתכננים, המפתחים והבונים מערכות שיש בהם סיכונים לאדם ולסביבה. כמעט בכל המערכות הצבאיות יש עיסוק בחיי אדם, והמטרה היא לוודא שאין במערכת סיכונים שאינם קבילים.

דרישות בטיחות מערכת מוגדרות בתקן MIL-STD 882E "ליישום של עקרונות, קריטריונים, וטכניקות ניהוליים והנדסיים כדי להגיע לרמת סיכון נסבלת של תרחישים מזיקים, וזאת במגבלות ישימות ויעילות תפעולית, זמן, ועלות במשך כל השלבים של חיי המערכת". כיום גישה זו אומצה כסטנדרט גם בתחומי תעשייה אזרחיים שונים, ויש מספר רב של תקנים נוספים הדנים במערכות אוטונומיות, מערכות תעופה ועוד. בטיחות מערכת משמשת כלי סטנדרטי בניתוח בטיחות של מערכות - ממערכות קטנות ועד למערכות נשק, כורים גרעיניים, תובלה אווירית ותעופת חלל, מערכות נשק עתירות אנרגיה, ועד מתקנים ותהליכים מסוכנים בתעשייה. לקחי העבר לימדו אותנו כי ביצוע ניתוח וטיפול בבטיחות מערכת בהתאם לדרישות התקנים מחויב כדי להבטיח את חיי המשתמשים ושלומו.

בטיחות מערכת מלווה את הפרויקט משלב התכנון הראשוני ועד שלב הפירוק או הגריטה של המערכת. הנחת העבודה בהגדרת התקן היא כי יש סיכונים במערכת. הכוונה להגיע לרמה נסבלת של סיכונים המתחשבת בצרכים התפעוליים ובמשאבים הנחוצים ליישום הבטיחות במערכת. הגדרה זו תואמת את עיקרון ה"ALARP (As Low As Reasonably Practical)". לפי עיקרון זה יש להשקיע מאמצים להפחתת רמת הסיכון כל עוד הדבר ניתן ומעשי.

מונחי יסוד בבטיחות מערכת

המונחים העיקריים של בטיחות מערכת מבוססים על תקן MIL-STD-882E, והם אלה:

מערכת (system): שילוב אינטגרטיבי של אנשים, תוצרים ותהליכים המאפשר סיפוק צורך או מטרה מוגדרים.
תתמערכת (sub-system): שילוב של מרכיבים המאפשר אוסף של ביצועים במערכת מוגדרת.
גורם סיכון (hazard): מצב ממשי או פוטנציאלי היכול לגרום לפגיעה, מחלה או מוות לאנשים; נזק או אובדן מערכת, ציוד או רכוש או נזק לסביבה.

תרחיש מזיק (mishap): מאורע או סדרה של מאורעות לא מתוכננים שתוצאתם הינה מוות, פגיעה או מחלת מקצוע, נזק או אובדן של ציוד או רכוש או נזק לסביבה.

סיכון של תרחיש מזיק (mishap risk): החומרה הפוטנציאלית של התרחיש המזיק וההסתברות לאירועו.

בטיחות (safety): היעדר מצבים העלולים לגרום מוות, פגיעה או מחלת מקצוע, נזק או אובדן של ציוד או רכוש או נזק לסביבה.

אליכשל (fail-safe): מאפיין של פיתוח המבטיח שהמערכת תישאר בטוחה, או, במקרה של כשל, גורם למערכת לעבור למצב שלא יגרום תרחיש מזיק. חשוב לציין כי כיוון שחלק זה הינו מורכב מאוד ודורש ידע הנדסי ויצירתיות רבה. נדרש לבצע חשיבה על שילובו מוקדם ככל הניתן.

³⁰ אל"ם (מיל") משה יצחקי שירת שנים רבות בחטיבה הטכנולוגית ליבשה ושימש, בין היתר, בתפקיד ראש מחלקת תקיפה ואיסוף, ראש מחלקת מערכות אלקטרואופטיות ומפקד יחידת הפיתוח. בתפקידו במילואים משמש יושב ראש ועדת הבטיחות לניסויים עתירי אנרגיה בזרוע היבשה.

