התעשייה האווירית לישראל

חטיבת הנדסה ופיתוח

ניתוח FMECA למערכות Fail-Safe מוטסות

יולי גולוב – תע"א

16.01.2017

סיווג: בלמ"ס

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

תוכן העניינים

- דרישות Fail Safe
- הגדרת אירועים קטסטרופליים
- מאורעות זרים – הגדרה, תכונות
- אופני כשל (Failure Modes)
- אמצעי גילוי תקלה (Detectability Means)
- The Lowest Indenture level
- ניתוח צירופים במסגרת FTA
- סיכום

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

מסמכים ישימים

- **MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, 24.11.1980**
- **ARP 4761 Guidelines and Methods For Conducting The Safety Assessment Process on Civil Airborne Systems And Equipment (Para 4.2 –FMEA, Para 4.3 – FMES), 12.1996**

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

Fail Safe Requirements

- **Reference Document: AC/AMJ No: 25.1309 System Design and Analysis, 10.06.2002, Para 6b (1) Fail-Safe Design Concept:**
  - **In any system or subsystem, the failure of any single element, component, or connection during any one flight should be assumed, regardless of its probability. Such single failures should not be catastrophic.**

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

Catastrophic Failure Condition

- **AC/AMJ No: 25.1309 System Design and Analysis, 10.06.2002 (para 7a (5)):**
  - **Catastrophic: Failure conditions which would result in multiple fatalities, usually with the loss of the airplane.**
  - **Note: A "Catastrophic" Failure Condition was defined in previous versions of the rule and the advisory material as a Failure Condition which would prevent continued safe flight and landing.**
- **MIL-STD-882E, SYSTEM SAFETY, 11.05.2012:**
  - **Could result in one or more of the following: death, permanent total disability, irreversible significant environmental impact, or monetary loss equal to or exceeding $10M.**

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

Catastrophic Failure Condition

- **STANAG 4761, Edition 2**
  - **Failure conditions that are expected to result in at least uncontrolled flight (including flight outside of pre-planned or contingency flight profiles/areas) and/or uncontrolled crash, Or**
  - **Failure conditions which could potentially result in a fatality to UAV crew or ground staff.**
- **MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, 24.11.1980**
  - **A failure which may cause death or weapon system loss (i.e., aircraft, tank, missile, ship, etc.)**

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

הגדרת אירועים קטסטרופליים - סיכום

- הגדרות אירועים במסמכי FAA/STD מאוד כללים (מוות, איבוד מטוס\ אנייה\ טנק וכו')
- חומרת האירוע בחלק מהמקרים תלויה בשלב המשימה
- לכן מעבר להגדרות לכלליות של אירועים קטסטרופליים רצוי להגדיר אירועים ברמת פונקציה/חומרה של המערכת שעלולות לגרום לאירועים קטסטרופליים

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

הגדרת אירועים קטסטרופליים - סיכום

- **דוגמה לאירועים ברמת פונקציה\חומרה:**
  - **Loss of Trust during Take-off**
  - **Loss/Erroneous Elevator control (all phases)**
  - **Inadvertent payload moving (Maintenance)**
  - **Misleading of Rudder Command (Landing)**

- **מקורות לאירועים**
  - **Functional Hazard Analysis – FHA**
  - **Preliminary Hazard List – PHL**
  - **דרישות הלקוח/מפרטים**
  - **הנדסת מערכת**

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

מאורעות זרים – הגדרה, תכונות

- מאורעות זרים – מאורעות שאינם יכולים להתרחש בו זמנית.
- ז"א שאם A ו- B מאורעות זרים וידוע כי מאורע A התרחש אזי לא יתכן כי מאורע B התרחש. כלומר התרחשות מאורע A פוסלת התרחשות מאורע B.
- דוגמא למאורעות זרים: בניסוי זריקת מטבע המאורע "התקבל עץ" והמאורע "התקבל פלי" הם מאורעות זרים.

$$\sum_{(i)} P_i = 1$$

- כאשר:
  - Pi - הסתברות להתרחשות מאורע i
  - (i) – כל המאורעות האפשריים (קבוצה שלמה)

