מיגון מערכות בפני טעויות מצב

אבי הראל
ארגולייט בע"מ

מטרות:

א. להציג את **המשמעות** אל טעויות מצב

ב. **לאפיין** את טעויות המצב

ג. לנתח את **הסיבות** לטעויות מצב

ד. להציע שיטות **למניעת** טעויות מצב

ה. דרך **להפקת לקחים** מ'כמעט-תאונות'

Background – Human Factors:

- Automation Surprise
- Cause: Upset of Situational Awareness
- Analysis: Mode Errors
- Larry Tesler PARC: Don't mode me in

שאלות המחקר:

א. האם טעויות מצב הן כוח עליון?

ב. האם טעויות מצב הן טעויות אנוש?

ג. כיצד ניתן להמנע מטעויות מצב?

ד. כיצד ניתן לאתר טעויות מצב קטלניות?

מאפיינים של טעויות מצב:

- כל יחידה פועלת על הנדרש
- הממשק בין היחידות פועל כנדרש
- היחידות אינן מתואמות ביניהן
- התנהגות מערכת בלתי סבירה
- התוצאה עלולה להיות קטלנית

שיטה:

1. ניתוח כשל טעויות אנוש קטלניות
   S. Casey: Set Phasers on Stun
2. ניתוח כשל מערכות ביתיות, משרדיות, מכוניות
   הממיר הדיגיטלי, אופיס, נוריות התרעה ...
3. הגדרת אחריות המפתח
   מודל תקרת פאל-קל
4. הפשטה – מודל מערכת של מערכות
   מודל הבעיה: תיאום מצבים שרת-לקוח
5. סקר ספרות בטיחות מערכות
   אוטומציה, בעיית השלימות
6. סקר ספרות עקרונות התיכון
   Use-cases, Ockham's razor, UCD ...
7. התאמת עקרונות התיכון לבעיית טעויות המצב
   כיוון, פישוט, תיאום ע"פ תרחישים
8. אבטחת איכות תפעולית
   מתודולוגיה, תקינה, כלים

בעית תיאום המצבים

1981: Therac-25

6 נפגעים
בשנים 1985-1987

- מוד X במקום E
- Malfunction 54
- treatment pause
- תקלה במצלמת וידאו

ניתוח התקלה

- שני מודי הפעלה (E,X)
- מעבר איטי בין המודים
- אין בדיקת סינכרון
- אין אינטרלוק
- התרעות סרק

