

מי צריך תקינה לשימושיות?

אבי הראל

ארגונומיה בע"מ

גבעון 6, חיפה 34335, טל' 4501-453-054, standards@upaisrael.org

איזוהי הדיסציפלינה של אבטחת איכות שעשויה למנוע אישור אבטיפוס של מכונית ללא מנוע? ההגדרה הפורמאלית של איכות מתייחסת אל התועלת שהמוצר מביא למשתמש. על פי הגדרה זו, מכונית ללא מנוע אינה נחשבת לאיכותית, מכיוון שאין בה תועלת: היא אינה שימושית. הבעיה היא שהפרקטיקה של אבטחת איכות אינה עונה על הדרישה לשימושיות: מוצרים רבים בשוק עברו את כל אישורי האיכות, אבל הם בבחינת מכונית ללא מנוע. הם חסרי תועלת.

במסגרת וועדת התקינה לאיכות של מכון התקנים הוקמה לאחרונה וועדה טכנית שעוסקת בתקינה לשימושיות. יותר מדי מוצרים גומרים פיתוח, עוברים את בדיקות האישור בהצלחה, יוצאים לשוק, ונכשלים, מסיבות שונות הקשורות לשימושיות: בגלל שהם חסרי תועלת, בגלל שהם מסובכים מדי לשימוש, בגלל שהם מאפשרים טעויות שימוש קריטיות. יותר מדי מערכות שמיועדות להגן על מתקנים ועל הציבור, פועלים היטב בשלב בדיקות האישור, אבל נכשלים בשעת מבחן, מכיוון שבשלב התכנון לא נשקלו גורמים הקשורים לתהליכי התפעול ולמאפיינים פסיכולוגיים של הציבור. יותר מדי זמן אנחנו מבזבזים בהפעלת תוכנה משרדית בניסיון להבין מהו מצב המערכת, ומה צריך לעשות כדי שהתוכנה תעשה את מה שאנחנו רוצים. או בניסיון להבין מדוע הטלביזיה הביתית מראה שלג במקום תמונה, ומה עלינו לעשות כדי למנוע מצבים כאילו.

בקרב מפתחים ומהנדסי איכות רווחת הדעה שגורמי האיכות בשימושיות הינם תלויי אינטואיציה - עניין של טעם וריח. במקרים של כשלון, הנטייה היא להטיל את האחריות על המשתמש. כך, לדוגמה, במקרה של אסון שנגרם באירוע בו המפעיל לא הבין את כוונת המתכנן, הנוהג הרווח הוא להטיל את האחריות על המפעיל, במקום על המתכנן. בכך נמנעת האפשרות לתקן את הליקוי ולמנוע את האסון הבא. תקינה לשימושיות תנחה את המפתחים כיצד להימנע מטעויות נפוצות בתכנן השימושיות, כאלה הגורמות לאובדן תפוקה, לירידה בבטיחות, לנזקים בגין תפעול שגוי ולחוסר שביעות כללית מהמוצרים.

תקינה בינלאומית לשימושיות קיימת כבר משנות התשעים. הבעיות בתקינה הבינלאומית הן: א. היא מסובכת מדי, ב. היא פונה אל אנשי מקצוע בתחום השימושיות, ולא אל המפתחים, ו-ג. הפתרונות המוצעים לבעיות קריטיות, כגון אלו שבדוגמאות לעיל, אינם מספקים. בארץ, עד כה לא היה ביקוש לתקינה. וועדת התקינה הישראלית לשימושיות שמה לעצמה מטרה ליצור תקנים שמיועדים לשימוש על ידי המפתחים, ושתועלתם למפתחים ולצרכנים אינם מוטלת בספק. בשאיפה, הכוונה היא לאמץ תקינה בינלאומית, אבל כבר כיום ברור לנו שעיקר התועלת תהיה מתקינה מקורית.

התקינה לשימושיות נמצאת כיום בראשית דרכה. וועדות מומחים מוקמות בימים אלו, להגדיר תקנים עבור מספר פרויקטי פיזי, כולל תקנים למפרכי קונטקסט הפעלה ומאפייני משתמש, תקנים לאבטחת שימושיות של התרעות במצבי חירום, תקנים לשילוב גורמי אנוש בתהליכי פיתוח ואבטחת איכות, תקנים לאבטחת שימושיות של אתרי אינטרנט, מילון מושגים ומנחי שימושיות, ועוד.

