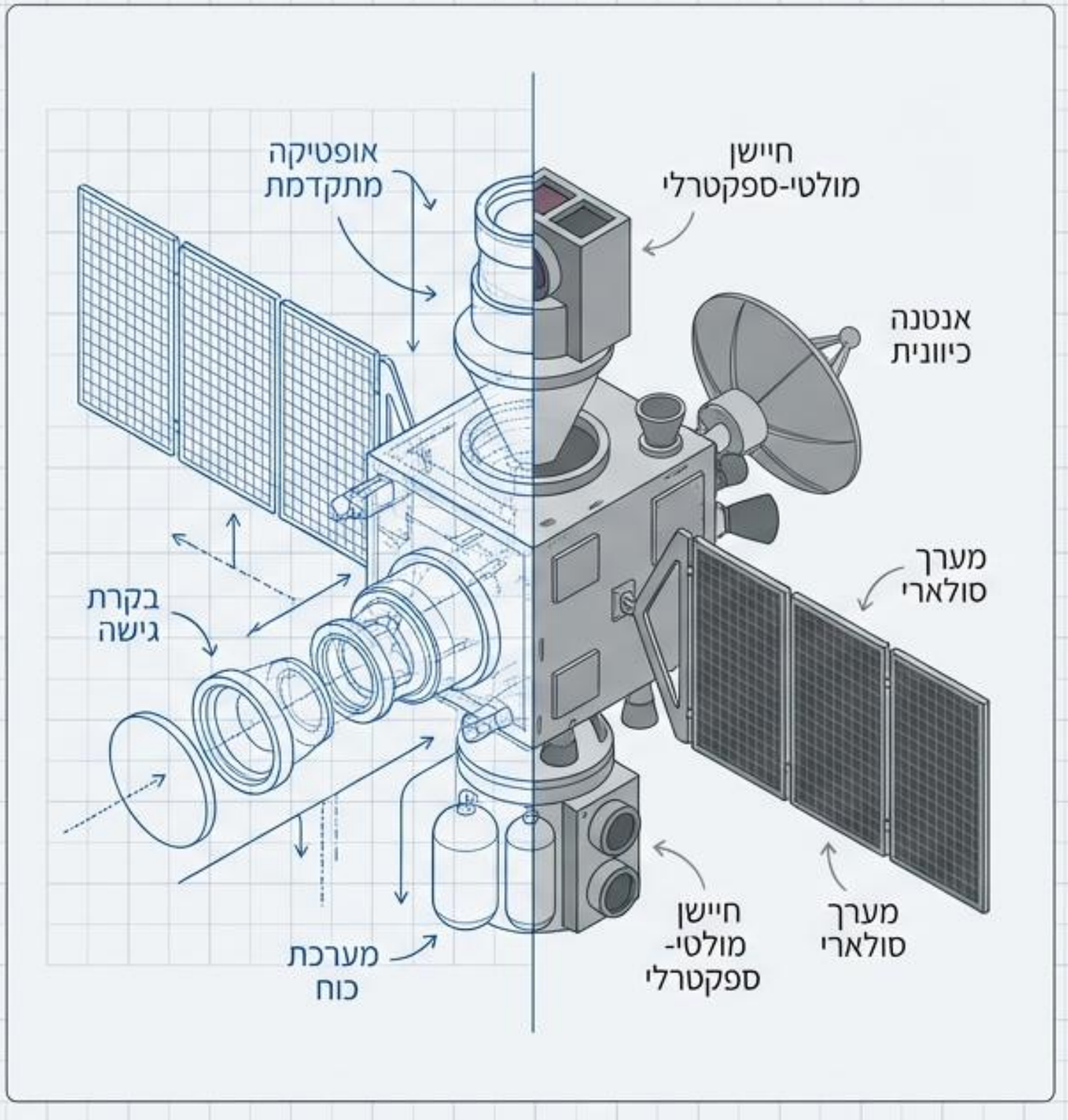
Noti Haim

מהנדס המערכת בחברות שונות בארץ ובעולם

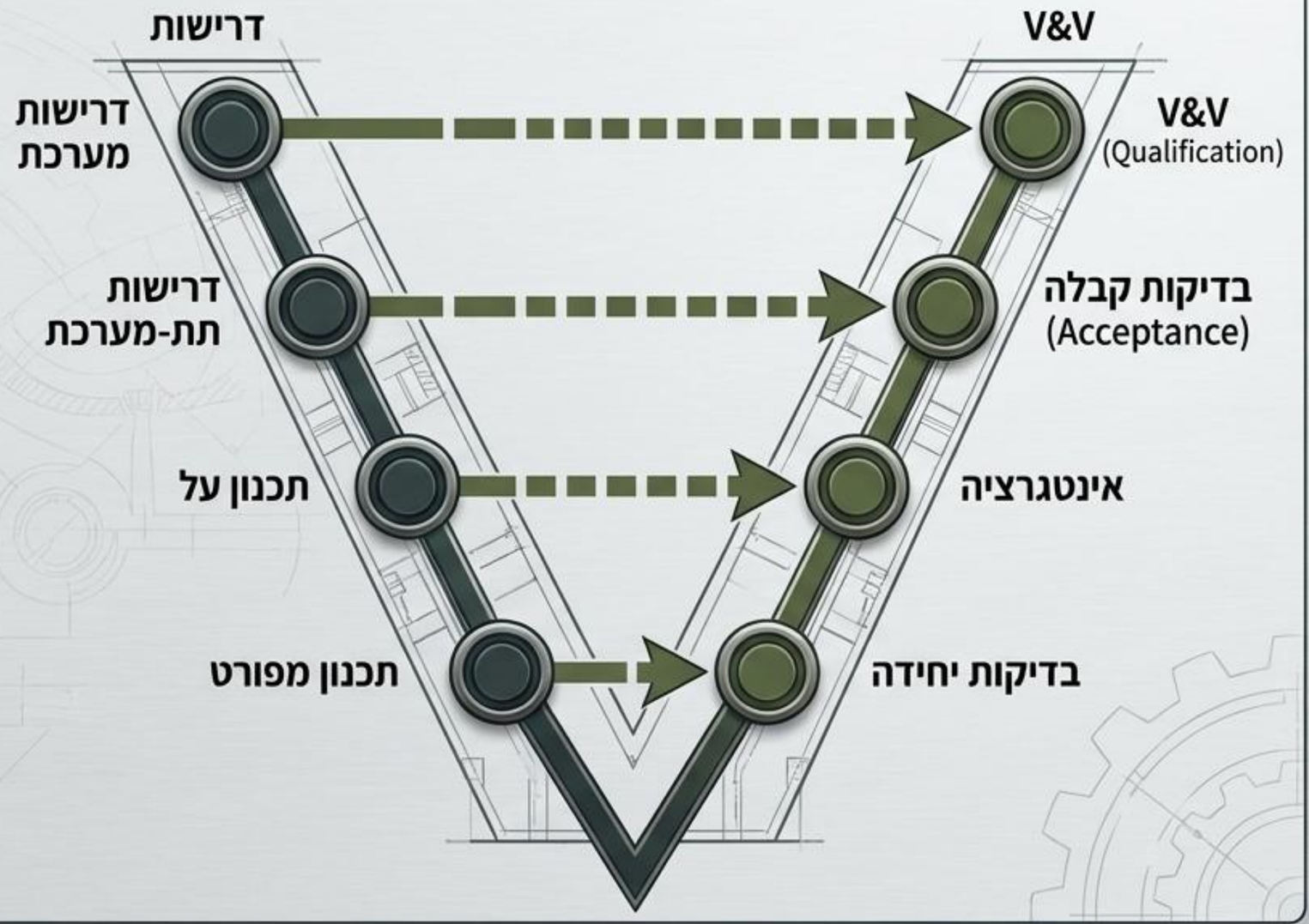
תובנות, השוואות ומתודולוגיות מתקדמות
(מבוסס על סקירת תעשיות ביטחוניות ואזרחיות ומתודולוגיית NASA).