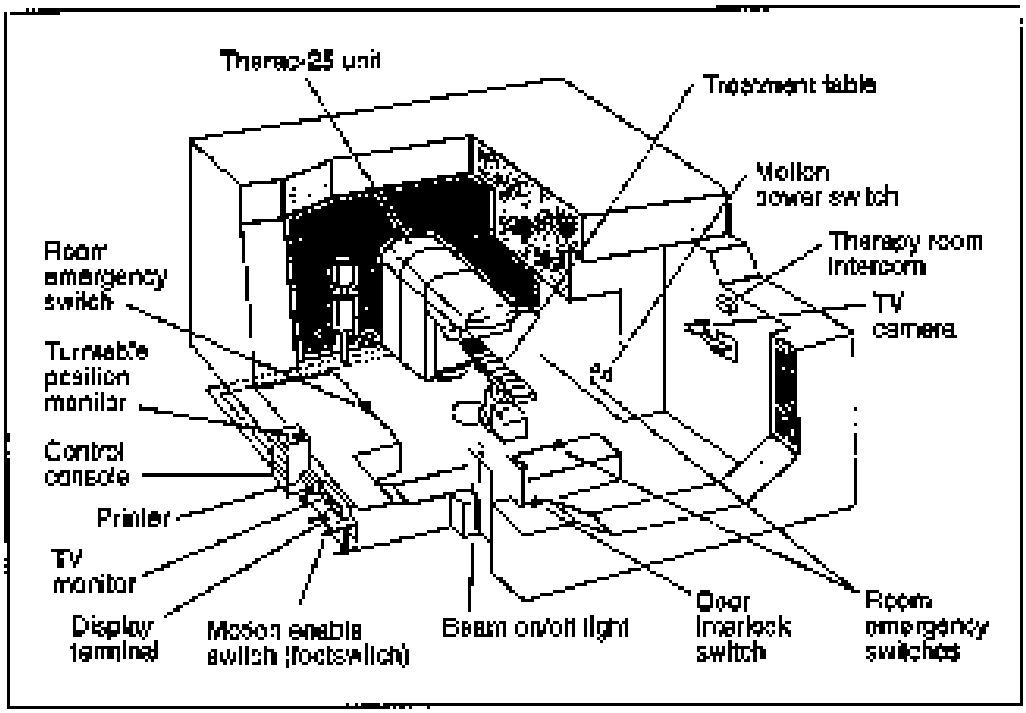
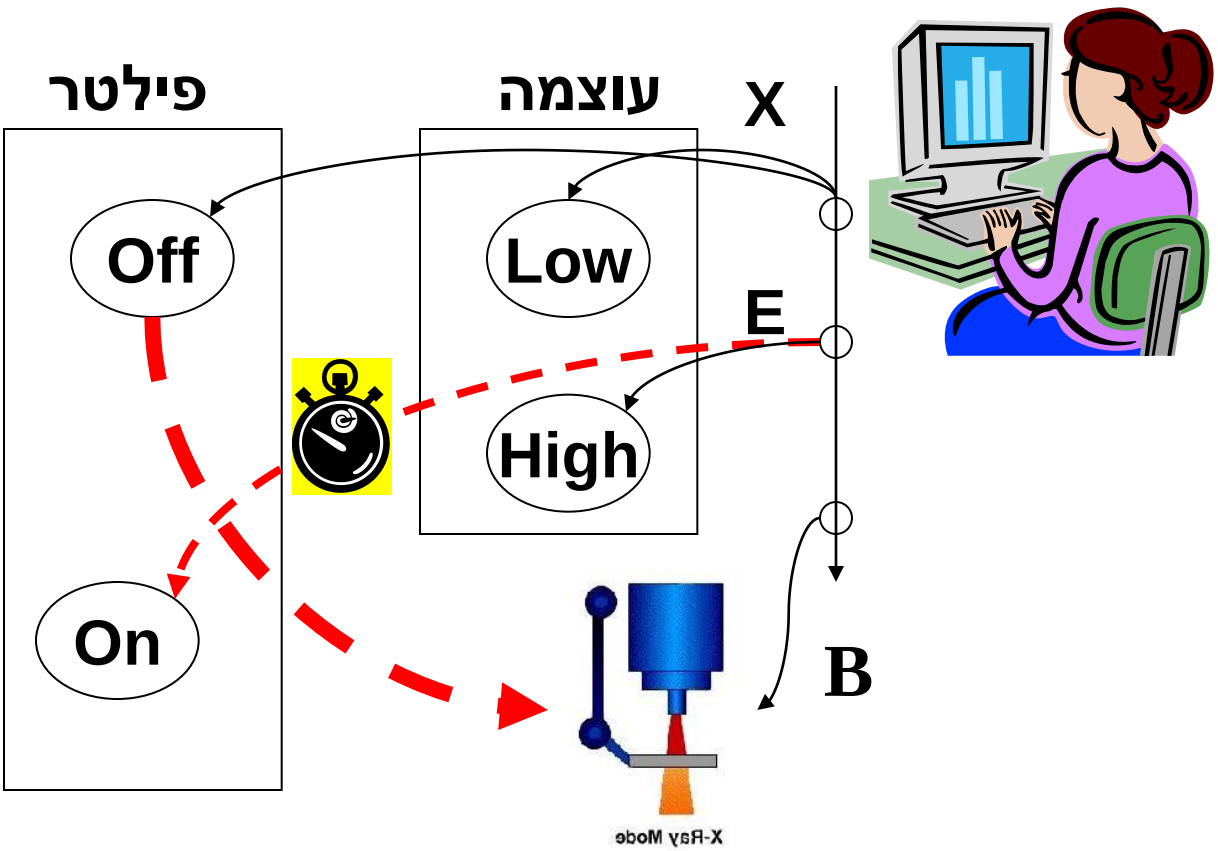


