

תקציר מאמר לכנס האיגוד הישראלי להנדסת מערכות בנושא:

## אופטימיזציה של בקרת האוטומציה

אבי הראל, ארגוליט  
רח' גבעון 6, חיפה 34335  
054-4534501

אחת השאלות המרכזיות בהגדרת מערכות היא אילו מהתפקידים יש להטיל על המערכת ואילו מהם יש להשאיר באחריות המפעיל.

הנטיה הטבעית של מהנדסי מערכת היא למחשב כל מה שאפשר, על מנת להפחית את העומס מהמפעיל. 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, ולכן נדרשת התערבות המפעיל לקביעת אופן ההפעלה.

באין ידיעה מראש לגבי הגורמים שיכתיבו את אופן ההפעלה, הנטיה הטבעית של מהנדסי מערכת היא לאפשר למפעיל להגדיר את כל הפרמטרים המשפיעים על בחירתה. במערכות מעשיות, הכוללות מספר רב של פרמטרים, המפעיל מתקשה לעקוב אחר ההשתנות של הפרמטרים במערכת, עובדה הגורמת לטעויות הפעלה, הגורמות לאובדן זמן, ובמקרים מסוימים עלולות להסתיים באסון.

השאלה של בקרת האוטומציה היא כיצד להציג למפעיל את הפרמטרים של בקרת האוטומציה, וכיצד לאפשר לו למצוא ולשנות אותם על פי דרישתו.

שני שיקולים מרכזיים בהגדרת הבקרה הם מיומנות המפעיל והסיכון של טעות הנובעת מהפעלה עם פרמטרים שגויים.

## אופטימיזציה על פי מאפייני הפעלה

מאפייני הפעלה כוללים מיומנות המפעיל, קצב הארועים המשפיעים על פרמטרי הפעלה, מצב עוררות ועוד.

הנטיה הטבעית של מהנדסי מערכת היא להתאים את בקרת הפעלה למפעיל המיומן, שהכרותו עם המערכת דומה להכרותם עמה. במערכות מעשיות רבות, המפעיל אינו מודע לכל הגורמים המשפיעים על אופני הפעלה באותה רמה כמו מהנדסי המערכת, ולכן נדרשת התאמה למצבים של הכרות חלקית.

דרך מקובלת להתמודד עם מצבים של הכרות חלקית לגבי פרוצדורות הפעלה היא על ידי "אשף הפעלה", תכנית מחשב שמנחה את המפעיל צעד אחר צעד. דרך זו מתאימה לתהליכים חד פעמיים, כגון, לאיתור תקלות, אך מקשה על הפעלה של תהליכים חוזרים ונשנים. במיוחד, דרך זו מתאימה להפעלה במצבי לחץ.

השאלה של בקרה על פי מיומנות המפעיל היא מהו שביל הזהב בין התאמה להפעלה חד פעמית לבין התאמה להפעלה חוזרת ונשנית. אחת הגישות להתמודד על בעיה זו היא על ידי אדפטציה אוטומטית על פי היסטוריה של הפעלה. הבעיה באדפטציה האוטומטית היא שהמערכת אינה מתנהגת באופן עקבי, עובדה המעמיסה את המפעיל בתפקיד נוסף, שאינו אינהרנטי לבקרת המערכת, דהיינו, מעקב שוטף אחר השינויים בהתנהגות המערכת.

ההרצאה תציג מתודולוגיה להגדרת ממשק הפעלה על פי השכיחות הצפויה של תהליכי הפעלה, בעזרת ניתוח על פי תרחישים ואימות על ידי בדיקת שימוש בשדה.

## אופטימיזציה על פי סיכונים

כאשר המפעיל עסוק בתפקידיו העיקריים, הוא אינו תמיד קשוב לשינויים במצבי המערכת. לפיכך, בהגדרת ממשק ההפעלה, מקובל להציג בפניו באופן שוטף את הפרמטרים החשובים, אילו שידיעתם חשובה להפעלה הנכונה של המערכת בהפעלה רגילה. הבעיה בגישה זו מתעוררת במצבים חריגים. במקרים אלו, מקובל לתת למפעיל התראה, ולאפשר לו גישה לפרמטרים הרלבנטיים.