אבטחת שימושיות ואבטחת איכות

איזוהי הדיסציפלינה של אבטחת איכות שעשויה למנוע אישור אבטיפוס של מכונית ללא מנוע?

נדמין לעצמנו יצרן מכוניות שהזמין פיתוח דגם חדש של מכונית, ופירט את כל הדרישות במפרטים, ודרש שהמכונית תעמוד בתנאי דרך קשים, ושהחומרים מהם תורכב המכונית יבטיחו פעולה תקינה של המכונית לאורך זמן, אבל פרט אחד הוא שכח לציין והוא שהמכונית צריכה לכלול מנוע. כי זה הרי מובן מאליה שהמכונית תכלול מנוע, כי ידוע שכל מכונית כוללת מנוע. תיאורטית, בתהליכי אבטחת איכות המקובלים, המכונית עלולה לעבור את כל המבחנים, מכיוון שהיא עשויה מחומרים טובים, שמבטיחים אחוז תקלות נמוך. המכונית הזו תיחשב לאיכותית, למרות שאינה שימושית.

דוגמה זו נראית לכאורה הזויה, אבל קל יותר לקבל אותה אם במקום מנוע, נחשוב על פין שצריך לחבר את המנוע אל תיבת ההילוכים. ההגדרה הפורמאלית של איכות מתייחסת אל התועלת שהמוצר מביא למשתמש (לדוגמה, ההגדרה ב- http://www.chesapeakebay.net/info/qa_glossary.cfm). על פי הגדרה זו, מכונית ללא מנוע, או ללא פין שמחבר את המנוע אל תיבת ההילוכים, אינה נחשבת לאיכותית, מכיוון שאין בה תועלת:

היא אינה שימושית. הבעיה היא שהפרקטיקה של אבטחת איכות אינה עונה על הדרישה לשימושיות: מוצרים רבים בשוק עברו את כל אישורי האיכות, אבל הם בבחינת מכונית ללא מנוע. הם חסרי תועלת.

המסמך ISO/IEC 9126-1 מגדיר איכות תוכנה על ידי שש תכונות, אחרת מהן היא השימושיות. האם אנחנו משקיעים מספיק בשימושיות? האם אנחנו מנסים לשפר אותה? כיצד? האם אנחנו דנים בכך בכנסים בנושא איכות? או, אולי אנחנו מעדיפים להשאיר את הנושא למהנדסי שימושיות? וכיצד אנחנו משלבים תהליך אבטחת שימושיות עם תהליך אבטחת איכות?

המסמך *ISO 9241-11 (1998) Guidance on Usability* מגדיר שימושיות של מוצר (או מערכת) כיכולת של משתמשים מוגדרים להשיג יעדים מוגדרים באפקטיביות, יעילות, ובשביעות רצון, בהקשר שימוש מוגדר. המושגים הללו מגדירים למעשה את התועלת שמתקבלת מהשימוש במערכת, ולכן מבחינת ההגדרה, שני המושגים קרובים ביותר זה לזה. בפרקטיקה, לעומת זאת, מדובר בשני עולמות שונים, כאשר באופן מסורתי תהליכי אבטחת איכות המקובלים בתעשייה מתעלמים מפגמים קריטיים בתיכון הקשורים בטעויות תפעול. בתהליכי אבטחת שימושיות המסורתיים, לעומת זאת, הנטייה היא להתמקד באבטחת איכות התפעול בשלבים הראשונים של תפעול המערכת: בשלב ההתנסות הראשונית ובשלב הלמידה. הנושא החשוב של התמודדות עם בעיות תפעול בתהליכים שגרתיים נופל בין הכיסאות. מדובר בשני סוגים של בעיות: מצבים של טעות תפעול, וקשיים של המפעילים להתמודד עם תקלות מערכת.

