פיתוח מדריך לאבטחת חסינות מערכות בפני טעויות תפעול

ד"ר אביגדור זוננשיין - הטכניון
אבי הראל – ארגולייט
מרכז גורדון להנדסת מערכות - הטכניון

מי צריך עוד מדריכים?

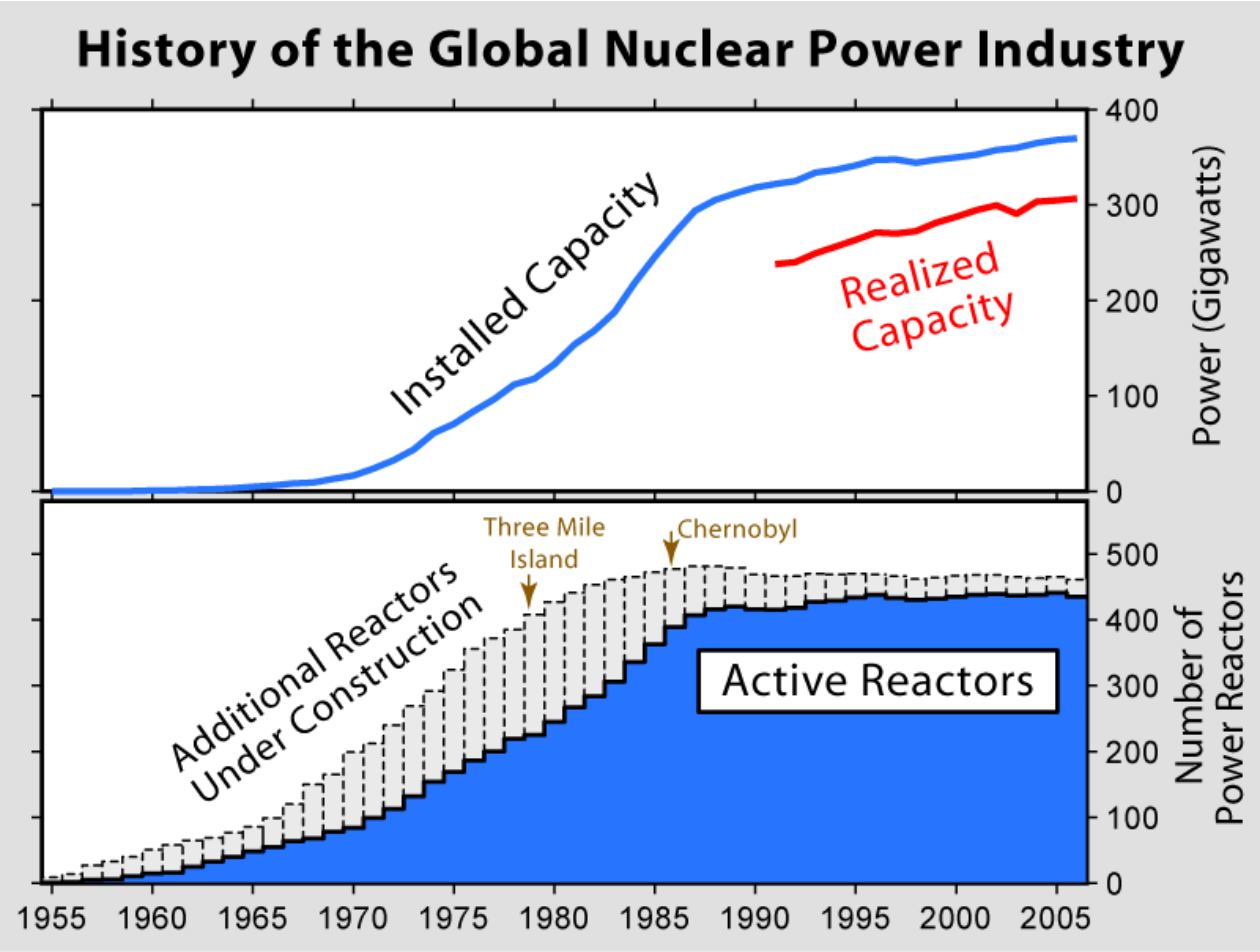
- יש ניתוח גורמי כשל
- יש ניהול סיכונים
- יש הנדסת גורמי אנוש

הבעיה היא בשילוב של כל הידע הקיים לכדי מתודולוגיה הנדסית.
צריך דוגמא

Three Mile Island – TMI 2– 1979

- כור חדש – 40 ימים בפעולה
- 5 ימים של היתוך הכור
- המפעילים אינם מתמצאים במצב

Effect on Industry



מה המפעילים נדרשו לדעת תוך 13 שניות

- תקלה במערכת הבקרה
- שתי משאבות עיבוי הפסיקו לעבוד
- שני ברזים במערכת קירור חירום סגורים
- שסתום שחרור לחץ נשאר פתוח
- תקלה באינדיקטור למצב השסתום

איך הם יכלו לדעת?