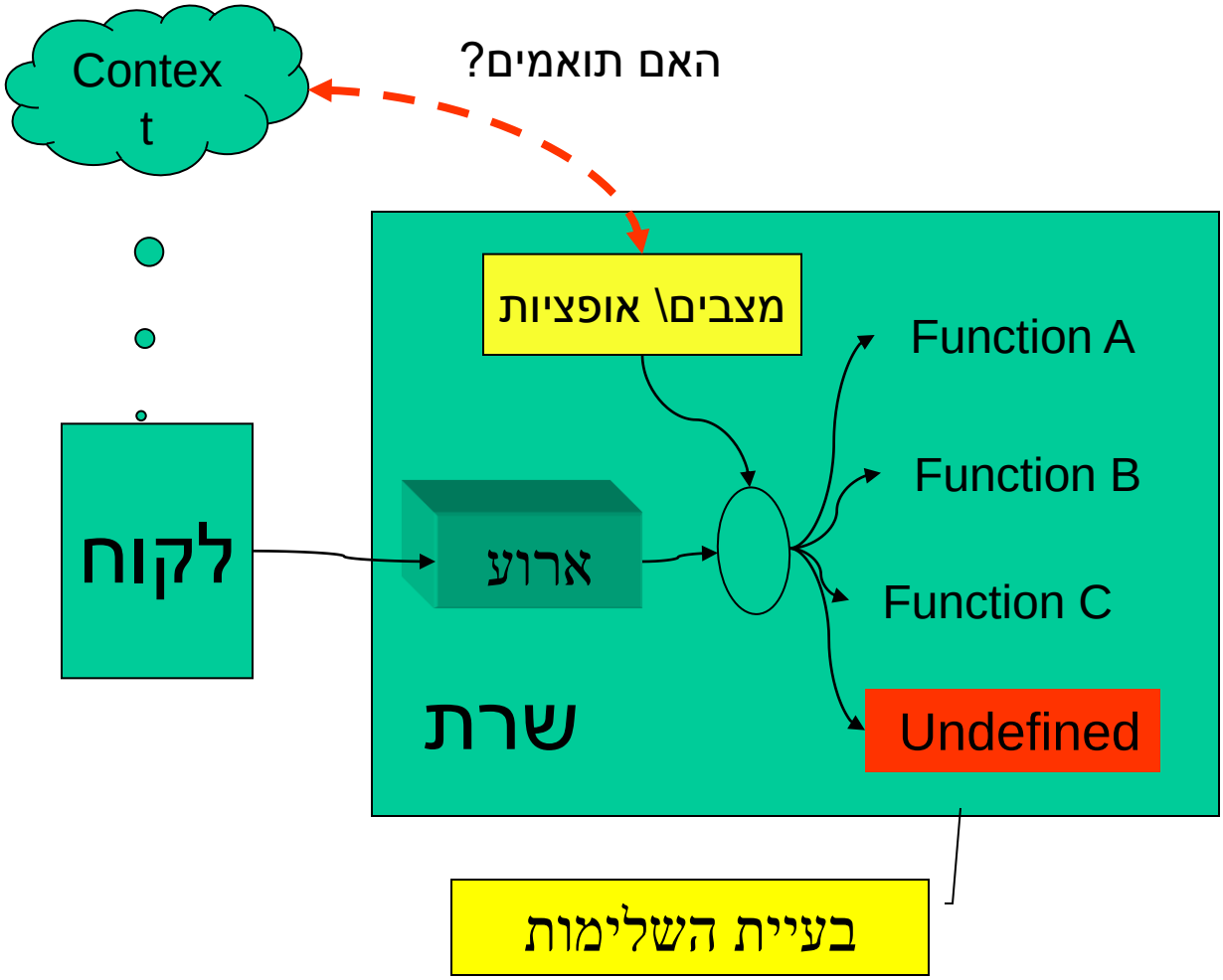
Figure 1. Typical Therac-25 facility.