הנדסת מערכת היא נגזרת של ניהול סיכונים

תעשיות הביטחון מקדשות שליטה מוחלטת בסיכונים

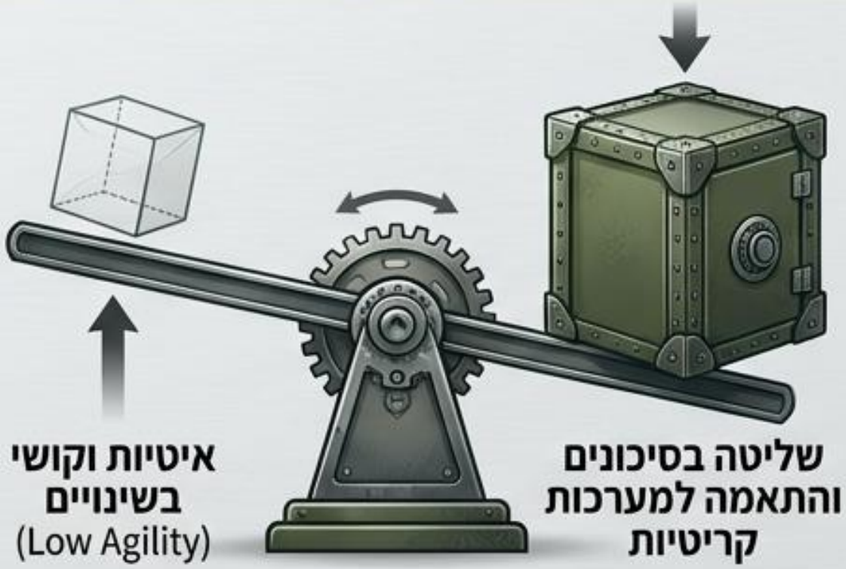
V-Model



Characteristics

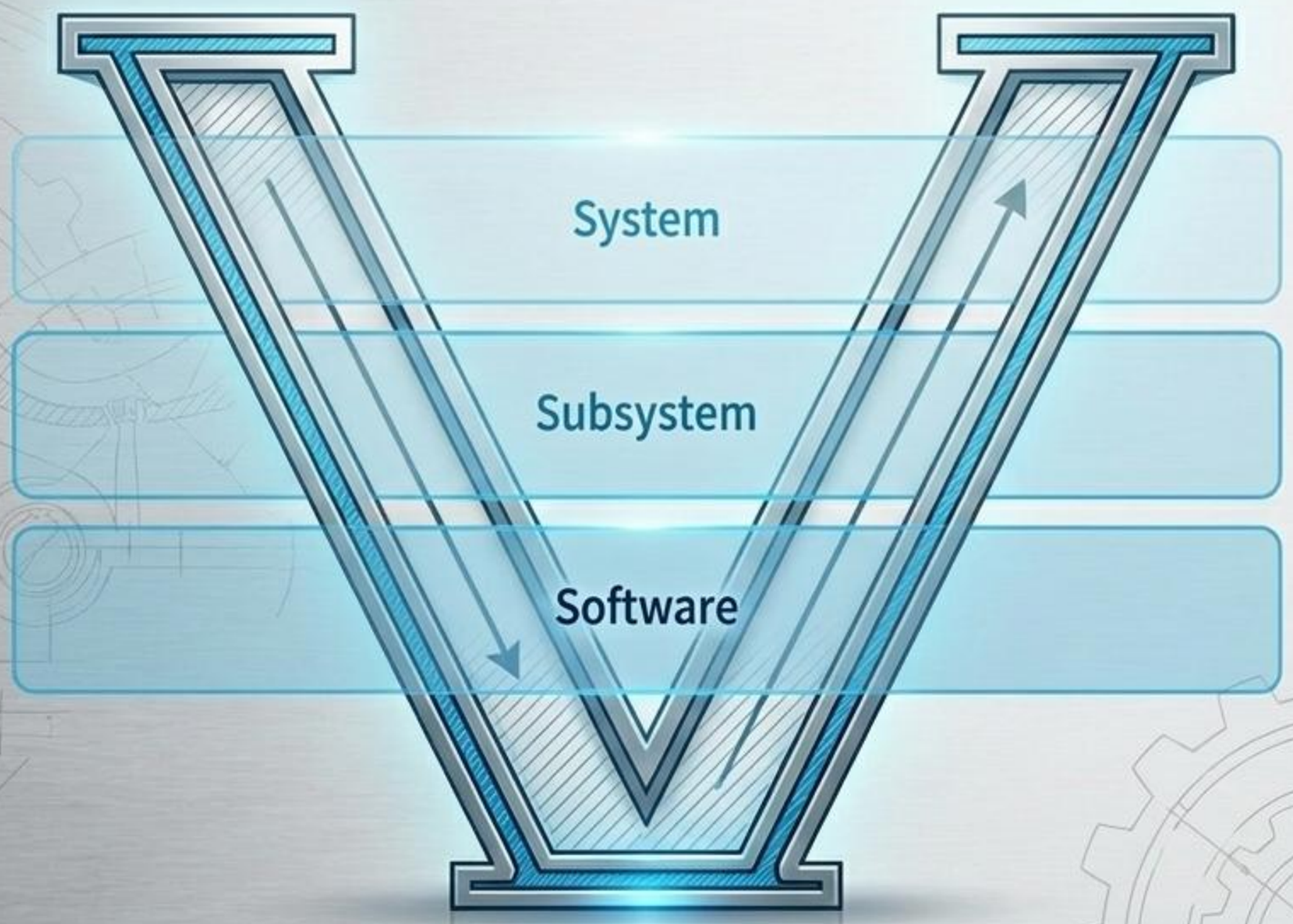
- תהליך קלאסי מבוסס V-Model
- דגש קיצוני על דרישות ו-Traceability
- שימוש בכלים כבדים (IBM Rational DOORS)
- תהליכי V&V קפדניים (Qualification, Acceptance)
- מחזורי פיתוח האורכים שנים

Visual Scale



עולם התעופה מוסיף רגולציה כבדה ומודלים מתקדמים

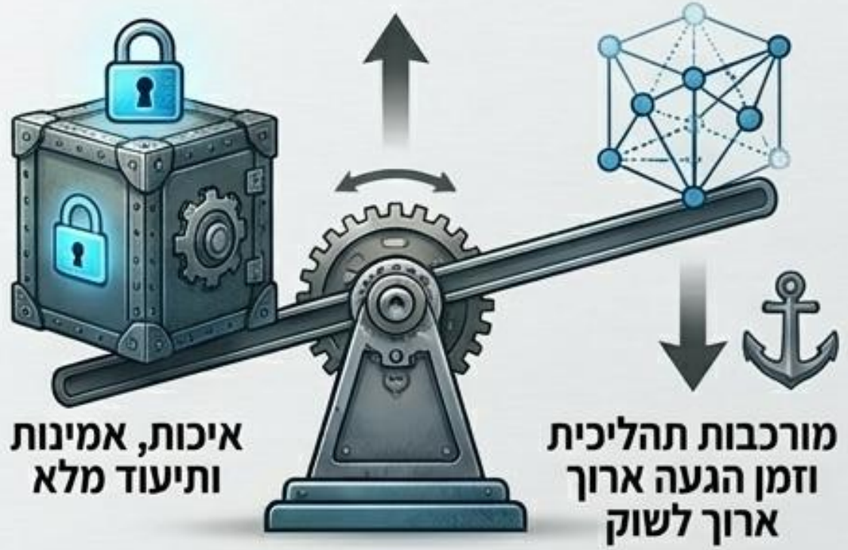
V-Model | DO-178C | ARP4754 | MBSE



מאפיינים (Characteristics)

