Quarterly
Reliability & Safety
NEWSLETTER
Issue: 01, June 2005

האיגוד הישראלי לאיכות
Israel Society For Quality (ISQ)
מיגזר אמינות

דבר יו"ר המגזר לאמינות

עמיתים/ות יקרים/ות,
אנו מחדשים את פעילותו של מגזר האמינות במסגרת האיגוד הישראלי לאיכות.
בספטמבר 2004 קיימנו ישיבת התנעה למגזר, בה היה לי הכבוד להיבחר כיו"ר המגזר. למגזר זה הקמנו ועדת היגוי אשר חבריה (שמותיהם מובאים בעמוד 6) משקיעים מאמץ רב לקידום האמינות בישראל.
ועדת ההיגוי קבעה את יעדי המגזר לשנים 2004-2005 והם מובאים בעמוד 4.

היעדים תורגמו לתכנית פעולה הכוללת את התוצרים הבאים:

1. פרסום newsletter אשר יהיה התווך בו נעביר ונשתף ידע בתוך קהיליית האמינות ובטיחות מערכות. כמו כן נאפשר שיתוף עם בעלי תפקידים נוספים הארגונים/חברות כמו מנהלי איכות, מהנדסי פיתוח, מנכ"לים ועוד.
   את עיקר העבודה עושים העורך הראשי – נתן שוורץ. והעורך המקצועי – ניקי ברנשטיין. כמו כן ועדת ההיגוי של המגזר משמשת כוועדה מייעצת.
2. קיום הרצאות מקצועיות (בדומה למתבצע באיגוד הישראלי לאיכות). ההרצאות יתמקדו בתחומי אמינות ובטיחות מערכות.
3. הקמת פורום אמינות באינטרנט.

פעילות ועדת ההיגוי חיונית וחשובה ותהיה בעלת ערך מוסף עם שיתוף הפעולה מכם – חברי המגזר.
השקענו מספר חודשים בגיבוש "רשימת התפוצה" של המגזר, זאת כדי לאתר אתכם, בעלי המקצוע המתעניינים בתחום האמינות ובטיחות מערכות. מספר גופים סייעו לנו בבניית "רשימת התפוצה" ולהם התודה:

1. הטכניון – היחידה לאבטחת איכות ואמינות שסיפקה לנו את כתובות הסטודנטים בתכנית לתואר שני.
2. חברת ALD, שסייעה בידי להגיע אל בוגרי קורסי אמינות שקיימה.
3. מזכירות האיגוד שאיתרה את מוסמכי CRE.
4. אחדים מכם שראו בחשיבות הנושא והעבירו (FORWARD) את "קול הקורא" שפרסמתי, לעמיתיהם.

כעת, קוראים אתם את הגיליון הראשון של ה- newsletter. גיליון זה לא יכול היה לראות אור ללא תרומתם של הכותבים ועל כך מגיעה להם התודה.
בהזדמנות זאת, אני מזמין כל אחד מכם לכתוב ולשתף את כולנו בידע, תובנות ורעיונות בתחומי האמינות ובטיחות מערכות. גם הצעה למתן הרצאה לחברי המגזר תתקבל בברכה.

כל הצעה והתיחסות למופיע בגיליון זה תתקבל בברכה בדוא"ל אליי oren.nakar@motorola.com או לנתן שוורץ natans@micronet.co.il.

להתראות בגיליון הבא.
אורן נקר

דרושים
ראה פרטים בעמוד 11

פנינים בגיליון זה:

מאמרים יתקבלו בשמחה-נא להפנות אל natans@micronet.co.il
עורך ראשי: שוורץ נתן
עורך מקצועי: ניקי ברנשטיין.
ועדת מייעצת: חברי ועדת ההיגוי למיגזר אמינות למיגזר אמינות

Quarterly
Reliability & Safety
NEWSLETTER
Issue: 01, June 2005

האיגוד הישראלי לאיכות
Israel Society For Quality (ISQ)
מיגזר אמינות

מאמרים וחוות דעת

PRISM® A NEW APPROACH TO RELIABILITY PREDICTION

Communicated by: Mr. **Nicky Bernstein***

For any company interested in predicting field reliability performance, finding a prediction technique that provides a high degree of fidelity to observed field data is essential. With the discontinuance of military handbook Mil-Hdbk-217, and the limited environmental applications of Telcordia SR-332, Reliability Prediction for Electronic Equipment, this newsletter note intends to inform the readers about the Reliability Analysis Center's (RAC) PRISM ® software tool, as a potential improved methodology in predicting the field systems reliability.
PRISM fills this void by providing a superior approach for reliability modeling under a broad range of applications.

PRISM® is the new Reliability Analysis Center (RAC) software tool that ties together several tools into a comprehensive system reliability prediction methodology. The PRISM concept accounts for the myriad of factors that can influence system reliability, combining all those factors into an integrated system reliability assessment resource.
The premise of traditional methods of reliability predictions, such as MIL-HDBK-217, is that the failure rate of a system is primarily determined by the components comprising that system. It is well known that more than 78% of failures stem from non-component causes, namely: design deficiencies, manufacturing defects, poor system management techniques such as inadequate requirements, wearout, software, induced, and no-defect found failures which have not been explicitly addressed in previous "analytical" prediction methodologies.

The PRISM methodology is structured to allow the user the ability to estimate a system failure rate in the early stages of the design, and is illustrated in Fig.1.(on Page 3)
An initial base reliability estimate is developed based on RAC Rates component models, RAC failure experience data, and/or user-defined failure rates.