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

אופני כשל (Failure Modes)

- אופני כשל של פריט כלשהו חייבים לעמוד בקריטריונים של מאורעות זרים
- ז"א לא יכול להיות גורם משותף שיגרום להופעת 2 אופני כשל או יותר בו זמנית
- כלל זה ניתן לקיים יחסית בקלות בפריטים פשוטים (כמו למשל דיודה):
- דוגמה:
  - Diode Open
  - Diode Short
- דיודה לא יכולה להיות בו זמנית גם מקוצרת וגם מנותקת. לכן אופני כשל של דיודה הם זרים

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

אופני כשל (Failure Modes)

- בפריטים מורכבים הגדרת אופני כשל יכולה להתבסס גם על אופני כשל פשוטים וגם על צירופים
- דוגמה:
  - Loss of Output A
  - Loss of Output B
  - Loss of both Outputs A and B

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

אופני כשל (Failure Modes)

- בחלק מהפריטים המורכבים, הגדרת הצירופים היא בלתי מעשית (כמות גדולה מאוד של צירופים)
- השיטה להגדרת אופני כשל מבוססת על העקרונות הבאים:
  - הגדרת אופני כשל בהנחה שאין צירופים
  - כל אופן כשל יוגדר באופן שיוכל להתפרש ככל צירוף אפשרי של אופני כשל בודדים
  - האפקט של הכשל הנ"ל חייב להיות לפחות כמו האפקט הגרוע ביותר של אופני כשל ללא צירופים (ניתוח במסגרת FMECA)
  - ניתוח הצירופים במסגרת FTA לפי שיטה שתוסבר בהמשך

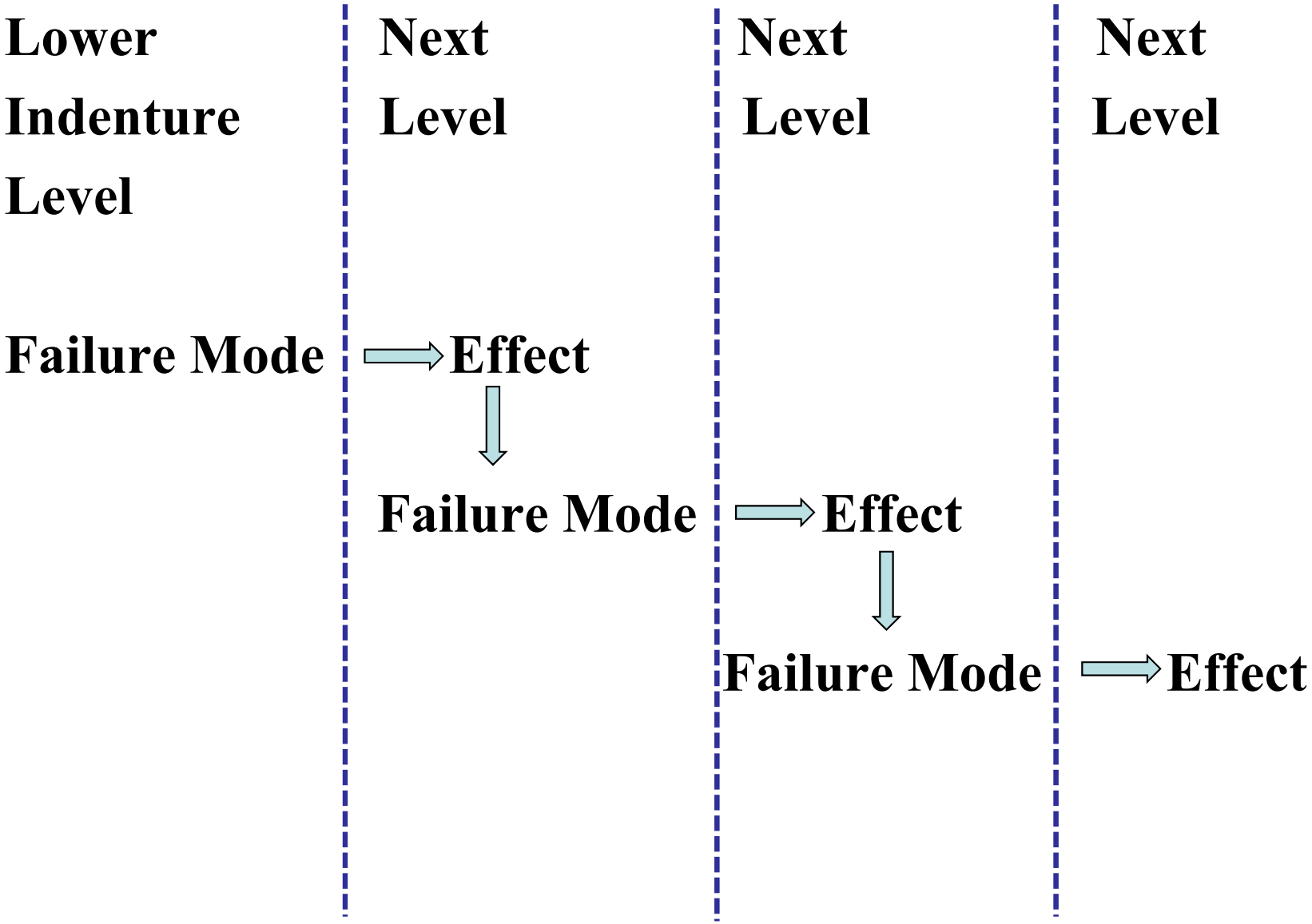
לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