- **הפרדה ברורה בין** System / Subsystem
  Subsystem / Software
- **דגש קריטי על** Certification **כחלק מובנה מהפיתוח**
- **אימוץ גובר של** MBSE
  (Model-Based Systems Engineering)

סקאלת השפעה (Visual Scale)



תעשיית הרכב מהווה את נקודת ההתנגשות ההיברידית

ISO 26262 | OTA Updates | Platform Engineering

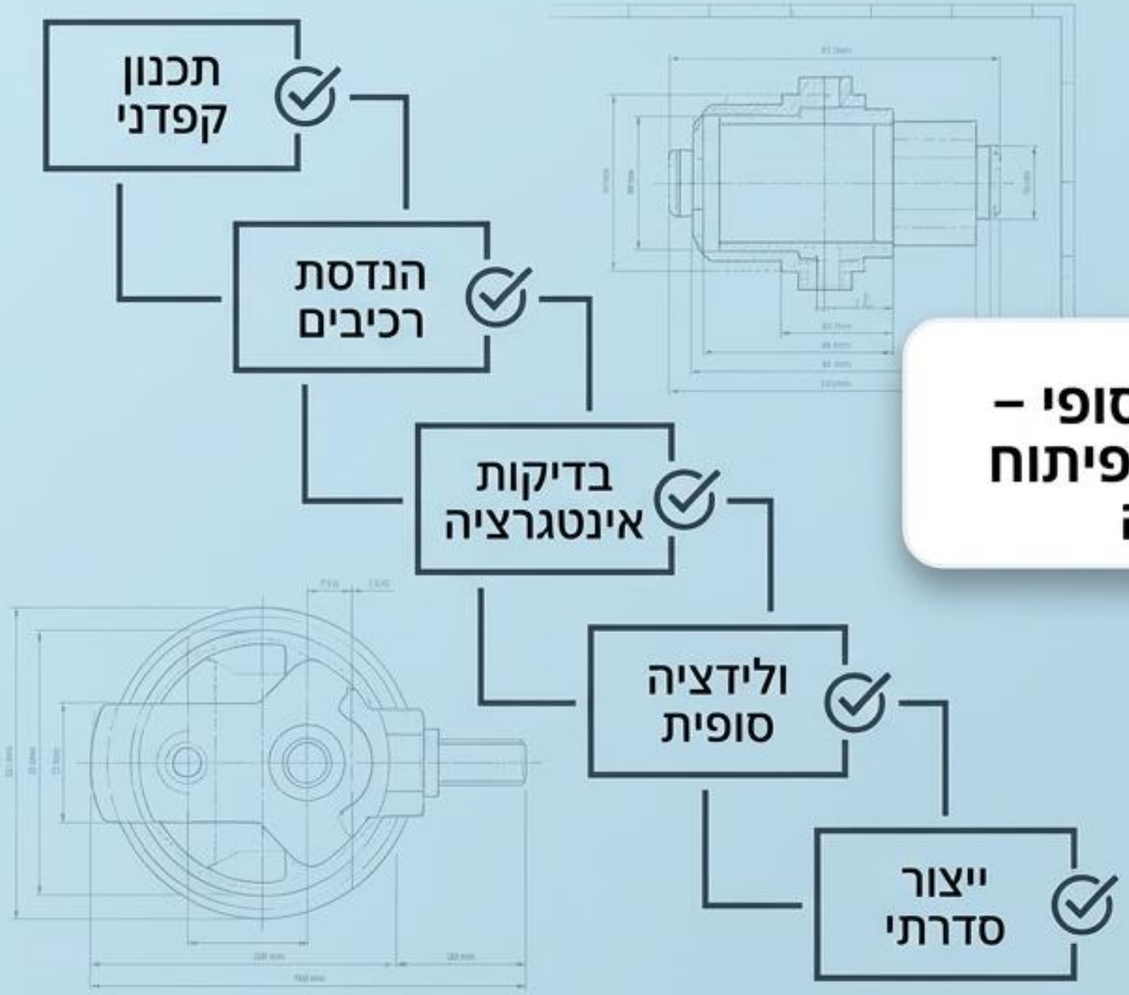
מאפיינים

- **שילוב היברידי:** V-Model למערכות חומרה/בטיחות, יחד עם Agile לתוכנה
- **דרישה לאינטגרציה מהירה ועדכוני תוכנה** דרך האוויר (OTA)
- **שימוש הולך וגובר בפלטפורמות הנדסיות**

