אתגרים בשילוב וניהול כולל של אמינות ובטיחות בפרויקטי פיתוח ברפאל

דר' עמית טלר

ראש תחום אמינות

מרכז אמינות ובטיחות מערכות

הכנס הלאומי לאיכות
נובמבר 2015

נושאי ההרצאה

1. הנדסת אמינות ובטיחות - מקומה בארגון.
2. פעילות מרכז אמינות מול חטיבת היבשה ברפאל.
3. פעילויות עיקריות.
4. מסקנות וסיכום.

הנדסת אמינות ובטיחות
תפקידה ומיקומה בארגון

הנדסת אמינות ובטיחות, דיסציפלינה הנדסית לכל דבר ועניין, משולבת בהנדסת המערכת ונותנת גיבוי מקצועי לראשי פרויקטים, למהנדסי מערכת ולמפתחים בקבלת החלטות טכניות, פרויקטאליות ומבצעיות.

הנדסת אמינות ובטיחות צריכה להשתלב בתהליך קבלת ההחלטות משלב התכן ופיתוח הראשוניים

- חקר ביצועים וניתוח מערכות
- ניתוח אמינות למערכות ורכיבים
- בטיחות מערכות
- ניתוחים הנדסיים
- מודלים הסתברותיים
- ניהול אמינות ובטיחות

מה זה אמינות?

"פסיכולוגי"
"איכותי"

בטחון בכך שהמערכת תעבוד ללא תקלות

מצד המשתמש

"הסתברותי"

