# בטיחות פונקציונלית
# Functional Safety

## as per IEC61508 and IEC61511

ד"ר אלכס כהן CFSP*, הזמט 2019

*Certified Functional Safety Professional

# Functional Safety

בטיחות פונקציונלית עוסקת במערכות הגנה מבוססות מכשור.
המונח בטיחות פונקציונלית מתייחס לכך שפונקציית הבטיחות הרצויה תפעל ברמת האיכות, האמינות והזמינות הרצויות כאשר שכבת ההגנה נדרשת.

<u>בסיס מקצועי</u>: סדרת התקנים IEC 61508
מימוש בתעשיה התהליכית: IEC 61511
בסקטורים אחרים ישנה לרוב הפניה לתקן 61508 בתוספת קביעת קריטריונים יחודיים לסקטור
התקנים מזוהים לעתים קרובות עם המושג Safety Integrity Level SIL

**IEC61508** Functional safety of electrical/electronic/programmable electronic safety-related systems
**IEC61511** Functional safety - Safety instrumented systems for the process industry sector

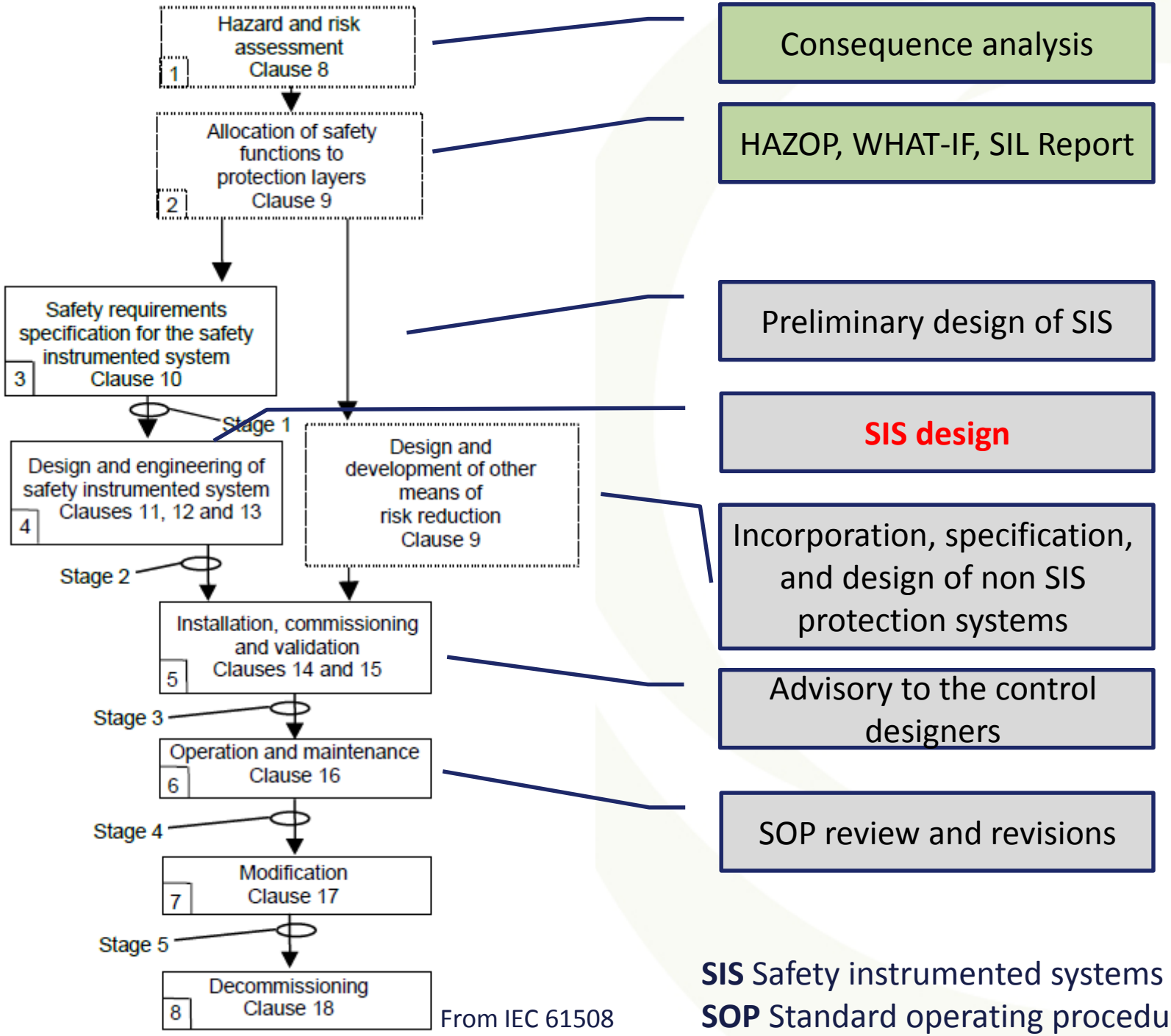
# Functional safety

תכנון מערכות הגנה מבוצע בשני שלבים עיקריים:

- תכנון רמת הגנה נדרשת: קביעת רמת האמינות והזמינות הנדרשת מפונקציית הבטיחות (ובמלה אחת: קביעת SIL). כאמור, למעט בתעשיה התהליכית, ה SIL נקבע לרוב מראש בתקן או על ידי הלקוח.
- תכנון הפונקציה: תכנון ארכיטקטורה מתאימה של פונקציית הבטיחות כך שתושג רמת ה SIL שנקבעה בשלב הקודם

תכנון פונקציית הבטיחות הולך לאיבוד אי-שם בין התכנון של המערכת (אז נקבע ה SIL) לבין התכנון המפורט (שם אמורה להיקבע הארכיטקטורה). התוצאה היא שפונקציית הבטיחות לא עומדת במה שנדרש ממנה*

**כמו בהרבה מאד תחומים בהנדסה, התכנון של שכבת הגנה הוא לא תהליך אינטואיטיבי אלא תהליך מקצועי לכל דבר ועניין. אגב, ברוב מוחלט של המקרים מדובר בארכיטקטורה שאינה מצליחה להגיע לרמת ה SIL הרצויה. נדירים מאד המקרים של Overdesign*




From IEC 61508

**SIS** Safety instrumented systems

**SOP** Standard operating procedure

# קביעת SIL

# *Functional safety: Identification*

'סידור עבודה' לזיהוי הצורך בהגנות בתהליך:

- זיהוי סטיות מתהליך העבודה המתוכנן
- זיהוי האופן שבו הסיכון מתממש לנזק (אופני-כשל, failure modes)
- ניתוח ההגנות הקיימות בתהליך (או המתוכננות).
- בדיקת 'פרצות' בשכבות ההגנה
- הוספת פונקציות הגנה עד שהסיכון השיורי קביל

ההחלטה מהי רמת המהימנות של פונקציית הבטיחות, או בשפת התקנים: מהי הבטיחות הפונקציונלית הנדרשת' – נעשית על ידי התאמה של ערכי SIL לאירוע ולשכבות ההגנה העוטפות אותו עד להתאמה מלאה.
תהליך זה נקרא **SIL allocation**

# Functional safety: SIL

Safety Integrity Level - SIL

על מנת ליצור בסיס אחיד וברור (ופשוט) להערכת הבטיחות הפונקציונלית,
לכל פונקציית בטיחות נקבע ערך SIL.

מטרת ה SIL:


לייצר שפה אחידה, ברורה ופשוטה
שתאפשר לקובעי המדיניות,
למשתמשים וליצרני המכשור לתקשר
ביניהם ללא טלפון שבור

# *Functional safety: SIL*

כך שהמשפטים הבאים יהיו ברורים לכולם:

- בהוראות הנהלה נקבע שתקלה במהלך חיי המתקן העלולה לגרום לפגיעה בעובד מעל יום היעדרות מחייבת פונקצית הגנה ברמת SIL2 לפחות ...
- שמתי פונקצית הגנה SIL3...
- הסיכון הכלכלי מחייב פונקצית הגנה ברמת SIL2 ומעלה...
- אני מחפש PLC שיהיה SIL1, הסיכון לא מצדיק רכישת מערכת יקרה של PLC ברמת SIL2 or SIL3...
- שלום, האם יש לכם במלאי משדר טמפרטורה ברמת SIL2 ?

וכך הלאה ...

# Targets for safety systems

| DEMAND MODE OF OPERATION | | |
|---|---|---|
| **Safety integrity level (SIL)** | **Target average probability of failure on demand** | |
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ | Success rate 99.99-99.999% |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ | 99.9-99.99% |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ | 99-99.9% |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ | 90-99% |

| CONTINUOUS MODE OF OPERATION | |
|---|---|
| **Safety integrity level (SIL)** | **Target frequency of dangerous Failures to perform the SIF (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 $< 10^{-5}$ |

From IEC 61511

HAZMAT

# *Functional safety: SIL determination*

קביעת SIL צריכה להיות:

- פרופורציונלית לסיכון.
- בעלת מימד 'כמותי' כלומר סטטיסטי.