עיקרי התקינה לשימושיות

במסגרת וועדת התקינה לאיכות של מכון התקנים הוקמה לאחרונה וועדה טכנית שעוסקת בתקינה לשימושיות. יותר מדי מוצרים גומרים פיתוח, עוברים את בדיקות האישור בהצלחה, יוצאים לשוק, ונכשלים, מסיבות שונות הקשורות לשימושיות: בגלל שהם חסרי תועלת, בגלל שהם מסובכים מדי לשימוש, בגלל שהם מאפשרים טעויות שימוש קריטיות. יותר מדי מערכות שמיועדות להגן על מתקנים ועל הציבור, פועלות היטב בשלב בדיקות האישור, אבל נכשלות בשעת מבחן, מכיוון שבשלב התכנון לא נשקלו גורמים הקשורים לתהליכי התפעול ולמאפיינים פסיכולוגיים של הציבור. יותר מדי זמן אנחנו מבזבזים בהפעלת תוכנה משרדית בניסיון להבין מהו מצב המערכת, ומה צריך לעשות כדי שהתוכנה תעשה את מה שאנחנו רוצים. או בניסיון להבין מדוע הטלביזיה הביתית מראה שלג במקום תמונה, ומה עלינו לעשות כדי למנוע מצבים כאלו.

תכנית התקינה

תקינה בינלאומית לשימושיות (http://www.usabilitynet.org/tools/r_international.htm) קיימת כבר משנות התשעים (לדוגמה - Bevan, 2001). הבעיות בתקינה הבינלאומית הן: א. היא מסובכת מדי, ב. היא פונה אל אנשי מקצוע בתחום השימושיות, ולא אל המפתחים, ו-ג. הפתרונות המוצעים לבעיות קריטיות, כגון אלו שבדוגמאות לעיל, אינם מספקים. בארץ, עד כה לא היה ביקוש לתקינה. וועדת התקינה הישראלית לשימושיות שמה לעצמה מטרה ליצור תקנים שמיועדים לשימוש על ידי המפתחים, ושתועלתם למפתחים ולצרכנים אינם מוטלת בספק (<http://www.usability-standards.com/Principles/Principles.htm>). תקינה לשימושיות תאפשר:

- א. הנחיה למפתחים
- ב. הגנת הצרכן
- ג. הפקת לקחים מתאונות שמיוחסות לטעות המשתמש
- ד. הפקת לקחים ממצבים של כמעט-תאונה.

תקינה לאבטחת שימושיות כעזר הדרכה למפתחים

בקרב מפתחים ומהנדסי איכות רווחת הדעה שגורמי האיכות בשימושיות הינם תלויי אינטואיציה - עניין של טעם וריח. במקרים של כשלון, הנטייה היא להטיל את האחריות על המשתמש. כך, לדוגמה, במקרה של אסון שנגרם באירוע בו המפעיל לא הבין את כוונת המתכנן, הנוהג הרווח הוא להטיל את האחריות על המפעיל, במקום על המתכנן. תקינה לאבטחת שימושיות תנחה את המפתחים כיצד להימנע מטעויות נפוצות בתכן השימושיות, כאלה הגורמות לאובדן תפוקה, לירידה בבטיחות, לנוקים בגין תפעול שגוי ולחוסר שביעות כללית מהמוצרים.

דוגמאות של טעויות תיכון נפוצות שניתן למנוע על ידי תקינה:

דוגמה בנושא תכנון מסכי מחשב: בהתלבטות בין העמסת מסך במידע, לבין חלוקת המידע בין מספר מסכים, הנטייה בקרב אנשי פיתוח היא לצמצם את מספר המסכים. לעומתם, אנשי השינוק נוהגים להנחות את אנשי הפיתוח לצמצם את כמות המידע על גבי המסך. התקינה בנושא זה תנחה את המפתחים לגבי התאמת סוג הפתרון למצבי התפעול.

דוגמא בנושא תכנון פקדים: טעות נפוצה אצל אנשי פיתוח היא להעמיס פונקציות דומות על פקד, כאשר בחירת הפונקציה נעשית על ידי תלות במצב המערכת. במקרים בהם המפעיל טועה בזיהוי מצב המערכת, הוא מפעיל בשוגג את פונקציה שאינה תואמת את כוונתו. טעויות מצב הן גורם עיקרי לסיבוכיות בהפעלה של ציוד בשימוש יומיומי, (כדוגמת **מערכות טלביזיה בכבלים**), וכן לתאונות רבות להפעלת מערכות בקרה בתעשייה, בתחנות כוח, בתחבורה – כולל במצבי חירום. התקינה בנושא זה תנחה את המפתחים כיצד למנוע מהמפעיל טעויות מצב, כיצד לאתר אותן וכיצד להגיב להן (**הראל, 2007a**).