סקאלת השפעה

קרב הגישות: מסורת מבוקרת מול מהירות מונחית-תוכנה

תהליך מסורתי ומבוקר

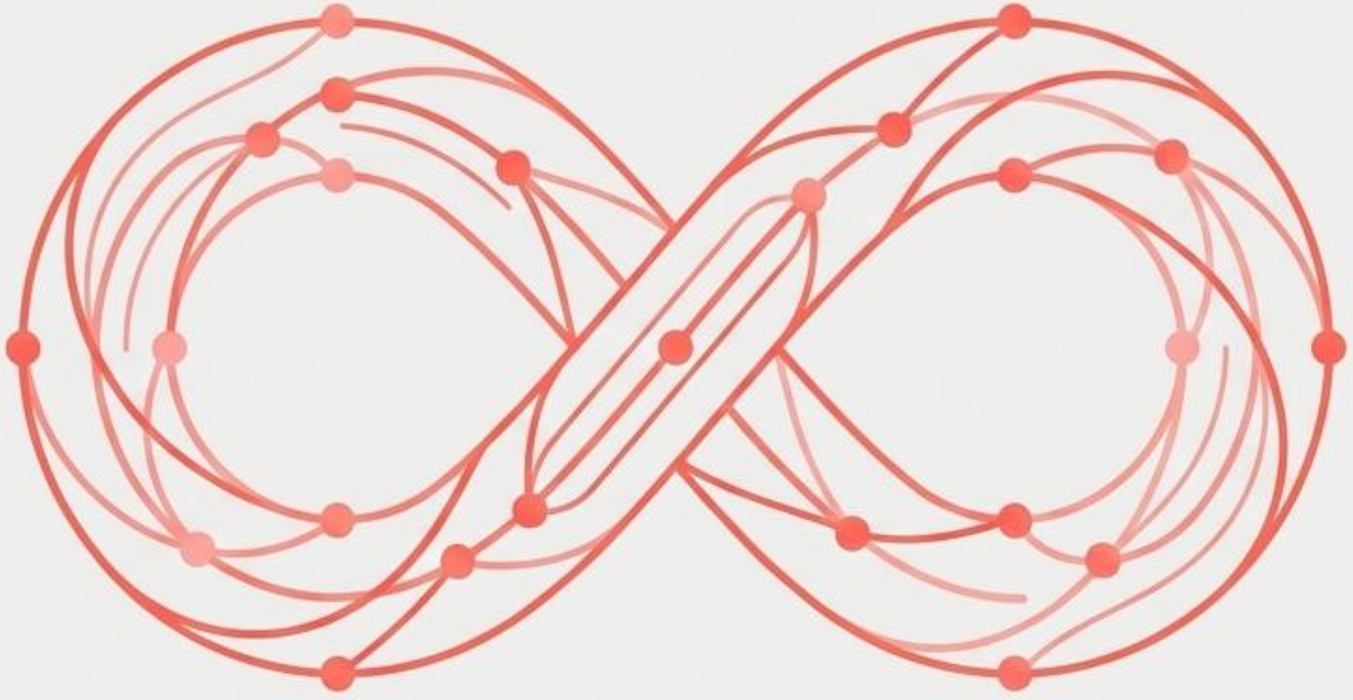


אותו מוצר סופי – פילוסופיית פיתוח הפוכה

Agile-ו Software-Driven

חברות הטכנולוגיה מפרקות את המבנה לטובת זרימה מתמדת

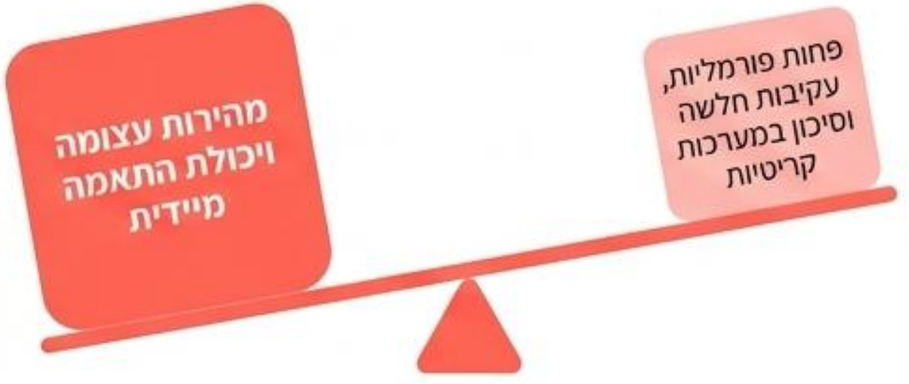
Agile/DevOps | Microservices | CI/CD | SRE



מאפיינים

- זניחת הדרישות הפורמליות לטובת איטרציות מהירות
- ארכיטקטורת Microservices המאפשרת פיתוח מקביל
- אינטגרציה ופריסה רציפה (Continuous Integration / Deployment)
- הופעת תפקידים חדשים כמו SRE (Site Engineering)

מזוינים

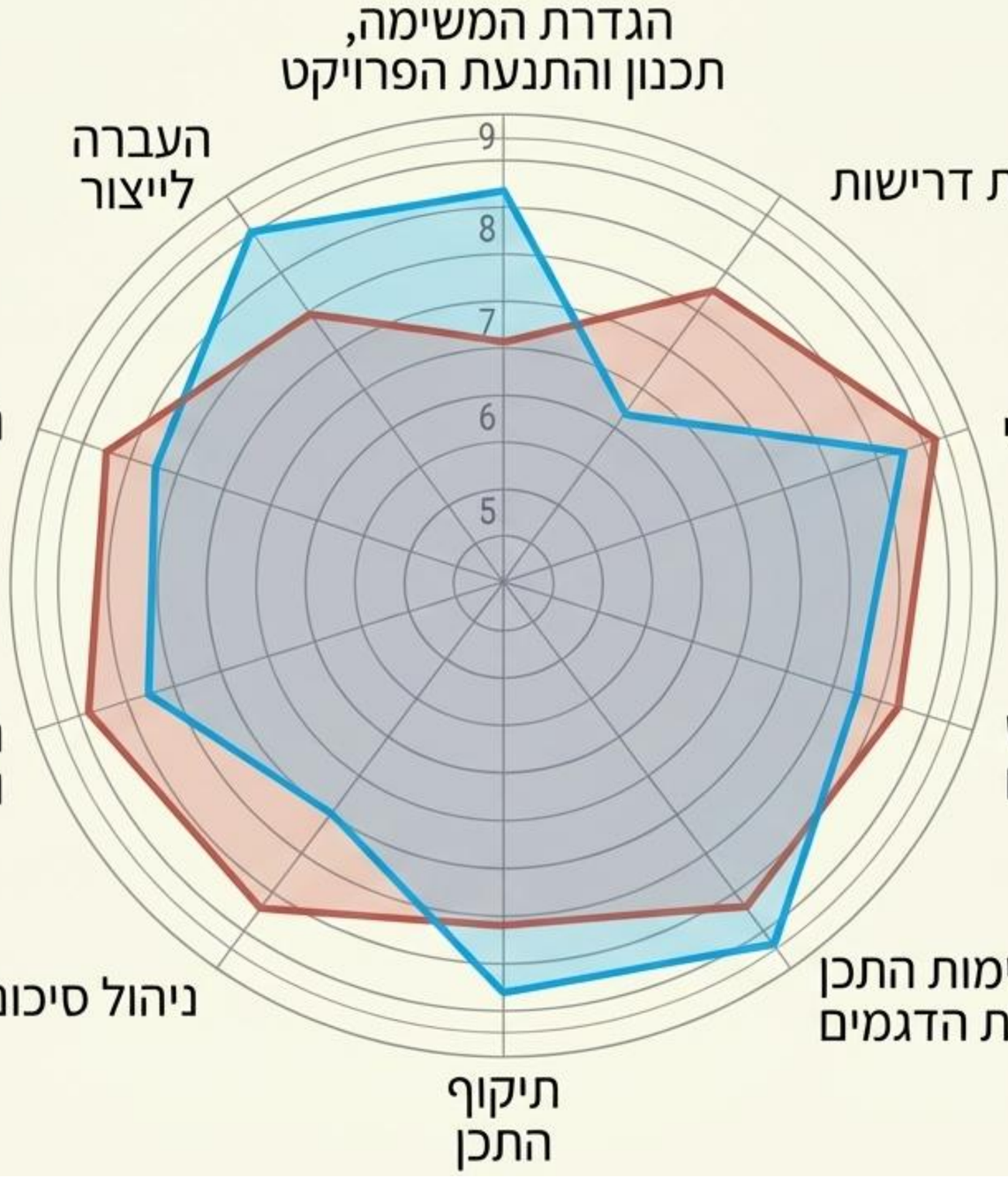


מטריצת הנדסת המערכות: השוואה רוחבית

	תוכנה	רכב	תעופה	ביטחוני
מתודולוגיה	Agile	Hybrid	V-Model + רגולציה	V-Model
דרישות	נמוך יחסית (10%)	בינוני-גבוה (50%)	מאוד פורמלי (100%)	מאוד פורמלי (100%)
Traceability (עקיבות)	מינימלי	חלקי (50%)	מלא (100%)	מלא (100%)
זמן פיתוח	קצר	בינוני	ארוך מאוד	ארוך מאוד
גמישות לשינויים	גבוהה מאוד	בינונית	נמוכה	נמוכה
V&V	אוטומציה	Safety-driven	קפדני + הסמכה	קפדני מאוד

השוואה דיאגנוסטית: שוק אזרחי לעומת שוק ביטחוני

שוק ביטחוני		שוק אזרחי
ארוך (כ-3 שנים). תהליכי הרכשה ממושכים.	 **זמן הגעה לשוק (TTM)**	קצר וקריטי (כחצי שנה). התנעה מהירה ויעילה.
שמרנות טכנולוגית ומבצעית, דרישות לקוח נוקשות, מגבלות מגבלות בטחון מידע.	 **מוקד טכנולוגי ועסקי**	חדשנות טכנולוגית, חווית משתמש, תחרות חריפה על מחיר.
ארוך (15-20 שנה). מבוסס על חוזי תחזוקה ארוכים ומכרזים (מונע לקוח).	 **מחזור חיים ולקוח**	קצר. לרוב אין לקוח מוגדר בשלב הפיתוח (מונע שוק).



יתרון ביטחוני:

- הנדסת דרישות: מוקפדת ויסודית יותר.
- ניהול סיכונים: מתוכנן ומובנה היטב (הלו"ז הארוך מאפשר תהליכי הפחתת סיכונים עמוקים).

יתרון אזרחי:

- אימות תכן (Verification): משופר משמעותית עקב כמויות ייצור עצומות וקנסות כבדים על כשלים.
- העברה לייצור: יעילות התנעה יעילות התנעה גבוהה וייצוריות מצוינת.