שתי התכונות הללו מובילות לשני היתרונות הגדולים של שימוש ב SIL:

1. ההבנה שאפשר לצרף מערכות שונות – כל אחת עם SIL משלה – כדי לקבל SIL גבוה יותר
2. ניתן להתייחס גם למערכות הגנה שאינן 'מכשור' ובתנאי שאני יכול לקבוע להם ערך אמינות וזמינות של SIL

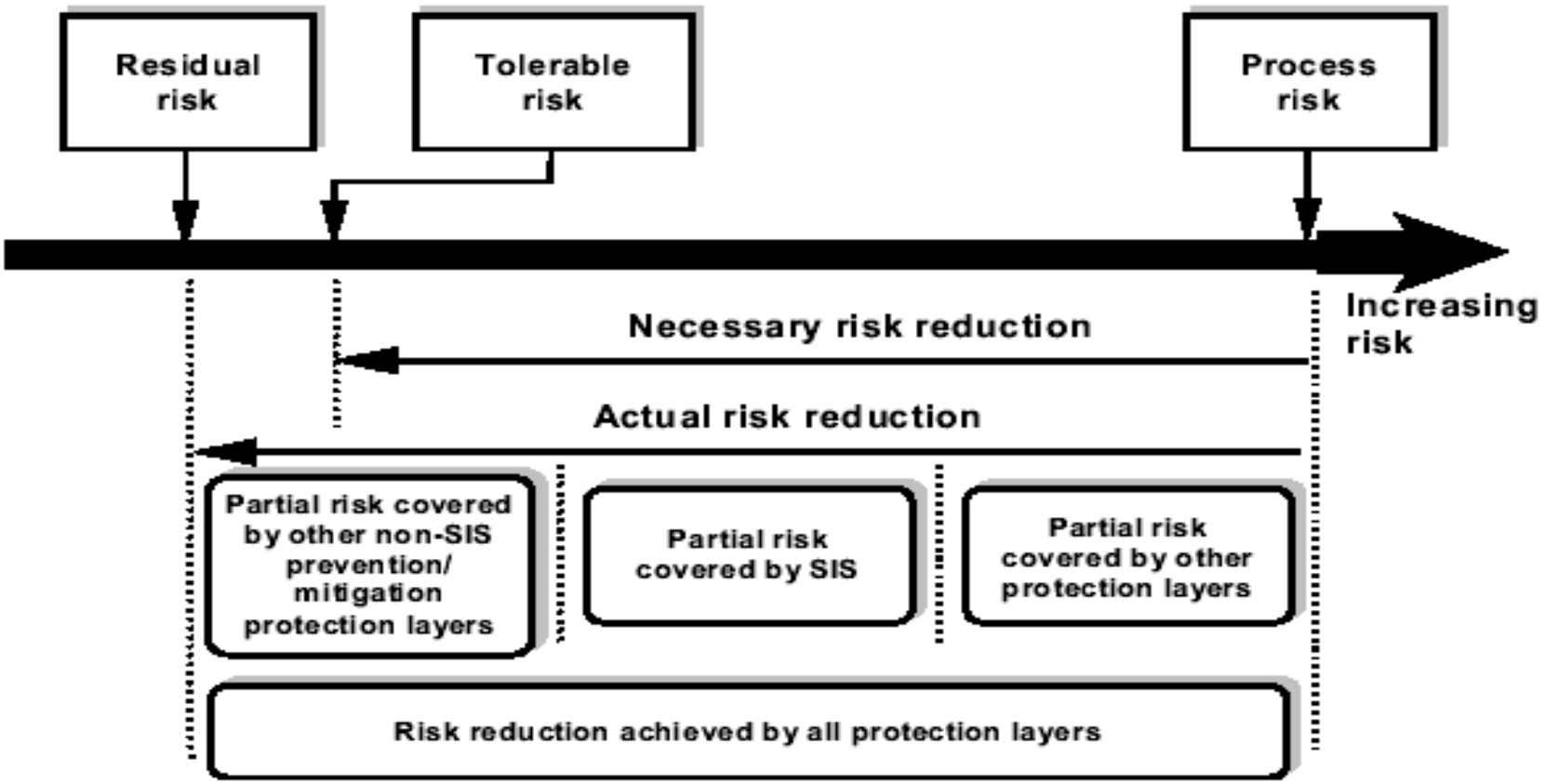
# *Functional safety: SIL determination (cont)*

