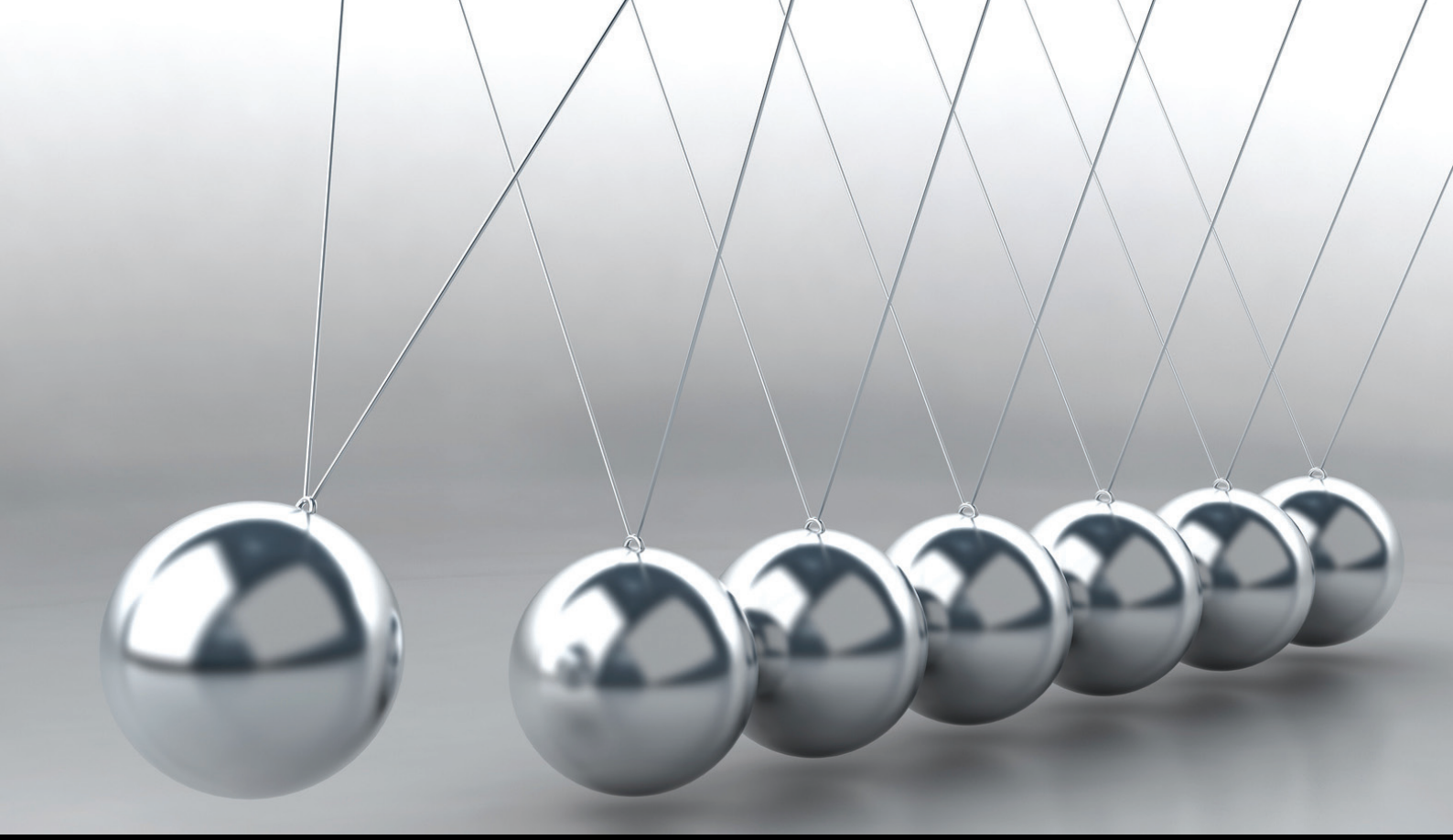


DO-178 – הדרך המהירה להסמכה

רועי פן, סיסטמטיקס

על פי הבדיחה, שאלו פעם בכנס של מהנדסים העוסקים בתחום התעופה מי מהם היה מוכן להשתתף בטיסת המבחן הראשונה של מטוס שהוא היה מעורב בפיתוחו. רוב המהנדסים, כצפוי, לא מיהרו להתנדב, פרט למהנדס אחד שהרים את ידו. ''כיצד אתה כל כך בטוח בחלקך בעבודה על מטוס חדשני ולא חושש שהוא יתרסק'', נשאל המהנדס, שבתגובה ענה: ''מטוס שאני עבדתי על פיתוחו בכלל לא ימריא''...