This initial base failure rate is then modified with system-level process assessment factors for the following failure causes: Parts, Design, Manufacturing, Wearout, Induced, and No Defect Found. These process grades correspond to the degree to which actions have been taken to mitigate the occurrence of system failure due to these failure categories. A RAC Rates model for the estimation of software reliability is also available since modern electronic systems typically contain significant amounts of software.

The PRISM Failure Rate model for a given assembly is as follows:

$\lambda_p = \lambda_{IA}(\Pi_P\Pi_{IM}+\Pi_D\Pi_G+\Pi_M\Pi_{IM}\Pi_E\Pi_G+\Pi_S\Pi_G+\Pi_I+\Pi_N+\Pi_W) + \lambda_{SW}$ where :

λ_P = predicted failure rate of the system
Π_{IM} = infant mortality factor
λ_{IA} = initial assessment of the failure rate
Π_D = design process multiplier
λ_{SW} = software failure rate prediction
Π_P = parts process multiplier
Π_M = manufacturing process multiplier
Π_E = environmental fact. mult.
Π_S = system management process multiplier
Π_I = induced process multiplier
Π_N = no-defect process multiplier
Π_W = wearout process multiplier
Π_G = reliability growth factor multiplier

The initial assessment of the failures rate, λ_{IA} is obtained by using a combination of newly developed RACRates component reliability prediction models, failure rate data contained in the RAC databases, or user-defined failure data.

The PRISM prediction is initiating the possibility and provides tools for considering:

- Process Assessment

- Reliability Growth
- Infant Mortality
- Environmental Factors
- Components Model Accelerating Factors
- Components Test Data
- Time basis of Component Models
- Software Models
- Historical and Field Data

The (predicted, new)/(predicted, predecessor) failure rate ratio accounts for the differences in application environment, complexity, stresses, date, etc. The predicted failure rates for the predecessor and the new system are determined by applying the complete PRISM detailed methodology to each system. The observed predecessor failure rate is entered directly into PRISM, and is used as a baseline against which the new system predicted failure rate is calculated.

The main features of this methodology are:

- Models reliability based upon observed failure mode distributions
- Incorporates RAC's new component reliability models, RACRates
- Incorporates software reliability (if desired)
- Models component reliability growth based upon observed industry trends
- Is tailorable based upon user failure experience data

RAC's new system reliability assessment methodology and the associated software tool, PRISM is a "living methodology", periodically updated based upon data and information collected by the RAC. Future updates will include the development of RACRates models for additional component types, continued refinement of the system level modifiers, on-going model verification, and modifications to reflect significant advances in the state-of-the-art in electronic systems and equipment.

Introduced in the last years, PRISM has already known an extremely wide application. Internet forums and extensive information is available on the Web. Demo software is available on-line.

The PRISM software is available from RAC (http://rac.alionscience.com) and other software companies, which sell it under license. Some software companies integrated the PRISM methodology in more powerful reliability tools, able to fit the user's complex needs, using the PRISM for their own reliability database, by flexible application of the existent available PRISM processing tools.

REFERENCES:

D. David Dylis, Mary Gossin Priore: A Comprehensive Reliability Assessment Tool for Electronic Systems: RAMS 2003

***Communicated by:** Mr. Nicky Bernstein*
"RelSafe" Ltd. - Reliability & Safety Consulting

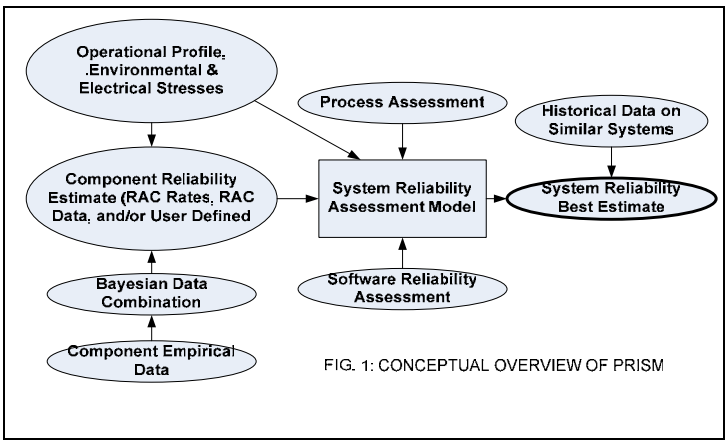

FIG. 1: CONCEPTUAL OVERVIEW OF PRISM

Quarterly
Reliability & Safety
NEWSLETTER
Issue: 01, June 2005

האיגוד הישראלי לאיכות
Israel Society For Quality (ISQ)
מיגזר אמינות

ULTRA RELIABILITY

כתבה: **סא"ל אולגה גלפנשטיין***

אחד מלקחי מלחמת המפרץ, הינו הצורך בהורדת הנטל הלוגיסטי. כחלק ממגמה זו נולד המושג "Pulse-Reliable", מערכות אשר לא תידרש להן אחזקה או תיקוני שיגרה (routine) במהלך פעימת קרב. דרישות אלה מכתיבות שהמערכת תהיה Ultra-Reliable.
מסתמן כי דרישות האמינות למערכות העתיד תהיה הרבה מעבר לערכים המוכרים לנו עד היום. לדוגמא, במערכת FCS – Future Combat System, דרישות האמינות הינן פי 4 עד פי 12 מהערכים המקובלים כיום. אירגונים מסוימים טוענים כי נדרשות רמות אף גבוהות יותר. *לא ניתן יהיה להגיע לרמות אמינות כאלה באמצעות גישות הנדסת האמינות המסורתיות.*
המאמר מציע מספר שינויים הנדרשים על-מנת להפוך את "Ultra-Reliability" ליותר מאשר סיסמא.
מודלי האמינות המקובלים: דיאגרמת בלוקים, FMECA (ניתוח אופני כשל והקריטיות) וכדומה, יכולים להיות מועילים רק כאשר הם משולבים במאמצי התכן ובמאמצים ההנדסיים. נדרשת הבנה עמוקה יותר של השיקולים ההנדסיים ושיקולי התכן במטרה למזער סיכונים ולספק מוצר אמין. MTBF (זמן ממוצע בין תקלות) אינו חזות הכל באמינות והיום נראה כי כלי האמינות החשובים ביותר הינם **מודלים מבניים, מודלים תרמיים, מודלי התעייפות, מכניזמים של כשל ורעידות** שצוות.
והרבה לפני שלב הבדיקות הפורמלי. כדוגמא לסוג בדיקה ממליצים על ביצוע בדיקות HALT (Highly Accelerated Life Testing).
הבדיקות צריכות להיות ממוקדות ומתוכננות בצורה חכמה. בדיקות תתי-מכללים חשובות לחיזוי תקלות ואיתור חולשות בתכן. בדיקות אינטגרציה חשובות לזיהוי בעיות שלא נצפו בממשקים.
המאמר ממליץ על ניתוחים ובדיקות כבר בשלבים המוקדמים של התכן, תוך שילוב עם בדיקות של תתי-מכללים ובדיקות אינטגרציה. אלה יתרמו לשיפורים עוד לפני הקפאת התכן.

אמינות גבוהה אינה בהכרח יקרה להשגה. כאשר האמינות היא חלק מובנה במערכת כבר מהשלבים הראשוניים של התכן, ניתן למנוע מקורות לכשל, בעלות מזערית.

התכן משתמש בהם על-מנת להבטיח שהמוצר יהיה בעל תקופת הפעלה ארוכה מספיק ללא תקלות

בנוסף, לספקים, לרוב אין כל תמריץ לספק מוצרים אמינים. גם כאשר האמינות היא חלק מהמכרז, בפועל התחרות היא על המחיר. יתרה מזו, הספקים מרוויחים מאספקת חלקי חילוף. לאור זאת, על הספק לראות רווח ויתרון באספקת מערכות בעלות אמינות גבוהה. מומלץ כי האמינות תהפוך לאחד מהמדדים בעלי העדיפות הגבוהה במסמך תכולת העבודה (SOW) ובמפרט הטכני.
לסיכום, אמנם המאמר נכתב באוריינטציה צבאית וכאחד מלקחי מלחמת המפרץ. אולם ההמלצות והרעיונות שבו נכונים לכל יצרן השואף ליצר מוצרים בעלי אמינות גבוהה.

**סא"ל אולגה גלפנשטיין, ראש מדור אמינות ביחידה לניסויים והבטחת איכות.*

מבוסס על מאמר "MAKING RELIABILITY A REALITY"
מאת: Stephen P. Yuhas ,David E. Mortin.
http://www.amsaa.mil/reliability technology/ improve reliability/

יעדי המגזר לשנים 2004-2005:

1) הגברת המודעות לאמינות ולבטיחות מערכות בקרב לקוחות הארגונים וצרכנים במדינת ישראל.
2) הגברת המודעות לאמינות ולבטיחות מערכות בתוך הארגונים.
3) החלפת ידע בין חברי האיגוד, תוך שימוש ב-benchmark, ימי עיון קבוצות דיון ועוד.
4) הסכמה ואימוץ שיטות משותפות לאמינות ולבטיחות מערכות (להגדלת האחידות בארגונים במדינת ישראל).
5) יצירת קשרים מקצועיים עם ארגונים מקבילים בחו"ל (כמו IEEE).

Quarterly
Reliability & Safety
NEWSLETTER
Issue: 01, June 2005

האיגוד הישראלי לאיכות
Israel Society For Quality (ISQ)
מיגזר אמינות

אמינות רכיבים – מה לומדים מדוחות יצרנים

כתב: מר **מיכאל טלמור***

באחרונה אנו עדים למגמה מאוד חיובית של פרסום דוחות אמינות על ידי יצרני רכיבים. אנו, מהנדסי אמינות בחברות יצרני מערכות חיכינו לכך מזמן. ביסוס חיזוי אמינות של הרכבות אלקטרוניות על מידע של קצבי תקלות מדוחות של יצרני רכיבים – מה יכול להיות טוב מזה. זה עדיין רחוק מי לספק את הצרכים, לא תמיד קל להגיע למידע, אבל הכיוון מעודד. מתוך סריקה של אתרי אינטרנט של יצרני רכיבים מובילים, רק כ- 15 מהם מפרסמים מידע כלשהו על אמינות. בדרך כלל המידע הוא בדוחות איכות רבעוניים (Quality/Reliability Quarterly Reports), חלקם מספקים מידע מלא על מבחני אורך חיים, חלקם מפרסמים תוצאה של חישוב קצב תקלות בלבד. בכל מקרה מה שמאפיין את הנתונים של רוב רובם של הדוחות של כל היצרנים:

- כמעת כולם מראים אפס תקלות בכל מבחני אורך חיים,
- במקרה של תקלה, לרוב לא ניתן למצוא פרוט לאופן ומנגנון הכשל,
- כולם משתמשים באותם מודלים של האצה (ערכי פרמטרים שונים לפעמים) – Arrhenius עבור טמפרטורה, Power Law עבור המתח וכו',
- חלק מיצרנים מפעילים האצה בטמפרטורה בלבד, חלקם משלבים עם האצה במתח.