בעית שלימות ההגדרות



ארוע Beam	פילטר	עוצמה
חוקי	On	High
	Off	Low
לא חוקי	On	Low
	Off	High

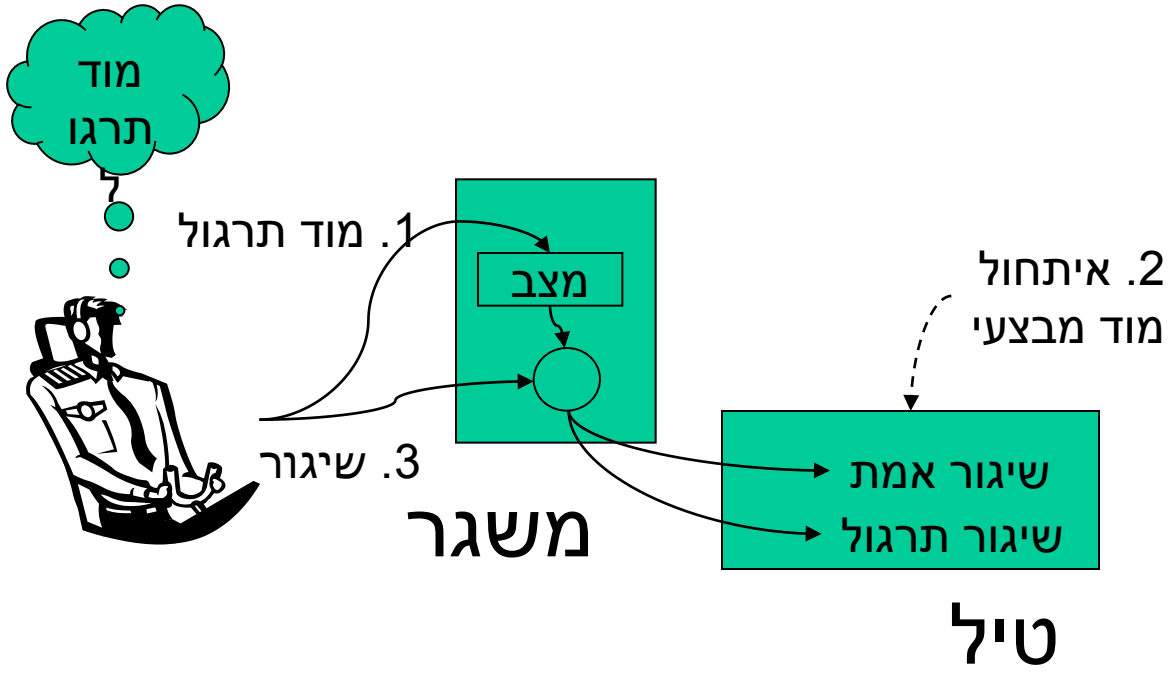
גורם הטעות
כפל משמעות הארוע



מתודולוגיה
הגנה בפני טעויות מצב

- **מניעת** טעויות מצב
  - כיווץ המערכת
  - פישוט המערכת
  - שכפול פונציונאלי ע"פ תרחישים
- **צמצום הסיכוי** לטעויות מצב
  - הגבלת התפעול לתרחישים
  - התרעות מצב חריג
  - התאמת הממשק לשלב התפעול
- **ספיגה** – תגובה לארוע החריג
  - דחית הארוע החריג
    - התעלמות (בסביבה רועשת)
    - התרעה (באינטגרציה)
  - היענות ללקוח
    - התאמת המצב לארוע
    - חזרה לשגרה