ההסתברות לפעול בצורה תקינה

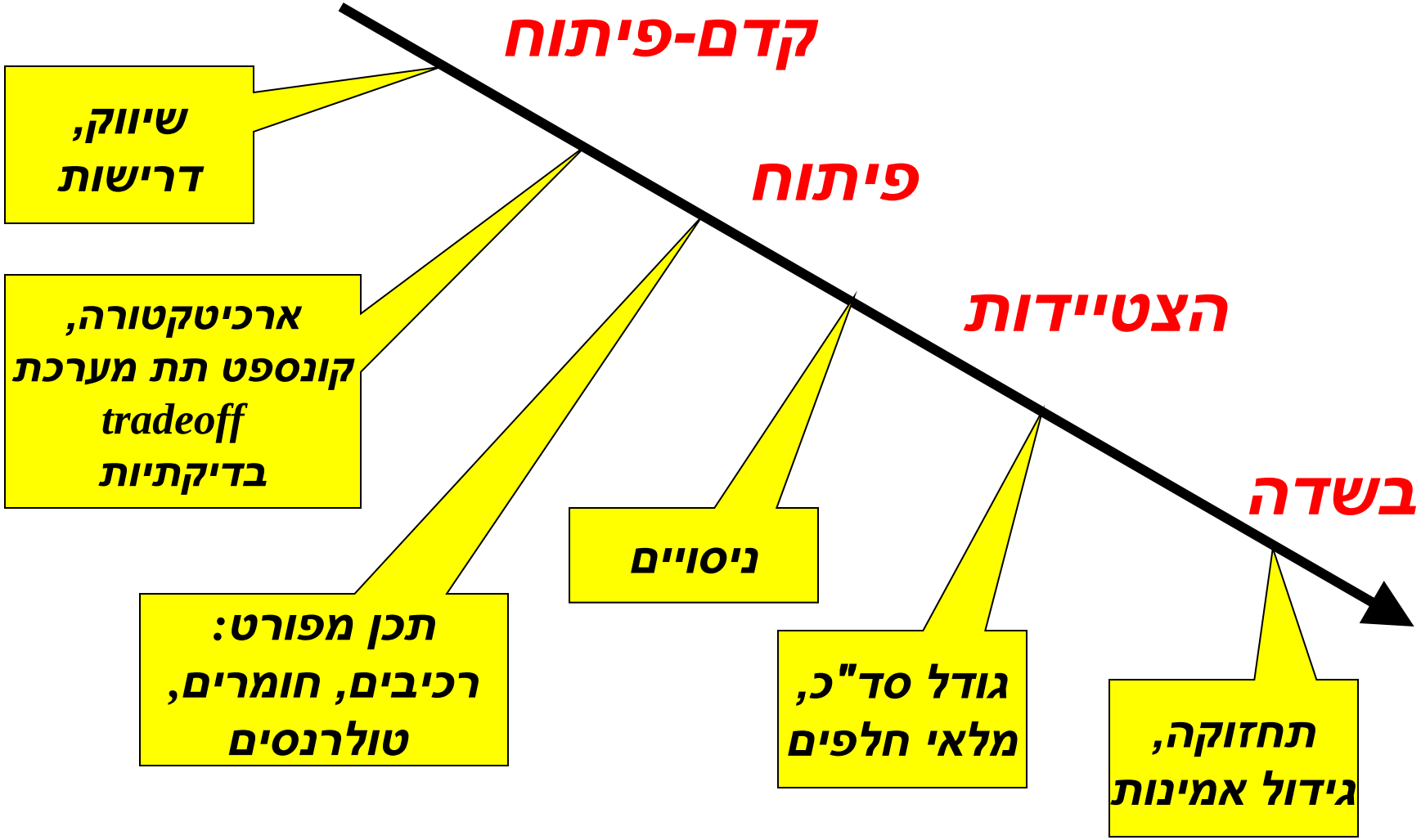
מצד מהנדס אמינות

"הנדסי"