מתוך כך, עולים מספר תהיות:

- אם חישוב של קצב תקלות ע"י יצרנים מתבסס על אפס תקלות וב- 60% מקדם ביטחון, מה הוא ערך הסטטיסטי לכך?
- האם אפשר לקבל מצב שבמקרה של תקלות, החישוב לא מתייחס לאופני כשל השונים (פרט למספר בודד של יצרנים) ומתבסס על אנרגית אקטיווציה אחד בלבד?
- האם זה נכון להכפיל מקדם האצה תרמי עם מקדם האצה של מתח (לדוגמה) כאשר ברור שאופני כשל שונים תלויים בצורה שונה בשינוי מתח וטמפרטורה?

ננסה כאן להבהיר במידת מה את הנושא. לצורך כך, נשתמש בדוחות רבעוניים של חברת ALTERA אשר מספקים מידע מפורט ומראים את החישוב של קצב תקלות. ALTERA מנתחת ומסווגת מנגנוני כשל ומחשבת קצב תקלות לכל מנגנון כשל בנפרד, כאשר קצב תקלות של רכיב הנו סכום שלהם. אם נשתמש בנתונים של ALTERA ובמודלי האצה שלה בלי לסווג מנגנוני כשל ונכפיל מקדם תרמי עם מקדם מתח, נקבל תוצאות שונות לחלוטין מאלה שחושבו ע"י ALTERA (ראה הטבלה להלן).

	Technology node				
	0.35u	0.22u	0.18u	0.15u	0.13u
Acc. Factor	406	272	272	647	647
FIT (calculated)	6.7	12	4.9	10.9	6.9
FIT (reported)	44.4	21.1	16.4	81.9	99.6

כמובן, דרך בו ALTERA חישבה את קצב התקלות היא הדרך הנכונה ולא זו של הכפלת מקדמים ללא סיווג של מנגנוני הכשל השונים.
הדבר גם אפשרי להוכחה מתמטית. נניח שברכיב קיימים שני אופני כשל – אחד מושפע מטמפרטורה בלבד והשני רק ממתח. נקבל:

$$AF_T = \frac{\lambda_1(T_2)}{\lambda_1(T_1)},\ T_1 < T_2 \qquad AF_V = \frac{\lambda_2(V_2)}{\lambda_2(V_1)},\ V_1 < V_2 \qquad (1)$$

כאשר V_1, T_1 מייצגים תנאי מאמץ אחד ו V_2, T_2 מייצגים תנאי סביבה שני, מואץ.
מקדם האצה ברמת רכיב יהיה

$$AF = \frac{\lambda_1(T_2,V_2) + \lambda_2(T_2,V_2)}{\lambda_1(T_1,V_1) + \lambda_2(T_1,V_1)} = \frac{\lambda_1(T_2) + \lambda_2(V_2)}{\lambda_1(T_1) + \lambda_2(V_1)} \qquad (2)$$

הביטוי האחרון ניתן לרשום, תוך הצבה של (1) גם כ-

$$AF = \frac{\lambda_1(T_2) + \lambda_2(V_2)}{\frac{\lambda_1(T_2)}{AF_T} + \frac{\lambda_2(V_2)}{AF_V}} \qquad (3)$$

או

$$AF = \frac{\lambda_1(T_1)AF_T + \lambda_2(V_1)AF_V}{\lambda_1(T_1) + \lambda_2(V_1)} \qquad (4)$$

Quarterly
Reliability & Safety
NEWSLETTER
Issue: 01, June 2005

האיגוד הישראלי לאיכות
Israel Society For Quality (ISQ)
מיגזר אמינות

אם נניח שסיכויים להופעת כל אחד ממנגנוני כשל בתנאי סביבה ראשון (תנאי שימוש, לדוגמה) זהים - $\lambda_1(T_1)=\lambda_2(V_1)$, נקבל:

$$AF=\frac{AF_T+AF_V}{2}$$

או, אם הסיכויים להופעת כל אחד ממנגנוני כשל זהים דווקא בתנאי סביבה מואצים, $\lambda_1(T_2)=\lambda_2(V_2)$, נקבל:

$$AF=\frac{2}{\frac{1}{AF_T}+\frac{1}{AF_V}}$$

לא קשה לראות שעבור N אופני כשל:

$AF=\frac{\sum_{i=1}^{n}AF_i}{n}$ או $AF=\frac{n}{\sum_{i=1}^{n}\frac{1}{AF_i}}$ בהתאם למקרה לעיל,

אפשר לראות שאם כל אחד מאופני כשל מואץ ברמה שווה (מקדמי האצה שווים), אז מקדם האצה הכולל שווה למקדם האצה של אופן כשל כלשהו. מעניין המקרה שאם האצה של אופן כשל אחד חזקה הרבה יותר מהאצה של האחרים $AF_k >> AF_i$. מתקבל שמקדם הכולל הנו 1/N של מקדם האצה המקסימלי (AFk) במקרה שתדירות של הופעת אופני כשל זהה בתנאי סביבה או, הפוך, מקדם הכולל יהיה חלק 1/N של מקדם האצה המינימלי במקרה שתדירות של הופעת אופני כשל זהה בתנאי המבחן.

בדיקה של ערכי קצבי תקלות המדווחים ע"י ALTERA מול חישוב על סמך המודלים לעיל (על בסיס נתונים של מבחני אורך חיים) מראה התאמה מלאה למקרה של הנחה על תדירות הופעת אופני כשל זהה בתנאי מבחן.

השאלה היא מה היא המדיניות/ יכולת של היצרן: לבקר מנגנוני/ אופני כשל כך שלא יהיה אחד דומיננטי בתנאי שימוש או בתנאי מבחן?

כמו כן, לא ברור האם יצרנים מודעים ויודעים להאיץ מנגנוני כשל בצורה שווה (פחות או יותר) או זה לא נשלט/ לא נלקח בחשבון.

