

תקציר מאמר לכנס האיגוד הישראלי להנדסת מערכות בנושא:

## הקצאת תפקידי אדם-מכונה במשימות שו"ב

אבי הראל  
ארגולייט בע"מ  
רח' גבעון 6, חיפה 34335  
054-4534501  
avi.1@ergolight-sw.com

במאמר זה, מערכת שליטה ובקרה (שו"ב) זוהי מערכת הפועלת על פי תוכנית קבועה מראש. דוגמאות של מערכות שו"ב כוללות בקרת יצור תעשייתי, יצור כוח, תחבורה, תהליכים כימיים, ניטור רפואי, ניהול תרגילי אש, איסוף מודיעין שדה, ועוד.

שאלת האוטומציה של מערכות שו"ב מוגדרת כבעיית הקצאת תפקידים: אילו מהתפקידים יש להטיל על המערכת ואילו מהם יש להשאיר באחריות המפעיל. המאמר מציג מתודולוגיה להגדרת מידת האוטומציה במשימות שו"ב.

### בעיית האוטומציה

הנטייה הטבעית של מהנדסי מערכת היא למחשב כל מה שאפשר, על מנת להפחית את העומס מהמפעיל. התועלת של גישה זו הודגמה באסון החללית סאליוט ב-29 ביוני 1971 (<http://ei.cs.vt.edu/~cs3604/lib/Safety/soyuz11.html>). גישה זו מחייבת ידיעה מראש של כל אופני הפעולה וזיהוי אוטומטי של הגורמים המכתיבים את אופן הפעולה הרצוי. במערכות מעשיות, הגורמים המכתיבים את אופן ההפעלה אינם ידועים מראש. במקרים מסויימים, האוטומציה גורמת לכך שהמפעיל אינו מודע לחריגות מהפעולה הרגילה. במקרים אחרים, המפעיל תופס את ההתנהגות החריגה של המערכת, אך מתקשה לזהות את מאפייני המערכת הגורמים לחריגה זו. כתוצאה מכך, המפעיל עלול להגיב באיחור. במערכות שו"ב רבות, איחור בתגובה עלול להסתיים באסון, דוגמת קריסת מערכת החשמל במנהטן ב-13 ביולי 1977 ([http://blackout.gmu.edu/archive/pdf/stress\\_strain.pdf](http://blackout.gmu.edu/archive/pdf/stress_strain.pdf)).

### בעיית השו"ב

לצורך קביעת רמת ההתערבות הנדרשת מהמפעיל, במאמר זה נגדיר את משימות השו"ב כגילוי, הערכה, התמצאות וזיהוי של חריגים ביחס לפעילות נורמלית של המערכת. פעילות נורמלית מוגדרת על פי סטנדרטים המגדירים מהי פעולה תקינה, כגון תחום טמפרטורות בתהליכים כימיים, זרימת מצבים המגדירה תהליך, זמינות משאבים, כגון טבלה בבסיס נתונים, וכד'. במאמר זה לא אעסוק בנושא חשוב אחר, של בחירת אופן ההתערבות של המפעיל לאחר זיהוי מקור הבעיה. בעיית ההפעלה במצבים חריגים היא שהמפעיל נדרש להתמודד עם מצבים שאינם מוכרים לו, כאשר ממשק ההפעלה מציב לו אתגר נוסף, של התמצאות בחלקים בהם לא התנסה לפני כן.

### בעיית הגילוי

בעיית הגילוי מוגדרת על ידי מצבים בהם המפעיל אינו מודע לחריגה מהפעילות הנורמלית. במערכות שו"ב אופייניות, תפקיד הגילוי מחייב עירנות מתמדת, ולכן תפקיד זה מוטל על המערכת. תפקיד המערכת למדוד בעזרת חיישנים את הפרמטרים המשמשים להגדרת פעולה תקינה, כגון, לחץ וטמפרטורה בתהליכים כימיים, לזהות את החריגה ולהתריע על כך למפעיל. במערכות מיושנות, בהן קיים חוסר בחיישנים, קיימת בעיית אמינות והמפעיל נדרש למדוד את הפרמטרים באמצעים ידניים, פעולה הגוזלת זמן ועלולה להסתיים באסון, דוגמת התפוצצות בבהופל בהודו, ב-3 בדצמבר 1984 ([http://www.hu.mtu.edu/hu\\_dept/tc@mtu/papers/bhopal.htm](http://www.hu.mtu.edu/hu_dept/tc@mtu/papers/bhopal.htm)). מהנדסי המערכת נדרשים לזיהוי אוטומטי של תקלות בחיישנים, על ידי כפל מדידות ועל ידי בדיקות שוטפות של התאמה לחוקי הפעולה.