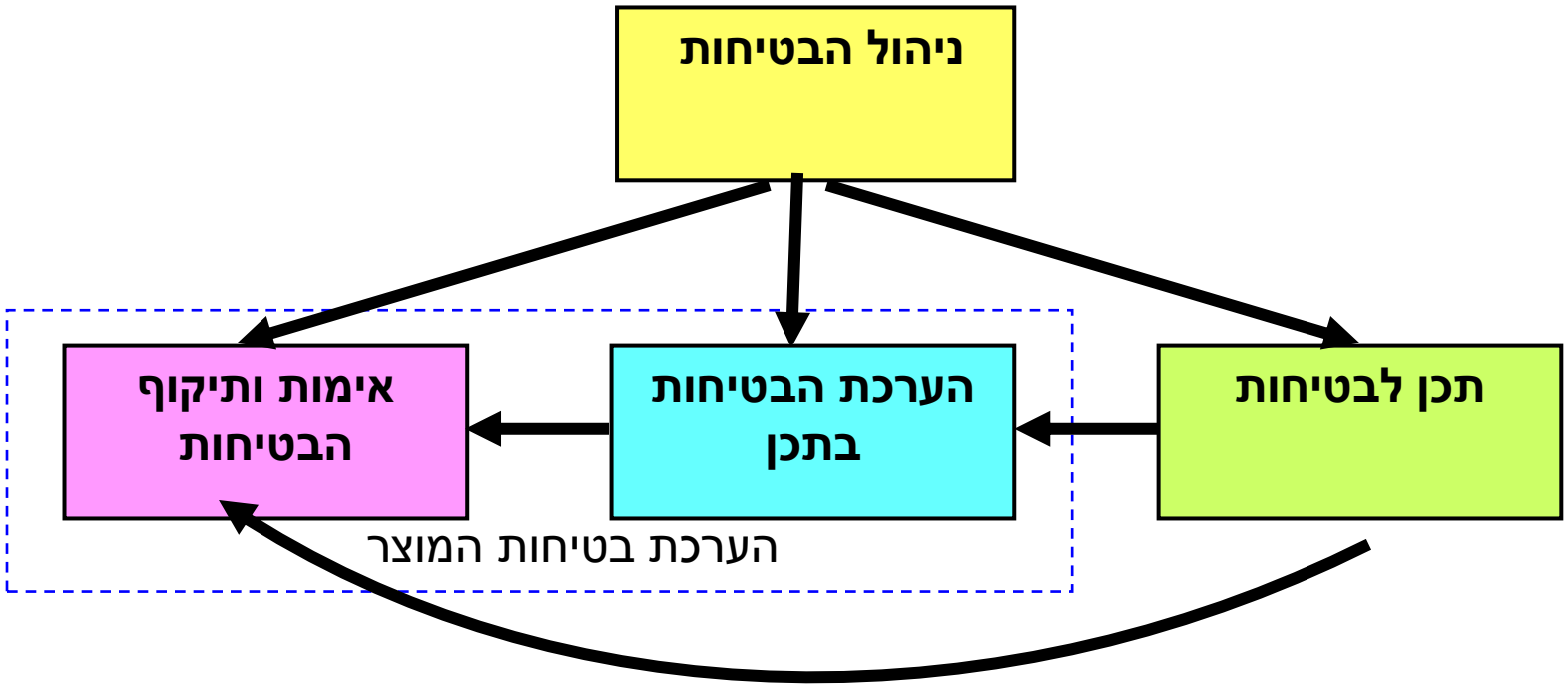
רובוסטיות, שולי בטחון חסינות לתקלות

מצד המפתח

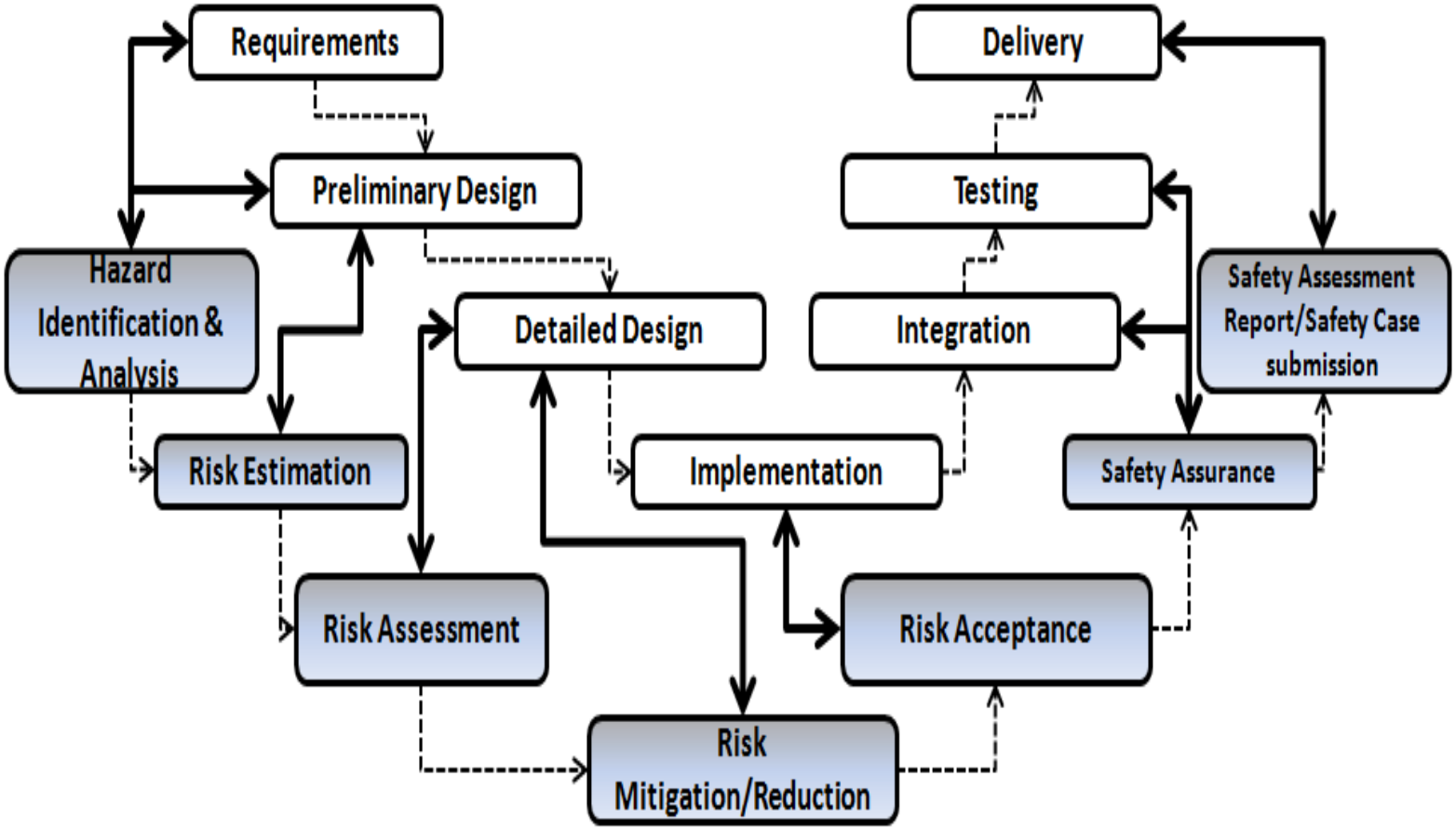
אמינות בשלבי הפרויקט



ובמקביל....
ערוצי פעילות להשגת יעדי הבטיחות



ליווי הפיתוח בהיבטי הבטיחות



מטרה עיקרית

צורך בטיפול מובנה וייעודי באמינות ובטיחות כחלק מכלל הדרישות ושיקולי התכן ושילובו בתהליך קבלת ההחלטות הטכניות והניהוליות.

<u>האתגר</u>: איך עושים את כל זאת בארגון המבצע מאות פרויקטים בכל זמן?

חטיבת יבשה ברפאל

פיתוח ושיווק מוצרים ופתרונות שלמים ואינטגרטיביים בתחומי התקיפה המדויקת, התמרון והלוחמה ברשת, מיגון ושרידות, הגנת גבולות ומתקנים ביבשה ובים ללקוחות בישראל ובעולם.

חטיבת יבשה

- **מנהלת נשק טקטי מדויק**
- **מנהלת מערכות לחימה ימיות**
- **מנהלת מערכות שרידות ותמרון**
- **מנהלת לוחמת מסגרת**

פעילות RAMS מול חטיבת יבשה (אפיון הפרויקטים)

- **פיתוח מלא (Full Scale Development - FSD)**
  - תהליך פיתוח מלא משלב הקונספט, פיתוח, ניסויים, ייצור והעברה ללקוח.