דוגמא בנושא ניהול האינטראקציה: טעות נפוצה אצל אנשי פיתוח היא לתמוך בכל הפונקציות האפשריות, בכל מצבי התפעול, כאשר האחריות לבחירת מצב התפעול מוטלת על המשתמש. התקינה בנושא זה תנחה את המפתחים להגדיר את האינטראקציה על פי תרחישים, ובכך למנוע בעיות התמצאות ושליטה, כגון בהפעלת ציוד ביתי (לדוגמא – **תנור המיקרוגל**) וכן זו המוכרת לנו בכתבת טקסטים בעברית בישומי חלונות.

דוגמא מתחום ההתרעות הקוליות במצבי חירום: מפעילי אזעקות נוטים להפעיל אותן בכל מקרה של ספק, וגורמים לציבור לאבד את האמון במערכת, בגלל ריבוי התרעות שווא. מפתחי מערכות התרעה נוטים להיענות לאופן תפעול שגוי זה (**הראל, 2007b**). תקינה בנושא זה תנחה את המפתחים כיצד לספק לציבור מגוון של אינדיקציות לגבי סוג ותוקף האיום, כולל זמנים קריטיים, באופן שיעורר את אימון הציבור בהתרעות (**Harel, 2006**).

דוגמא מתחום הבטיחות באימונים: הוראות הבטיחות נבנות על פי לקחים מתאונות, בשכבות עבות, שמונעות למעשה לעמוד ביעדי האימון. בשטח, המפקדים נאלצים למצוא קיצורי דרך, על מנת לעמוד במשימות. תקינה בתחום זה תנחה את המפקדים כיצד להבטיח איתור טעויות מצב מבעוד מועד (**הראל, 2007c**).

דוגמא מתחום הבטיחות בשימוש במים חמים: הברזים המקובלים בשוק מאפשרים למשתמש לפתוח ברז מים לוהטים מבלי משים, ולגרום בטעות לכוויות. תקינה בנושא זה תנחה את המשווקים להעדיף ברזים בעלי מנגנוני וויסות טמפרטורה הכוללים התקנת חסם על הטמפרטורה המרבית.

דוגמא מתחום מנעולי דלת כניסה למכונית, לבית ולמשרד: המנעולים הדומיננטיים בשוק מאפשרים למשתמש בהם לנעול את דלת הכניסה מבחוץ בטריקה, כאשר המפתח נמצא בתוך המכונית, הבית או המשרד. תקינה בנושא זה תנחה את המשווקים להעדיף מנעולים שמאפשרים טריקת דלת מתוך המכונית, הבית או המשרד, אך לא מבחוץ.

בעיות בתקנים הקיימים

- הנסיון מוכיח שמפתחי מערכות אינם מכירים את התקנים, אינם לומדים אותם, ואינם מנסים אפילו לישם אותם. הסיבות לכך הן מגוונות, אבל השורה התחתונה היא יחס גבוה מדי של עלות-תועלת. הסיבות לכך הן:
- 1. הכמות:** כמות התקנים בנושא שימושיות היא עצומה. הכמות העצומה מעידה על הצורך שיש לתעשייה בתקנים, אבל, היא גם מהווה אבן נגף, מכיוון שמרוב עצים לא רואים את היער.
 - 2. שרירותיות:** במקרים רבים, התקינה אינה מבוססת על מחקר בסיסי בגורמי אנוש, וההחלטות השרירותיות הן לעתים שגויות. לדוגמא: <http://www.cja-jca.org/cgi/content/full/50/3/221>
 - 3. התיישנות:** חלק ניכר מהתקנים הוא ספציפי לטכנולוגיה. תקנים רבים שנכתבו לפני עשור כבר אינם רלבנטיים כיום.
 - 4. רלבנטיות:** הנחיות רבות הן רלבנטיות למצבי תפעול מסויימים, כאשר ישומן למצבי תפעול (תרחישים) אחרים יוצר בעיה למשתמש (ראה דוגמת 'דילמת עומס מסך' אצל הראל, 2007a). בכל פרויקט ספציפי, רק חלק קטן מהתקנים הוא רלבנטי, אבל קשה למצוא את החלקים הרלבנטיים, ולהעריך ולשפוט את מידת הרלבנטיות שלהם למצבי התפעול. ביחוד, מכיוון שבעיות המשתמש הן לעתים בלתי צפויות.
 - 5. קשיים להעריך את תרומת התקנים:** בסקר התקנים שערכתי לא מצאתי הוכחות חד משמעיות לתרומת התקנים לשיפור השימושיות (הסבר אפשרי: http://www.taskz.com/ucd_righi2_indepth.php) כתוצאה מכך, מפתחי מערכות נוטים להמעיט בחשיבות התקנים כדרך לשיפור השימושיות. מסקנה מכך היא שיתכן, ואף סביר ביותר, שוועדת התקינה תיאלץ להשקיע בתקינה מקורית יותר מאשר בהתאמת תקנים בינלאומיים.

