โปรแกรมคอมพิวเตอร์เพื่อช่วยออกแบบระบบวัดคุมนิรภัย
Computer - Aided Design of Safety Instrumented System

ปรียฉัตร ร่องแก้ว[1] และ ธงไชย โรหิตะดิษฐ ศรีนพคุณ[2*]
สาขาวิชาวิศวกรรมความปลอดภัย คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์[1]
ภาควิชาวิศวกรรมเคมี คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์[2*]
E-mail: preeyachat.r@ku.th[1], thongchai.sr@ku.th[2*]
* ผู้ประพันธ์บรรณกิจ (corresponding author)

บทคัดย่อ

บทความนี้มีวัตถุประสงค์ในการพัฒนาโปรแกรมคอมพิวเตอร์ในการคำนวณระบบวัดคุมนิรภัย ตามมาตรฐาน IEC 61508/61511 เพื่อช่วยในการคำนวณหาค่าความเสี่ยงในกระบวนการอุตสาหกรรม ตรวจสอบระดับความปลอดภัยของอุปกรณ์ และค่าระดับความผิดพลาดของอุปกรณ์ เพื่อช่วยในการคำนวณและออกแบบระบบวัดคุมนิรภัย จากการศึกษาพบว่าสามารถช่วยลดระยะเวลาการคำนวณการตรวจสอบออกแบบระบบวัดคุมนิรภัย ลดความผิดพลาดจากการคำนวณ และช่วยหาแนวทางการแก้ไขปัญหาการออกแบบระบบวัดคุมนิรภัย

คำสำคัญ: ระบบวัดคุมนิรภัย; ระบบฟังก์ชันนิรภัย; อัตราความผิดพลาดนิรภัย; ระดับความปลอดภัย; การประเมินความเสี่ยง

Abstract

The objective of this article is to develop a computer program for calculating Safety Instrumented Systems bared on the IEC 61508/61511 standards. This program help in performing hazard analysis in industrial processes by risk values, assessing the safety integrity level of devices, and determining device error rates, thereby assisting in the design and evaluation of Safety Instrumented Systems. The results revealed that calculation time of Safety Instrumented Systems were reduced, mistakes from calculation were decreased and Safety Instrumented Systems design problems were defined proper solutions.

Keywords: Safety Instrumented Systems; Safety Instrumented Function; Safe Failure Fraction; Safety Integrity Level; Risk Assessment

1. บทนำ

ในอุตสาหกรรมการผลิตปัจจุบันได้มีการนำระบบวัดคุมนิรภัย มาใช้ในการป้องกันการเกิดอุบัติเหตุ ซึ่งเป็นส่วนสำคัญในโรงงานอุตสาหกรรม ในการป้องกันและควบคุมความเสี่ยงที่เกิดจากกระบวน การผลิตอุตสาหกรรม โดยจะประกอบไปด้วย

1) อุปกรณ์วัด (Sensors)
2) อุปกรณ์ประมวลผล (Logic solver)
3) อุปกรณ์สุดท้าย (Final elements)

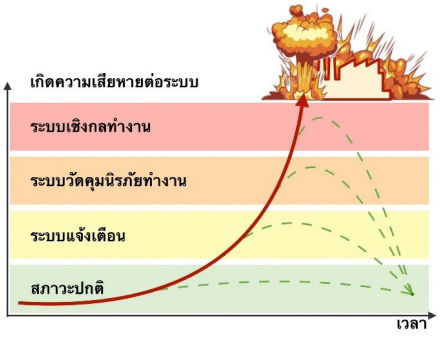
อุปกรณ์เหล่านี้จึงต้องตรวจสอบระดับความปลอดภัยของอุปกรณ์ และจำนวนอุปกรณ์สำรองเพียงพอหรือไม่ จากระดับความอันตรายของกระบวนการผลิตและระดับความปลอดภัยของระบบฟังก์ชันวัดคุมนิรภัย ให้ระบบวัดคุมนิรภัยอยู่ในระดับที่ยอมรับได้ตามมาตรฐานที่กำหนดไว้ ส่งผลให้ลดต้นทุนจากความเสี่ยงในการผลิตและความน่าเชื่อถือได้ [1]