על מנת לגרום למהנדסים וללא-מהנדסים להרגיש בטוחים יותר במטוסים שבהם הם טסים, חובר לפני שלושים שנים מסמך ה-DO-178, שהפך דה-פקטו לסטנדרט בטיחות בינלאומי לתהליכי פיתוח של תוכנות המשמשות במטוסי נוסעים, כלי טייס לא מאוישים ובמערכות מוטסות (מערכות תקשורת, תצוגה, מערכות בקרה וכדומה). התקן דורש תיעוד מפורט של תהליך הפיתוח, לצד מסמכים תומכים רבים, כאשר מידת הפירוט וכמות המסמכים הנדרשות נקבעות על פי רמת הריסָיון בה מעוניינים. הרמות השונות, D, C, B, A ו-E, תואמות את ההשלכות האפשריות של כשלון של התוכנה: קטסטרופה (מוות ודאי של כל הנוסעים או חלקם), סכנה חמורה (פוטנציאל למוות של מספר אנשים), סכנה גדולה (פגיעות גופניות קשות), סכנה קטנה (פגיעות גופניות קלות) או העדר השפעה על המשך בטוח של הטיסה והנחיתה, בהתאמה.

תקן ה-DO-178 מכסה את כל מחזור החיים ההנדסי - משלב דרישות התכנון, דרך שלב הפיתוח ועד לשלב הבדיקות של התוכנה. לפי התקן, כל כלי לוריפיקציה של תוכנה המשמש לפיתוח מערכת מוטסת חייב לעבור ריסָיון באם הפלט שלו אינו נבדק (כלי לוריפיקציה של תוכנה מוגדר ככלי שאינו גורם לשגיאות, אך עלול לא לגלות שגיאות קיימות). והאחריות לריסָיון הכלי מוטלת על המשתמש בו, ולא על מפתח הכלי.

תהליך ההסמכה לפי תקן DO-178 מאריך באופן משמעותי את זמני הפיתוח של תוכנות. ''כלל האצבע קובע כי בהשוואה לפרויקט לא-מרושיין, התוספת לזמן הפיתוח הנדרש לפרויקט אשר אמור להיות מרושיין לתקן ה-DO-178 היא 150%-75% מהזמן הדרוש לפיתוח הפרויקט הלא-מרושיין, בתלות ברמת הריסָיון אליה מכוונים'', אומר ביל פוֹטֶר, מנהל שיווק טכני בחברת MathWorks האמריקאית, מפתחת התוכנות MATLAB ו-Simulink, ''אבל עם כלים מתאימים ניתן לקצר את משך התוספת ל-25% עד 40% בלבד''. פוטר הצטרף לחברה לפני כחמש שנים אחרי 26 שנות עבודה בחברת הענק Honeywell, והינו חבר בוועדה העובדת בימים אלה על הגרסה השלישית של התקן, DO-178B, המיועדת להתאים לטכנולוגיות פיתוח מודרניות

ביל פוטר

הדגמה של כלי MathWorks במסגרת הכנס על ידי מהנדס האפליקציה אריאל רובנקו

ולענות על מספר פערים בגרסה הנוכחית שלו, DO-178B. הוא הגיע לארץ בתחילת דצמבר לכנס ראשון מסוגו בישראל בנושא הסמכה לתקן DO-178, אותו ארגנה חברת סיסטמטיקס, מפיצת MathWorks בארץ. בכנס, אליו הגיעו עשרות משתתפים, נטלו חלק גם נציגים מחברות מובילות בתחום, דוגמת Atego HighRely, LDRA ו-Vector Software. "אנחנו נוהגים לקיים כנסים משותפים עם חברות אחרות, מתוך מטרה שנשלים האחד את השני וניתן למשתתפים פתרון כולל", אומר פוטר, "אבל זו הפעם הראשונה שבה השתתפתי באירוע עם כל כך הרבה חברות, אשר חלק מהן מתחרות זו בזו. אני מאמין שהישראלים העוסקים בתחום רק הרוויחו מכך".