פונקציה קריטית בטיחותית (safety critical): מונח המתייחס לכל מצב, מאורע, תפעול, תהליך או פריט אשר הזיהוי, השליטה, הביצוע או הסיבולת שלהם הינם חיוניים להפעלה או תמיכה בטוחה במערכת. **ניהול בטיחות מערכת (system safety management):** כלל התוכניות והפעולות המבוצעות באופן שיטתי כדי לזהות, להעריך, להפחית - וכן לעקוב באופן שוטף, לשלוט ולתעד - סיכונים סביבתיים, בטיחותיים ובריאותיים של תרחיש מזיק העלול לקרות בעת פיתוח, בדיקה, רכישה, שימוש ופירוק של מערכת, תת-מערכת או ציוד.

סיכון שיורי של תרחיש מזיק (residual mishap risk): הסיכון של תרחיש מזיק שנותר לאחר שכל האמצעים להפחתת הסיכון נוצלו או ננקטו על-פי העקרונות של מדרג בקרת הסיכונים.

תהליך בטיחות מערכת

תהליך הבטיחות של המערכת כפי שמובא ב-MIL-STD-882E מכיל שמונה שלבים, וכמובן שביניהם יש אינטראקציות ומעגלים החוזרים על עצמם. השלבים הם אלה: קבע את תפיסת הבטיחות המערכתית; זהה את הסיכונים; הערך את הסיכונים; זהה את האמצעים לצמצום הסיכונים; צמצם את הסיכונים; אמת וודא את הפחתת הסיכונים; קבל את הסיכונים; נהל את הסיכונים בכל מחזור החיים.

שלב 1: קבע את תפיסת הבטיחות המערכתית

תהליך ניהול הבטיחות בפרויקט מתחיל בקביעה של גישת הבטיחות של המערכת לניהול סיכונים ובתיעודה כחלק בלתי נפרד מתהליך הנדסת המערכת. הדרישות הבסיסיות לגישת הבטיחות כוללות את אלה:

1. תיאור של המאמץ לניהול הסיכונים הבטיחותיים ושילובו בתהליך הפיתוח, הנדסת המערכות והמבנה הניהולי הכולל של התוכניות;
2. זיהוי הדרישות שיש להן היבט בטיחותי ושנקבעו ונגזרות על המערכת; דוגמאות לכך כוללות דרישות בטיחות תחמושת, דרישות תאימות אלקטרומגנטית, דרישות איכות הסביבה ושיקולים טכנולוגיים. לאחר זיהוי הדרישות, יש להבטיח את הכללתם במפרט המערכת ואת העברת הדרישות גם על קבלני משנה וספקים;
3. הגדרה הדדית בין הלקוח והספק של האופן שבו סיכונים וסיכונים נלווים מקובלים באופן רשמי על-ידי הלקוח;
4. תיעוד סיכונים עם סגירות במערכת למעקב סיכונים (HTS Hazard Tracking System). ה-^{HTS} יכול, לכל הפחות, את הנתונים האלה: סיכונים מזוהים, תקלות קשורות, הערכות סיכונים, אמצעים מזוהים להפחתת סיכונים, אמצעי הפחתה נבחרים, מצב הסיכונים ותיעוד קבלת הסיכונים.

שלב 2: זיהוי הסיכונים

סיכונים מזוהים באמצעות תהליך ניתוח שיטתי הכולל חומרה ותוכנה של המערכת וממשיקי מערכת, לרבות ממשקים אנושיים. תהליך זיהוי הסיכונים יהיה לאורך כל מחזור החיים של המערכת. ההשפעות האפשריות על כוח-אדם, תשתיות וסיכונים מזוהים יתועדו ב-HTS.

שלב 3: הערכת סיכונים

רמת החומרה ורמת ההסתברות של התקלות הפוטנציאליות עבור כל סכנה בכל מצבי המערכת נבחנים באמצעות ההגדרות בטבלאות הבאות. כדי לקבוע את החומרה המתאימה, עבור סיכון מסוים בנקודת זמן

נתונה, יש לזהות את הפוטנציאל למוות או לפציעה, להשפעה סביבתית או להפסד כספי. לסיכון מסוים יש פוטנציאל להשפיע על אחד או יותר משלושת התחומים שהוזכרו. יש להתייחס לתוצאה הסבירה הקשה ביותר הצפויה, בהנחה שהתרחיש המזיק קורה.