עקרונות התקינה לשימושיות

- 1. עקרון האטרקטיביות למפתח**

הגישה היא שהדרך של שכנוע המפתחים בכדאיות ההשקעה בישום תקנים עדיפה על פני הדרך של כפייה. עקרון האטרקטיביות פירושו:

- א. התועלת שבישום התקנים צריכה להיות מפורשת וברורה,
 - ב. התקנים צריכים להיות קלים ללימוד ולישום.
- עקרון האטרקטיביות ישים גם לתקינה מקורית, וגם לאימוץ של תקנים בינלאומיים.
2. עקרון הרצף לאבטחת רלבנטיות לאורך זמן
חוסר הרלבנטיות של התקנים הבינלאומיים נובע במידה רבה מתלותם בטכנולוגיה. עקרון הרצף מיועד להבטיח שהתקנים יהיו רלבנטים לאורך זמן. זאת, על ידי ניסוח התקנים בדרך של עקרונות כלליים, במונחים שאינם תלויים בטכנולוגיה.

הוכחת התועלת למפתח

1. אמות מידה להוכחת התועלת למפתח, לתעשייה ולציבור
דרך אפשרית להוכיח את התועלת שבתקן היא בעזרת קריטריונים כגון ערכה של מקרים לדוגמה (benchmark) או תרחישים, כאשר את תרומת התקן המוצע משווים לעומת החלופות על פי המקרים שבדוגמאות. דוגמאות של קריטריונים כאלו (ישימות לתקנים עבור מוצרים או מערכות) הן קלות ההתמצאות במערכת ורגישות לטעויות משתמש, בתרחישים של התקנה, איתחול, תפעול שוטף ופיתרון בעיות.
2. הגדרת תוקף התקן ומגבלותיו
על מנת לשכנע את המפתחים שהתקנים הינם רלבנטים למערכת שבאחריותם, צריך להגדיר ולציין בפירוט את תוקפם ואת מגבלותיהם של התקנים.
3. הנחיה לתכנון ממוקד משתמש
מפתחי מערכות מתקשים להתאים את אפיון המערכת לצרכי המשתמש. הטעות האופיינית בקרב מפתחים היא להניח שהמשתמשים יפעילו את המוצר באופן דומה לאופן בו הם מפעילים אותו במהלך הפיתוח. התקנים צריכים לכלול הנחיות לגבי התאמת ממשק ההפעלה לתרחישי ההפעלה של המשתמש. לדוגמה, למפתחי תוכנה, שמפעילים אותה באופן אינטנסיבי, נוח להשתמש במקשי קיצור במהלך הבדיקות. אצל המשתמש, הפעלה בטעות של מקשי הקיצור גורמת לעתים להתנהגות מביכה של התוכנה. התקנים צריכים להנחות את המפתחים לגבי התאמת מקשי הקיצור לצרכי המשתמש.
4. התאמה לעולם המושגים של המפתח
על מנת להבטיח את אטרקטיביות התקן למפתח, צריך לאפשר למפתח להפעיל את המוצר במהלך הפיתוח בדרך הפעולה העדיפה עליו. זאת, מבלי שיכפה על המשתמש את דרך החשיבה שלו ואת תהליכי התפעול המועדפים עליו. לדוגמה, תקנים למוצרים או מערכות צריכים לאפשר למפתח לכלול במערכת מוד הפעלה המותאם לו, ולאפשר לו לישם מוד זה לצורך בדיקות. בנוסף, התקנים צריכים ולהנחות את המפתח להגדיר את מוד ההפעלה של המשתמש כמועדף על פני זה של המפתח. לדוגמה, התקנים צריכים לאפשר למפתח להגדיר מקשי קיצור רבים לצורך בדיקות, ולהנחות את המפתח להפעיל אותם בשלב הבדיקות בלבד.