המסקנה החשובה כאן היא שלא ניתן להשתמש בנתוני אמינות של יצרנים בצורה עיוורת.

** מר מיכאל טלמור, מרכז אמינות ברפא"ל.*

Quarterly
Reliability & Safety
NEWSLETTER
Issue: 01, June 2005

האיגוד הישראלי לאיכות
Israel Society For Quality (ISQ)
מיגזר אמינות

FUNCTIONAL SAFETY and SAFETY INTEGRITY LEVELS

Communicated by: Mr. **Nickv Bernstein***

Background
Starting with 1996, in response to an increasing number of industrial accidents, the Instrument Society of America (ISA) enacted a standard to drive the classification of safety systems for the process industry within the United States. This standard, ISA S84.01, introduced the concept of Safety Integrity Levels.
Subsequently, the International Electrotechnical Commission (IEC) enacted an industry neutral standard, IEC 61508, to help quantify safety in programmable electronic safety-related systems. This approach considers both system related hardware, software and human operation. Since it was discovered that many of the parameters central to Safety
Integrity Levels (SIL), once optimized, provided added reliability and up time for the concerned processes, the new rationale of safety analyses related to functional safety and safety integrity, is being close related to system's reliability. The new concept and methodology was extremely fast adopted by the safety community and even the military standards (such as the British Def Stan 00-55&56, NATO Safety Standards, and the transport safety standards, adopted immediately the Safety Integrity and SIL classification as basic concepts.

The reaction of the USA DOD was to immediate release the MIL-STD-882D which envisages but still not standardizes the safety integrity, being a small step
in adopting the new revolutionary and extremely complex approach and
implementation. Anyway, any safety related product or system manufactured for Europe, Australia and the Pacific Rim, shall mandatory be approached and classified with one of the SIL levels.

Purpose
The purpose of this communication is to introduce the concepts of the safety integrity and SIL classification, and briefly describe available methods for determining Safety Integrity levels. Lastly, a brief citation of the governing standards will be presented.

Definitions
Risk Reduction: The risk reduction that must be achieved to meet the tolerable risk which can be stated qualitatively or quantitatively.
Safety Integrity: the probability of a safety–related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.
Safety Integrity Level (SIL): discrete level (one out of a possible four) for specifying the safety integrity
requirements of the safety allocated to the safety-related systems, where the safety integrity 4 has the
highest level of safety integrity and SIL 1 has the lowest.

The rest of the definitions and acronyms of the safety related terms is very comprehensive and they must be perfectly understood, given the significant differences
between the actual accepted safety definitions (e.g. MIL-STD-882D) and the new functional safety concept definitions (IEC61508/Part 4).

What are Safety Integrity Levels (SIL)
Safety Integrity Levels (SIL) are measures of the safety of a given system or process. Specifically, to what extent can the end user expect the system in question to perform safely, and in the case of a failure, fail in a safe manner? It is important to note that no individual product can carry a SIL rating. Individual components of processes or systems can only be certified for use within a given SIL environment.

The need to derive and associate SIL values with processes is driven by Risk Based Safety Analysis (RBSA). RBSA is the task of evaluating

a process for safety risks, quantifying them, and subsequently categorizing them as acceptable or unacceptable. However risks
are justified, the goal is to arrive at a safe process. A typical RBSA might proceed as follows. With a desired level of safety being a starting point, a "risk budget" is established specifying the
amount of risk of unsafe failure to be tolerated. By combining these risk levels, a
comparison of actual risk can be made against the risk budget. It is important to note that simply combining process components rated to be used in a given SIL rated environment does not guarantee the process to be rated at the specified SIL. The process SIL must still be determined by an appropriate method. These are: Simplified Calculation, Fault Tree and Markov Analysis. An example of a tool used to estimate what SIL rating to target for a given process is that of the Risk Assessment Tree (RAT). See figure 1 (on page 9). As the example below illustrates, by optimizing certain process parameters, the SIL value of the process can be affected.

SIL's versus Reliability

While the main focus of the SIL ratings is the interpretation of a process/system inherent safety, an important byproduct of the statistics used in calculating SIL ratings is the statement of a product's reliability. In order to determine if a product can be used in a given SIL environment, the product must be shown to "BE AVAILABLE" to perform its designated task at some predetermined rate.
Subsequently, the reliability data, combined with statistical measurements
of the likelihood of the product to fail in a safe manner, known as Safe Failure Fraction (SFF), determine the maximum rated SIL environment in which the device(s) can be used. SIL ratings can be equated to the Probability to Fail on Demand (PFD) of the system in question. The following tables (on page 9) give relationships based on whether the process is required "Continuously" or "On Demand".

The above explanations arte just an extremely brief introduction to the new
concept which also includes the preparation of the *Safety*
Case an a safety assessment document. The European military standards such as DEF-STAN 00-56, taking into account international standardization, are requiring the SIL classification. This standard, recently release under a new issue,
provides generic information and guidance on the safety management requirements for safety related systems. The concept of risk and its consequences is described in part 1 section 7.4 of this standard as well as an interesting technique for SIL selection (denoted by the letter S in the document) as defined by IEC 61508. A matrix format is used to classify the integrity levels based on two parameters, the probability of failure of a safety-related component performing its primary function and the accident severity (as shown below) which is the bridge to the best-known Risk Assessment Matrix (RAM) dating from the Blaise Pascal period. This matrix is given in Table 3 (on page 9)
IEC 61508 adopts a similar approach through the use of a risk graph. However, four parameters are used in IEC 61508 to select the SIL's
instead of two. By including the probability of avoidance, and the frequency of exposure of the unwanted event combined with the two parameters mentioned above, the SIL changes dramatically. Nonetheless, it is an
interesting way of classifying SIL's.