דרגת חומרה	קטגוריה	קריטריונים סביבתיים, בטיחותיים ובריאותיים
קטסטרופלי	I	עלול לגרום לאחת או יותר מהפעולות הבאות: מוות, נכות מוחלטת קבועה, השפעות סביבתיות בלתי הפיכות או הפסד כספי העולה על 10 מיליון דולר.
קריטי	II	עלול לגרום לאחת או יותר מהפעולות הבאות: פציעות או מחלת תעסוקה העלולה לגרום לאשפוז של לפחות שלושה אנשי צוות, להשפעה סביבתית משמעותית, אך הפיכה, או הפסד כספי העולה על 1 מיליון דולר אך נמוך מ־10 מיליון דולר.
שולי	III	עלול לגרום לאחת או יותר מהפעולות הבאות: פגיעה או מחלה תעסוקתית שיובילו לאובדן יום עבודה אחד או יותר, להשפעה סביבתית מתונה, אך הפיכה, או הפסד כספי העולה על 100,000 דולר אך נמוך מ־1 מיליון דולר.
זניח	IV	עלול לגרום לאחת או יותר מהפעולות הבאות: פציעה או מחלה תעסוקתית שאינה גורמת לאובדן יום עבודה, השפעה מינימלית על הסביבה או הפסד כספי הנמוך מ־100 אלף דולר.

כדי לקבוע את רמת ההסתברות המתאימה, כפי שמוגדרת בטבלה הבאה, עבור סיכון מסוים בנקודת זמן מסוימת, יש להעריך את הסבירות להתרחשות תקלה. העמודה של קבוצה או מלאי מתארת את ההשפעה של סדרה, כמו צי כלי רכב, או סדרות המכילות פריטים דומים רבים. רמת ההסתברות F משמשת לציון מקרים שבהם הסיכון אינו קיים עוד. התקן מדגיש כי הגדרת שיטת הפעלה, הדרכה, אזהרה או ציוד מגן אישי אינם מציינים יכולת לגרום לסיכון לקבל את הרמה F.

קבוצה או מלאי	פריט בודד ספציפי	רמה	הסתברות
קורה כל הזמן.	צפוי לקרות לעיתים קרובות במהלך חיי הפריט, עם הסתברות לאירוע הגדולה מ- 10^{-1} במהלך חיי הפריט.	A	שכיח (frequent)
יקרה לעיתים קרובות.	יקרה פעמים אחדות במהלך חיי הפריט, עם הסתברות קטנה מ- 10^{-1} , ¹ אך גדולה מ- 10^{-2} במהלך חיי הפריט.	B	אפשרי (probable)
יקרה פעמים אחדות.	צפוי שיקרה פעם במהלך חיי הפריט, עם הסתברות קטנה מ- 10^{-1} , ² אך גדולה מ- 10^{-3} במהלך חיי הפריט.	C	מדי פעם (occasional)
לא צפוי, אך סביר להניח שאולי יקרה.	לא צפוי, אך עלול לקרות במהלך חיי הפריט, עם הסתברות קטנה מ- 10^{-3} , אך גדולה מ- 10^{-6} במהלך חיי הפריט.	D	קלוש (remote)
לא צפוי, אך אפשרי.	בלתי צפוי במידה כזו, שניתן להניח שכנראה לא יקרה כלל במהלך חיי הפריט, עם הסתברות הקטנה מ- 10^{-6} במהלך חיי הפריט.	E	לא סביר (improbable)
	לא מסוגל להתרחש. רמה זו משמשת כאשר סיכונים פוטנציאליים בוטלו מאוחר יותר.	F	מבוטל (eliminated)

הסיכונים המוערכים באים לידי ביטוי כקוד הערכת סיכונים (RAC - Risk Assessment Code) שמקצה רמת סיכון גבוהה, חמורה, בינונית או נמוכה לכל שילוב של קטגוריית חומרה ורמת הסתברות.

כחלק מתוכנית הבטיחות יתועדו כל ההגדרות המספריות של ההסתברות ששימשו בהערכת סיכונים כנדרש בשלב 1 שהוגדר והסיכונים המוערכים יתועדו ב-HTS.