אבטחת קלות הלימוד והשימוש בתקנים

הכמות העצומה של תקנים יוצרת בעיה למפתח, להכיר את התקנים הקיימים ולזהות את אלו מהם שהם רלבנטיים לפרויקט ספציפי. מפתחי תוכנה מתקשים ללמוד ולישם את התקנים הקיימים. כאשר מחייבים אותם, הם נאלצים להעזר בחברות יעוץ או בספרות הדרכה. תכנית העבודה שאושרה לוועדה זו כוללת פיתוח של מורה נבוכים למפתח, מערכת תומכת החלטות המאפשרת למפתח התמצאות מהירה, בעזרת קישורי HTML. האתגר שלנו הוא לבנות מורה נבוכים כזה, שמאפשר למפתח למצוא את ההנחיות המתאימות למאפייני התפעול הספציפיים לתרחיש.

תקינה להגדרת אחריות היצרן בנושא טעויות משתמש

בספרו "מים נושקים למים" מספר סמי מיכאל על מקרה של מודד מים שנכלא בתחנה הידרומטרית הרושמת את תנודות המים בירדן. דלת הכניסה לתחנה הייתה משורינת והיא כללה ידית פתיחה חיצונית, ללא מנגנון פתיחה מבפנים. הרוח העזה של עמק החולה טרקה את הדלת אחריה, והוא נשאר נעול בפנים למשך שלשה ימים. יוסף היה מודע לסכנה, אבל צירוף מקרים גרם לכך שהשאריר את הדלת פתוחה, היסח הדעת. יוסף היה מודע לסכנה זו עוד בטקס הפתיחה של התחנה, והוא העיר על כך למהנדס. על הערתו זו המהנדס הגיב בזלזול: "רק טמבל ייתן לדלת משורינת כזו לקבור אותו מבפנים." ([קישור לפרנס ברשת](#)).

הדרך המקובלת להתייחסות למצבי טעות היא להטיל את האחריות למצב על המפעיל. דרך זו נוחה למפתח ולאחראים על הבטיחות, מכיוון שהיא משחררת אותם מאחריות למחדלי תיכון. באופן טיפוסי, מפתחי מערכות נוטים להכחיש את עצם קיום הבעיה. ההליך המקובל של הכחשת בעיה הוא על ידי בחינה עצמית: אם אני מסתדר עם הפעלת המערכת, אין שום סיבה מדוע אחרים לא יוכלו להסתדר עם זה. באופן תגובה

זה, המפתחים מתעלמים מקבוצה חשובה של משתמשים, אנשי עסקים, אנשי אקדמיה, מנהלים ומפקדים בכירים, שאין להם עודפי זמן, לבזבז על לימוד דרך החשיבה של מפתחי המערכת.

מבחינה זו הצרכן משתף פעולה עם היצרן, בניגוד לאינטרס שלו. בניגוד למצבים של תקלת חומרה, בדרך כלל המפעילים נוטים לקחת אחריות לפעולות שהם ביצעו. בדרך כלל, המפעילים אינם מודעים לכך שמצב הטעות הוא תוצאה של טעות תיכון, ומייחסים את המצב לפעולה השגויה שלהם. בדרך כלל הם אינם מודעים לזכותם לקבל מערכת שהיא חסינה בפני טעויות, בדומה לזכותם לקבל מערכת ללא תקלות חומרה. לדוגמה, במקרה של תקלה בשלט רחוק של הטלביזיה בכבלים, המשתמש הטיפוסי יודע להתלונן ולבקש להחליף את השלט. לעומת זאת, אם בתפעול השלט רחוק, המשתמש טועה בהעברת המוד לפני פעולת ההדלקה, הכיבוי או החלפת הערוץ, וכתוצאה מכך המערכת אינה מתפקדת, המשתמש הטיפוסי מסתפק בכך שמישהו יחזיר עבורו את המצב לקדמותו, ואינו דורש את החלפת השלט לדגם שהוא גם יהיה חסין בפני טעויות מוד.

דוגמה אחרת היא מתחום הרכב. בעלי רכב בדרך כלל מודעים לזכותם לאמינות של כלי הרכב לאורך זמן. לעומת זאת, אם הם טועים בהבנת המשמעות של נוריות ההתרעה בלוח השעונים, וכתוצאה נגרם נזק לרכב, הם נוטים לקחת אחריות על הנזק, גם במצבים שהנזק נגרם בגלל הטעיה של נוריות החיווי. כך, למשל, במקרה של דליפת מי קירור, החיווי של חום מנוע אינו אמין, מכיוון שהוא מבוסס על מדידת הטמפרטורה של מי הקירור. במקרה של נזק למנוע כתוצאה מנסיעה במצב זה, היצרן אינו מקבל עליו את האחריות, למרות שהחיווי לגבי חום מנוע היה תקין.