אופני כשל (Failure Modes)

- דוגמה:
  - Loss of Output A
  - Loss of Output B
  - Loss of Output C
  - Loss of any Combination of Outputs

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

תהליך ביצוע FMECA



לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

תהליך ביצוע FMECA

- גם מבחינה תיאורטית וגם מבחינת השימוש בתוכנות FMECA, הניתוח מתבצע ב-2 רמות:
  - אופן כשל
  - אפקט
- אפקט של אופן כשל הוא אופן כשל ברמה יותר גבוהה
- לכן גם אפקטים צריכים להיות זרים.
- כלל זה צריך להתקיים מרמת הנמוכה ביותר של הניתוח ועד לרמה של מערכת

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

אמצעי גילוי תקלה (Detectability Means)

- מטרות
  - לבחון האם האמצעי לגילוי תקלות מאפשר לעבור לערוץ גיבוי (במידה שנבנתה מערכת Fail Safe המבוססת על הפעלה של ערוץ יתיר)
  - לזהות תקלות רדומות
- שלבי ניתוח מבחינת אמצעי לגילוי תקלות
  - שלבי פעולת המערכת שבהם נדרשת עמידה ב-Fail Safe (למשל שלבי טיסה במטוסים)
  - כל שלבי תפעול המערכת (למשל בדיקות קדם טיסה)

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

שלבי ניתוח של אמצעי גילוי תקלה

- זיהוי הבדיקה\ חיישן שבעזרתם המערכת מגלה שיש תקלה (גילוי ב-100%)
- בדיקה האם קיים דווח על תקלה
  - האם קיימת התראה למפעיל (עבור הפעלת יתירות ידנית)
  - האם קיימת התראה למערכת רלוונטית (עבור הפעלת יתירות אוטומטית)
- האם ניתן לנטרל\ לנתק מערכת תקולה (בהתחשב בזמן נדרש לניתוק)
- האם ניתן להפעיל מערכת יתירה (בהתחשב בזמן נדרש לניתוק)
- הניתוח חייב להתבסס על
  - נוהל תפעול (עבור הפעלת יתירות ידנית)
  - דו''ח לוגיקת מערכת (עבור הפעלת יתירות אוטומטית)