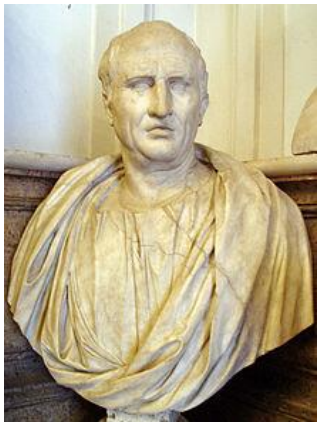
- 800 התרעות
- 300 התרעות מהבהבות תוך 5 דקות
- היו אינדיקציות לכך שהברזים סגורים
  – איש בחדר הבקרה לא הבחין באינדיקציות הללו
- מידע שגוי לגבי שסתום שחרור הלחץ
- מידע סותר לגבי מצב הכור
- חוסר וודאות לגבי הסיכונים בגין טעות החלטה

הצורך במניעת טעויות תפעול

- 90% מהתאונות בתעשיה
- 75% מהתאונות בתחבורה
- 50% מתפוקת העובדים
- קריטי למערכות ביתיות
- קריטי למערכות לשירות הציבור

נושא זה צריך להכלל ברשימת
הנושאים להתייחסות בכל פרויקט.
צריך להבין למה זה קורה.

To err is human



Cicero 106-43 BC

Weinberg 1971

במקום להאשים את המפעיל ...
צריך להבין את הפסיכולוגיה של
המתכנתים.

גירסת חוק מרפי בנושא טעויות תפעול

אם התכן מאפשר למפעיל לטעות –
במוקדם או במאוחר הטעות קרה תקרה.

יש למנוע כל אפשרות לטעות מפעיל

מטרות המדריך לאבטחת חסינות

- להציג דרכים לאיתור ולאיבחון גורמי כשל ואופני הכשל בעוד מועד, עוד בשלב התכן
- להציג שיטות למניעת הכשלים המזוהים
- לתמחר את הפתרונות, במונחי חסינות ועלות יישומה

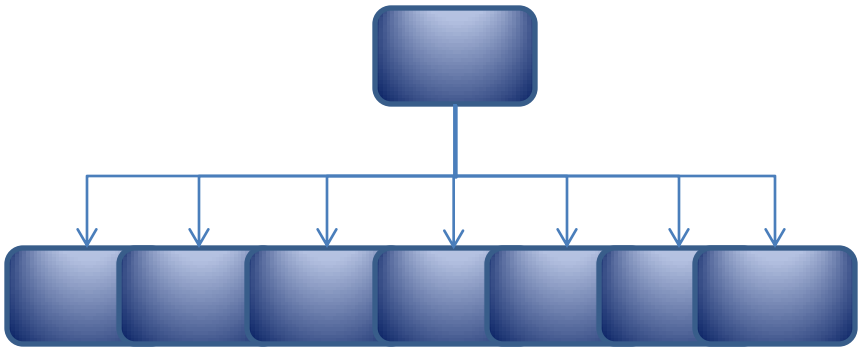
צריך להסביר מדוע עד היום
עדיין לא פותח מדריך כזה.

מי צריך עוד מדריכים?

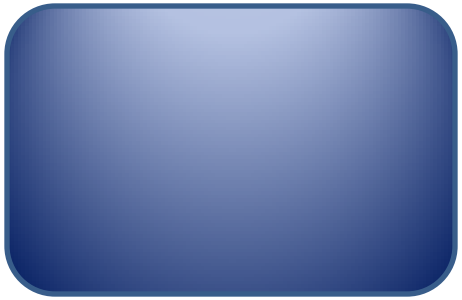
- יש ניהול סיכונים
  – אפשר להשוות פתרונות, אבל מהם הפתרונות?
- יש ניתוח גורמי כשל (FTA, ETA, FMEA, HAZOP)
  – האם המפעיל ידע להתמודד עם התקלות?
- יש הנדסת גורמי אנוש
  – האם המומחה מכיר את תנאי ההפעלה?

צריך דוגמא

טעויות בתכן עומס המסך



רחוק מהעין – רחוק מהלב!



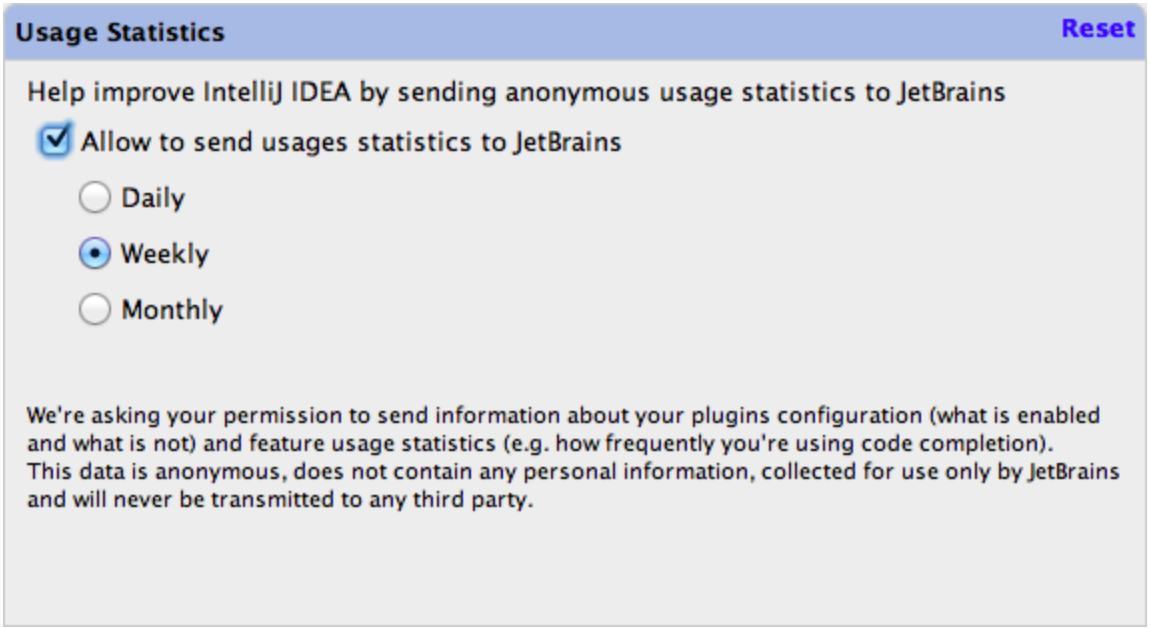
תפסת מרובה – לא תפסת!