התקינה להגדרת אחריות היצרן בנושא זה תגדיר את אחריות היצרן לחסינות המערכת בפני טעויות תפעול, כולל פעולה במוד שגוי, ולנזקים שנגרמים בגין מידע בלתי מדויק או בלתי מספק.

תקינה לתחקור תאונות שמיוחסות לטעות משתמש

במקרים של טעות שמסתיימת בתאונה, אין אפשרות להתכחש לקיום הבעיה. במקרים בהם חוקרי התאונה מתקשים לפענח את מנגנון הכשל, הדרך המקובלת לחפות על האין-אונות שלהם או על חלקם ביצירת מצב שאיפשר את התאונה, היא על ידי הענשת הקורבן, דהיינו, המפעיל שנפל בפח שהטמינו לו, בחוסר תשומת לב, המפתחים. כך, למשל, קברניט המיכלית שגרמה לאסון האקולוגי בשנת 1967 פוטר מעבודתו, והושעה מכל פעילות ימית (http://en.wikipedia.org/wiki/Torrey_Canyon). להצדקת האשמת הקורבן, בדרך כלל נוהגים לחקור את האירוע באופן יסודי ולמצוא מספר נקודות בהן הקורבן לכאורה התנהג שלא כראוי. כך, למשל, קברניט מטוס האיירבאס 320 בטיסה 296 של אייר-פרנס, הואשם בשורה של נושאים שאינם קשורים כלל לסיבת התאונה, כגון, חוסר מוכנות לתמרון, חוסר תיאום בין אנשי הצוות, תמרון שלא על פי התכנון, רצף אירועים מהיר מדי, זחיחות דעת, יהירות, אווירת החג במפגן האווירי והשפעת הדיילות שביקרו בתא הטייס. טייס אחר שהיה עד לתאונה והעיד מטעם ההגנה, הושעה מעבודתו ללא פיצויים, בטענה של אי-שפיות. כל זאת, על מנת לאפשר את הרשעת הקברניט באשמת הריגה, ולדון אותו למאסר (http://en.wikipedia.org/wiki/Air_France_Flight_296). כך גם, בין השאר, קציני צה"ל שהיו מעורבים בתאונות האימונים בצאלים, הורשעו בדין והוכנסו לכלא, באמתלות שאינן קשורות לפליטת הפה של קצין הקישור ([קישור למאמר ב-Wiki](#)).

לדרך זו יש יתרונות מסוימים:

- א. היא משחררת את הממונים על הבטיחות מאחריות למחדל
- ב. במקרה של תאונה קטלנית, האשמת המפעילים מסייעת לשיכוך כאבי הקורבנות, ולשיכוך פחדי הציבור מפני תאונות דומות
- ג. הענשת המפעילים מסייעת להם להתמודד עם רגשות האשם.

דרך זו מתאפשרת מהסיבות הבאות:

- א. המפעיל אינו בקיא בפרטים של דרך פעולת המערכת במצבי חריגים, ואינו מסוגל להצביע על מקור הבעיה בליקויי התיכון
- ב. המפעילים נוטים לקבל על עצמם את האחריות לטעות המצב, ולשחרר בכך את המפתחים מאחריותם
- ג. במקרה של טעות קטלנית, החוקרים מתקשים להצביע על המצב החריג ולשחזר את האירוע הקטלני

הדרך של הענשת קורבן הטעות היא בעייתית בכך שהיא מונעת פתרון בעיית התיכון, מכיוון שהיא מסיחה את הדעת מהגורמים המבניים לתאונה. במקום לחקור את התאונה, לנתח ולהבין את הסיבות לה, משליכים כמה אנשים לכלא. בגישה זו, החוקרים של תאונות קטלניות נכשלים בכך שאינם פועלים למנוע בעיות דומות בעתיד (Norman, 1990). התוצאה היא שהתאונה חוזרת על עצמה. כך, 19 חודשים לאחר התאונה של

מטוס האיירבאס 320 במפגן האווירי, התרסק מטוס נוסעים מדגם זה בבאנגלור שבהודו ו-94 אנשים מצאו את מותם, בגלל אותה תקלה ([קישור למאמר ב-Wiki](#)). חקירה רצינית של הגורמים לתאונה הראשונה החלה רק אחרי התאונה השנייה. כך גם, שנתיים לאחר תאונת צאלים א', קרתה תאונת צאלים ב', בגלל כשל חוזר של מניעת ירי על כוחותינו ([קישור למאמר ב-Wiki](#)). נהלי הבטיחות של הסיוע הארטילרי, שלא מנעו את תאונת צאלים א' נבחנו מחדש רק לאחר תאונת צאלים ב'.