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

The Lowest Indenture level

- רמה שבה ניתן לגלות תקלה ב-100%
- רמה שבה קיימת יתירות

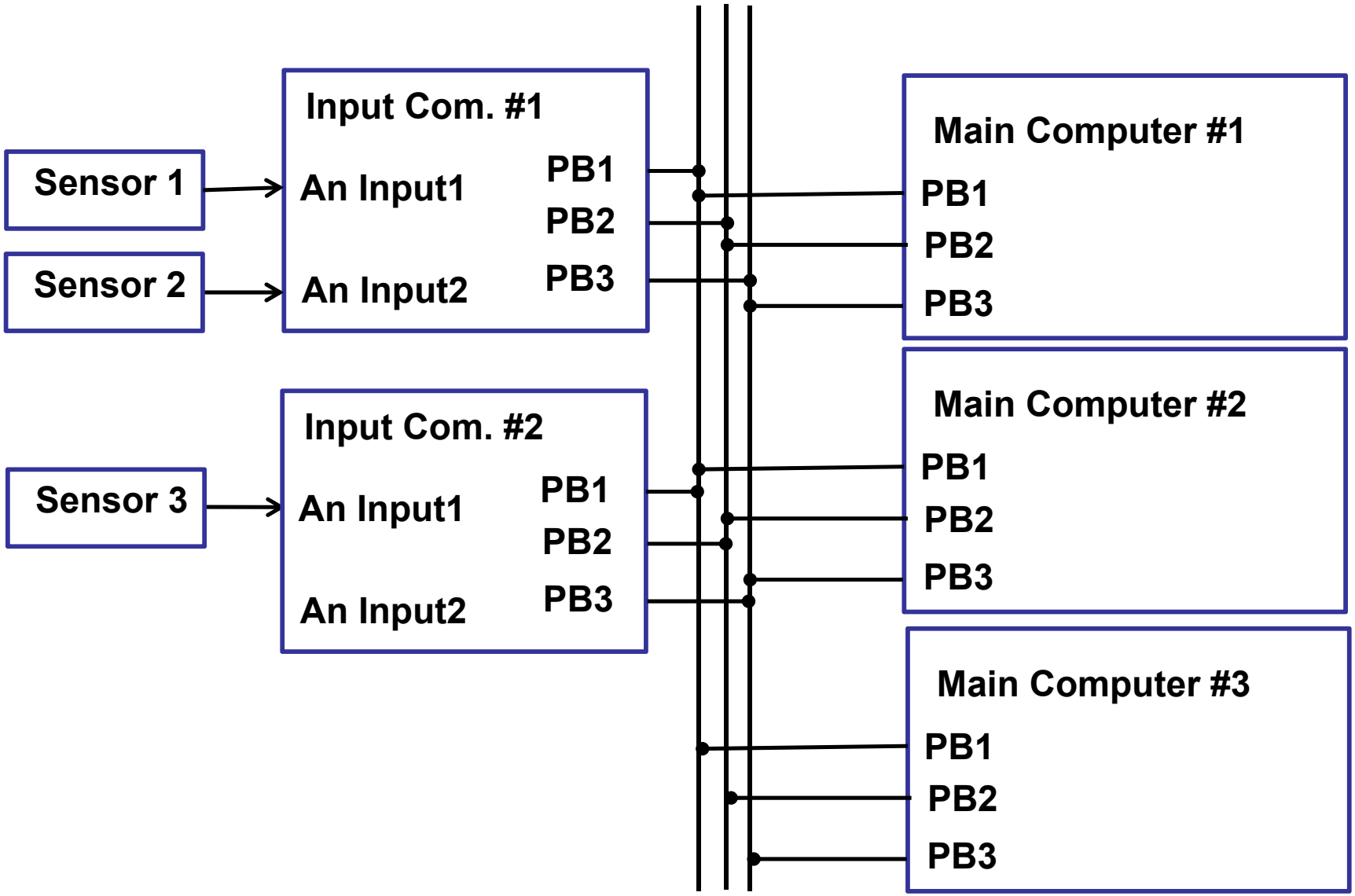
לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

ניתוח צירופים במסגרת FTA

- מגדירים אופני כשל של פריט ללא צירופים
- מגדירים אופן כשל שמיצג צירופים אפשריים של אופני כשל בודדים (למשל: Improper Operation)
- בכל פעם שמוסיפים ב-FTA אופן כשל של פריט ללא צירופים, מוסיפים גם אופן כשל של צירופים
- מבצעים בדיקת Cut-sets של FTA. במידה שאופן כשל של צירופים מופיע כתקלה בודדת אזי יש חשד לתקלה בודדת
- ע"י ה- FTA מזהים את אופני הכשל שצירוף שלהם גורם להופעתו של אירוע קטסטרופלי ובודקים ישימות של הצירוף בפועל
- במידה שצירוף ישים – משנים את התכן (תקלה בודדת). במידה שלא – מעדכנים את ה-FTA