שיטות לקביעת SIL

- **חישוב 'מדויק'.** חישוב כמותי של הסיכון והתאמת שכבות ההגנה בהתאם, על פי המדיניות של הארגון*.
- **מטריצת SIL.** שיטה המדרגת נזק וסבירות בצורה איכותית.
- **מטריצה משודרגת.** שיטה המדרגת נזק וסבירות בצורה חצי כמותית (כלומר לפי קטגוריות – כמו שמוגדר ה SIL עצמו)
- **SIL Graph.** שיטה חצי כמותית המתייחסת לגורמים כמו אכלוס, והמאפשרת 'כיול' לפי הגדרת מדיניות של הארגון
- תקן IEC61511 מציג עוד מספר שיטות הנבדלות בהיקף החישוב הנדרש לצורך הערכה סטטיסטית של הנזק ושל ההסתברות להופעה שלו.

*הארגון אמור לאמץ מדיניות, בפרט במקומות בהם המחוקק לא עשה כן:
בבטיחות, סביבה, נכסים, המשכיות עסקית ומוניטין.
בבטיחות ארגונים נוהגים לאמץ את המדיניות הבריטית לסיכוי למוות בשנה (מתקנים חדשים): $10^{-4}$ לעובד, $10^{-5}$ לעובד מתהליך יחיד, $10^{-6}$ לאוכלוסייה לא מעורבת.

