11 ביוני, 2014

סיכום מפגש 6 של קבוצת העבודה "תכן לאבטחת מסינות מערכות"

בנושא ניהול האוטומציה

רשם: גלעד סגל, ערך: אבי הראל

רשימת המשתתפים במפגש כאן

מהלך המפגש

בחלק הראשון, עזריאל אובסטבאום הציג ששה אירועים בתחום התחבורה האוירית, בהם היתה בעיה הקשורה בניהול האוטומציה

1. טיסת Air France 296
2. טיסת Lufthansa 2904
3. טיסת Lufthansa 44
4. טיסת Air France 447
5. טיסת Colgan Air 3407
6. טיסת Asian 214

בחלק השני היה דיון בו ניסינו להציע פתרונות למקרה של טיסת Colgan Air 3407 .

נקודות שעלו בדיון

אבי – בטיסה זו המטוס התרסק כתוצאה מהזדקרות. הסיבה להזדקרות היתה טעות של הטייס בתגובה להתרעה על אובדן מהירות. במקום לדחוף את הסטיק, הוא משך אותו. על פניו, נראה שאפשר להגדיר אילוצים שמאפשרים למטוס לקבל שליטה, ולהתגבר על הפעולה השגויה של הטייס. השאלה לדיון היא האם ניתן להגדיר אילוצים כאלו, ומהם הסיכונים בהגדרת אילוצים כאלו.

ארז/יזהר – הבעיה באירוע הספציפי הייתה בחוסר מיומנות של הטייסים בהזדקרות בגלל החלטה ניהולית של מנהל התעופה האמריקאי.

עזריאל – כשמטוס מזדקר הטייס נדרש לדחוף קדימה את הסטיק. באירועים שהוצגו, הטייסים משכו סטיק.

יזהר – הבעיה היתה שההתרעה לא היתה מובחנת מהתרעות אחרות, בהן הטייס נדרש להעלות את זוית העלרוד. לכן, מתוך הרגל, הטייס העלה את זוית העלרוד במקום להוריד אותה.

ארז – אולי הטייסים טעו בהבנת ההתרעה. צפצוף לרוב מציין קירבה לקרקע ואז האינטואיציה היא למשוך. בהזדקרות התגובה נדרשת להיות שונה, אך ייתכן וסוג ההתרעה הקולית הייתה זהה.

אלון – צריך להוסיף התרעות ספיצפיות. לדעתו אם כל התרעה תהיה שונה, להערכתו יהיו כמה עשרות התרעות.

אבי – מעלה את המחקר שעשו בבית חולים שאחיות מסוגלות להבחין בעד שלוש התרעות מבין מגוון ההתרעות השונות שהמכשירים מזמרים (8 בסה"כ).

יזהר – במטוסים צבאיים (אינני זוכר אם F16 או F15) המטוס יכול "לדבר" עם הטייס ולהתריע על בעיות ספציפיות שהטייס הגדיר.

עזריאל – טיסת Quantas שנפגעה בהרבה מערכות העסיקה את טייס המשנה מרגע הפגיעה ועד הנחיתה בפתרון תקלות בעזרת המחשב, שכלל תמיכה בבד"ח.

יזהר – העלה מקרה בו הטייס פתח את הספר תקלות בעמוד הלא נכון וטיפל לא נכון בבעיה.

אלון – הטייס נדרש להבין תמונת מצב אמיתית בעזרת כל המכשירים. החיווי צריך להיות אמין. הטייס נדרש לבצע בכל רגע הערכת מצב המבוססת על שילוב של מספר מכשירים, כך שיוכל לצפות את התרחשות המצב החריג לפני התרחשותו בפועל. במקרה של הנחיתה על ההדסון – ה"מזל" היה שלא הספיקו להעביר את המטוס למצב של טייס אוטומאטי.

אלון –כיום כבר יש מערכות שיודעות לבצע באופן אוטומאטי את כל מהלך הטיסה (המראה, שיוט, נחיתה).

שרון – המערכות כיום בנויות כך שלמשתמש יש פחות מקום במצב רגיל, אך כאשר המצב חריג ונדרשת מעורבות אנוש אזי רמת המיומנות/יכולת של המפעיל נמוכה יחסית.

עזריאל –לא תמיד הנחיות חברת הטיסה תואמות את הנחיות חברת הייצור של המטוס בנושאי בטיחות (לרעה).

יזהר – ישנם מטוסים בהם ברגע שיש תקלה, והמטוס מזהה אותה נפתח אוטומאטית הדף הרלוונטי לתקלה, לפי זיהוי של המערכות.

אלון – בהנחה שיש תמונת מצב וחיווי נכון של התקלה.

אבי – האם ניתן להגדיר אילוצים שימנעו אוטומטית את ההזדקרות

ראובן – אפשר לעבוד עם STAMP, אך ברגע שמתחילים עם מעט אילוצים מהר מאוד מגיעים למצבים בהם אין פיתרון מלא.

שרון – לדעתה STAMP לא יעבוד במקרה שכזה. לדעתה המודל יעבוד בסיטואציות יותר דיסקרטיות, אך לא עובד טוב במערכות אנלוגיות. איזור בו יש יותר סיכויים לצאת ממצב חריג הוא איך מספקים מודעות מצב טובה יותר למשתמש. לדעתה עדיף על פני אלגוריתמיקה.

אבי – לסיכום, לא מיצינו את הדיון בנושא הסיכונים בגין הטסה בכפוף לאילוצים למניעת הזדקרות. הנושא חשוב, וכדאי להמשיך את הדיון באחד המפגשים הבאים.