

תקציר מאמר לכנס האיגוד הישראלי להנדסת מערכות בנושא:

הבטי אמינות של מערכות אינטראקטיביות

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

מאמר זה עוסק בהבטי אמינות באינטראקציה בין מערכות, בין תת-מערכות, בין אדם למכונה ובין מפעילים של מערכות מורכבות. המאמר מציג את בעיית האמינות כבעיית סטייה מפעילות נורמלית, ומציע מתודולוגיה להגדיר מהי פעילות נורמלית, לאבחן מצבים של סטיות, למנוע מצבים כאלו במידת האפשר, ולהגיב באופן סלחני לסטיות בלתי נמנעות, על ידי סינכרון ביניהם. בדומה לשיטת HAZOP המקובלת, המתודולוגיה מבקשת לאתר מצבים בלתי צפויים מראש, ולהעריך את הסיכונים של מצבים אלו. בניגוד ל-HAZOP, המצבים המבוקשים אינם מצבים של המכונה, כי אם מצבים של האינטראקציה. ובניגוד ל-HAZOP, הסטיות המבוקשות אינן בהשוואה לכוונת המתכנן, כי אם לכוונת המפעיל.

הגדרת אינטראקציה תקינה

האינטראקציה בין מערכות מתארת את התנהגותן בתגובה להודעות העוברות ביניהן. בניגוד לתקשורת בין מערכות, המתייחסת לארועים קצרי מועד. האינטראקציה בין מערכות מתארת את יחסי הגומלין המתמשכים ביניהם. בדומה לתקשורת בין מערכות, אינטראקציה תקינה מתוארת על ידי פרוטוקול. אבל, בניגוד לפרוטוקול תקשורת, שפרוטוקול האינטראקציה הוא תלוי מצב. לדוגמא, הפרוטוקול המתאר את האינטראקציה בין קו יצור כימי לבין מערכת בקרת טמפרטורה מאפשר תחילת יצור רק לאחר פיקוד ממערכת הבקרה, בתלות במדידת הטמפרטורה.

אמינות האינטראקציה

בדומה לבעיית אמינות התקשורת, אמינות האינטראקציה מוגדרת היא במונחים של התנהגות בתנאי רעש. ספציפית, שאלת אמינות האינטראקציה מוגדרת כבעיה של התנהגות המערכת במקרים של סטיות מהפרוטוקול המגדיר אינטראקציה תקינה. לדוגמא, במערכת בקרת ירי הכוללת מכלול בקרה ומכלול ירי בתצורת שרת-לקוח. דוגמא של סטייה קריטית מהפרוטוקול היא כאשר מכלול השרת עובר ממצב תרגול למצב חמוש, מבלי שמכלול הלקוח יקבל את האינפורמציה על כך.

אינטראקציה אדם-מכונה

טעויות אנוש הן כוח עליון, אבל התאונות בעטין ניתנות לעתים למניעה. ניתן להתייחס אל המכונה ואל האדם המפעיל אותה כאל מכלולים, ב"מערכת מוכללת", ולתאר את האינטראקציה בין האדם לבין המכונה על ידי פרוטוקול. לדוגמא, המפעיל של מערכת קו יצור נדרש להפעיל קודם את מערכת בקרת הטמפרטורה, ולהתחיל בתהליך היצור רק לאחר שהטמפרטורה הגיע לתחום הרלבנטי. פרוטוקול האינטראקציה עם המפעיל מוגדר באמצעות מודל מנטלי, המתאר את אופן התפיסה שלו את מצבי המכונה. ניתן להתייחס אל טעויות אנוש, כגון, התחלת יצור בטמפרטורה בלתי מתאימה, כאל רעש, המתבטא בסטייה מהפרוטוקול. התאונות הקשורות במכשור הרדיוטרפיה משנות השמונים Therac-25 (<http://sunnyday.mit.edu/papers/therac.pdf>) וכן האסון האקולוגי שנגרם על ידי התבקעות המיכלית באיי סילי ב-18 במרץ, 1967, (<http://www.lboro.ac.uk/departments/hu/ergsinhu/aboutergs/torrey.html>) אלו הם דוגמאות של תאונות הנובעות מסטייה מהפרוטוקול. דוגמא נוספת היא התאונה בסלון האוירי ב-26 ביוני 1988 בצרפת, בה הטייס ביקש פיקוד שלא תאם את מוד הטיסה (<http://aviation-safety.net/database/record.php?id=19880626-0>)

חסינות פרוטוקול האינטראקציה

בדומה לפרוטוקול תקשורת, גם פרוטוקול האינטראקציה רגיש לרעשים. באופן דומה, ניתן להגדיר פרוטוקול חסין לטעויות אנוש אל ידי הוספת מנגנונים דומים לאיתור שיבושים בשל רעש. למשל בקידוד פקודות, ניתן להגדיר מרחק בין פקודות חוקיות, שיעלה על סטייה סבירה. כך, על ידי קידוד כזה, ניתן היה למנוע את התאונה האוירית ב-20 בדצמבר 1995 בקולומביה (<http://sunnyday.mit.edu/accidents/calirep.html>)

בעית הסינכרון באינטראקציה

בעית הסינכרון באינטראקציה מוגדרת על ידי מקרים של שינוי מצב באחד המכלולים, שמתבטא בסטיה מהפרוטוקול. באינטראקציה אדם-מכונה, בעית הסינכרון מתבטאת בכשל של המפעיל בזיהוי מצב המערכת, או בכשל של המכונה בתגובה לפעולה בלתי צפויה של המפעיל. לדוגמא, במעבד תמלילים, במקרה שהמשתמש לוחץ בטעות על CAPS LOCK. הסטיה מהפרוטוקול במקרה זה מתבטאת בשינוי מצב המכלול הממוחשב, כאשר מצב המפעיל נשאר ללא שינוי. תהליך הסינכרון כולל שלשה מרכיבים: איתור מצבי חוסר סינכרון, קביעת הגורם למצבי של חוסר הסינכרון ותיקון.