# Risk reduction concept



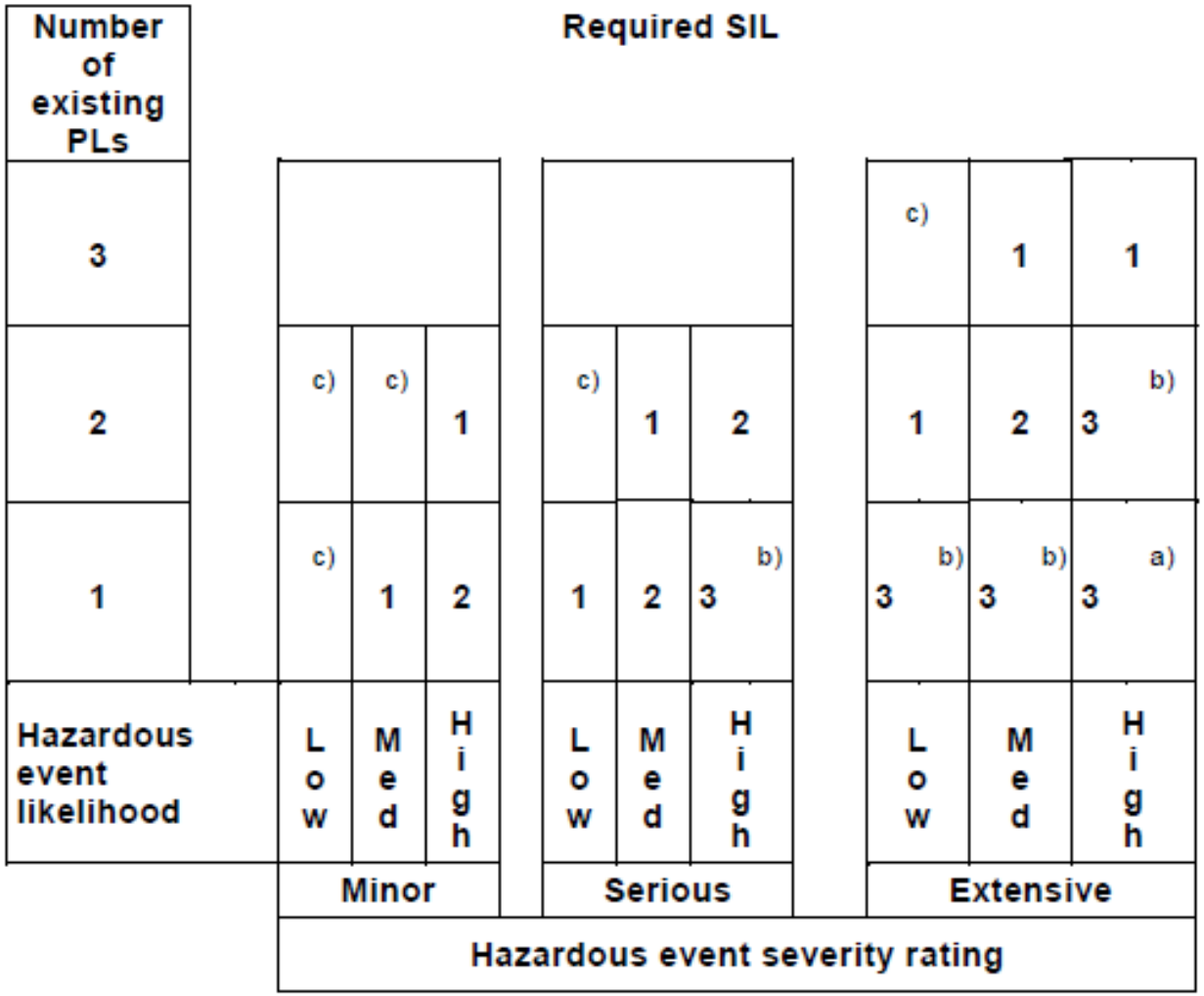

From IEC 61511

# Safety Layer Matrix (SIL matrix)

| Type of events | Likelihood |
|---|---|
| | Qualitative ranking |
| Events such as multiple failures of diverse instruments or valves, multiple human errors in a stress free environment, or spontaneous failures of process vessels. | Low |
| Events such as dual instrument, valve failures, or major releases in loading /unloading areas. | Medium |
| Events such as process leaks, single instrument, valve failures or human errors that result in small releases of hazardous materials. | High |
| * The system should be in accordance with this standard when a claim that a control function fails less frequently than $10^{-1}$ per year is made. | |

| Severity rating | Impact |
|---|---|
| Extensive | Large scale damage of equipment. Shutdown of a process for a long time. Catastrophic consequence to personnel and the environment. |
| Serious | Damage to equipment. Short shutdown of the process. Serious injury to personnel and the environment. |
| Minor | Minor damage to equipment. No shutdown of the process. Temporary injury to personnel and damage to the environment. |

From IEC 61511




a) One SIL 3 safety instrumented function (SIF) does not provide sufficient risk reduction at this risk level. Additional modifications are required in order to reduce risk.

b) One SIL 3 SIF may not provide sufficient risk reduction at this risk level. Additional review is required.

c) SIS protection layer is probably not needed.

# תכנון ל SIL

# איך נראית פונקצית בטיחות?

בדיוק כך:


גלאי (אפשר כמה)
לוגיקה – logic solver
פעולה נגזרת לפי הגדרות הלוגיקה
...ולפעמים נדרשת יותר מיחידה אחת לצרכי יתירות

העיקר שפונקציית הבטיחות תעמוד **כולה** ב SIL שנקבע

דוגמאות:

- השמטה (trip) של מבער כשאין להבה: גלאי להבה – PLC – ברז ניתוק גז
- כיבוי אוטומטי בריאקטור: גלאי טמפרטורה – PLC – פתיחת ברז מים
- בלימה ברכב אוטונומי: מצלמה ומכ"מ – PLC – הפעלת בלמים

# אם כבר נקבע SIL, מדוע נדרש לתכנן ארכיטקטורה והאם לא ניתן להסתפק ברכש מכשור ברמת ה SIL המתאימה?

כי היצרן מפרסם את תדירות הכשל של הפריט בתנאים מעבדתיים, ולכל פריט כשהוא לעצמו, ללא פריטים נוספים ובהנחה שכל התחזוקה והדיאגנוסטיקה מבוצעים בצורה מושלמת.
ובמציאות:

1. הפריט הוא חלק מתוך מערכת שלמה המהווה את פונקציית ההגנה. מערכת זו צריכה לעבוד בצורה משולבת. (למשל: ריבוי סיגנלים ב DCS)
2. מערכת ההגנה צריכה לתפקד בתנאי התהליך השגרתיים וכמובן גם בתנאי ההשמטה (התנאים בהם מערכת ההגנה אמורה להיכנס לפעולה). תנאי השמטה, בדרך כלל, רחוקים מהנורמה...
3. לא תמיד ניתן לבצע דיאגנוסטיקה לפי מה שהיצרן דורש
4. היצרן לא לוקח בחשבון שפעולות כמו כיול או בדיקה תקופתית מקטינות את זמינות המערכת
5. היצרן חשוף בעצמו לטעויות סיסטמטיות: פגמים ביצור, תכן לקוי, הרכבה לקויה ועוד.

