

סיכום מפגש מס' 4 של קבוצת העבודה

"תכן לחסינות מערכות"

ערך: אבי הראל

דילמת השליטה

בחלק הראשון של המפגש אבי הציג את דילמת השליטה: האם במצב חריג, השליטה תהיה אצל המפעיל או אצל המכונה?

הצורך באוטומציה במצבי חירום הודגם על ידי התאונה בחללית סויוז 11 בשנת 1971. בתאונה זו, הצוות נספה מכיוון שלא הצליח להתגבר על תקלת דליפת חמצן בזמן הקצר שעמד לרשותו.

היבטים שליליים של האוטומציה:

- אובדן שליטה בשעת חירום
- אובדן מיומנויות הדרושות לפתור בעיות בשעת חירום
- התמכרות לאוטומציה (הסתמכות על המכונה).

בתהליך פיתוח אופייני, במקרים רבים מהנדס המערכת אינו מרגיש בטוח בכך שיוכל לאפיין את התגובה ההולמת לכל המצבים החריגים האפשריים. במקרים אלו מהנדס נוהג להטיל את האחריות לפתרון הבעיה על המפעיל.

במקרה של מצב חריג, במקרים רבים המפעיל נדרש לפתור בעיה אותה הוא אינו מכיר, ובתנאי לחץ. במקרים כאלו, המפעיל סומך על המהנדס שחשב על הבעיה בתנאי מעבדה, ולכן המפעיל פועל על פי ההרגל, למרות שיתכן שההרגל מתאים לתפעול במצבים שגרתיים, ולא למצבים החריגים.

התוצאה היא "האירוניה של האוטומציה" (ע"פ Bainbridge, 1983): האוטומציה אינה גורמת להפחתת הסיכון אלא להיפך - להחמרה בסיכון.

הערות של חברי קבוצת העבודה לדילמת השליטה:

- **רון חג'אג'**: כדאי להדגיש שמושג האירוניה מתייחס לרמת הסיכון, ולא לסיכוי
- **יעקב**: דוגמא לנטילת אחריות לכאורה על ידי המהנדסים בדרך של אוטומציה היא בטיסות עם מכשירים, כאשר הטייס אמור לפעול על פי הנחות עבודה.
- **ראובן**: הטייס נדרש להפעיל ביקורת על המידע ועל התנהגות המערכת.
- **אלון**: בעת אירוע חירום עומס העבודה עולה, עם זאת, באותו הזמן אוטומציה עלולה לגרום דווקא להכבדה של העומס ולא להקלתו.

מצגת של ראובן גרינברג

ראובן הציג רשימה של מיתוסים באבטחת חסינות, והדגים אותם בשני אירועי כשל: תאונת איירבאס 320 בטיסת AF 286 בשנת 1988 באלזס בצרפת, ותאונת בואינג 757 בטיסת AA 965 בשנת 1996 ב-Cali.

הערות חברי קבוצת העבודה במהלך המצגת של ראובן ואחרי המצגת:

- **דב:** יתכן שהאוטומציה מקלה על העומס בשוטף, אבל מגדילה את סיבוכיות המערכת.
- **אמנון:** לעיתים מתכנני המערכות מתעלמים או אינם מודעים לידע החסר של משתמשי המערכות שלהם.
- **עזרי:** דוגמא למערכת איזון דלק בבואינג 747, מערכת שהפכה לאוטומטית, והוותה פתח לשאלה - מהו הקריטריונים בעזרתם נוכל לומר על פונקציה שהיא טובה עבור אוטומציה? (שניתן להפכה לאוטומטית מבלי לייצר סיכונים או תחת סיכונים פחותים יחסית)
- **עזריאל \ אלון \ אמנון \ רון:** מהם המאפיינים של אוטומציה מוצלחת? אילו שיקולים יש לקחת בחשבון בבואנו להפוך תהליך לאוטומטי?
- **נחום:** הצעה לפתרון של דילמת השליטה - מכונה אדפטיבית שתלמד התנהגויות וסביבות ותתאים את עצמה
- **אמנון:** הרעיון של אדפטיביות לא יכול לעבוד, כי במציאות המצבים הם מורכבים, והמודל אותו המכונה לומדת הוא מקרה פרטי, ואינו מייצג את המורכבות הזו.
- **אביגדור:** נדרש לתת אינדיקציות היכן ניתן לתת לאוטומציה להמשיך ולפעול והיכן צריך המפעיל לקחת את השליטה לידי
- **יאיר:** נדרש חידוד של דילמת השליטה, הבעיה עוד לא הובהרה עד סופה
- **ראובן:** תכנון לקוי של האוטומציה עלול להביא לתוצאות הפוכות מאלה אליהן התכוונו המתכננים.
- **יאיר:** יש צורך במדדים לתועלת שבאוטומציה
- **דבאביגדור/רון/אמנון:** מעבר לשיקולים ההנדסיים, יש לקחת בחשבון שיקולים פסיכולוגיים, חברתיים, פוליטיים.
- **אביגדור:** צריך לזכור שהמוצר ההנדסי מיועד לשרת את המשתמשים, ולכן צריך להתחשב בהם בתכנ המוצר.
- **אמנון:** מציע להזמין אנשי מקצוע להציג את נושא השפעת הבדלי התרבות על התכן.

בעיית המשוב החלקי למפעיל

אבי הציג את התזה של דונאלד נורמן, על פיה בעיית האוטומציה אינה למעשה בעיה באוטומציה, אלא בוסר משוב בלתי מספק מהמכונה למפעיל. בעיית המשוב הודגמה בשלשה אירועים.

הערות של חברי קבוצת העבודה בנושא בעיית המשוב:

- **עזרי:** שתי דוגמאות לתקלות טיסה עקב שילוב אוטומציה מבלי לעדכן את הטייסים, תוצאה של אחת מהן היתה יצירה של צוות FIA שנועד לייצר אוטומציה של תהליך מאוד מורכב בהנחת מטוס (שימוש במצערות כדי להנחית את המטוס)

השיפורים במדריך

אבי הציג את המדריך המשופר, והדגים את אופן השימוש בו לצורך מניעת טעויות בהקלדת נתונים בעזרת [התאונה ב-Cali](#).

הערות של חברי קבוצת העבודה בנושא המדריך:

- **שמואל:** להוסיף למדריך התכן ביאור ומונחים באנגלית.
- **אביגדור:** צריך להוסיף מראי-מקום, היכן לשים לב לאמינות התכן, איך מתקפים את אמינות התכן ואיך מתקפים את איכות התכן עצמו

- אמנון: נדרשת הוספה של פרק סדר פעולות נכון : אכיפת התהליך, וידוא התהליך, תיקוף התהליך,
- תהליך FMEA וכו' אלון: הצעה לתוספת של GATE או DR בנוגע לרזיליות כפרוייקטים עצמם

ההבדל בין שליטה לחווית השליטה

אבי הציג את התאונה של [Torrey Canyon המיכלית](#) כמקרה של חווית חוסר שליטה, כאשר בפועל, לצוות היתה שליטה, ואת חווית חוסר השליטה יש לייחס לכך שהמכונה לא סיפקה משוב למפעילים.

הערות של חברי קבוצת העבודה בנושא חווית השליטה:

- אלון: נושא אמינות המידע ומהימנותו הוא קריטי ויוצר את ההבדל בין שליטה של ממש לחווית השליטה

למפגש הבא

חברי הקבוצה מתבקשים להציע נושאים לדיון במפגש הבאה, וכן מרצים מקרב הקבוצה.

בנושא זה חברי הקבוצה הציעו להזמין מרצה מבחוץ מהתחום של פסיכולוגיה קוגניטיבית. אבי יבדוק בקרב חברי האגודה הישראלית לארגונומיה וגורמי אנוש.