- **פרויקטי שדרוגים והתאמות**
  - פיתוח טכנולוגי המבוסס על מערכת קיימת – שדרוג טכנולוגי, הוספת יכולות, שינויים פונקציונאליים
- **פרויקטים "מיוחדים"**
  - חקר ביצועים - עדכון של גזרות סיכון (Weapon Danger Area) למערכות נשק
  - ניהול בטיחות – בניית Safety Case
  - ניתוחי אמינות ובטיחות של מערכות משולבות (System of Systems)
- **תשתיות ניהוליות**
  - מענים למכרזים, הצעות תמחור, ניהול ובקרה על קבלנים

פעילות RAMS בפרויקטים
פרויקטי פיתוח מלא FSD -

- מטרה: <u>חבילת RAMST המותאמת לדרישות הלקוח</u>
  - אמינות – תוכנית ניהול אמינות, מודל אמינות, חיזוי אמינות, ניתוח אופני כשל, תוכנית גידול אמינות
  - בטיחות – תוכנית בטיחות (SSPP) , זיהוי/ניתוח סיכונים ראשוני (PHL/PHA) , ניתוח סיכונים מערכתי (SHA) , ניתוח סיכונים פונקציונאלי (FHA), דו"ח הערכת סיכונים (SAR)
  - אחזקתיות – ניתוח אחזקתיות דרג א'/ב'
  - בדיקתיות – ניתוח בדיקתיות
  - זמינות – ניתוח זמינות