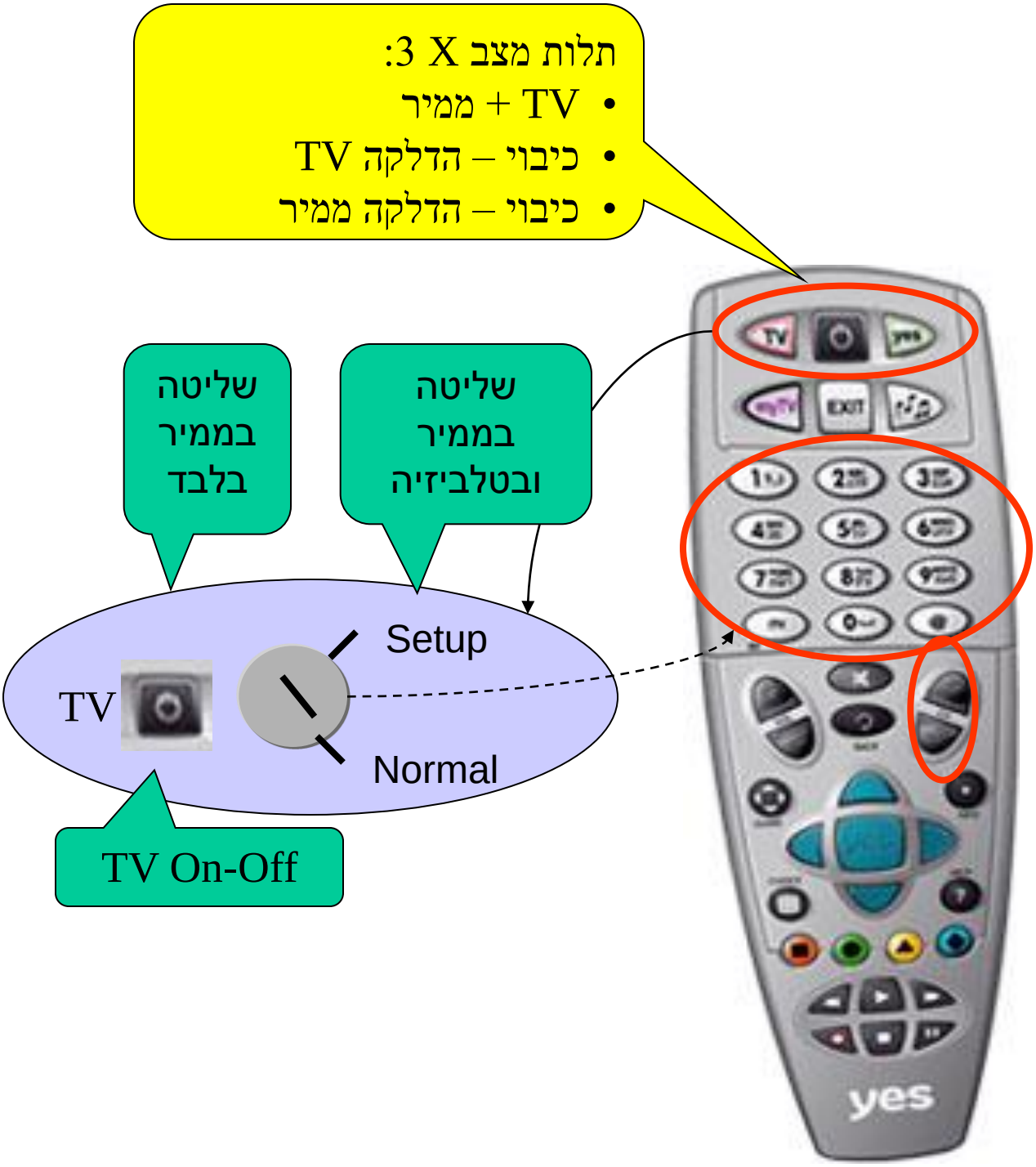
מניעת טעויות מצב
על ידי כיווץ מצבים