על מנת לאפשר חקירה יסודית של גורמי הכשל, יש להימנע מהטלת האשמה על המפעיל, ולחקור את הגורמים המערכתיים אשר אפשרו את הכשל. כך, למשל, וועדת חקירה שנייה שחקרה את תאונת המטוס הניו-זילאנדי בקוטב הדרומי הפכה את מסקנות וועדת החקירה הראשונה, זיכתה את צוות המטוס מאשמה, וסללה בכך את הדרך לחקירה יסודית של גורמי הכשל (http://en.wikipedia.org/wiki/Air_New_Zealand_Flight_901).

התקינה לתחקור תאונות תחייב מינוי חוקרים מארגונים שאינם מעורבים בתאונה, תעודד את המפעיל לשתף פעולה בשיחזור נסיבות התאונה ותחייב את החוקרים לחקור את הנסיבות התפעוליות והארגוניות שאיפשרו את התאונה.

תקינה לתחקור מצבים של כמעט-תאונה

כנגד כל תאונה ניתן לזהות עשרות עד מאות מצבים של כמעט-תאונה, מהם ניתן היה ללמוד לגבי הנסיבות שגרמו לתאונה. התקינה לתחקור מצבים של כמעט-תאונה תחייב למנות צוותי בטיחות קבועים שתפקידם לתחקר, להמליץ על ישום ולוודא ישום ההמלצות, עבור כל מקרה של כמעט-תאונה.

מבנה אופייני של תכנית תקינה

בשאיפה, תהליך התקינה של כל תקן שיוגדר בוועדת השימושיות יכול את היעדים הבאים:

1. אמות מידה להוכחת התועלת למפתח, לתעשייה ולציבור
2. הצעת תקן והערכתה על פי אמות המידה
3. הגדרת תוקף ומגבלותיו
4. התאמה לעולם המושגים של המפתח
5. בניית מדריך אינטראקטיבי לתקן

סיכום

בשאיפה, הכוונה היא לאמץ תקינה בינלאומית, אבל כבר כיום ברור לנו שעיקר התועלת תהיה מתקינה מקורית. התקינה לשימושיות נמצאת כיום בראשית דרכה. וועדות מומחים מוקמות בימים אלו, להגדיר תקנים עבור מספר פרויקטי פיילוט, כולל תקנים למפרטי קונטקסט הפעלה ומאפייני משתמש, תקנים לאבטחת שימושיות של התרעות במצבי חירום, תקנים לשילוב גורמי אנוש בתהליכי פיתוח ואבטחת איכות, תקנים לאבטחת שימושיות של אתרי אינטרנט, ועוד.

מקורות

Bevan N., 2001, International standards for HCI and usability, *International Journal of Human-Computer Studies*, Volume 55, Number 4, pp. 533-552(20), Academic Press (available at: http://www.usabilitynet.org/tools/r_international.htm)

Casey, S., 1998, *Set Phasers on Stun*, Aegean Publishing Company, Santa Barbara, Ca.

Harel, A., [2006 - Alarm Reliability. User Experience Magazine, Vol 5., Issue 3.](#)

Norman, D. A., 1983, Design rules based on analyses of human error, *Communications of the ACM*, v.26 n.4, p.254-258, April 1983 (available at http://cpe.njit.edu/dlnotes/CIS/CIS732_447/Cis732_1R.pdf)

Norman, D. A., 1990, Commentary: Human Error and the Design of Computer Systems, Editorial published in *Communications of the ACM*, 1990, 33, 4-7.

הראל, א., 2007a, [מיגון מערכות בפני טעויות אנוש, הכנס הרביעי של INCOSE ISRAEL הרצליה](#)

הראל, א., 2007b, [לקחים מהפעלת הצופרים במלחמת לבנון השניה הכנס הלאומי להנדסת בטיחות](#)

הראל, א., 2007c, [מיגון מערכות בפני טעויות מצב, פוסטר בכנס הרביעי של INCOSE ISRAEL הרצליה](#)