2. ทฤษฎีที่เกี่ยวข้อง

การตรวจสอบระบบวัดคุมนิรภัยมีความสำคัญในการควบคุมอันตรายที่อาจเกิดขึ้น โดยพิจารณาตามมาตรฐาน IEC 61508 และ IEC 61511 เพื่อลดความเสี่ยงของอุบัติเหตุและความเสี่ยงที่เกิดจากการใช้งานระบบอิเล็กทรอนิกส์และระบบควบคุมอัตโนมัติในสายงานอุตสาหกรรม

2.1 ระบบวัดคุมนิรภัย (Safety Instrumented Systems : SIS)

ระบบ SIS จะทำงานหลังจากสัญญาณแจ้งเตือนเมื่อระบบควบคุมพื้นฐานไม่สามารถควบคุมได้ ระบบวัดคุมนิรภัยจะเข้าควบคุมการทำงานให้กลับเข้าสู่สภาวะปกติ แต่หากยังไม่สามารถหยุดอันตรายได้ ระบบเชิงกลจะทำงานในการระบายความร้อนและแรงดัน ซึ่งเป็นด่านสุดท้ายหากยังไม่สามารถควบคุมได้จะส่งผลอันตรายต่ออุตสาหกรรม การควบคุมอันตรายในแต่ละชั้นมีวัตถุประสงค์ให้การทำงานเข้าสู่สภาวะปกติ ดังภาพที่ 1



ภาพที่ 1 การทำงานระบบวัดคุมนิรภัย [2]

2.2 ระดับความปลอดภัย (Safety Integrity Level : SIL)

การกำหนดระดับความปลอดภัย หรือการคำนวณออกแบบระบบวัดคุมนิรภัยตามมาตรฐาน IEC 61508 และ IEC 61511 จะแบ่งระดับความปลอดภัย SIL เป็น 4 ระดับตามความปลอดภัย และแบ่งเป็น 2 รูปแบบ ดังนี้

1) กระบวนการผลิตที่มีอัตราเกิดเหตุต่ำ

โดยอัตราการเกิดเหตุอันตรายไม่มากกว่า 1 ครั้งต่อปี และไม่มากกว่า 2 เท่าของความถี่ในการตรวจสอบ ซึ่งระดับความปลอดภัย SIL จะพิจารณาค่าเฉลี่ยความน่าจะเป็นของความล้มเหลวรวมในช่วงการตรวจสอบ ของระยะเวลาในการตรวจสอบตามสมการที่ 4 ดังตารางที่ 1

ตารางที่ 1 Average Probability of a angerous Failure on Demand [3]

Safety Integrity Level	Average Probability of a Dangerous Failure on Demand of the Safety Function
SIL 4	$10^{-5} \le PFD_{avg} < 10*10^{-5}$
SIL 3	$10^{-4} \le PFD_{avg} < 10*10^{-4}$
SIL 2	$10^{-3} \le PFD_{avg} < 10*10^{-3}$
SIL 1	$10^{-2} \le PFD_{avg} < 10*10^{-2}$

2) กระบวนการผลิตที่มีอัตราเกิดเหตุสูง

โดยอัตราการเกิดเหตุอันตรายมากกว่า 1 ครั้งต่อปี และมากกว่า 2 เท่าของความถี่ ในการตรวจสอบ ซึ่งระดับความปลอดภัย SIL จะพิจารณาจากค่าเฉลี่ยค่าความน่าจะเป็นของความล้มเหลว ณ เวลาการตรวจสอบ ตามสมการที่ 14 ดังตารางที่ 2

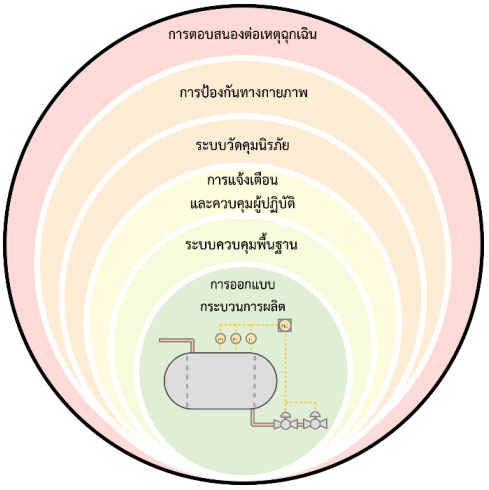
ตารางที่ 2 Average Frequency of a Dangerous Failure [3]