הבעיה היא שמהנדס המערכת
אינו יודע מה לדרוש מהמתכנן

תהליך פיתוח המדריך

- רקע אישי
  - הנדסת תוכנה => מערכות => גורמי אנוש
- ארגולייט
  - פיתוח כלי תוכנה לאיתור טעויות תפעול
- אילטם-אינקוזי
  - ק"ע ניהול סיכונים => גירסת פיילוט של המדריך
  - ק"ע אבטחת חסינות => תיקוף המדריך
- מחקרים במרכז גורדון
- תיקוף ראשוני - עבודת מסטר של גלעד סגל מרפאל

ההתחלה: ארגולייט



Ergolight - Tools for Usage Analysis

- 1996 – Patent – automated usability testing
- 1997 – Article to CHI 98 rejected
- 1998 – Article to Leveson conference rejected
  - Usability Problem Indicator (UPI) => STAMP
- 1999 – Best of Comdex/Israel

ד"ר משה ויילר: ק"ע ניהול סיכונים - 2009

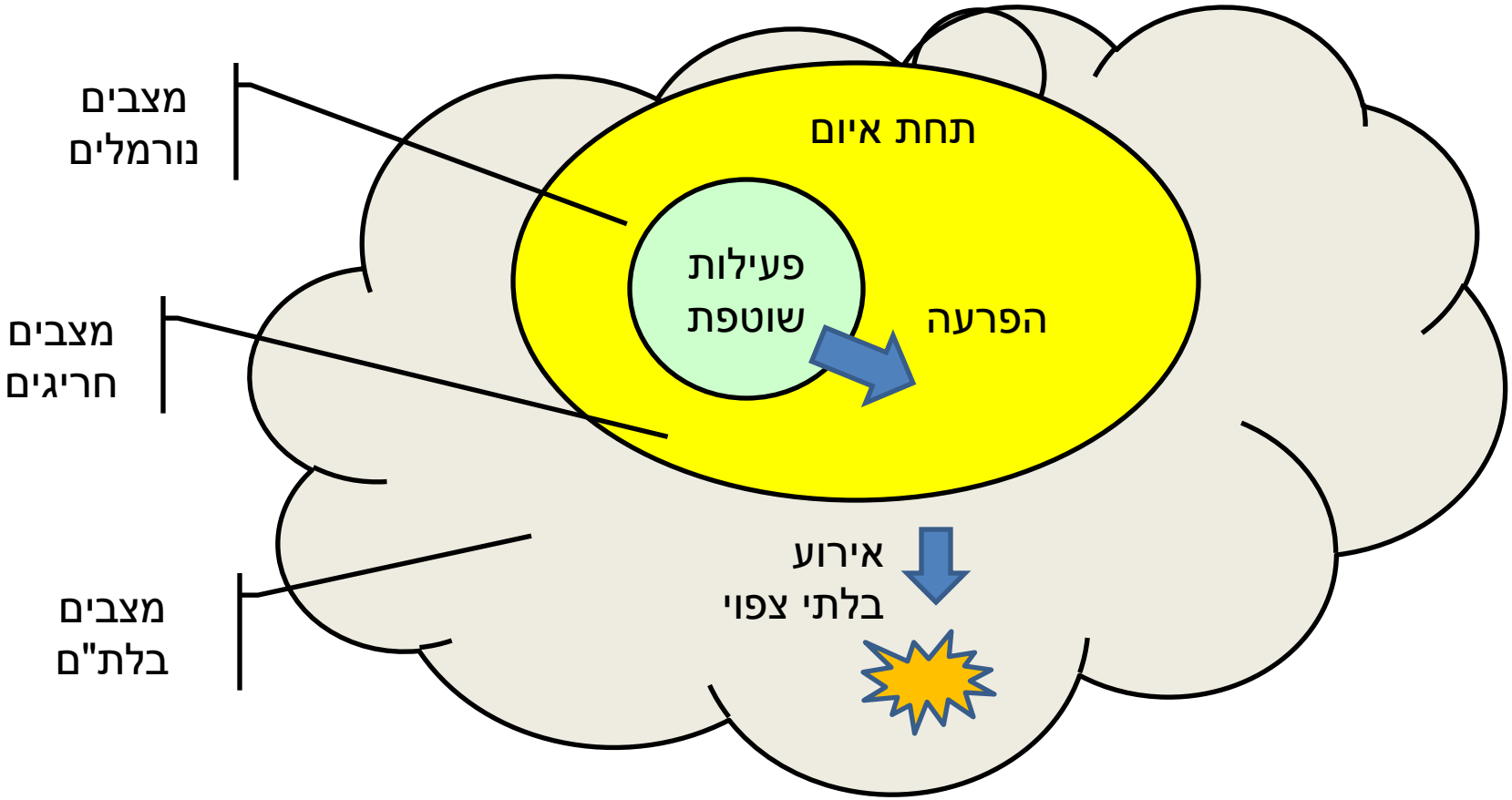
- 2 מפגשים: ניהול סיכוני תפעול
- ניתחנו 15 מקרים הקשורים בטעות אנוש
  – מסקנה: להתמקד באיפיון מצבים חריגים
- אפיינו 6 קטגוריות של טעויות
  – מסקנה: להתמקד בסיכונים של המצבים החריגים
- הצענו שיטות להתמודדות עם הטעויות הללו