Conclusions

The present communication is, from far, the tip of an iceberg. The evidence is that is an unanimous agreement about providing compliance with the safety related requirements adopting the Functional Safety, concept which includes the safety integrity concept and complex tools, as the SIL classification and the preparation of safety case. It seems that this is the way to be followed,

mainly for complex systems with embedded software. The reliability engineering is trying to accommodate with the technology changes. In fact, reliability deals with getting profits by producing reliable products. But, safety deals with human lives and as processes and systems became extremely complex, the safety engineering methodology must became more powerful and diverse.

References: *IEC 61508*, Functional Safety of programmable electronic
systems, Part 5 : Examples of methods for the determination of Safety Integrity Levels
DEF STAN 00-56: Part 2: Safety Management for Defence Systems, Issue 3, Section 7, December 2004

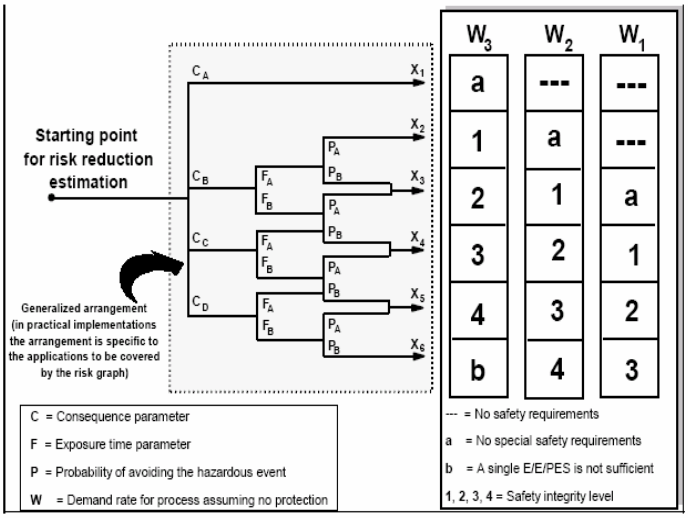

Figure 1

DEMAND MODE OF OPERATION		
Safety Integrity Level (SIL)	Average Probability of Failure on Demand	Risk Reduction
4	$\geq 10^{-5}$ to $<10^{-4}$	>10,000 to ≤ 100,000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to ≤ 10,000
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤ 1000
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤ 100

Table 1– Safety integrity levels: probability of failure on demand

CONTINUOUS MODE OF OPERATION	
Safety Integrity Level (SIL)	Frequency of Dangerous Failures Per Hour
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

Table 2 – Safety integrity levels: frequency of dangerous failures per hour

Failure probability of 1st function	Accident severity			
	Catastrophic	Critical	Marginal	Negligible
Frequent	Level S4			
Probable		Level S3		
Occasional			Level S2	
Remote				
Improbable			Level S1	

Table 3- SIL selection matrix

***Communicated by:** Mr. Nicky Bernstein "RelSafe" Ltd. - Reliability & Safety Consulting*

רשמים מכנס האמינות בסן-דייגו

כתבה: **סא"ל אולגה גלפנשטיין***

בין התאריכים 18-20.5.2005, התקיים כינוס בהנדסת אמינות "Applied Reliability Symposium" בארה"ב.

בכינוס השתתפו כ-250 איש, רובם מארה"ב, חלקם ממדינות אירופה וכ-5 נציגים מישראל.

הייחוד והיתרון בכינוס זה הינו הדגש על הרצאות מעשיות על-ידי מהנדסי אמינות המתפקדים בפועל בארגונים ופחות על הרצאות אקדמיות.

לאורך שלושת ימי הכינוס, התקיימו שני מושבים במקביל.

ייחוד נוסף של הכינוס, הרצאות יחסית ארוכות של כשעה על-מנת לאפשר הצגה מעמיקה של הנושאים ומתן אפשרות לדיונים הדדיים בין המשתתפים.

נושאים ייחודיים – מספר גדול של הרצאות בכינוס היה מתחום תעשיות הרכב וההנדסה המכאנית. כאן בארץ, עיקר החשיפה והטיפול מתבצעים בדרך-כלל בנושאים מתחום הנדסת האלקטרוניקה ולכן התרומה של הרצאות אלה הייתה רבה.

כמו-כן זכינו להרצאות של נציגי הזרועות השונות מצבא ארה"ב:

הרצאה של Vice Admiral Scott Fry שפרש לאחרונה מה-Navy, הרצה על ניסיונו כמפקד ספינות ותרומת האמינות לספינות.

הרצאה של רס"ן מה –Marine בנושא ניתוח נתוני אחזקה וניסיונו בנושא.

בין המרצים נכללו גם מספר "גורואים" בתחום. למשל הרצאתו של Larry Crow בנושא גידול אמינות.

בלטה לטובה בכינוס הרצאת נציג רפאל, צבי בנימיני, בנושא "הנדסת אמינות בעולם של מערכות".

הרצאה מעניינת נוספת הייתה הרצאה בנושא "תנודות במדיניות הנדסת האמינות ב-DoD – שינויים לאורך השנים". הרצאה זו סיפקה נקודת מבט מעניינת על השינויים שחלו בתחום ב-50 השנים האחרונות.

ניתנו מספר הרצאות בנושא ניסויים ובדיקות מואצים.

כתבה: סא"ל אולגה גלפנשטיין, ראש מדור אמינות ביחידה לניסויים והבטחת איכות.