Safety Integrity Level	Average Frequency of a Dangerous Failure of the Safety Function h^{-1}
SIL 4	$10^{-9} \le PFH < 10*10^{-9}$
SIL 3	$10^{-8} \le PFH < 10*10^{-8}$
SIL 2	$10^{-7} \le PFH < 10*10^{-7}$
SIL 1	$10^{-6} \le PFH < 10*10^{-6}$

2.3 การประเมินความเสี่ยง (Risk Assessment)

การวิเคราะห์ความเสี่ยงในระบบอุตสาหกรรม เป็นสิ่งที่ควรประเมินเป็นอันดับแรก เพื่อตรวจสอบความปลอดภัย ทั้งผลกระทบต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อม โดยการตรวจสอบระดับอันตรายมีหลายวิธีดังนี้

1) การประเมินความเสี่ยง ด้วยวิธีการแบ่งระดับชั้นป้องกัน (Layer of Protection Analysis :LOPA) โดยการพิจารณาและวิเคราะห์ชั้นของอันตราย (Demand Rate) และความถี่ของเหตุการณ์ที่ยอมรับได้ (Hazard Rate) โดยระดับความแม่นยำขึ้นอยู่กับข้อมูลความผิดพลาดที่อาจจะเกิดขึ้นในแต่ละชั้น [2] ดังภาพที่ 2



ภาพที่ 2 การประเมินความเสี่ยง ด้วยวิธีการแบ่งระดับชั้นป้องกัน LOPA [5]

2) การประเมินความเสี่ยง ด้วยวิธีการเมทริกซ์ความเสี่ยง (Risk Matrix) เป็นการพิจารณาเปรียบเทียบตามความถี่ที่อาจเกิดอันตราย และระดับความอันตรายในแต่ละผลกระทบ เพื่อหาค่าระดับความอันตราย SIL ตามตารางที่ 3 ซึ่งสามารถประยุกต์ใช้ได้ง่ายในการคำนวณ แต่ความแม่นยำไม่ละเอียด [2]

2.1) ความถี่ของเหตุการณ์ (F)

2.2) ผลกระทบต่อชีวิต (H)

2.3) ผลกระทบต่อทรัพย์สิน (L)

2.4) ผลกระทบต่อสิ่งแวดล้อม (E)

ตารางที่ 3 การประเมินความเสี่ยง ด้วยวิธีการเมทริกซ์ความเสี่ยง (Risk Matrix)

F	ระดับความอันตราย SIL				
F0	-	SIL 2	SIL 3	SIL 4	b
F1	-	SIL 1	SIL 2	SIL 3	SIL 4
F2	-	-	SIL 1	SIL 3	SIL 3
F3	-	-	-	SIL 1	SIL 2
H	H0	H1	H2	H3	H4
L	L0	L1	L2	L3	L4
E	E0	E1	E2	E3	E4

3) การประเมินความเสี่ยง ด้วยวิธีกราฟความเสี่ยง (Risk Graph) เป็นการตรวจสอบระดับความเสี่ยงโดยการพิจารณาตามกราฟที่กำหนดตามเส้นระดับผลกระทบ ซึ่งการประยุกต์ใช้งานมีความละเอียดขึ้น [1] ดังภาพที่ 3

3.1) อัตราการเกิดเหตุ (W)

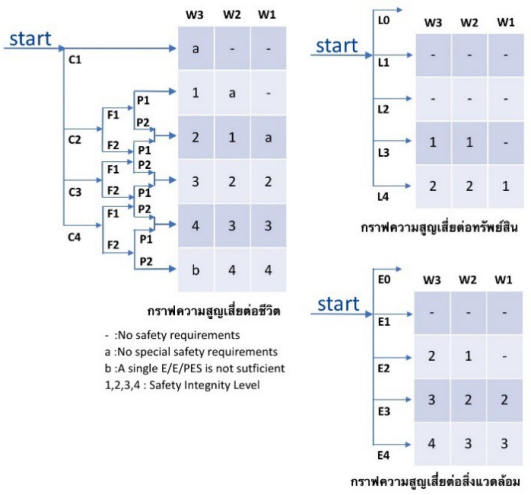
3.2) ผลกระทบต่อชีวิต (C)