גורמי סטיה מהפרוטוקול

גורמי סטיה של מכלולים ממוחשבים כוללים: שגיאות תיכון הקשורות לסיבוכיות של מעברי מצבים, איתחול בלתי מבוקר, כגון בהתאוששות מתקלה, ואיתחול כתגובה לפקודה על ידי "צד שלישי". גורמי סטיה של מפעילי מערכת כוללים טעויות הפעלה שגורמות לשינוי במצב המכונה. כמו כן, בהפעלת חירום, לעתים המפעיל גורם במכוון לשינוי מצב המכונה שלא על פי הפרוטוקול.

מניעת בעיות סינכרון

בעיות סינכרון שניתנות למניעה כוללת שגיאות תיכון וטעויות הפעלה מסוימות, שמתאפשרות על ידי פקודות תלויות מצב. לדוגמא, ניתן היה למנוע את התאונות במכשור הרדיותרפיה Therac-25 על ידי החלפת פקודת ההפעלה בשתי פקודות הפעלה נפרדות למצבים של תרפיה ברנטגן או בקרן אלקטרוניים. כמו כן, ניתן היה למנוע את האסון האקולוגי של התבקעות המיכלית באיי סיסיל על ידי מניעת מעבר מוד ההפעלה ממצב ניהוג למצב תחזוקה, במהלך שיוט רגיל. שגיאות תיכון הגורמות ליציאה מסינכרון ניתן למנוע על ידי צמצום הסיבוכיות, על ידי מודולציה של ניהול המצבים.

גילוי סטיה מהפרוטוקול

דרך אפשרית לאיתור סטיה מהפרוטוקול היא על ידי מעקב אחר התנהלות האינטראקציה באמצעות מודל המתאר התנהלות תקינה. הסטיה מתגלית על ידי בדיקת התאמת הארועים הנקלטים למצב המכלול על פי המודל. את המודל אפשר לתאר בעזרת תרשים מעברי מצבים, או באמצעות state charts. במערכת ממוחשבת, אפשר לייצג את המודל באמצעות תרשים זרימת מצבים, הכולל את מצבי כל המכלולים זה בצד זה, ואת ההודעות בין המכלולים אפשר לתאר כארועים הרלבנטיים למצבי המערכת המוכללת. מעבר המצבים מיוצגים על ידי ארועים הגורמים לשינויי המצב.

זיהוי מקור הסטיה

זיהוי מקור הסטיה מתאפשר על ידי שידור הודעה לשותף לגבי כל מקרה של שינוי מצב. לדוגמא, במקרה של איתחול אחד המכלולים בתהליך התאוששות מתקלה, מכלול זה צריך לשדר לכל השותפים הודעת איתחול, שתאפשר להם להסתנכרן אליו. במקרה של סטיה מהפרוטוקול על ידי מפעיל המכונה, הסיבה לסטיה יכולה להיות טעות הפעלה או סטיה במכוון. במקרה זה, המכונה יכולה לתשאל את המפעיל, לבקש את אישורו לפני ביצוע הפעולה. תגובת המפעיל מזהה למעשה את מקור הסטיה.

תגובה לארוע המחייב סטיה מהפרוטוקול

כדי למנוע טעויות מצב, בתצורת שרת-לקוח, מהנדס המערכת נדרש להגדיר תגובה עקבית לפקודות הלקוח, כלומר, תגובה שאינה תלויה מצב. באינטראקציה אדם-מכונה, במצבים בהם נדרשת שליטה מוחלטת של המפעיל, כגון בהפעלת חרום, אין למנוע את אפשרות הסטיה מהפרוטוקול, אבל ניתן לדרוש את אישור המפעיל לסטיה מהפרוטוקול, והשרת צריך לציית ולהסתנכרן למצב החדש. ניתן היה למנוע את תאונת האימונים "צאלים א" על ידי מנגנון לאיתור סוג זה של סטיה.

בדיקות איכות הפרוטוקול וממשק ההפעלה

הקלטת האינטראקציה וניתוחים סטטיסטיים של הסטיות מהפרוטוקול מאפשרים ללמוד לגבי הצורך בשינויי תיכון, באופן שארועים שנחשבו לבלתי צפויים הם למעשה צפויים ונחוצים להפעלה תקינה. מסטטיסטיקה של אישורים וביטולים של המפעיל בתגובה לתשואול המכונה, ניתן להסיק לגבי אופן השינוי הנדרש בפרוטוקול ובממשק ההפעלה.