**DCS** distributed control system

# אם כבר נקבע SIL, מדוע נדרש לתכנן ארכיטקטורה והאם לא ניתן להסתפק ברכש מכשור ברמת ה SIL המתאימה? (המשך...)

6. היצרן לא לוקח בחשבון אופני הפעלה שונים מהצורה בה הוא תכנן את המערכת (למשל עבודה בסביבה אחידה לעומת סביבה משתנה)
7. היצרן לא לוקח בחשבון את זמן התיקון של תקלה שאותרה במכשיר
8. היצרן לא יכול לקחת בחשבון שגיאות סיסטמטיות של המתכנן / המפעיל / המכשירן (בקיצור שגיאות של כל מי שנוגע בפריט והוא לא היצרן עצמו)
9. היצרן גם לא יכול לקחת אחריות על מידת הנגישות שיש למשתמש הקצה/המפעיל/המהנדס לתוכנת ההפעלה/בקרה של המכשור
10. היצרן לא יכול להתייחס ל common mode failures - הגורם העיקרי להכשלת מערכות הגנה מורכבות
11. וגם: כמעט שלא ניתן להשיג מכשור ברמת SIL4 ומכשירים ברמת SIL3 הם יקרים מאד. ולכן לא ניתן להסתפק ברכישת מכשיר בעל SIL גבוה במערך של


כל אלה (ועוד) מפחיתים מאד את מידת האמינות של הפריט ונדרשת מידה רבה של אופטימיזציה, ולעתים אף השקעה בציוד נוסף, כדי להתקרב לערכים של היצרן.

*לכן היצרן ההוגן נמנע מלציין מהו ה SIL של המכשיר המסופק אלא רק מה תדירויות הכשל שלו.

# Functional safety

**אז מה בעצם כולל תכנון הארכיטקטורה של מערכות הגנה לפי תקן?**

1. תכנון הלוגיקה ומתוך כך תכנון המבנה (ארכיטקטורה) כך שניתן יהיה להגיע לערכי ה SIL הנדרשים מפונקציית הבטיחות. למשל שימוש ב voting
2. תכנון יתירות לפי כללי HFT (hardware fault tolerance) לכל הפחות, בפרופורציה לסיכון (סיכון גבוה משמע HFT גבוה)
3. תכנון מעקפים לצרכי דיאגנוסטיקה כך שהפגיעה בבטיחות (ולמעשה ב SIL) תהיה מינימלית. המעקפים יכולים להיות לוגיים/תוכנתיים ו/או פיזיים.
4. קביעת תדירות דיאגנוסטיקה (online) לשמירה על SIL בהתאם לתכונות diagnostic coverage של הציוד (בין אם ידוע ובין אם מחושב).
5. התאמת SIL לפי מידת הנגישות לתוכנה של מפעילים/מהנדסים/גישה-מרחוק וכו'
6. קביעת תדירות proofing (offline) בהתאם לדרישות ה SIL, התייחסות לזמן ה deadtime, רמת החשיפה לשגיאות סיסטמטיות* ו diagnostic coverage
7. שילוב מערכות הגנה שאינן מערכות מכשור בתוך פונקצית ההגנה הכוללת
8. תכנון מערכות הגנה שאינן מבוססות מכשור (בין היתר לצורך הקטנת ערכי SIL של מכשור יקר)
9. עמידה בתקנים של בטיחות תהליכית ככל שישנם כאלה

HAZMAT

# *Functional safety (cont)*

**שגיאות סיסטמטיות והטיפול בהן**

1. התאמת מכשור לשימוש ותנאי השימוש הרצויים (טמפ', מאמצים, קורוזיה, לחצים, ועוד)
2. התאמת מכשור לתנאי ה trip (לרוב, תנאים החורגים מהשימוש השגרתי)
3. הגדרת: דרישות מהתוכנה, בדיקות תוכנה, שימוש ב watchdog וכו'
4. שימוש בטכניקות הערכת סיכונים (HAZOP או WHAT-IF) לזיהוי common-mode failures ונטרולם או לחילופין עדכון מערכת ההגנה בהתאם
5. שימוש בטכניקות הערכת סיכונים (checklist or FMECA) לזיהוי ונטרול שגיאות סיסטמטיות ובמידת הצורך עדכון הארכיטקטורה של מערכת ההגנה בהתאם
6. עדכון תפ"מ והלוגיקה של הפעלת פונקציות הבטיחות