בעיה מרכזית בהגדרת מערכת היא הגדרה של מצבים נורמלים לעומת מצבים חריגים. ריבוי התראות לגבי מצבים חריגים עלול להיות בעייתי, מכיוון שהמפעיל עלול להתייחס אל התראה חמורה כאל התראת שווא. דרך מקובלת לצמצם את הסיכוי למצבים חריגים היא על ידי איפוס אוטומטי של פרמטרים, על ידי הצבה של ערכי ברירת מחדל. הבעיה בדרך זו היא שהמפעיל אינו תמיד מודע לאיפוס האוטומטי, ועלול לטעות ולפעול באופן שגוי. בהרצאה אציג תהליך של ניתוח סיכונים איפוסים אוטומטיים, מניעתם והתמודדות עם מצבים של הפעלה במצב שגוי.

אחד הסיכונים במערכות מורכבות הוא הזנת נתונים שגויים. בהרצאה אסקור שיטות לאיתור טעויות בהזנת נתונים, והשוואה ביניהם בשיקולים של סיכון הפעלה עם נתונים שגויים.

## סינכרון הקשר אדם-מכונה

גורם מרכזי בכשל מערכות הוא בעיות בסינכרון הקשר עם המפעיל, כאשר המפעיל נכשל בזיהוי מצב המערכת, או כאשר המערכת נכשלת בתגובה לפעולה בלתי צפויה של המפעיל.

הקשר אדם-מכונה מוגדר בעזרת מודל זרימת מצבים של המערכת המוכללת, הכוללת את מצבי המכונה, את מצבי המפעיל ואת המעברים ביניהם. בעיות סינכרון מוגדרות כמצבים של סטייה ממודל הזרימה. תהליך הסינכרון כולל שלשה מרכיבים: איתור מצבי חוסר סינכרון, קביעת הגורם למצבי של חוסר הסינכרון ותיקון.

איתור מצבי חוסר סינכרון מבוסס על מימוש מודל זרימת המצבים במערכת, ועל איתור פעולות של המפעיל שהן בלתי צפויות על פי מודל זה. הגורם לסטייה ממצב של סינכרון יכול להיות פעולה חריגה של המפעיל, כגון במצב חרום, או קושי של המפעיל לעקוב אחר מצב המערכת. הדרך לקביעת הגורם למצב של חוסר סינכרון היא על ידי התראה למפעיל, תוך הצעה לשינוי מצב המערכת. תיקון מצב הסטייה נקבע על ידי פעולת התגובה של המפעיל להצעת המערכת: אישור או ביטול.

## התראות ואיתור תקלות

בעיה נוספת בהגדרת מערכת היא אופן ההתראה לגבי מצבים חריגים. התראה מתמשכת עלולה להפריע למפעיל להתרכז בפתרון הבעיה. לעומת זאת, אם מאפשרים למפעיל להפסיק את ההתראה, קיימת סכנה שבמקרים מורכבים דעתו תוסט לבעיה אחרת, ובהמשך הוא ישכח לטפל בבעיה המקורית. בהרצאה אציג דרך למעקב אחר התראות במצבים מורכבים.

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. בהרצאה אציג את העקרונות של מימוש התרעה קולית.

בעיה נוספת בהגדרת מערכת היא של זיהוי המצב החריג שגרם להתראה, דהיינו, איתור תקלות. בעיה זו היא בדרך כלל מורכבת ביותר, ולכן במערכות הנדסיות רבות, איתור התקלות ממומש במערכות עזר נפרדות. הבעיה בגישה זו היא שבמצב חריג יש להפסיק את ההפעלה השוטפת של המערכת, עד לשלב ההתגברות על התקלה. בהרצאה אציג דרך לאיתור תקלות מובנה, בתגובה לסט של התראות.