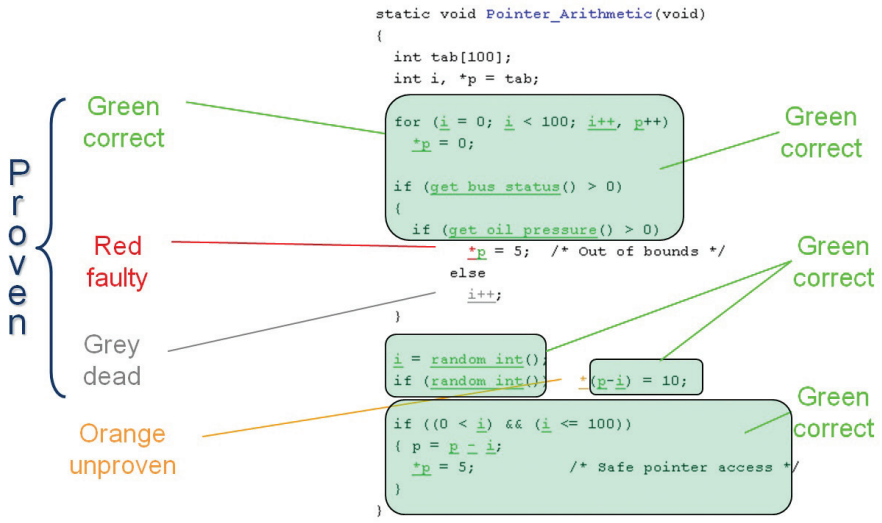
בכנס הודגם תהליך העבודה להסמכה לתקן DO-178 באמצעות כלי MathWorks (הרחבה על הכלים הרלוונטיים – בהמשך). בין היתר, הוצגה בו שיטת התכנון מבוסס-מודל (Model-Based Design), והודגם כיצד ניתן לבנות מודל בסביבת הפיתוח האינטואיטיבית Simulink, לקשר את החלקים השונים של המודל למסמכי דרישות ולוודא את תקינותו ועמידתו בסטנדרטים שונים (באמצעות ממשק ידידותי למשתמש הנקרא model advisor). כמו כן, הוצג כיצד ניתן לבצע בדיקות כיסוי (coverage להחלטות, תנאים, טבלאות חיפוש, טווחים של סיגנל ומימדים של סיגנל בגודל משתנה), ליצור טסטים באופן אוטומטי, להפיק דו"חות בצורה אוטומטית, לאמת ולתקף את המודל, להמיר אותו לקוד C או HDL באופן אוטומטי, להשתמש ב-formal methods על מנת לאמת ולתקף את הקוד, לבצע אוטומציה לתהליך ה-code review ולרשיין כלים לוריפיקציה של תוכנה המעורבים בתהליך. בנוסף, הוצגו בכנס הכלים המשלימים של החברות LDRA ו-Vector Software לבדיקת הקוד המיוצר באופן אוטומטי ממודל ה-Simulink, וניתנה סקירה של חברת Atego HighRely על הגרסה העתידית של התקן, DO-178C.

"היתרון הגדול של כלי MathWorks הרלוונטיים להסמכה לפי תקן DO-178 הוא בכך שהם מאפשרים אוטומציה של תהליך הבדיקות, דבר הבא לידי ביטוי הן בחסכון של זמן והן בשיפור איכות המוצר, שכן עבודה ידנית מכניסה שגיאות לתהליך", אומר פוטר. "כלי MathWorks שימשו עד כה לרישיון פרויקטים שאושרו על ידי הרשויות בארצות-הברית (FAA) ובאירופה (EASA), כאשר רוב הרישיונים היו לרמות הגבוהות ביותר, A ו-B. חברת Honeywell, למשל, מצהירה בפומבי על קיצוץ של 60% בזמני הפיתוח הודות לשימוש בכלי ההמרה מ-Simulink לקוד C במסגרת פרויקט בו פותחה מערכת לבקרת-טיסה. אבל אסור לטעות ולחשוב ש-MathWorks פעילה רק בתחום ה-DO-178, שכן יש לחברה כלים המאפשרים לייצר קוד לחומרה ולהסמיך אותו לפי תקן ה-DO-254. חברת BAE Systems, לדוגמה, פיתחה אלגוריתם בקרה ב-Simulink, ויצרה ממנו בצורה אוטומטית קוד HDL שאותו היא הורידה ל-FPGA, במסגרת פרויקט שעבר אישור לרמה A. המהנדסים שם אמרו שהקוד האוטומטי מאוד קריא, והיו מרוצים מהקישוריות שלו אל מסמכי הדרישות".