# *Functional safety (support)*

**סטטיסטיקה נדרשת:**

1. שימוש בנתונים סטטיסטיים של היצרן לצורך תרגומם ל SIL
2. בהיעדר נתוני יצרן, שימוש בנתונים ספרותיים מתאימים ככל האפשר לציוד המותקן
3. ניתוח של diagnostic coverage (DC) של ציוד שהיצרן לא סיפק די מידע לגביו, או לחילופין, להעריך DC באמצעות FMECA, או לחילופין שימוש ביתירות כדי להקטין אי וודאות בכל הנוגע ל diagnostic coverage
4. בדיקת החשיפה לשגיאות סיסטמטיות לפי התקן והקטנת הסבירות לשגיאות שכאלו.
5. הערכות של זמן מת (החל מקרות התקלה, דרך משך זמן האיתור שלה, משך זמן התיקון, ומשך זמן ההתקנה מחדש) והמלצות על מלאי של ציוד קריטי.
6. במערכות קיימות: שימוש בנתונים סטטיסטיים בארגון לצורך המידע הסטטיסטי על הציוד כגון: תדירות כשל בסיסית (SIL), תדירות של בדיקות דיאגנוסטיקה, הערכות זמן מת מאיתור תקלה ועד לחזרה מלאה לכשירות.
7. במערכות קיימות: בהתאם לניתוח הסטטיסטי ביצוע review של מערכת ההגנה כולה ועמידותה בדרישות SIL ובמידת הצורך גם תכנון של הגנה משופרת.
8. הדרכת משתמשים: מפעילים, אנשי בקרה, כיצד יש לשמר בכל עת (לאורך חיי מערכת ההגנה) את רמת ה SIL הנדרשת

# שלבים בתכנון ל SIL

**תכנון ראשוני preliminary design:**

1. הכרת תרחישי הייחוס להם מוקמת פונקציית הבטיחות ודירוג התרחישים לפי קריטיות
2. אמצעי הגילוי monitoring ובדיקת הכיסוי שלהם (אפקטיביות)
3. אמצעי התגובה response/action ובדיקת אפקטיביות
4. דרישות יתירות ו hardware fault tolerance (HFT) ובחירה בשיטת ה voting המועדפת XooY.
5. דרישות SIL ממערכת הבקרה logic-solver ודרישות יתירות
6. הגדרת דרישות ממערך התקשורת
7. הנחיה עקרונית לגבי תוכנה – הרשאות גישה, בדיקות קבלה, שימוש ב watchdog וכו'.
8. הנחיות מינימום לערכי *FIT (נתוני כשל או **MTBF) של פרטי הציוד
9. הנחיה עקרונית לגבי דיאגנוסטיקה
10. הנחיה עקרונית לגבי כיול ו proofing
11. הנחיה עקרונית לגבי רמות מלאי

*Failure in time (failures per $10^6$ or $10^9$ working hours)

**Mean time between failures

# שלבים בתכנון ל SIL (המשך)

**תכנון מפורט detailed design:**

1. איסוף נתונים (יצרן, ספרות, נתוני שימוש וכל מקור אפשרי אחר) לכשל של פריטי הציוד לרבות: ערכי FIT, diagnostic coverage, הבחנה בין נתוני כשל שמייצרים סיכון, לכשלונות שאינם מייצרים סיכון (fail-safe).
2. הערכות סיכונים מסוג FMECA או HAZOP לאיתור כשלונות של פריטי ציוד שאינם מכוסים בשימוש הרגיל, ובפרט בתנאים שאמורים להפעיל את פונקציית הבטיחות.
3. חישוב מקדם הפחתה של systematic failures והנחיה על טכניקות להגנה בפני systematic failure (ניהול איכות, בקרת תהליך, בדיקות קבלה, commissioning ועוד)
4. הערכות סיכונים מסוג: WHATIF או HAZOP או כל דרך מתאימה אחרת לצורך זיהוי common-mode-failures
5. בכל מקום שבו יש אי התאמה בין רכיב/קונפיגורציה/קוד לערך SIL המטרה, יועלו אופציות ליישוב אי-ההתאמות לבחירת הלקוח.
6. הערכות של זמן-מת (הזמן שחולף מאיתור תקלה ועד להחזרת המערכת לקדמותה), וקביעה עם הארגון כיצד להתייחס לתקלות (תקלות משביתות לעומת תקלות שמאפשרות לעבוד במצב bypass)
7. השלמת ארכיטקטורה שעומדת ב SIL
8. השלמת דוח SIL מפורט בהתאם למידע שנאסף בשלבים הקודמים. דוח זה אמור להיות מוצג ללקוחות/משתמשי-קצה כהוכחה לעמידה בדרישות SIL.