שלב 4: זהה את האמצעים לצמצום הסיכונים

יש לזהות מנגנוני צמצום סיכונים ולבצע ניתוח הפחתת הסיכונים הצפויים של החלופות תוך תיעוד הנושא ב-HTS. המטרה צריכה להיות תמיד למנוע את הסיכון, אם אפשר. אם לא ניתן לנטרל סיכון, יש להפחיתו לרמה הנמוכה ביותר המקובלת במגבלות העלות, לוח הזמנים והביצועים. יישום חלופות לשיטות צמצום הסיכונים יהיה על־פי מידת האפקטיביות בהתאם לסדר הבא:

1. באופן אידיאלי, את הסיכון יש לבטל באמצעות בחירת חלופת תכן או חומר שמסיר את הסיכון לחלוטין;

2. אם לא ניתן לנטרל את הסיכון באמצעות שינוי התכנון, יש לשקול שינויים בתכנון המפחיתים את החומרה או את ההסתברות לפוטנציאל התקלה הנוצר בעקבות המפגעים;
3. אם הפחתת הסיכון באמצעות שינוי התכנון אינה אפשרית, יש להפחית את החומרה או את ההסתברות לפוטנציאל התקלה שיצרו המפגעים על ידי שימוש באמצעים הנדסיים אשר יפריעו לרצף תקלות ובכך יפחיתו את הסיכון של תקלה;
4. אם האמצעים הנדסיים אינם אפשריים או שאינם מורידים במידה מספקת את חומרתם או את סבירותם של התקלות שגרם הסיכון, יש לכלול מערכות גילוי ואזהרה כדי להזהיר את המשתמשים (מפעילים ומאחזקים) מפני מצב מסוכן או התרחשות של אירוע מסוכן;
5. אם מנגנוני התרעה אינם יכולים להקטין במידה מספקת את החומרה או ההסתברות של פוטנציאל התקלה שגרם הסיכון, יש להוסיף שילוט, נהלים, הדרכה ואמצעי מיגון אישי; עבור סיכונים המסווגים לקטגוריות קטסטרופליות או קריטיות יש להימנע משימוש בשילוט, נהלים, הדרכה ואמצעי מיגון כשיטה יחידה להפחתת הסיכון.

שלב 5: הקטן הסיכונים

אמצעי הפחתת הסיכונים שנבחרו, ייושמו על־מנת להשיג רמת סיכון מקובלת. יש לשקול ולהעריך את העלות, את ההיתכנות ואת האפקטיביות של שיטות הפחתת הסיכונים כחלק מתהליך הנדסת המערכת הכוללת. במסגרת הסקרים השונים יש להציג את הסיכונים הנוכחיים, את חומרתם ואת הערכות ההסתברות שלהם ואת מצב מאמצי הפחתת הסיכון.

שלב 6: אמת וודא את הפחתת הסיכונים

אמת את היישום ואת האפקטיביות של האמצעים הנבחרים להורדת הסיכון באמצעות ניתוח, בדיקה, הדגמה או בדיקה מתאימים. יש לוודא כי תיעוד האימות מופיע ב-HTS.

שלב 7: קבלת הסיכונים (לפני חשיפת גורמים לסיכון)

לא תמיד ניתן להקטין את הסיכונים לרמות מקובלות. לכן לפני מבצוע או ניסוי האמצעים על ידי אנשים, יש להגדיר את הסיכונים הידועים הקשורים למערכת. רמת הסיכון מחויבת להיות מקובלת על הסמכות שהוגדרה לכך. תצורת המערכת והתיעוד הנלווה התומכים בהחלטת קבלת הסיכון הפורמלית יישמרו לאורך חיי המערכת. החלטה על קבלת סיכון שיש לה הצדקה בשלב פרויקט מסוים ייתכן כי תתייתר עם הזמן, ונכון שהנושא יתועד. ההטמעה בשדה, קבלת לקחים או ניסיון ממערכות אחרות יישמשו לביצוע הערכה מחודשת של הסיכונים שנשארו כיוון שיתכן שסיכונים מסוימים הוערכו בצורה גבוהה או נמוכה מדי.

שלב 8: ניהול סיכונים בכל מחזור החיים

לאחר מבצוע של המערכת יש להשתמש בתהליך לזיהוי סיכונים ולשמור אותם ב-HTS. לאורך מחזור החיים יש לבחון כל שינוי שיכלול, בין השאר, את הממשקים, המשתמשים, החומרה, התוכנה, נתוני התקלות או המשימות של המערכת. נדרש כי התהליכים יתקיימו כדי להבטיח שהמשתמשים ומנהלי המוצר יהיו מודעים לשינויים אלה, למשל באמצעות הכללתם כחלק מתהליך בקרת התצורה או שחרור גרסה. אם יתגלה סיכון חדש או שייקבע סיכון ידוע שיש לו רמת סיכון גבוהה יותר מזו שהוערכה קודם לכן, הסיכון החדש או

המתוקן יצטרפו לעבור ניתוח של הסיכונים ומתן המלצות על אמצעים להפחתת הסיכון, במיוחד כאלו שימזערו טעויות אנוש.