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

ניתוח צירופים במסגרת FTA - דוגמא



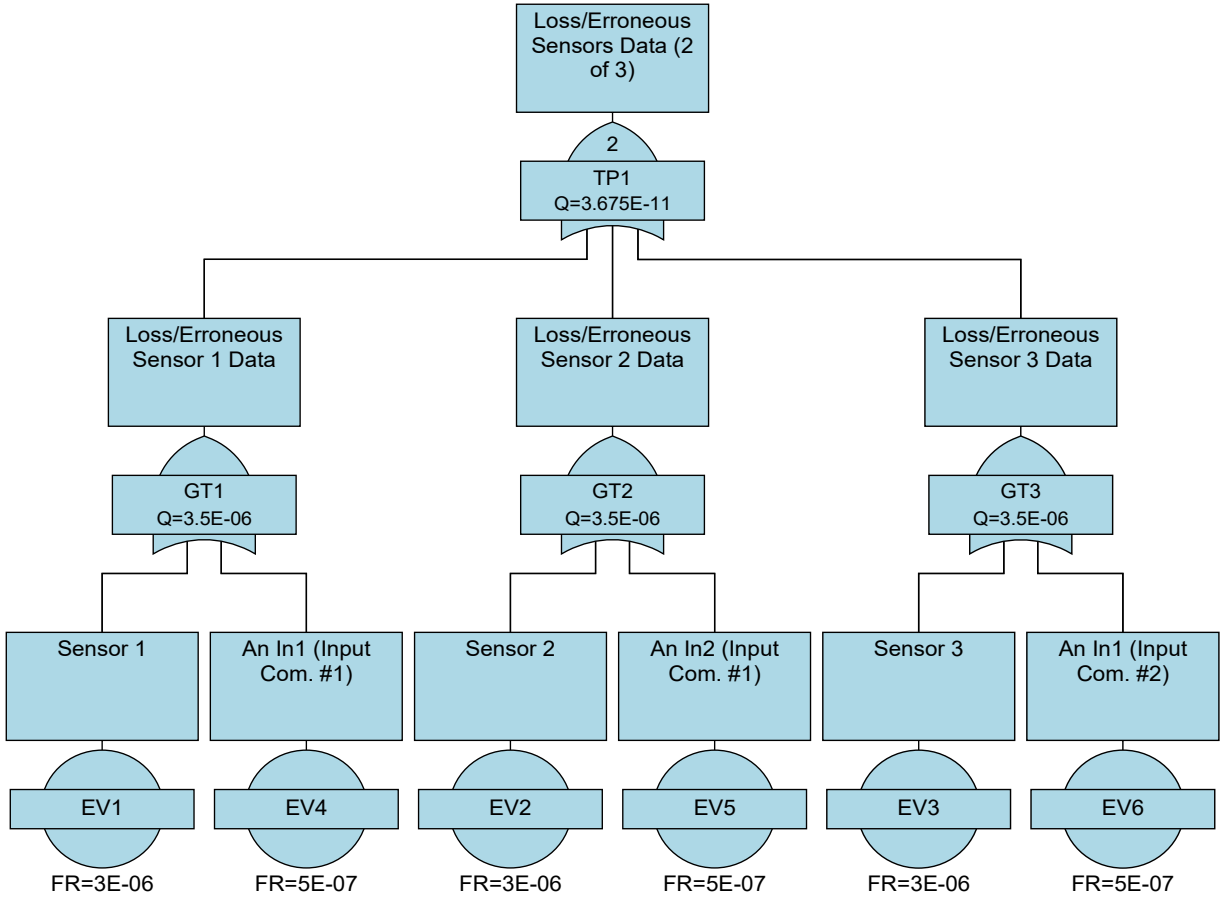
לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