כלים רלוונטיים

כלי MathWorks הרלוונטיים להאצת תהליכי ההסמכה לפי תקן DO-178 שהוצגו במהלך הכנס הינם:

Simulink - סביבת פיתוח וסימולציה רב-תחומית המייעלת את תהליכי הפיתוח של מערכות בגישת תכנון מבוסס-מודל. הסביבה מאפשרת לבנות דיאגרמת בלוקים הניתנת להרצה, ואשר יכולה להכיל בתוכה קוד MATLAB. החל מגרסת R2011b הכלי כולל ממשק בשם Simulink Projects, המאפשר לייצר סביבה אחידה הנגישה



תוצאות בדיקת קוד על ידי כלי PolySpace - צבע ירוק פירושו "קוד תקין", אדום פירושו "קוד בעייתי בכל אופן הרצה", אפור פירושו "קוד מת, אשר כלל אינו מתבצע" וכתום פירושו "קוד אשר קיים אופן הרצה שיגרום לבעיות".

לחברי הצוות השונים העובדים על פרויקט, דבר המקל על שיתוף הפעולה ביניהם ומייעל את העבודה בגישת תכנון מבוסס-מודל.

Simulink Coder - כלי הממיר מודלים של Simulink לקוד C או ++C בצורה אוטומטית.

Embedded Coder - כלי המייצר קוד C או ++C קריא, יעיל ומהיר במיוחד מתוך מודלים של Simulink. הכלי מאפשר ביצוע אופטימיזציות לצורך קבלת קוד המיועד לפעול על מערכות Embedded וכן מסוגל להתממשק עם סביבות פיתוח של חברות אחרות, למשל לצורך ביצוע בדיקות של Processor-in-the-loop.

Simulink HDL Coder - כלי הממיר קוד MATLAB ומודלים של Simulink בצורה אוטומטית לקוד HDL - Verilog או VHDL. הקוד יכול לעבור סימולציה וסינתזה באמצעות כלים סטנדרטיים, ואז לרדת ל-FPGA או ASIC.

Simulink Code Inspector - כלי שהושק עם גרסת R2011b של כלי MathWorks, המשמש לאוטומציה של source code reviews לתקני בטיחות. הכלי יוצר דו"ח קישוריות דו-כיוונית בין מודל Simulink לבין קוד המקור שנוצר ממנו בצורה אוטומטית על ידי ה-Embedded Coder, וכן הוא מאפשר וריפיקציה של ה-object code למול מודל ה-Simulink.

DO Qualification Kit - אוסף תבניות, מקרי מבחן ונהלי בדיקה בהם ניתן להשתמש על מנת לרשיין את כלי וריפיקצית התוכנה של MathWorks לתקני DO-178 ו-DO-254. הכלי מאפשר לרשיין מרכיבים משמעותיים מתוך ארבעת הכלים הבאים:

כלי PolySpace - כלים המשמשים לוריפיקציה של קוד מכל סוג שהוא - קוד ידני או קוד שנוצר על ידי כלי אוטומטי - וכל זאת ללא הרצה בפועל של הקוד או הכנה של מקרי מבחן. הכלים מאתרים סוגים שונים של שגיאות run-time, מגלים קטעי קוד "מתים" ובוחנים תאימות של הקוד עם מגוון כללי MISRA-C. הכלים מייצרים דו"ח בו קטעי הקוד צבועים בצבעים שונים (ראה תמונה), ובאם נמצאה בעיה בקוד קל להגיע מהדו"ח אל המקום המתאים במודל ה-Simulink אשר גרם לה.

Simulink Verification and Validation - כלי המשמש לוריפיקציה של מודל ה-Simulink ושל הקוד המיוצר ממנו, אוטומציה של תהליך המעקב אחר מילוי דרישות הפרויקט, אכיפת סטנדרטי מידול ומדידת model coverage.

SystemTest - כלי לניהול בדיקות לצרכי אימות ותיקוף של המערכת - הכלי מסייע בהגדרת הבדיקות, הרצה שלהן, ניתוח תוצאותיהן ויצירת דו"חות המסכמים אותן.

Simulink Report Generator - כלי המייצר דו"חות עבור מודלי Simulink, המתעדים את מקרי המבחן השונים ותוצאות הסימולציות.

Simulink Design Verifier - כלי המשתמש ב-Formal methods על מנת לסייע בהוכחת מילוי דרישה שהמשתמש דורש ובגילוי טעויות באלגוריתם (כמו חלוקה ב-0). הכלי מייצר וקטורי בדיקה, ובכך לסייע בוריפיקציה של המודל למול דרישות הפרויקט.