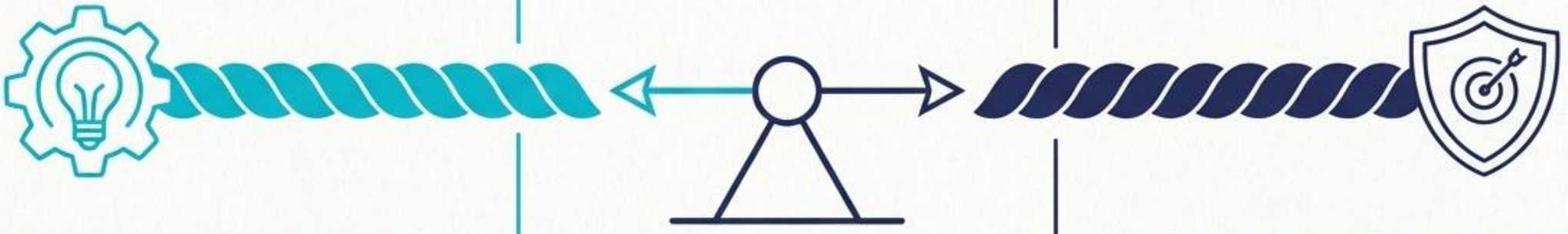
יתרון אזרחי:

- **אימות תכן** (Verification): משחדית יותר (הל"ז הפחחות סינויים ערמוקים).
- **העברה לייצור:** יעילות התונעה גבוהה וייצוריות וייצוריות מצווינת מחק כמויות ייצור עשומות קנגדים על קוס הוגודיים משלים.

סיכום: חוזקות הנדסיות מנוגדות (Trade-offs)

אימות תכן (Verification):
חזק משמעותית בשל קנסות כבדים על כשלי ייצור המוני.

העברה לייצור:
יעילות גבוהה, מותאם לכמויות גדולות.



הנדסת דרישות:
קפדנית, מובנית ושיטתית הרבה יותר.

ניהול סיכונים: מעמיק. הלו"ז הארוך מאפשר הפחתת סיכונים אסטרטגית, בעוד בשוק האזרחי הוא הישרדותי ("מהיום למחר").

חיכוך מערכתי:
נקודות תורפה בממשקי מהנדס המערכת

הממשק השיווקי

קשר חלש בין הנדסת המערכת לשיווק מוביל להתפתחות איטית של פורטפוליו המוצרים מול צרכי השוק.

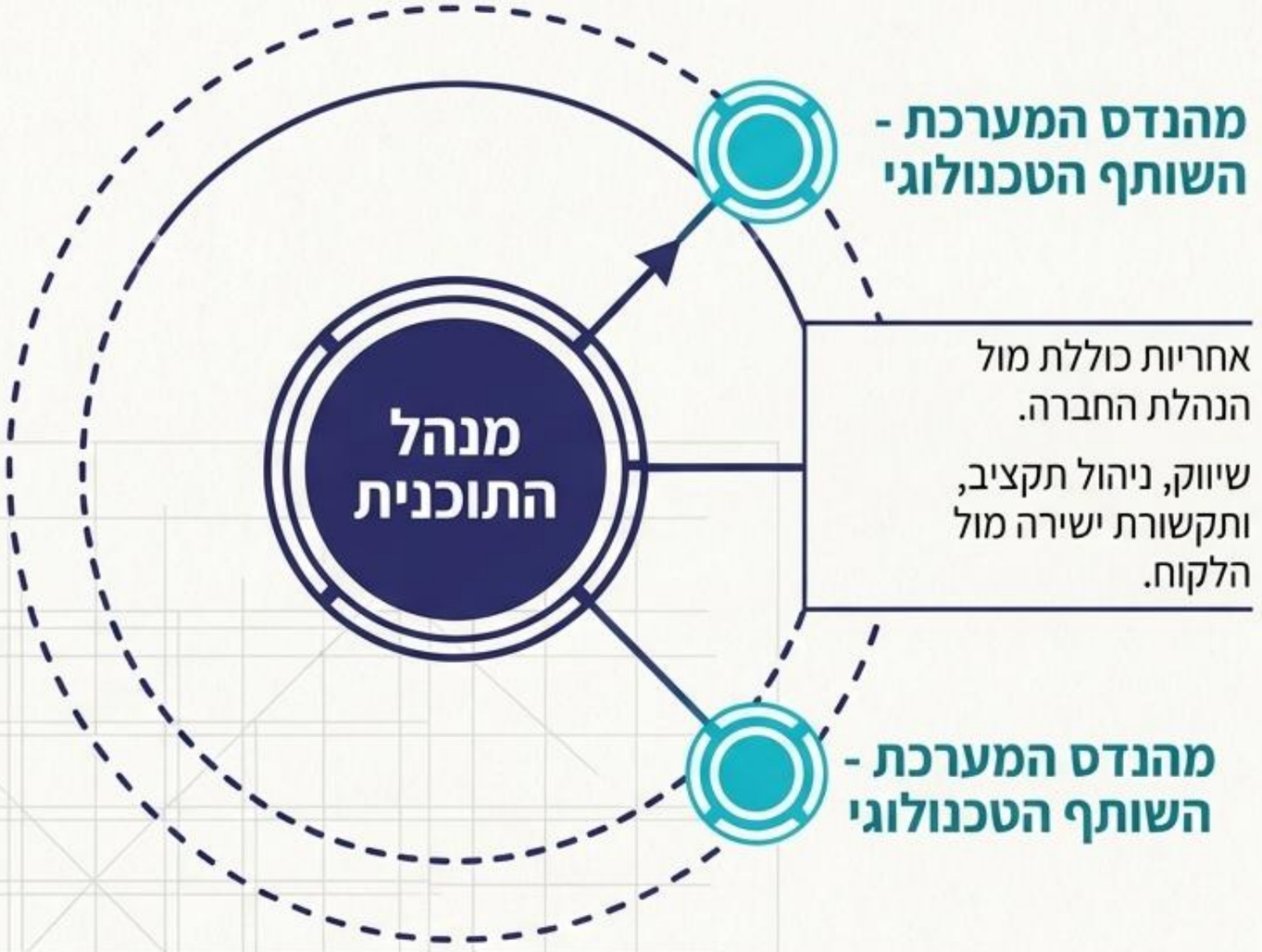
ריחוק מהלקוח

הממשק עם הלקוח נעשה כמעט תמיד דרך מנהל התוכנית. המהנדסים הדיסציפלינריים כמעט ואינם במגע ישיר עם משתמשי הקצה.

ניגודי אינטרסים

מנהל האיכות, המשמש כנציג הלקוח וגורמי הרישוי, נמצא לעיתים קרובות בניגוד אינטרסים מובנה מול חתירת מנהל התוכנית לעמידה בלו"ז.

היררכיה תפעולית בניהול פרויקטים ביטחוניים



שליח טכנולוגי

משמש כזרוע הטכנולוגית של מנהל התוכנית, ללא עיסוק ישיר בשיווק.

שומר הסף של התכן

מנהל את תכן המערכת, הניסויים וסיכוני הטכנולוגיה בלבד.

הנדסה משולבת

אחריות על מעבר לייצור, בדיקתיות (RAMST) ותחזוקה.

הדרך לשדרוג יכולות הנדסת המערכת בארגון

שלב 4: הטמעת קורסים להכנסת כלים מתקדמים (כמו מערכות לניהול דרישות) והעמקת שיטות העבודה.

שלב 3: הכשרת מהנדסים מובילים לתפקידי מהנדסי מערכת (ממ"ע) ייעודיים.

שלב 2: החלטות ניהוליות מחייבות – יישום תהליכי הנדסת מערכות הופך לחובה בכל פרויקט חדש.

שלב 1: הקמת מנהל משותף להנדסת מערכות ופורום מהנדסי מערכות מקצועי.