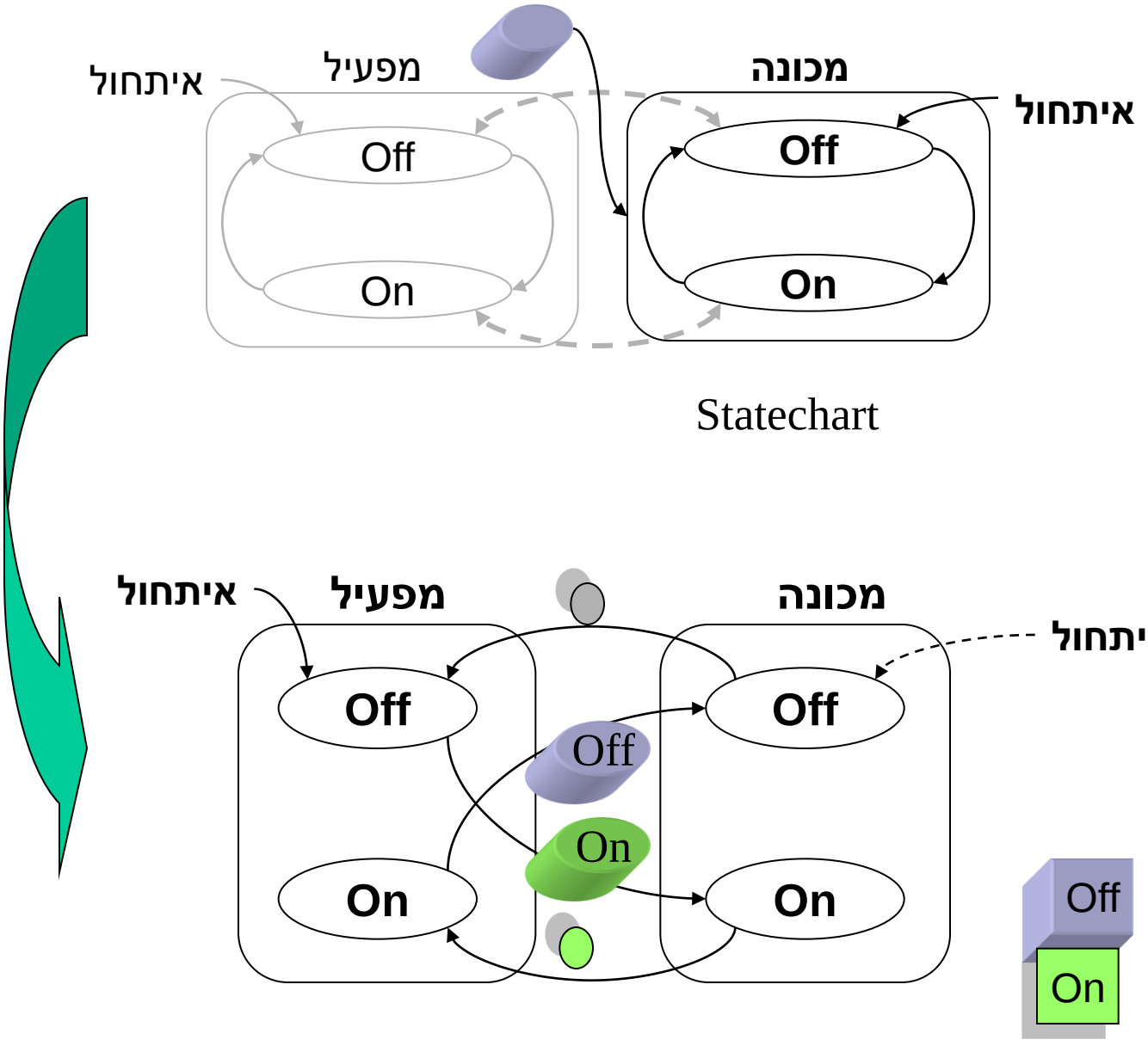
העקרון: שרת ללא זכרון
שיטה: ארוע + 2 מצבים => 2 ארועים נפרדים