ניתוח צירופים במסגרת FTA - דוגמא

- כל מחשב ראשי בוחן את החיישנים (Sensors) ומכריע על סמך הרוב (Voter Monitor).
- הניתוח צומצם ללוגיקת ניהול חיישנים בלבד

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

ניתוח צירופים במסגרת FTA - דוגמא



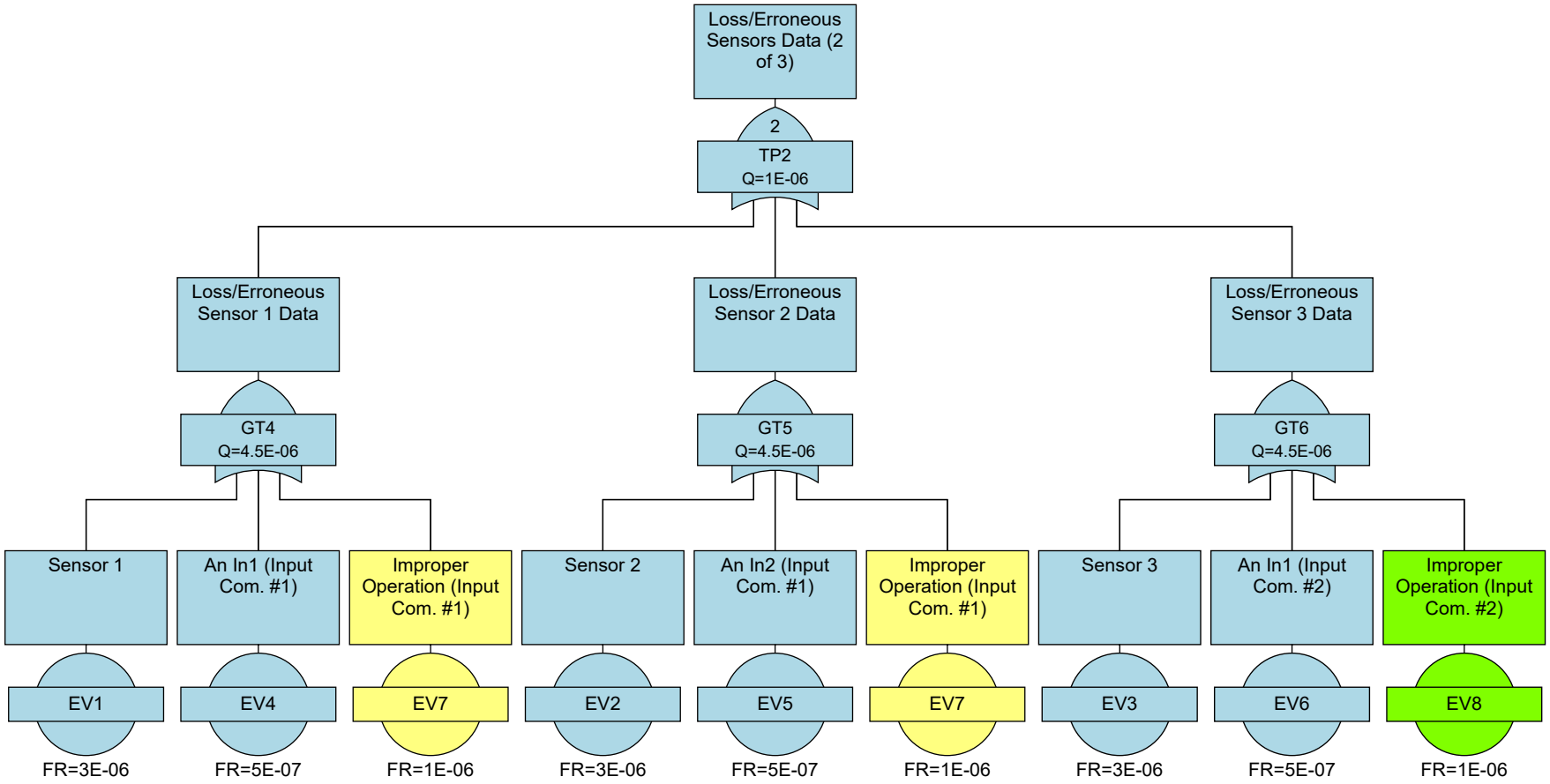
לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