מקרה בוחן, אלאופ: מעבר לניהול דרישות ממוחשב

היוזמה: הארגון ביצע מהלך אסטרטגי להכנסת כלי ממוחשב לניהול דרישות פרויקטליות.

הביצוע: נערכו קורסים ייעודיים, הדרכות אישיות, ליווי צמוד בהכנסת דרישות, סינון, קישור ומעקב אחר שינויי לקוח.

התוצאה בשטח: למרות המאמץ האדיר, רק חלק מהמהנדסים בחרו לאמץ את הכלי ולעבוד איתו בפועל. למה?

+50 מהנדסי מערכת

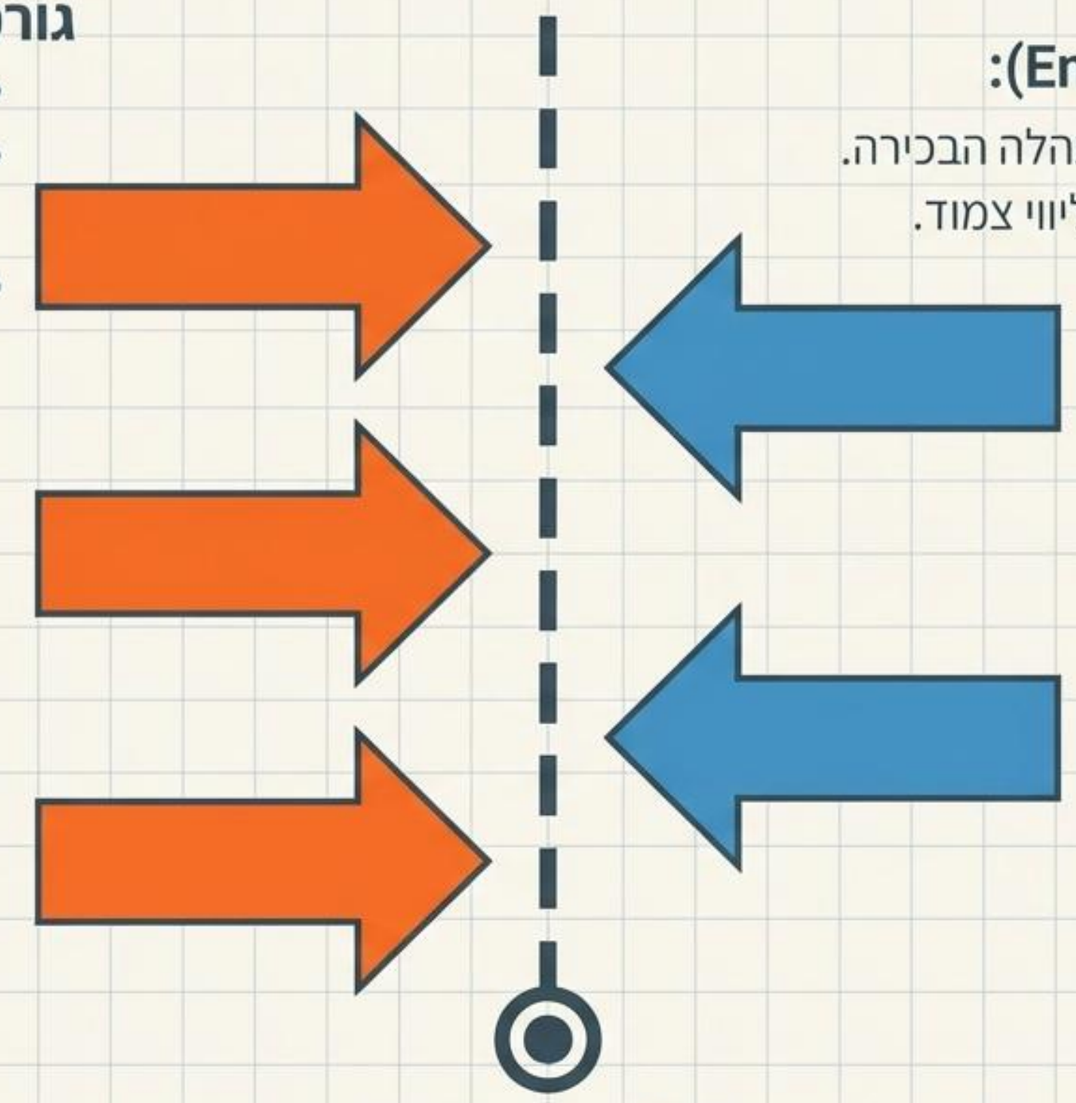
מבנה מטריציוני:
כפיפות ארגונית ליחידות עסקיות, וכפיפות מקצועית למינהל הנדסת מערכות.

גורמים מאפשרים (Enablers):

- מחויבות פומבית וברורה של ההנהלה הבכירה.
- הדרכה אישית מותאמת (1:1) בליווי צמוד.

גורמים מעכבים (Blockers):

- עומס עבודה שוטף כבד.
- סדרי עדיפויות סותרים (פיתוח מול מנהלה).
- מאפייני אישיות (התנגדות טבעית לשינוי).



הצלחת ההטמעה

לקחים קריטיים להטמעה ארגונית

1. עיתוי (Timing)

קביעה נכונה ומדויקת של מועד כניסת הכלי במחזור החיים של הפרויקט, כך שיתאים ללוח הזמנים ולא ייצור עומס מלאכותי.

2. אנשים (The Champion)

בחירת האדם המתאים בפרויקט לשמש כ"אלוף" (Champion), תוך שקלול מדוקדק של עומס העבודה הקיים שלו והתאמתו האישיותית להובלת שינוי.

3. שיווק פנימי (The Pitch)

"מכירה" נכונה של הכלי למקבלי ההחלטות (מנהלי פרויקטים, ראשי מנהלים). ללא מעורבות מלאה של ההנהלה בקבלת ההחלטות, ההטמעה תיכשל.

בנינו את זה נכון, או שבנינו את הדבר הנכון?

Verification (אימות)

השאלה:
האם המערכת עומדת בדרישות שהוגדרו במפרט הכתוב?

התהליך:
פורמלי וטכני. שימוש בבדיקות, ניתוחים, סקירות או הדגמות.

המטרה:
להוכיח שרכיבי החומרה והתוכנה תואמים לנייר.

Validation (תיקוף)

השאלה:
האם המערכת עונה על הצורך המבצעי בסביבת האמת?

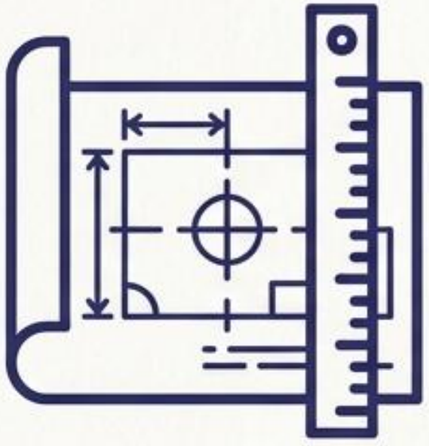
התהליך:
בחינת התוצר הסופי בפעולה אמיתית על ידי הלקוח/משתמש.

המטרה:
להבטיח שהמוצר אכן משרת את המשימה לשמה הוא נוצר.

תיקוף (Validation)

האם בנינו את המערכת הנכונה?