Quarterly
Reliability & Safety
NEWSLETTER
Issue: 01, June 2005

האיגוד הישראלי לאיכות
Israel Society For Quality (ISQ)
מיגזר אמינות

ספרים חדשים

NEW RELIABILITY BOOKS

Recurrent Events Data Analysis for Product Repairs, Disease Recurrences, and Other Applications, by Wayne B. Nelson
(ASA-SIAM Series on Statistics and Applied Probability), ASA-SIAM, 2003, ISBN 0-89871-522-9, 151 pages, $59.50

Recurrence count data arise when an observational unit or group of units is monitored over time and the times of a particular event or class of events are recorded. Examples include counts of maintenance actions on repairable systems, transactions with customers, recurrences of a disease, and the birth of children. More generally, each event may have an associated "value" (e.g., the cost of a maintenance action or the size of an order). Questions of interest include the behavior of the recurrence rate (or cost accumulation rate) as a function of time (i.e., whether the rate is increasing, decreasing or constant over time). The population mean cumulative number of events (or mean cumulative cost) per unit at a particular time (e.g., at the end of the warranty period) is also of primary interest. Such a cumulative function is called, generically, a mean cumulative function (MCF). The need to compare MCFs (e.g., for units manufactured in different manufacturing periods or individuals receiving different treatments for a disease) is also common.

This is Wayne Nelson's third book-length contribution to the statistical/ engineering literature. Like its predecessors, this book provides a timely, self-contained treatment of an important area of application. All of the material is carefully motivated by actual applications. The examples consist of an interesting mixture of applications from engineering, medical science, and other areas. In spite of the fact that some of the material is technically difficult, the writing style is crystal clear.

This book has the following chapters:

1. Recurrent events data and applications
2. Population model, MCF, and basic concepts
3. MCF estimates for exact age data
4. MCF confidence limits for exact age data
5. MCF estimate and limits for interval age data
6. Analysis of a mix of events
7. Comparison of samples
8. Survey of related topics

קוראים/ות יקרים/ות,
זהו הגיליון הראשון שאנו מכנים אותו NEWSLETTER.
ניסינו למצוא לו שם הולם בישיבות ועדת ההיגוי אך הגענו למסקנה שרק אתם יכולים להעניק לו את השם המתאים.
לכן אנו יוצאים היום במודעת דרושים.

דרוש שם לגיליון ה- newsletter.

דרוש לוגו לגיליון.

את הצעותיכם אנא העבירו לידי נתן שוורץ natans@micronet.co.il.
רשימת השמות המוצעים תועבר לעיונכם ולבחירתכם.
כן, אתם תשפיעו בכך שתצביעו.
לחברי ועדת ההיגוי יהיה גם משקל מה בבחירת השם המועדף.
בחירת השם לגיליון והלוגו ייעשו בצורה אנונימית.
מציע השם (והלוגו) הנבחר יזכה בתלושי שי לרכישת ספרים בסך 200 ₪ מתנת האיגוד הישראלי לאיכות.

Quarterly
Reliability & Safety
NEWSLETTER
Issue: 01, June 2005

האיגוד הישראלי לאיכות
Israel Society For Quality (ISQ)
מיגזר אמינות

אירועים בעתיד

Upcoming Reliability Conferences:

1. איכות ובטיחות מעצימים מצוינות- הכינוס הלאומי ה-8 של האיגוד הישראל' לאיכות- 23-24 נובמבר 2005, מלון דוד איטרקונטיננטלת חל אביב- www.isas.co.il/quiality2005

2. **ESREL 2005 European Safety and Reliability Conference, Gdynia , Poland, 27-30 2005 Try-City Gdansk, Spot**

The Conference ESREL 2005 is focused on the problems of creation and assurance of safety and reliability in every-day practice. It is addressed to university and research institute scientists, industry and transport employees, government and municipal bodies, reliability and safety consultants and other persons interested in the conference topics.
http://esrel2005.am.gdynia.pl/

3. **23-rd International System Safety Conference 2005, San-Diego, USA, Westin Hotel, 22-26 August 2005.**

The conference is an international forum for the technical presentation and discussion of all aspects and issues regarding system safety engineering and management.

The conference theme is *Safety is No Accident*. This theme embodies the principle that system safety is a formal, disciplined approach to hazard management. The conference will emphasize topics to enhance the knowledge and skills necessary to create and apply system safety solutions to meet today's diverse needs in a variety of industries. The spectrum of topics will cover both the art and science of system safety, and the organizational issues influencing the effective management of system safety in the product life cycle.
This is the major conference for system safety and related professionals, with a week of technical sessions, tutorials, workshops, special events, social affairs, luncheons, and the society's conference awards banquet. The conference proceedings are the premier collection of work in the system safety field. For more information, visit the conference . web site at www.system-safety.org

4. **2005 Asia Pacific Conference on Risk Management and Safety Challenges in Engineering Applications and Advances in Technologies 1-2 December 2005, Hong Kong**

The objective of the Conference is to provide a platform for engineers and safety practitioners from different industries and countries to share their view and experience in the applications of risk management and safety. The Conference Organizers and the Technical Advisory Panel sincerely invite those who are committed to improving safety in their areas of responsibility to participate in the Conference.
http://hkarms.org/Conference

5. International Conference on Probabilistic Safety Assessment and Management, on May 14-19, 2006 at the New Orleans Marriott Hotel, New Orleans, Louisiana, USA, (www.psam8.org)

1. Innovative methods of system health monitoring and fault diagnosis
2. RAMS modeling, simulation and optimization
3. Reliability modeling of network systems
4. Uncertainty and Sensitivity Analysis
5. Quantitative modeling for risk-informed decision making

6. Computerized Maintenance Management Summit (CMMS-2005)
Westin Indianapolis
July 26-28, 2005
Indianapolis, IN
Learn more... **http://www.maintenanceconference.com/cmms/**

7. Predictive Maintenance Technology Conference & Expo (PdM-2005)
Sheraton Atlanta Hotel
September 19-22, 2005
Atlanta, GA
Learn more... http://www.maintenanceconference.com/pdm/

8. The 20th International Maintenance Conference (IMC-2005)
Tampa Convention Center
December 6-9, 2005
Tampa, FL
Learn more.. http://www.maintenanceconference.com/imc/index.htm.