סיכוני תוכנה

החידוש של MIL-STD-882E הוא בנתח המשמעותי שהוא מייחס לנושא התוכנה. בשנת 2016 פורסם מדריך עזר לנושא התוכנה שמתייחס גם לסוגיית הערכת הסיכונים בתהליך פיתוח "זמיש" - "זריז וגמיש" (Agile). הסיבה לשינוי נבעה מההבנה כי הערכת הסיכון של תוכנה וכתוצאה מכך מערכות מבוקרות תוכנה או עתירות תוכנה, אינה יכולה להסתמך אך ורק על חומרת הסיכון והסתברותו. קביעת ההסתברות לכישלון של פונקציית תוכנה אחת היא קשה, וברוב המקרים היא אינה יכולה להתבסס על נתונים היסטוריים בדומה לחומרה. התוכנה היא בדרך כלל ספציפית ליישום, ופרמטרי אמינות משויכים לסביבה שבה היא נמצאת. לכן פותחה גישה נוספת שתשמש להערכת תרומות התוכנה לסיכון המערכת. השיטה בוחנת את חומרת הסיכון הפוטנציאלית של התוכנה ואת מידת השליטה שהתוכנה מפעילה על החומרה.

בקרת הסיכונים במערכות עתירות תוכנה מתבצעת בהתאם לטבלאות האלה:

1. טבלת רמות בקרת תוכנה (SCC - Software Control Categories) המגדירה את מידת השליטה של התוכנה;
 2. טבלת קריטיקליות בטיחות תוכנה (SSCM Software Safety Criticality Matrix) מקצה מדדי קריטיקליות תוכנה (SwCI Software Criticality Index) - בהתאם לחומרת הסיכון ולקטגוריות שליטת התוכנה;
 3. טבלת רמת ההקפדה (LOR – Level Of Rigor) הנדרשות בהתאם ל-SwCI הספציפי. למרות הדמיון במראה של מטריצת הערכת הסיכון, ה-SSCM אינה משמשת להערכה של הסיכון אלא משמשת להגדרת המשימות המינימליות הנדרשות בהתאם לרמת השליטה של התוכנה.
- נדרש להעריך רמות בקרת תוכנה מחדש גם אם התוכנה מבוססת על חבילות תוכנה מדור קודם (Legacy). יש לבדוק את הפונקציות הישנות הן בממשקים הפונקציונליים והפיזיים כדי לקבוע האם יש אפשרות להשפעה ברמה הגבוהה ביותר ובגורמים סיבתיים מסוכנים.

רמת שליטת תוכנה	קטסטרופלי I	קריטי II	שולי III	זניח IV
1	SwCI 1	SwCI 1	SwCI 3	SwCI 4
2	SwCI 1	SwCI 2	SwCI 3	SwCI 4
3	SwCI 2	SwCI 3	SwCI 4	SwCI 4
4	SwCI 3	SwCI 4	SwCI 4	SwCI 4
5	SwCI 5	SwCI 5	SwCI 5	SwCI 5

משימות ה־LOR מובאות בטבלה הבאה:

משימות ה־LOR	SwCI
התוכנית תבצע ניתוח של דרישות, ארכיטקטורה, תכן וקוד ותבצע בדיקות עומק ספציפיות לבטיחות.	SwCI1
התוכנית תבצע ניתוח של דרישות, ארכיטקטורה ותכן ותבצע בדיקות עומק ספציפיות לבטיחות.	SwCI2
התוכנית תבצע ניתוח של דרישות וארכיטקטורה ותבצע בדיקות עומק ספציפיות לבטיחות.	SwCI3
התוכנית תבצע בדיקות עומק ספציפיות לבטיחות.	SwCI4
אם מהנדס בטיחות העריך שאין לפריט השפעה בטיחותית, לא יידרשו פעילויות נוספות.	SwCI5

משימות ה־LOR יבוצעו כדי להעריך את רמת הסכנה של המערכת. התוצר של משימות ה־LOR מספקות רמת ביטחון בתוכנות בעלות אספקטים בטיחותיים ומשמשים כפקטור משמעותי בנכונות להקל בנוגע לסיכונים. תוצאות משימות ה־LOR ייכללו בתוכנית ניהול הסיכונים. התרומה של התוכנה לסיכון המערכת, כולל תוצאות של יישום משימות ה־LOR, יתועדו ב־HTS.