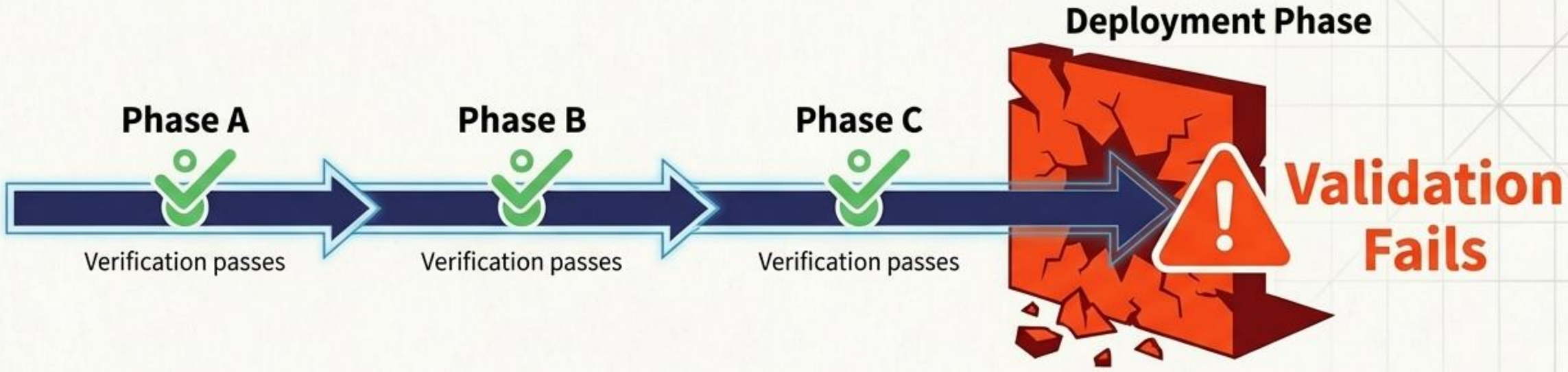
בחינה מול המציאות. האם המערכת ב באמת עונה על הצורך המבצעי האמיתי של בעלי העניין בסביבת העבודה הסופית.



אימות (Verification)

האם בנינו את המערכת נכון?

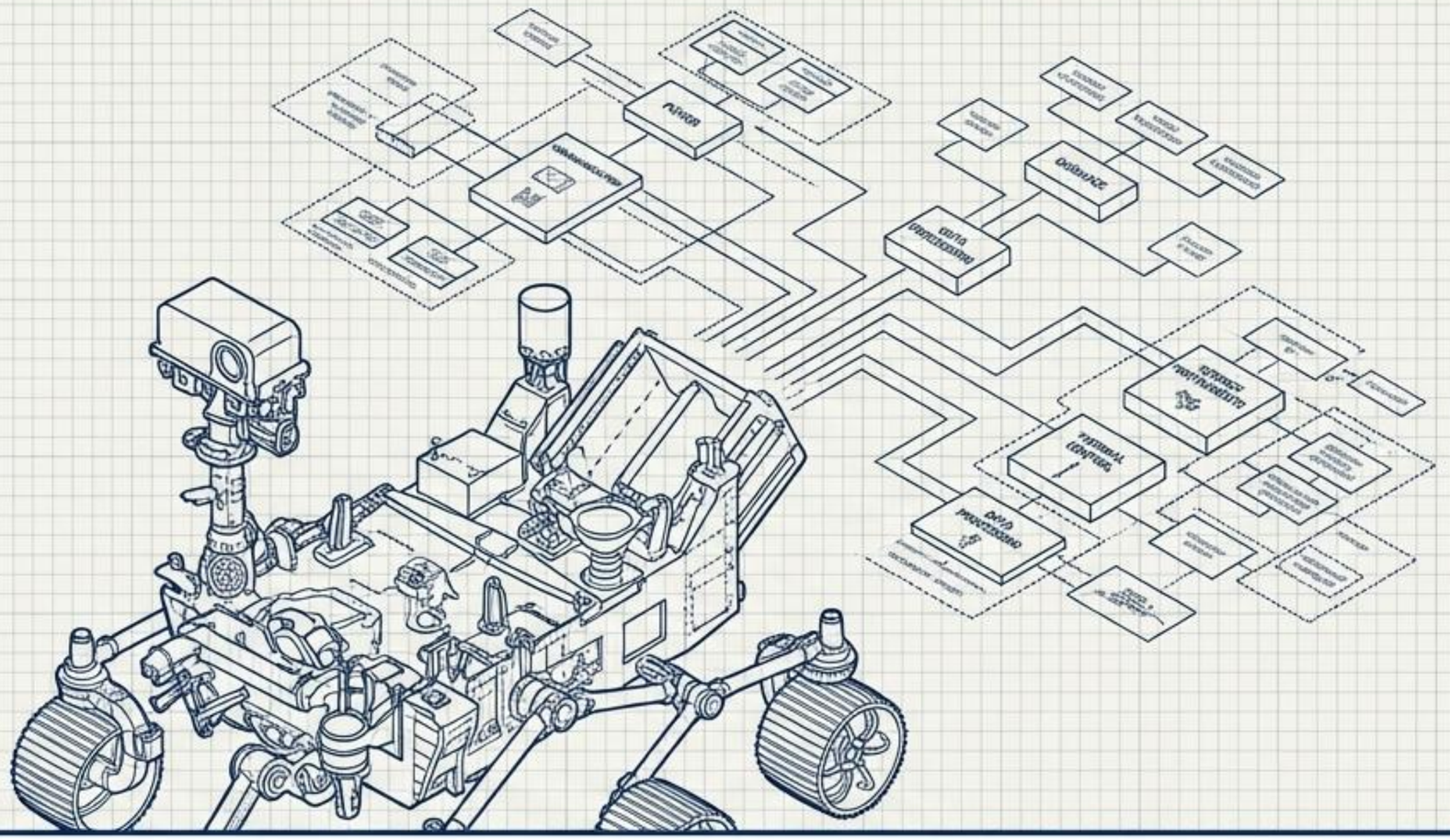
תהליך פורמלי (בדיקה, אנליזה, הדגמה). מוודא שהחומרה/תוכנה עומדת במדויק בכל הדרישות והמפרטים שהוגדרו.



הסכנה הקריטית: המערכת צולחת את כל מבחני האימות (עומדת במפרט), אך **נכשלת בשלב התיקוף** הקריטי מול הלקוח במציאות.

המחיר: עיכובים אדירים, עבודות חוזרות (Rework) יקרות, ופגיעה באמון.
(דוגמאות: פרויקטי תשתית צבאיים ואזרחיים כמו 'רמב"ם' או מטרות אוויריות).

התרופה המונעת: פיתוח ConOps חזק בשלבים הראשונים, בשילוב תקשורת איטרטיבית שוטפת עם הלקוח.



The Gold Standard: NASA מתודולוגיית

מעבר ממקרי בוחן מקומיים לסטנדרט העולמי המוביל. גישת NASA לניהול מורכבות, הפחתת סיכונים שיטתית, וניהול מחזור חיים קפדני המחבר בין ההנדסה לדרישות המבצעיות האמיתיות.

מילון המונחים המדויק: הסטנדרט של NASA

Verification (אימות)

השאלה: האם בנינו את המערכת נכון?
הגדרה: תהליך פורמלי המוודא שהמערכת עומדת במדויק בכל דרישות המפרט ההנדסי.

Validation (תיקוף)

השאלה: האם בנינו את המערכת הנכונה?
הגדרה: הוכחה שהמערכת מספקת מענה אמיתי לצרכים ולתרחישים המבצעיים של משתמש הקצה (מבוסס ConOps).

Qualification (הסמכה)

הגדרה: וידוא שתכן המערכת מסוגל לעמוד ולפעול כנדרש בתנאי הסביבה הקיצוניים הצפויים.

Acceptance (קבלה)

הגדרה: בדיקות פרטניות המבוצעות על כל יחידת ייצור להוכחת איכות עבודת הייצור מול התכן שאושר, טרם מסירה ללקוח.

מחזור חיים של פרויקט: מתודולוגית NASA

תהליך זה מתפקד בפועל כפיתוח אג'לי - הדרישות נבחנות ומתעדכנות באופן איטרטיבי מול ציפיות בעלי העניין.