צריך לפתח ולאמת את השיטות המוצעות

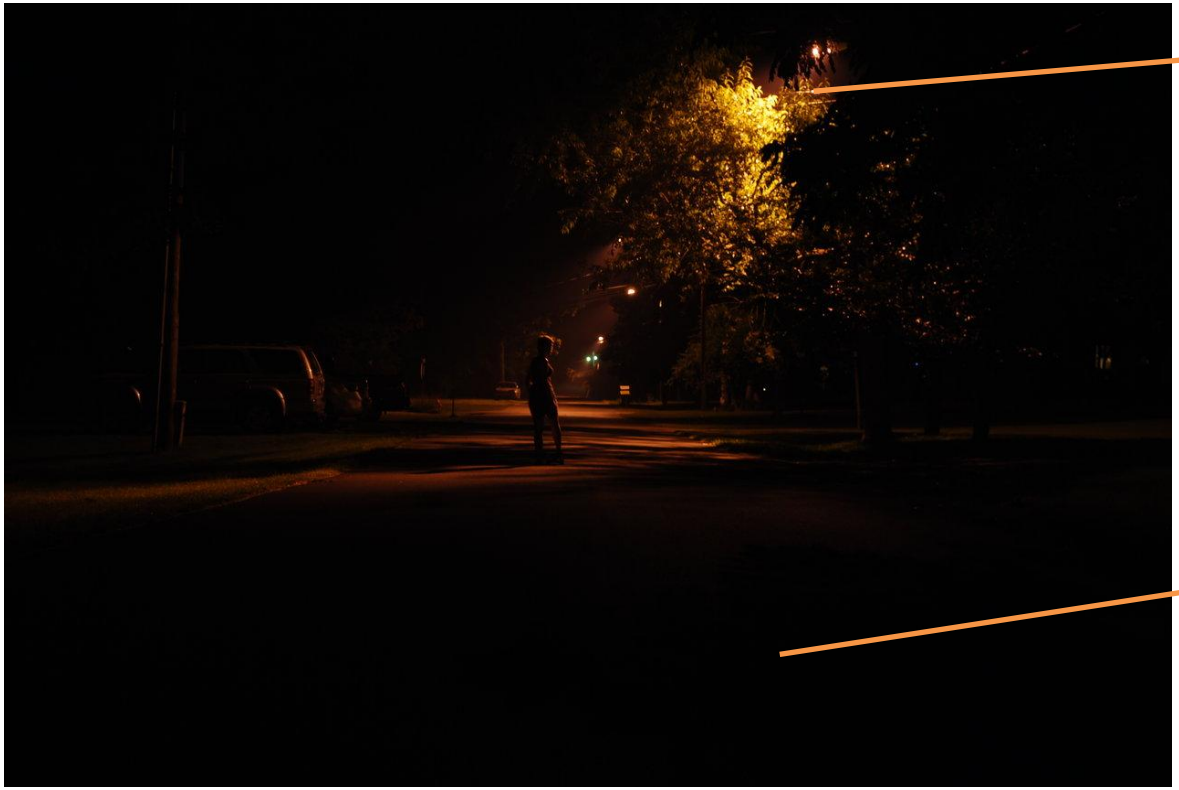
מחקרים בתמיכת מרכז גורדון בטכניון

- 2010 תכן להתמודדות עם אירועים בלתי צפויים
- 2011 ניהול סיכוני תפעול – מקרה ITS
- 2012 מודל חסינות ומדריך לחסינות
- 2013 ק"ע תכן לחסינות – תיקוף המודל והמדריך

מודל של כשל תפעולי



המודל הליניארי



טריגר

איומים
סמויים

מודל של ניתוח תאונות

בהמחשת מטפורת הגבינה השוויצרית

פרוסות הגבינה מייצגות שכבות הגנה

איום

החורים מייצגים כשלים בשכבות ההגנה

נזקים

Swiss cheese model by James Reason published in 2000.