9. Singapore 18-19 August 2005, Orchard Hotel
Applied Reliability Symposium, Asia Pacific
The **International Applied Reliability Symposium** provides a forum for expert presenters from industry and government to come together with reliability practitioners to discuss the application of reliability principles to meet real world challenges.
http://arsymposium.org/asia/index.htm

Upcoming Reliability Workshops:

PROACT® Root Cause Analysis Methods Workshop
July 12-13, 2005 - Hopewell, Virginia
August 9-10, 2005 - Hopewell, Virginia

This "hands on" workshop is designed to provide you with the skills and knowledge to successfully realize tremendous costs savings through the identification and elimination of CHRONIC undesirable events for good! We encourage all of our students to bring in an actual recurring problem to be analyzed during class using RCI's PROACT® System, and patented **PROACT® RCA software** in order to eliminate or drastically reduce its recurrence.

RCA Justification Tools & Techniques Workshop
July 14, 2005- Hopewell, Virginia
August 11, 2005- Hopewell, Virginia

In RCA Justification Tools & Techniques 1 Day workshop you will learn various ways to prioritize what you should be working on, no matter the type of backlog of tasks or events that you may face. You not only learn these techniques, but you will apply them through structured activities for each of the justification tools & techniques presented.

Basic Failure Analysis Workshop
August 15-19, 2005 - Hopewell, Virginia
October 17-21 , 2005- Hopewell, Virginia

The Basic Failure Analysis Workshop is intended to provide facility personnel the requisite skills and knowledge to eliminate chronic problems that they are experiencing everyday on the job.

You are provided instruction on a unique 4-step process that guides you through the technique of solving problems and failures down to their root cause(s) using real world examples. This is a train-the-trainer format so you can return to your facility and teach this process yourself to your workforce.

Human Error Reduction Workshop
July 26-27, 2005- Hopewell, Virginia
September 27-28, 2005- Hopewell, Virginia

This course explains the underlying reasons why humans make errors and how you can prevent these errors. The techniques learned in this course will enable you and your workers to reduce human errors in the work place by as much as 20 days per year.

Quarterly
Reliability & Safety
NEWSLETTER
Issue: 01, June 2005

האיגוד הישראלי לאיכות
Israel Society For Quality (ISQ)
מיגזר אמינות

פינת הטיפים

1. QUANTERION

The very known RADC "veterans" MacDiarmid, Seymour Morris, and David Mahar authors of many known standards and handbooks such as MIL-HDBK 217, MIL HDBK-781, MIL-STD 1683, RADC Reliability Toolkit, etc. started a company with a goal of providing high quality quantitative engineering services to be used as criterion for critical decision making, hence the name Quanterion.
They offer a free Software Tools, based on The Reliability Toolkit, which allows is called Quaternion Automated Reliability Toolkit. This tool allows you to calculate:
Redundancy Calculation, Derating, Reliability Adjustment Factors, Reliability Growth, Part Counts Analysis, Reliability Potential, Reliability Tailoring, Reliability Growth Test, Reliability Demonstration Test, Reliability Cost Estimator, Design of Experiments, Sparing, Weibull analysis , etc, and an Index to Reliability Toolkit. You may download it from: http://quanterion.com

2. RAC TOOLS

The RAC site is offering two very useful reliability calculation tools.

A. *Reliability for One-Shut Devices*

Reliability analysis of "One-Shot" devices is based on the binomial distribution. The Binomial distribution requires a set of calculations that can be tedious, time consuming and can easily result in errors. RAC has developed two tools for the RAC user: Tables that can be viewed and/or downloaded to approximate the number of samples required for a given proportion defective to achieve a desired confidence level; and a calculator that can determine the precise confidence level and an approximate number of samples or number of rejects allowed to satisfy a set of given conditions. Go to : http://rac.alionscience.com/Toolbox/Rac_OneShot.html

B. Poisson Distribution

This RAC calculation tool has been developed for the RAC user to handle arduous Poisson discrete distribution calculations for reliability analysis. Similar to the Binomial Distribution Calculator, also found in the RAC Toolbox, this calculator lets the user solve for:

- Confidence Level
- Failure Rate
- Time Period
- Maximum Number of Failures

In addition, this calculator can solve for:

- Probability of Failure
- Sparing Analysis

Sparing Analysis feature is an option that lets the user to determine the number of spare Line Replacement Units (LRU) that must be initially available in order to ensure an acceptable level of mission or usage availability.

Go to :
http://rac.alionscience.com/Toolbox/Rac_poisson.html

3 ReliaSoft's Weibull SPRT Tool for Sequential Probability Ratio Test Analysis

ReliaSoft's Weibull SPRT software is a sequential probability ratio test utility that uses Weibull sequential testing and allows you to test samples in a sequential manner. The SPRT utility performs all calculations required in order to determine whether to accept or reject the hypothesis that the samples are from a given Weibull life distribution and meet a given reliability requirement.

To install on your computer, go to:

http://www.weibull.com/freetools/index.htm#sprt.

4 Reliability Prediction by Internet

If you are interested in fast Reliability Prediction (MTBF) by various methodologies (MIL-HDBK-217F, Telcordia, etc.), you may order them directly (payment involved) via the internet, ready on the same day at:
www.e-reliability.co