מחזור החיים השלם: מגיבוש רעיון ועד סיום משימה

Formulation (גיבוש ותכנון)

White Assistant
Pre-Phase A & A: לימוד קונספט, בניית אב-טיפוס להורדת סיכונים והגדרת דרישות מפתח.

White Assistant
Phase B: תכן ראשוני, בדיקת דרישות מורחבות אל מול התרחישים המבצעיים.

Approval (אישור)

Implementation (יישום)

White Assistant
Phase C & D: תכן מפורט סופי, ייצור, הרכבה, אינטגרציה ובדיקות.

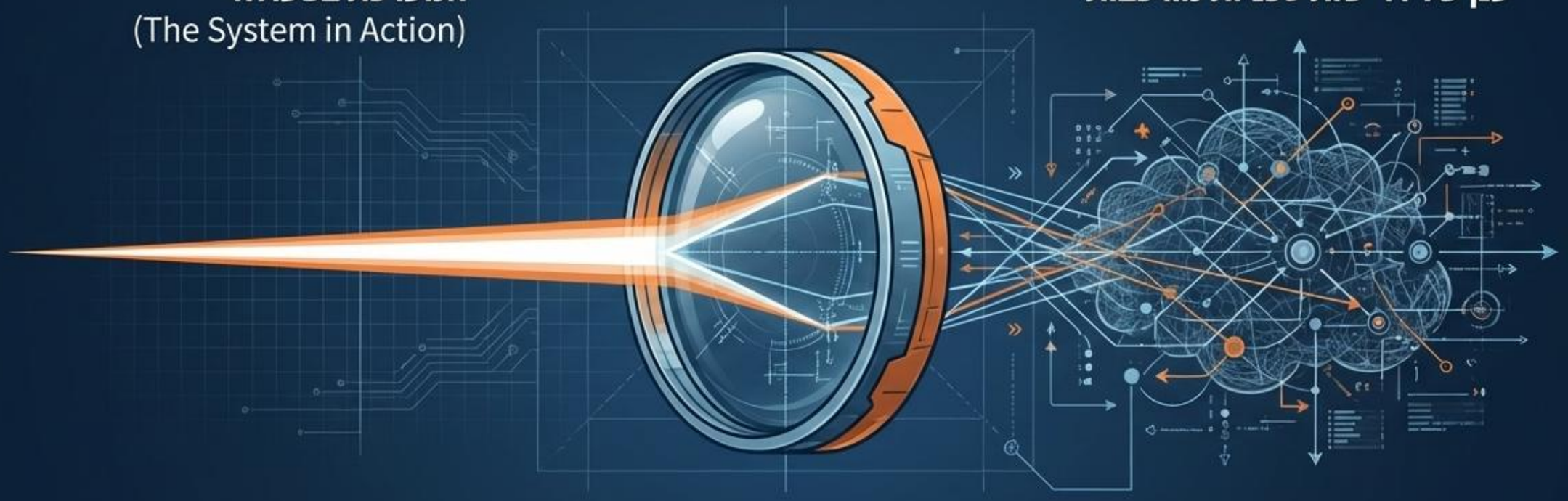
White Assistant
Phase E & : תפעול, תחזוקה, ולבסוף - סגירה ופירוק המערכת.

White Assistant
פרדוקס התדמית: למרות התדמית הנוקשה, מדובר למעשה בתהליך פיתוח אג'ילי – הדרישות נבחנות ומתעדכנות ללא הרף כדי לעמוד בציפיות בעלי העניין (שינויים לאחר אישור ייחשבו כפיתוח חדש).

ConOps: המצפן של הנדסת המערכות

ענן של דרישות טכניות מורכבות

המערכת בפעולה
(The System in Action)



ככל שדרישות המערכת הופכות למפורטות ועמוסות טכנית, קשה יותר לבעלי העניין לדמיין את התוצר הסופי.

ה-ConOps (Concept of Operations) פותר זאת על ידי תרגום הדרישות לתרחיש מבצעי מוחשי בשטח.

בקרת איכות מובנית: ה-ConOps משמש כמנגנון בקרה קריטי קריטי לאיתור דרישות חסרות או סותרות בשלבים המוקדמים.

יסודות הניהול הטכני החוצה-ארגון (Crosscutting)

קריאות סיכון תחום : DOMAIN RISK READOUTS

עקרונות הליבה טכני: TECHNICAL MANAGEMENT CORE PRINCIPLES

ניהול ממשקים: הגדרה קפדנית של סמכויות ואחריות בכל ממשק, פנים וחוץ ארגוני. ארגוני.

הבנת תכולת העבודה: השקעת זמן מראש בפיתוח מבנה תכולת עבודה (WBS) טכני טכרי מקיף.

סקרי אבני דרך: אינם רק סימון 'וי' חוזי, אלא הערכה קריטית המבוצעת רק כאשר קריטריוני הכניסה מתקיימים במלואם.

בקרת תצורה (Configuration Control): קריטית להבנת ההשפעה של כל שינוי תכן על המערכת ועל תוצאות ניתוחים קודמים.

התמונה המלאה

עמידה במפרט (Verification) היא תנאי הכרחי אך לא מספיק.

הצלחה נמדדת מבצעי (Validation) מבוסס ConOps איתן משלב אפיס.

שותפות ממוקדת

מהנדס המערכת הוא חהנדס הכענות השותף והשליח הטכנולוגי – עליו עליו להשאיר את המעטפת הניהולית הניהולית והשיווקית למנהל הפרויקט, ולהתמקד באינטגרציה ותכן.

התאמה מוסדית

הנדסת מערכת אינה תבנית אחידה.

התעשייה האזרחית מכוונת TTM וייצור (אימות), בעוד הביטחונית דורשת ניהול סיכונים סיכונים כבד ודרישות קפדניות.

הנדסת מערכות: השלם הגדול מסך חלקיו

מצפן מבצעי (נאס"א):

בסביבות קריטיות, ה-ConOps וההבחנה הבלתי מתפשרת בין אימות **אימות לתיקוף** הם הגבול בין כישלון להצלחה.

מהירות ומיקוד (השוק האזרחי):

הצורך ב-TTM מהיר מחייב גמישות אג'ילית, התמקדות בלקוח הקצה ויעילות בייצור.

הגורם האנושי (אלאופ):

תהליכים לא עובדים בוואקום. הצלחה הצלחה תוגולה תלויה במחויבות ההנהלה ובהבנת עומסי המהנדס בשטח.

הנדסת מערכות אינה רק אוסף נהלים – היא התרבות המאפשרת תרגום צרכים מורכבים למציאות עובדת. מנהל התוכנית אחראי על השורה התחתונה; מהנדס המערכת אחראי לכך שהיא אכן תעבוד.

סיכום אסטרטגי: 3 עוגנים לשיפור ארגוני

1. אימוץ תפיסה אג'לית בהנדסת מערכת

אימוץ הגישה של התעשייה האזרחית ושל NASA: בחינה ועדכון איטרטיבי מתמיד של הדרישות מול ציפיות בעלי העניין, ולא הסתמכות על מסמך סטאטי.

2. השקעה מאסיבית ב-ConOp

בניית תרחישים מבצעיים יחד עם השיווק והלקוח עוד לפני הצלילה לתכן מפורט. זהו הגשר היחיד לפתרון הנתק התחק השיווקי ולמניעת כשל ב-Validation.

3. מחויבות הנהלה כתנאי סף

תהליכי שינוי עמוקים (כמו ניהול דרישות מתקדם) לא קורים מעצמם. הם דורשים בחירת אלופים, עיתוי עיתוי מדויק, ומעורבות אקטיבית וגלויה של ההנהלה הבכירה.