שכבות הגנה בפני כשל

1. אוטומציה
2. מניעת איומים
3. התמודדות עם איומים
4. מניעת הסלמה
5. תכן התפעול בחירום
6. אימות ותיקוף
7. ניהול החסינות

1. אוטומציה

- אוטומציה – כשיש דרישה לדיוק ולמהירות ביצוע
  – דוגמא – טייס אוטומטי
- מגבלות – כשכוונת המפעיל אינה ידועה מראש
  – דוגמא – טיסת AF 296 בשנת 1988
- דילמת השליטה: מתי עוברים מידני לאוטומטי?
  – Bainbridge (1983) The Irony of Automation
- המלצות: להגדיר אילוצים לאוטומציה (STAMP)

2. מניעת איומים

איומים סמויים

- תקלה בחומרה
- טעות מפעיל
- תקלת תיאום
- מצבים בלתי צפויים

המלצות

- אמצעים לאיתור תקלות
- אימות לפני ציות
- תכן מונחה תרחישים
- תכן מונחה STAMP

2004 - STAMP פרדיגמת

Alain Colmerauer

תכנות לפי אילוצים
Prolog, 1967

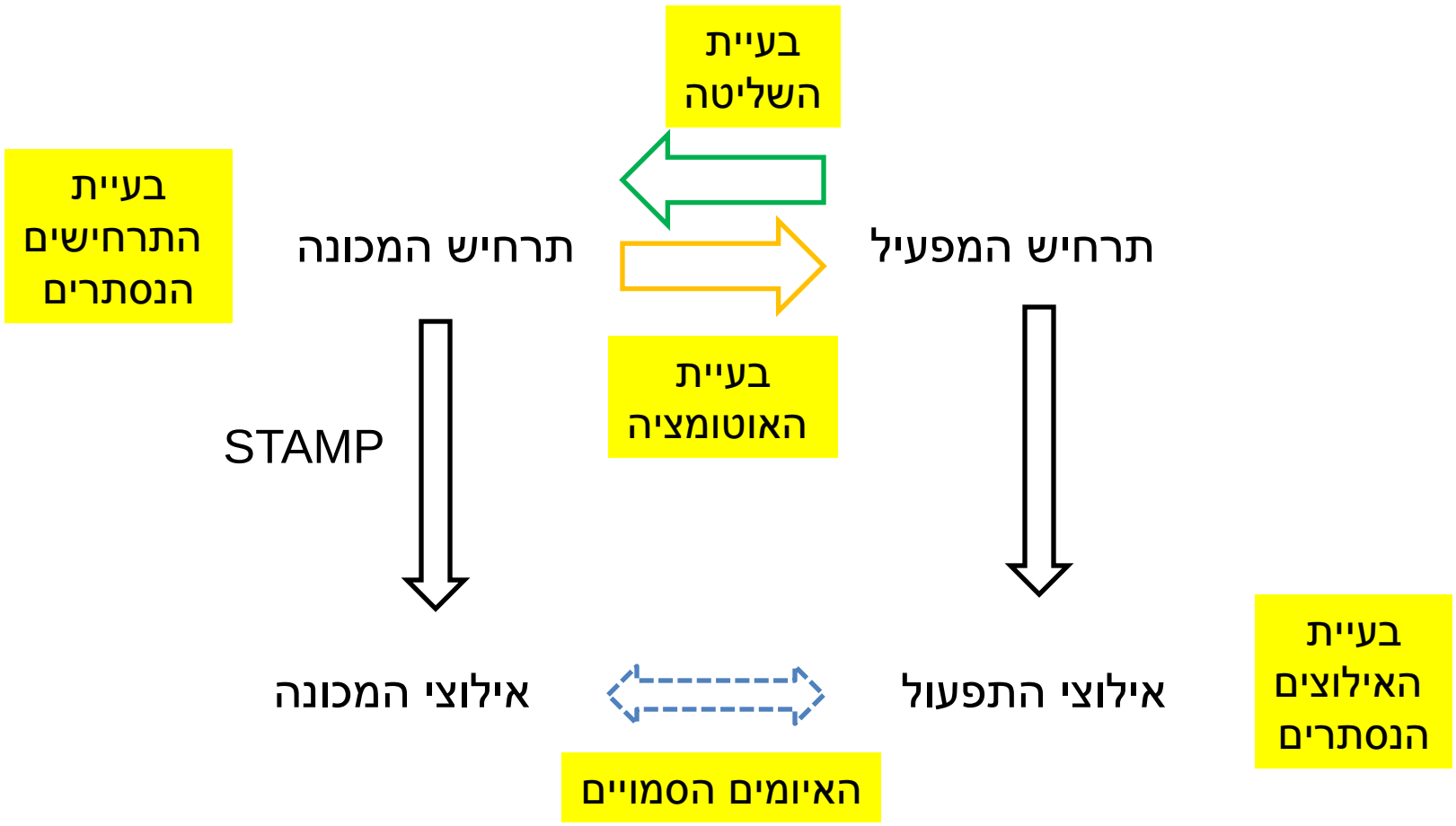
Ergolight

מעקב וניתוח אחר
פעילות המשתמשים
UPI, 1999

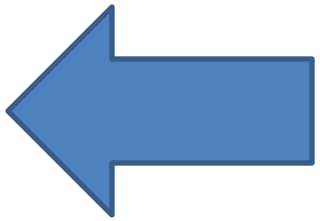
Nancy Leveson

בעיית
האילוצים
הנסתרים

אבטחת תיאום מפעיל-מכונה

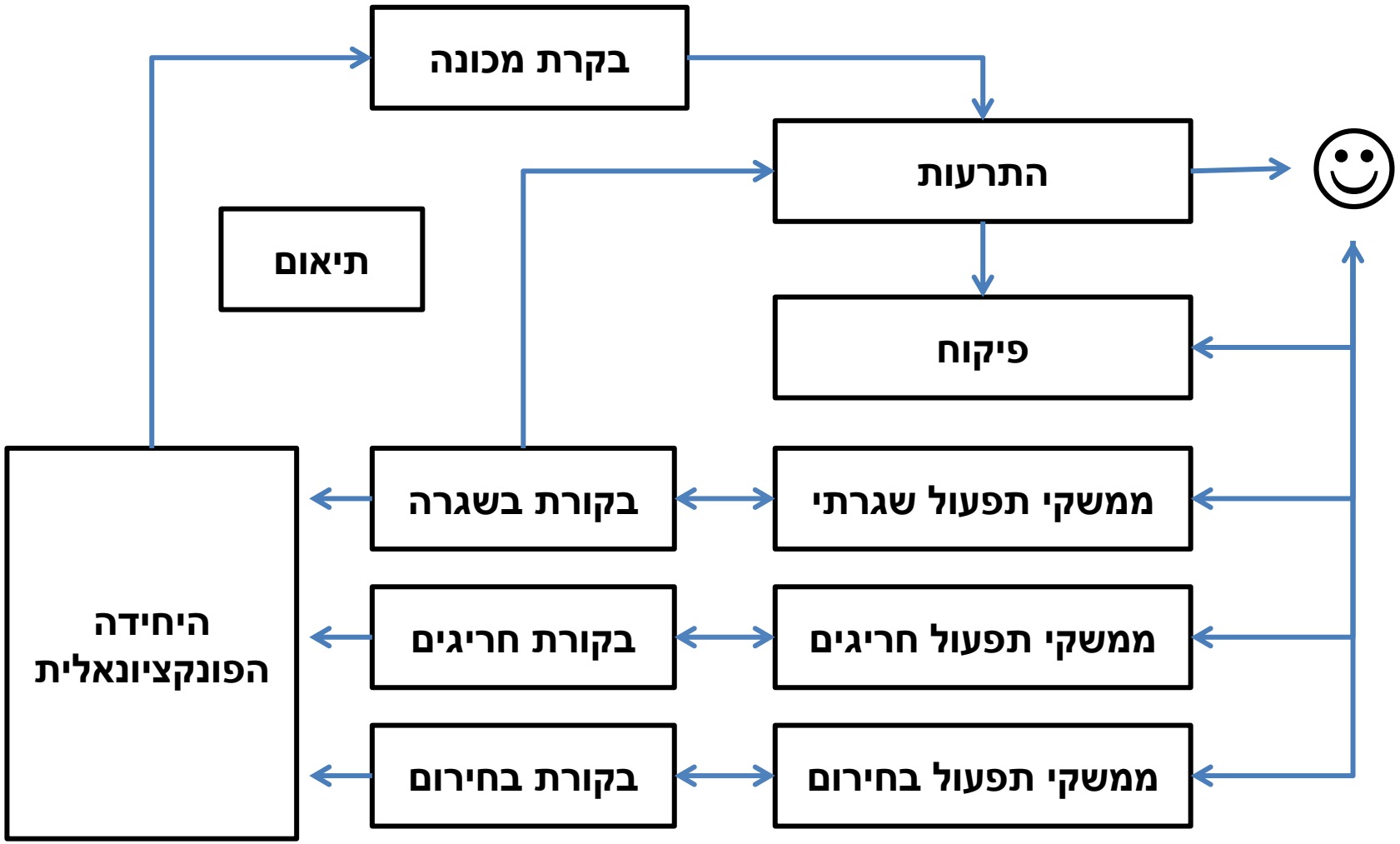


תכן בורר התרחישים

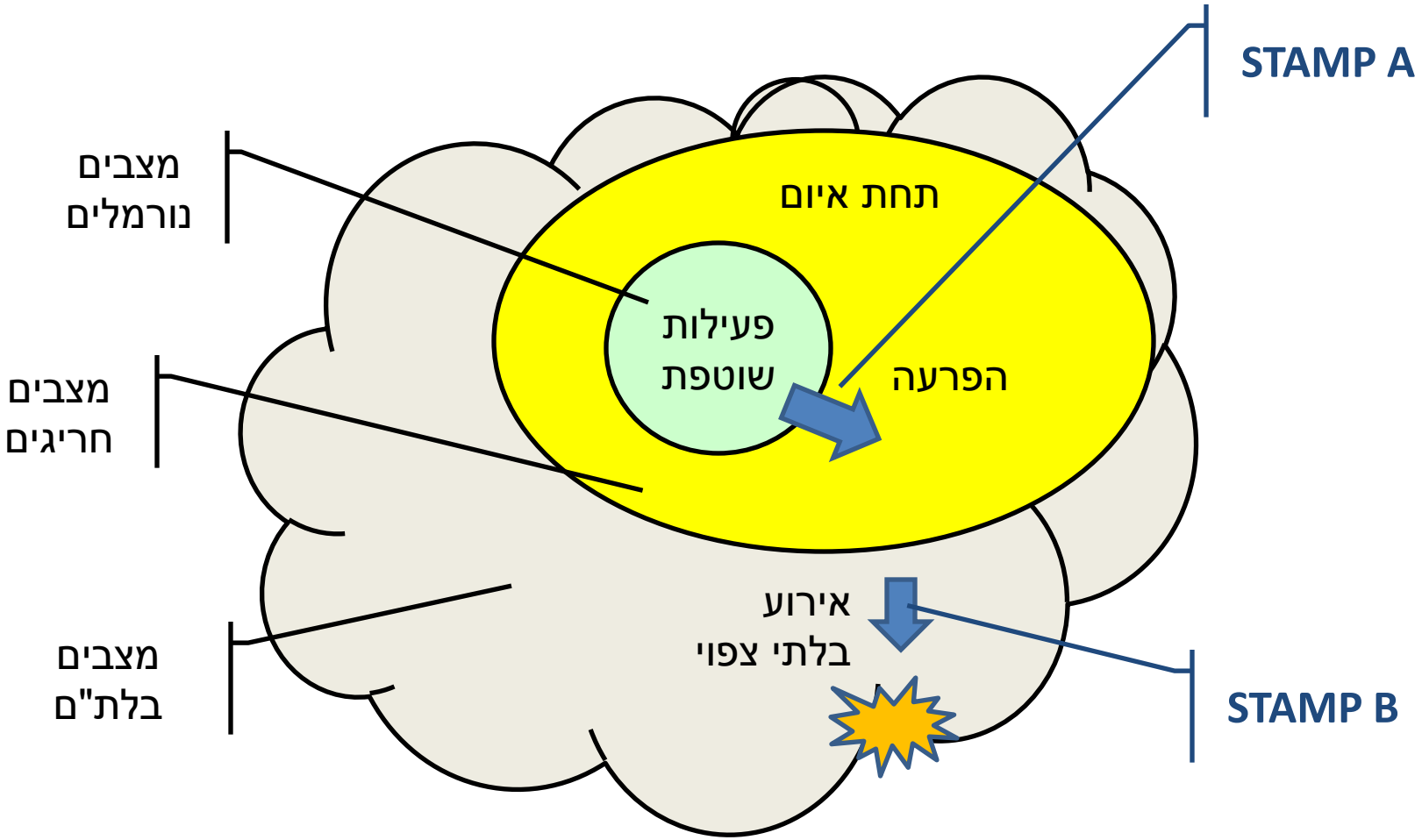


עקרון המיפוי הישיר: כוונה לפעולה
עקרון התרחישים המפורשים