סוגי כיווץ אחרים:
- פונקציונאלי
- תצוגה
- פקדים

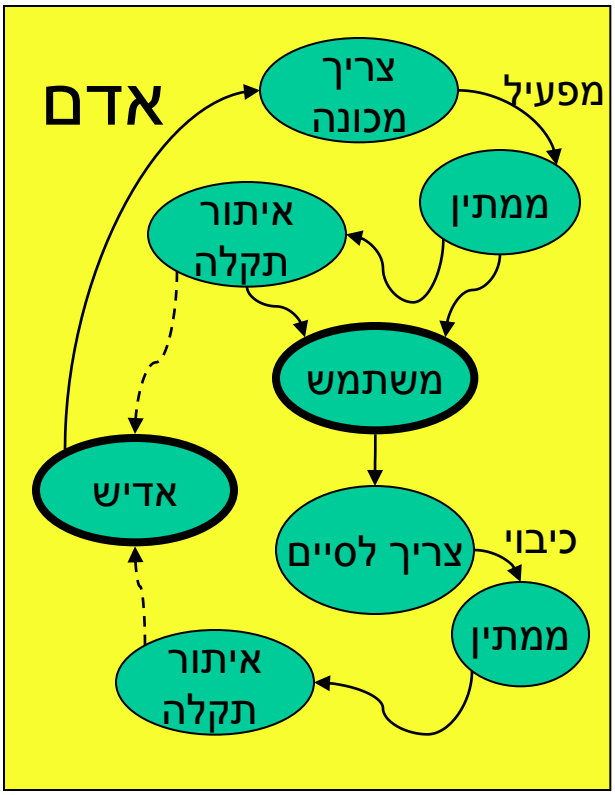
תכן פקדים ע"פ תרחישים

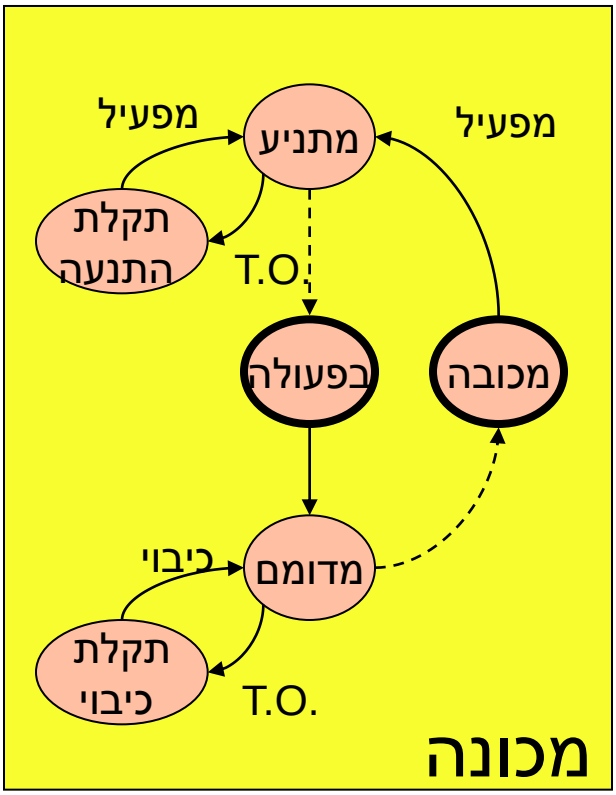


מפרטי אינטראקציה



מגבלת מפרטי תת-מערכות

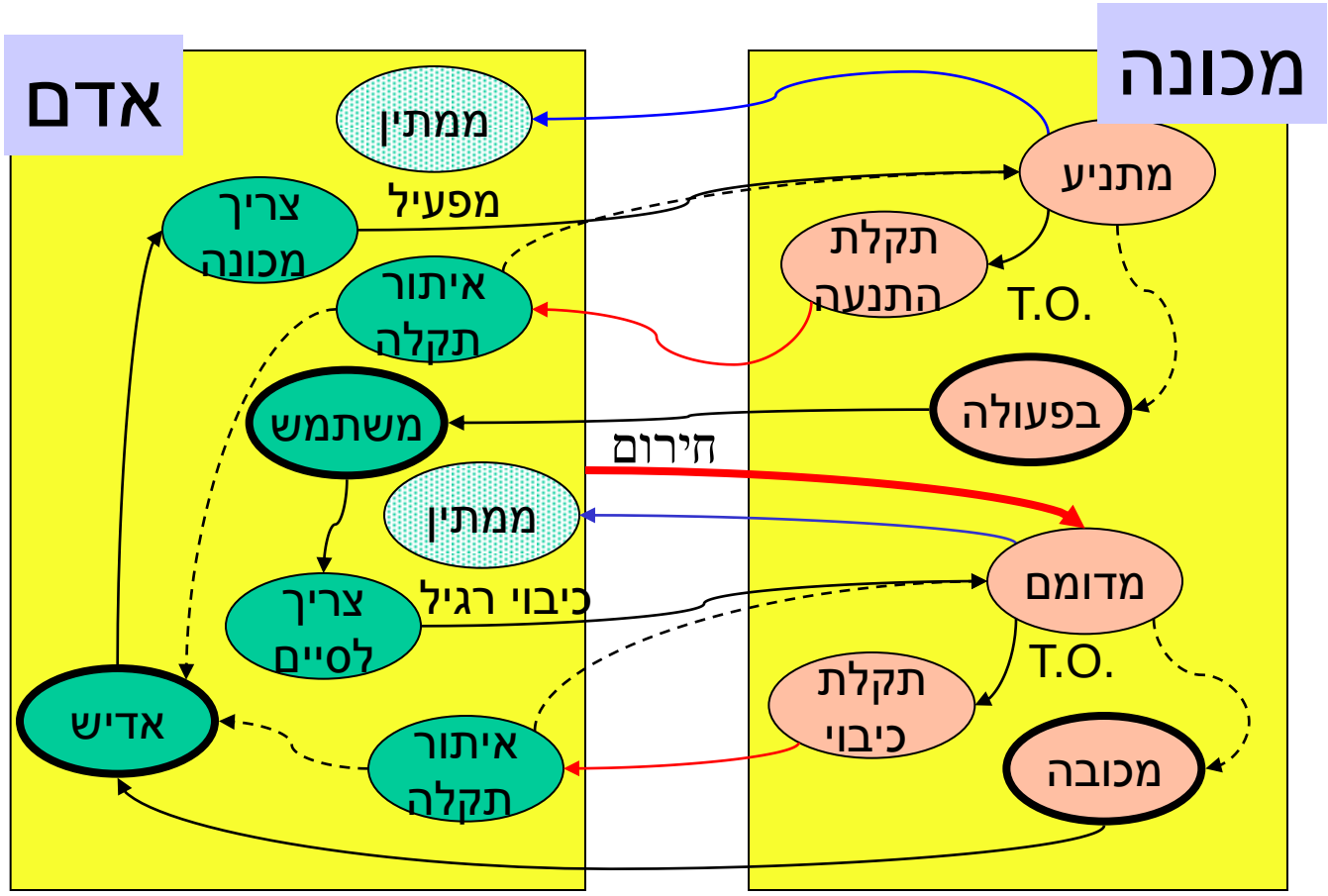




מה לא רואים:

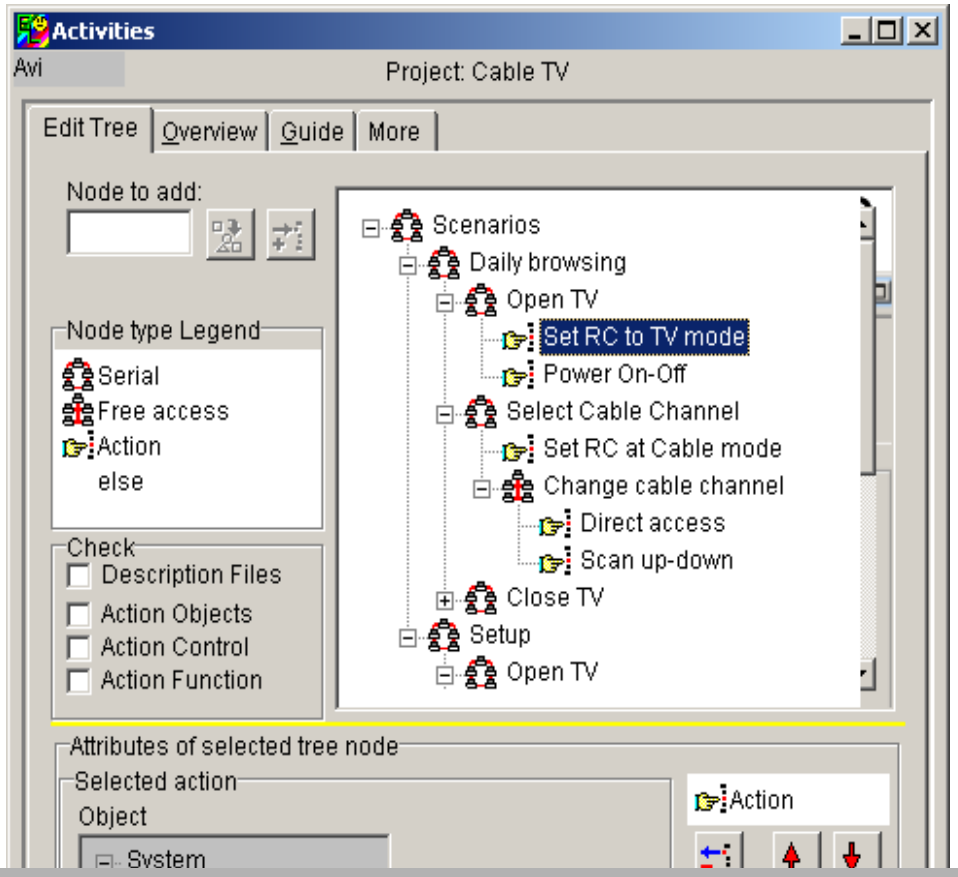
- הודעות על מצבי ביניים מהשרת ללקוח
- משוב תקלות מהשרת ללקוח
- אימות לפני חריגה מפרוטוקול

מפרטי האינטראקציה



State Charts
=> State Structure (use cases+consistency)
+ Inter-Activity Charts (scenario+defense)

אבטחת איכות תפעולית
Activity-based Protocols



- זיהוי מצבים של כפל משמעות
- איתור אובייקטים, פונקציות, פקדים, מצבים ... ללא שימוש
- כיצד צמצום פונקציות או מצבים משפיע על סיבוכיות
- המלצות לפישוט:
  - שכפול פקדים: אמיתי, וירטואלי
  - צמצום פונקציות או מצבים

ממצאים

תקלה	מניעה
Therac-25	פישוט
שיגור במוד תרגול	כיווץ מצבים
Torrey Canyon	תרחישים, התרעת מצב חריג
Cod Edison	תרחישים
AF296 A320	התרעת מצב חריג
Caps Lock	מוד זמני (תרחישים)
עברית-אנגלית	תרחישים
Insert, Num Lock	כיווץ פונקציונאלי
Ctrl-A	כיווץ אופציות
כיבוי ממיר דיגיטלי	שכפול (פישוט)
החלפת ערוץ TV	כיווץ פונקציונאלי, תרחישים
רדיו שעון	תרחישים
תנור מיקרוגל	תרחישים
סלולרי Nokia	כיווץ, פישוט, תרחישים
צאלים א'	שכפול (פישוט)
מתנע	תרחישים
בקרת מהירות	התרעת מצב חריג
מוניטור חדר טיפול נמרץ	התרעת מצב חריג
שלט נעילה מרכזית במכונית	כיווץ מצבים
התרעהת חום מנוע במכונית	התרעת מצב חריג

מסקנות

- ניתן למנוע טעויות מצב
  - ניתן לזהות אפיונים של טעויות מצב
  - ניתן לאתר טעויות פוטנציאליות בשלב המפרטים
  - ב-100% מהמקרים ניתן היה למנוע את התקלה
- קשה לנהל טעויות מצב בלתי צפויות
  - יש לתכנן רשת בטחון
  - יש לחקור את הטעות תוך כדי תפעול
  - יש לוודא תפעול על פי פרוטוקולים
- סדר עדיפות במניעה:
  1. כיווץ המערכת
  2. פישוט הסיבוכיות במערכת
  3. פרוטוקולים ע"פ תרחישים