Minimal Cut Sets (TP1)

Cut set event descriptions	Cut set	Probability of Occurrence
Sensor 1, Sensor 2	EV1,EV2	9e-12
Sensor 1, Sensor 3	EV1,EV3	9e-12
Sensor 2, Sensor 3	EV2,EV3	9e-12
Sensor 1, An In2 (Input Com. #1)	EV1,EV5	1.5e-12
An In1 (Input Com. #1), Sensor 2	EV4,EV2	1.5e-12
Sensor 1, An In1 (Input Com. #2)	EV1,EV6	1.5e-12
An In1 (Input Com. #1), Sensor 3	EV4,EV3	1.5e-12
Sensor 2, An In1 (Input Com. #2)	EV2,EV6	1.5e-12
An In2 (Input Com. #1), Sensor 3	EV5,EV3	1.5e-12
An In1 (Input Com. #1), An In2 (Input Com. #1)	EV4,EV5	2.5e-13
An In1 (Input Com. #1), An In1 (Input Com. #2)	EV4,EV6	2.5e-13
An In2 (Input Com. #1), An In1 (Input Com. #2)	EV5,EV6	2.5e-13

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

ניתוח צירופים במסגרת FTA - דוגמא



לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

Minimal Cut Sets (TP2)

Cut set event descriptions	Cut set	Probability of Occurrence
Improper Operation (Input Com. #1)	EV7	1e-6
Sensor 1, Sensor 2	EV1,EV2	9e-12
Sensor 1, Sensor 3	EV1,EV3	9e-12
Sensor 2, Sensor 3	EV2,EV3	9e-12
Sensor 1, Improper Operation (Input Com. #2)	EV1,EV8	3e-12
Sensor 2, Improper Operation (Input Com. #2)	EV2,EV8	3e-12
An In1 (Input Com. #1), Sensor 2	EV4,EV2	1.5e-12
Sensor 1, An In2 (Input Com. #1)	EV1,EV5	1.5e-12
Sensor 1, An In1 (Input Com. #2)	EV1,EV6	1.5e-12
An In1 (Input Com. #1), Sensor 3	EV4,EV3	1.5e-12
Sensor 2, An In1 (Input Com. #2)	EV2,EV6	1.5e-12

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

Minimal Cut Sets (TP2)

Cut set event descriptions	Cut set	Probability of Occurrence
An In2 (Input Com. #1), Sensor 3	EV5,EV3	1.5e-12
An In1 (Input Com. #1), Improper Operation (Input Com. #2)	EV4,EV8	5e-13
An In2 (Input Com. #1), Improper Operation (Input Com. #2)	EV5,EV8	5e-13
An In1 (Input Com. #1), An In2 (Input Com. #1)	EV4,EV5	2.5e-13
An In1 (Input Com. #1), An In1 (Input Com. #2)	EV4,EV6	2.5e-13
An In2 (Input Com. #1), An In1 (Input Com. #2)	EV5,EV6	2.5e-13

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

שימושים נוספים

- הוספת מתח אספקה (כפריט משותף) – בדיקת השפעת התקלה של Bus חשמלי (איבוד Bus)
- בדיקת נקודות חיבור לאדמה

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.

סיכום

- **בניתוח FMECA של מערכות מורכבות עלולים לא לגלות חלק מתקלות בודדות**
- **המתודולוגיה של בניית FTA שהצענו מאפשרת להרחיב את הניתוח ולגלות תקלות בודדות גם במערכות מורכבות**
- **ניתוח FTA מומלץ לצבע ברמה (Level) הגבוה ביותר (רמת מטוס, מערכת וכ')**

לתעשייה האווירית לישראל בע"מ זכויות קניין במידע שבמסמך זה. אין להעתיק לשכפל ולגלות תוכן מסמך זה כולו או חלקו, או לעשות בו שימוש כלשהו, אלא על פי הסכמה מראש ובכתב של התע"א.