## בעיית ההערכה

בעיית ההערכה מוגדרת על ידי מצבים בהם המערכת מתרעה למפעיל לגבי החריגה מהפעילות הנורמלית, אך המפעיל מתקשה להעריך את המשמעות של חריגה זו. לדוגמא, ההתרעה יכולה לנבוע מתקלה באחד החיישנים. על מנת להעריך את משמעות ההתרעה, המפעיל נדרש לבחון פרמטרים קריטיים של המערכת, הקשורים לחריגה. לדוגמא, לאחר קבלת התרעה על טמפרטורה חריגה במיכל בו מתבצעת פעילות כימית, המפעיל נדרש לבדוק גם את הלחץ במיכל זה, מכיוון שעלית לחץ עלולה להסתיים בפיצוץ. בעיית ההערכה קשורה לסיון התרעות. מצד אחר, עודף התרעות עלול לגרום למצב של שיתוק המפעיל, דוגמת התקלה ב-28 במרץ 1979 בריאקטור הגרעיני ב"אי שלושת המיילים" (<http://www.nei.org/index.asp?catnum=2&catid=57>). מצד שני, במצב של הצפת התרעות, המפעילים עלולים לנטרל חלקים במערכת ההתרעות. מיעוט התרעות עלול לגרום לכך שהמפעיל אינו מודע לפרמטרים חשובים לתפיסת המצב, דוגמת התקלה בכור בצ'רנוביל. מהנדסי המערכת נדרשים למצוא את שביל הזהב בין שני המצבים, ולהגדיר מערכת לאבטחת התרעות, תוך מינימום הפרעה להפעלת המערכת בחירום. בעיית ההערכה היא חמורה במיוחד במצבים של עודף מוטיבציה של המפעיל, הגורם לו להתעלם מהתרעות ברורות וחד משמעיות, כמו בכור בצ'רנוביל, וכמו באסון של צי המשחתות ה-11 של ארה"ב ב-7 בספטמבר 1923. בהתראה קולית מתמשכת, המפעיל עלול לנתק את מערכת ההתראה, שמפריעה לו להתרכז במשימה של התמודדות עם התקלה. בהמשך, לאחר שהתקלה תוקנה, המפעיל עלול לשכוח לחבר את מערכת ההתראה. מערכת אבטחת ההתרעות צריכה לכלול זיהוי אוטומטי של ניטרול התרעה קולית, וגיבויים למקרים של ניטרול התרעות, כגון על ידי הקצבת זמני ניטרול.

## בעיית ההתמצאות

בעיית ההתמצאות מוגדרת על ידי מצבים בהם המפעיל אינו מכיר את מצב המערכת במצב של התנהגות חריגה. במערכות מעשיות, המפעיל מתקשה לעקוב אחר ההשתנות של הפרמטרים במערכת, עובדה הגורמת לטעויות הפעלה, הגורמות לאובדן זמן, ובמקרים מסוימים עלולות להסתיים באסון, דוגמת האסון האקולוגי של התבקעות המיכלית באיי סילי ב-18 במרץ, 1967 (<http://www.lboro.ac.uk/departments/hu/ergsinhu/aboutergs/torrey.html>). מהנדסי המערכת נדרשים לספק למפעיל את המידע הרלבנטי למצב. באין ידיעה מראש לגבי הגורמים שיכתיבו את אופן ההפעלה בשטח, הנטייה הטבעית של מהנדסי מערכת היא להמנע מקביעת דרך פעולה מסוימת מראש, ולאפשר למפעיל להגדיר את כל הפרמטרים המשפיעים על בחירתה. במערכות מורכבות, מספר הפרמטרים המשפיעים על התנהגות המערכת הוא רב, הגישה למידע על ידי מערכת תפריטים היא בעייתית, מכיוון שהמפעיל עלול להתקשות במציאת הפריט הרלבנטי למצב שהוא בלתי מוכר. האתגר של מהנדסי המערכת הוא להציג למפעיל את המידע הרלבנטי למצב המערכת, ואפשר לו להגיע למידע החיוני באופן הדרגתי, מבלי להציף אותו במידע. הפתרון של "אשף הפעלה" מתאים אמנם להפעלה בתנאי לחץ, אבל כאמצעי בלעדי הוא בעייתי, מכיוון שאינו מאפשר גישה מהירה למידע.

## בעיית הזיהוי

בעיית הזיהוי מוגדרת על ידי מצבים בהם המפעיל מודע לפרמטרים הקריטיים של המערכת, אך מתקשה לזהות את הגורם למצב התקלה. הקושי בזיהוי יכול לנבוע ממיעוט מידע, דוגמת המקרה משנות השמונים של טעות התיכון במכשור הרדיותרפיה Therac-25 (<http://sunnyday.mit.edu/papers/therac.pdf>), או מחוסר התמצאות במערכת, דוגמת מערכת הגיבויים של תחנות כוח. מהנדסי המערכת נדרשים לפתח מערכת איתור תקלות אינטגרטיבית למערכת השו"ב, המספקת רשימה של גורמי תקלה אפשריים, ותיאור התנהגות המערכת במצבי תקלה כנ"ל, כגון בטכניקות של PHA ו-FMEA או על ידי סימולציה. במערכות מעשיות, גורמי התקלה האפשריים הם רבים. להתמצאות מהירה, המערכת, צריכה לכלול מנגנון סינון גורמי תקלה על פי הסימפטומים של המצב הבעייתי.

## הפקת לקחים מתקלות קלות

במערכות מעשיות, מרבית החריגות מפעולה נורמלית מסתיימות ללא נזק משמעותי, בדרך של שיתוף פעולה נכון בין המפעיל לבין המערכת. במקרים מסוימים, אסון יכול להמנע רק ברגע האחרון. מכל מקרה של חריגה המצביעה על סיכון, ניתן ללמוד ולהפיק לקחים, על מנת למנוע הישנות שלה. קיים קושי לקבל מידע זה מהמפעילים, שאינם מודעים למצב המערכת ולמשמעותו, ובדרך כלל מתקשים לדווח על הסיבה לתקלה. במקרים רבים, המפעילים אינם מדווחים על תקלות מכיוון שהם מייחסים את המצב הבעייתי לשגיאה אישית שלהם, במקום לטעות בתכנון. מהנדסי מערכות נדרשים לספק מנגנון שמאפשר שחזור מצבים בעייתיים וחקירתם. לדוגמא, מנגנון להקלטה ושחזור של תוכנת ההפעלה של ציוד הרדיותרפיה Therac-25 היה יכול לאפשר זיהוי הבעיה ותיקון תוכנת ההפעלה מיד בפעם הראשונה לאחר שהתעורר חשד לתקלה במכשיר.