עקרון האילוצים המפורשים

3. התמודדות עם איומים



4. מניעת הסלמה



5. תכן התפעול בחירום

- דילמת השליטה: מתי עוברים מידני לאוטומטי?
  - Bainbridge (1983) The Irony of Automation
- שאלות:
  - מי שולט?
  - מי מחליט מי ישלוט?
- המלצות:
  - בדרך כלל - החלטת מפעיל
  - בסיכון אקוטי – אוטומציה (STAMP)

6. בדיקות עם מפעילים

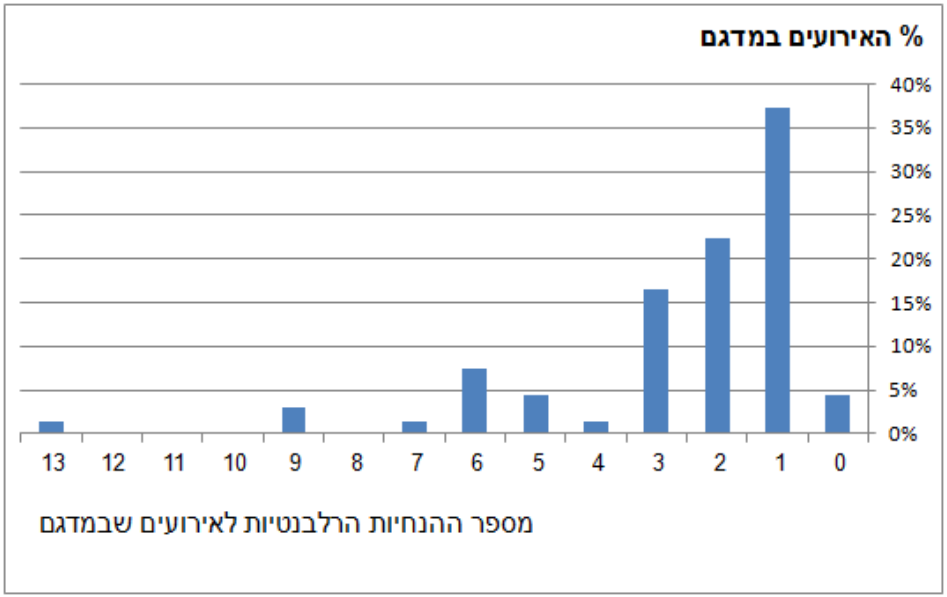
- טעויות נפוצות בבדיקות תפעול
  - בדיקות ע"י מומחי מצוות הפיתוח
  - בדיקות שימושיות קלאסיות
- המלצות
  - בדיקות עם מפעילים
  - יזום תקלות
  - תשתית להדמיית מצבי תקלה