פעילות RAMS בפרויקטים
פרוייקטי שדרוגים והתאמות

- "חבילת בטיחות"
  - תוכנית בטיחות (SSPP) , זיהוי/ניתוח סיכונים ראשוני (PHL/PHA) , ניתוח סיכונים מערכתי (SHA) , דו"ח הערכת סיכונים (SAR) .
- אמינות
  - הערכת אמינות מערכת ("דלתא" לעומת חיזוי אמינות)

ערוצי השתלבות מרכז אמינות בפרויקט והאתגרים

פעילות	אתגרים	פתרונות
ועדת בטיחות פרויקטאלית	"ועדת ייעוץ" <-----> "מנגנון פורמאלי"	• החלטה ספציפית בפרויקט
דרישות בטיחות	• הגדרת דרישות בטיחות ספציפיות מעבר לדרישות הסטנדרט (MIL-STD-882)	• תקנים ומדריכים
רשימה וניתוח סיכונים ראשוני	• במקרים רבים ארכיטקטורת המערכת לא בשלה. • הערכות איכותיות להסתברות אירועים בטיחותיים.	• שימוש ב brainstorming • שימוש בניתוחים קודמים בעלי רמת בשלות גבוהה
ניתוח סיכונים מערכתי	• הערכה הסתברותית לכשלים בבטיחות תוכנה ואירועי טעויות אנוש. • שינויי תכן מבוצעים לקראת סיום הפיתוח ושאינם באים לידי ביטוי בדו"ח הבטיחות	• הערכות הנדסיות על בסיס ניסיון העבר. • עבודה עפ"י העיקרון של "מסמך מתגלגל"

ערוצי השתלבות מרכז אמינות בפרויקט והאתגרים

פעילות	אתגרים	פתרונות
ניתוחי אמינות	• מתבצעים רק בפרויקטי פיתוח מלא על אף השפעתם על התכן ועל תכנון ILS	• "הערכת אמינות" המתבססת על עבודות קודמות תוך התאמה למערכת הספציפית ואופי פעולתה.
אמינות בתכן	• ממשק נדרש מול מפתחי המכלולים ולא מול הנהלת הפרויקט והנדסת המערכת	• ביצוע עבודות ממוקדות בדיסציפלינות ההנדסיות
מעקב תקלות בשדה	• לא מתקבלים נתונים מהלקוחות במקרים בהם אין חוזה לתהליך גידול אמינות	• הכללת תהליך גידול אמינות ב SOW
ניסויי אמינות (אימות ותיקוף)	• לא מתבצע כיום במרבית הפרויקטים	• מתבצע תהליך מעקב אמינות

אתגרים ייחודיים בהתנהלות מול חטיבת יבשה

- תוכנית עבודה גמישה – לא ניתן לחזות תכולות עבודה יותר משלושה חודשים מראש עקב תנאי השוק הדינמיים .
- פרויקטים "נמרחים" - שינויי תכן משמעותיים נעשים לעתים לאחר CDR בעקבות תקלות המתגלות ב QUAL . זהו שלב שבו הפוקוס הוא על סיום הפרויקט.
- ממשקים מול חטיבות אחרות ובין מנהלות בתוך החטיבה – מרכז אמינות כגורם הנמצא בתווך.
- דגש מועט לעבודות אמינות לעומת בטיחות עקב העניין הרב בבטיחות.

בשורה התחתונה –
תרומת פעילות אמינות ובטיחות לפרויקט

- תמיכה בקבלת החלטות, בכל הרבדים (לקוח, מערכת, הנדסה):
  - טיפול מתודי ומובנה בדילמות הקשורות להתמודדות עם כשלים.
  - נתונים ומידע תומכי החלטה.
- הצפת בעיות מוקדמת בשלב הנייר.
- הצגת סטאטוס אמינות צפויה של המערכת, באופן שקוף וברור לפרויקט, למפתחים, וללקוח.

תודה רבה!