# שלבים בתכנון ל SIL (המשך)

**תכן סופי ובדיקות קבלה commissioning:**

1. דיאגרמת causes & effects ובדיקת התאמתה לתכנון המקורי
2. השלמת הלוגיקה של מערכת ההפעלה (תפ"מ או SOP)
3. הנחיות למלאי מינימום בהיבט של קיום ה SIL
4. הכנת פרק SIL ב "ספר המתקן"
5. הדרכת משתמשים: מפעילים, אנשי בקרה, כיצד יש לשמר בכל עת (לאורך חיי מערכת ההגנה) את רמת ה SIL הנדרשת

Hazmat,
risk engineering team

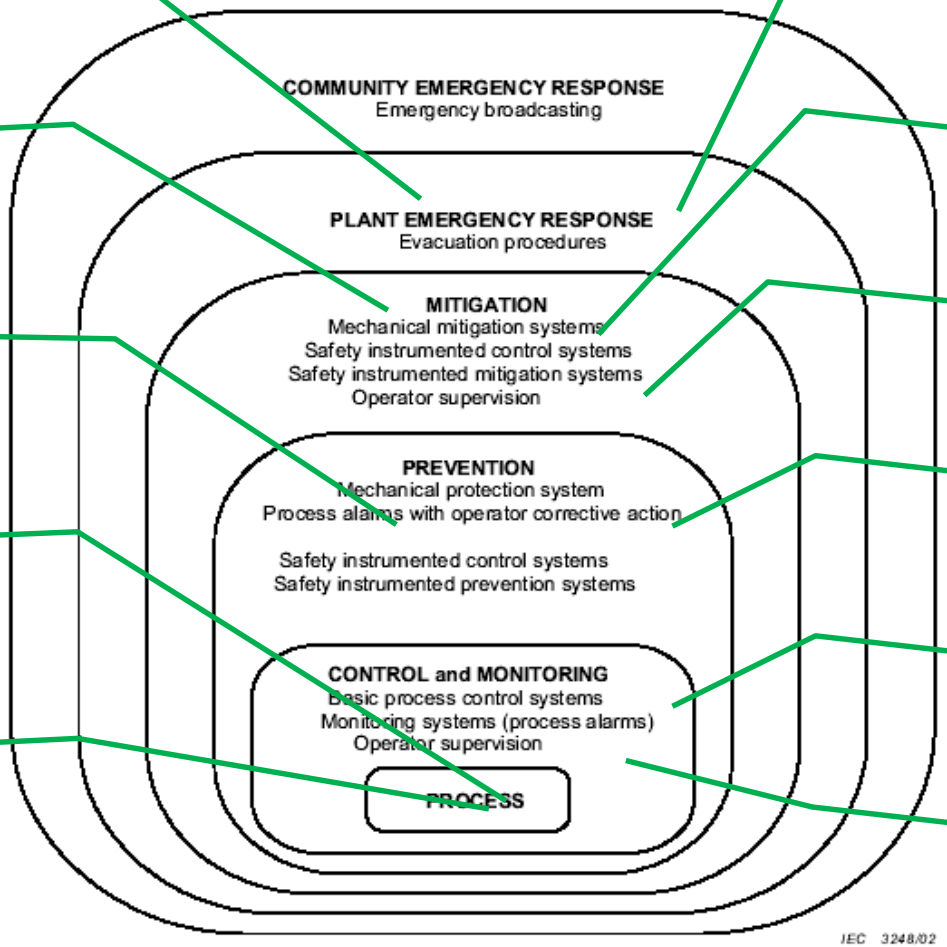
Egress modelling

SIL Studies

Design of safeguards

HAZID

Design for safety




Design of safeguards

Design of safeguards

CFD, QRA, Consequences risk assessment

HAZOP, SIL Design to SIL

HAZOP, FMECA, WHAT-IF

Design of safeguards

*All about us in two words:* ***protection layers***