7. לימוד מאירועי כשל

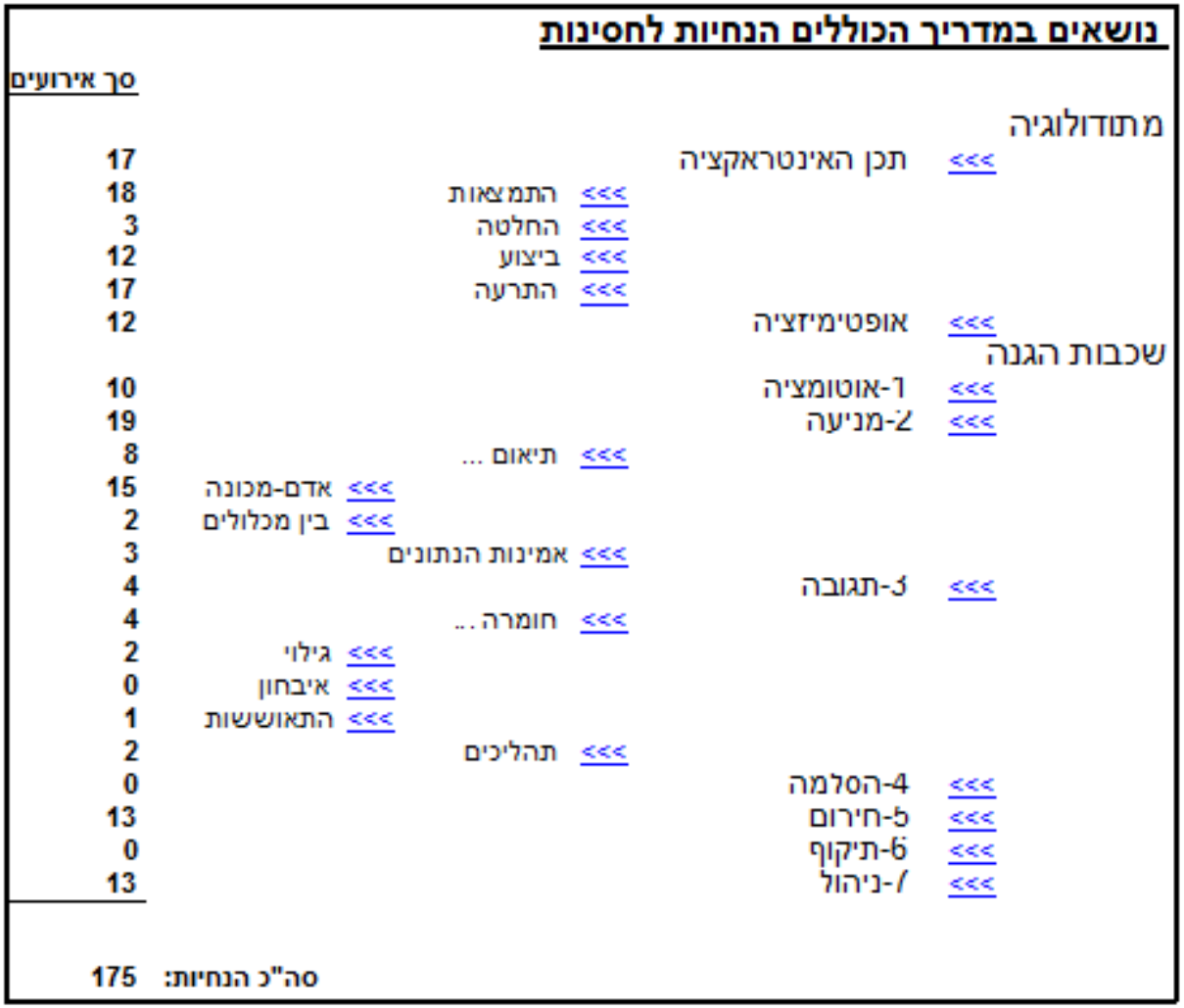
- טעות נפוצה – הסחת התחקור
  – דוגמא – תקן IEC 60601-1-8 התרעות ברפואה
- מניעת הסחה בתחקור
  – נהלים להפקת לקחים (הצעה לתקן)
- כלים לאיסוף ולניתוח נתונים (נוסח ארגולייט)

תיקוף

- עבודת מסטר של גלעד סגל מרפאל – 11 אירועים
- מאגר אירועי כשל – 67 ארועים:
  - ציון חסינות: 2.6 (ממוצע הנחיות לחסינות אירוע)
  - כיסוי: 96%



תיקוף המדריך לאבטחת חסינות - גירסא Guide-v8 יום 5 בינואר 2015



סיכום

- ק"ע באילטם-אינקוזי
  – חברי אילטם מוזמנים להצטרף
- מבוקשים: פרויקטים ללמוד להתגלח עליהם
- המדריך זמין לכל דיכפין

resilience.ergolight-sw.com