3.3) ระยะเวลาในบริเวณอันตราย (F)

3.4) การเลี่ยงจากบริเวณอันตราย (P)

3.5) ความสูญเสียต่อทรัพย์สิน (L)

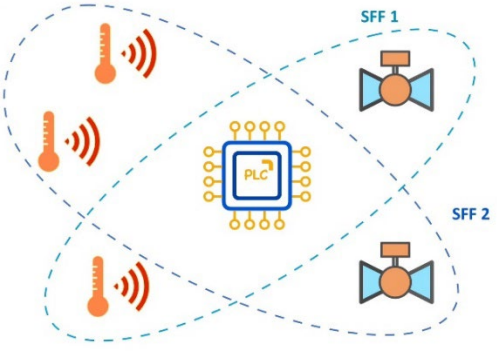
3.6) ความสูญเสียต่อสิ่งแวดล้อม (E)



ภาพที่ 3 กราฟความเสี่ยง (Risk Graph)

2.4 ฟังก์ชันวัดคุมนิรภัย (Safety Instrumented Function : SIF)

ระบบวัดคุมนิรภัยจะประกอบไปด้วย ระบบฟังก์ชันวัดคุมนิรภัย SIF หลายระบบ หรือระบบเดียว ดังภาพที่ 4



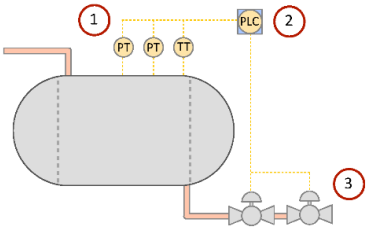
ภาพที่ 4 รูปแบบระบบฟังก์ชันวัดคุมนิรภัย

โดยแต่ละระบบฟังก์ชันวัดคุมนิรภัย SIF ประกอบด้วย 3 องค์ประกอบ ดังภาพที่ 5 ดังนี้

1) อุปกรณ์วัด (Sensors) ใช้ในการตรวจสอบสถานะที่ต้องการตรวจสอบ เช่น อุปกรณ์วัดอุณหภูมิ อุปกรณ์วัดแรงดัน อุปกรณ์วัดปริมาณ อุปกรณ์วัดอัตราการไหล เป็นต้น

2) อุปกรณ์ประมวลผล (Logic solver) ใช้ในการรับข้อมูลสถานะ และควบคุมการทำงานของระบบเมื่อเกิดเหตุ

3) อุปกรณ์สุดท้าย (Final elements) อุปกรณ์ควบคุม การเปิด-ปิดของวาล์วนิรภัย



ภาพที่ 5 อุปกรณ์ในระบบวัดคุมนิรภัย

รูปแบบการเชื่อมต่ออุปกรณ์ในระบบวัดคุมนิรภัย มีรูปแบบพื้นฐานของอุปกรณ์ที่ใช้กันอย่างแพร่หลายในการออกแบบระบบวัดคุมนิรภัย ซึ่งจะส่งผลต่อระดับความปลอดภัยของระบบ ดังภาพที่ 6 ดังนี้

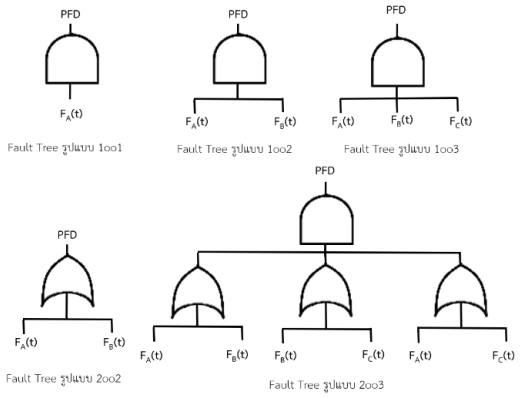
1) รูปแบบ 1oo1 (One out of One) ใช้อุปกรณ์ 1 ตัว ซึ่งเป็นระบบเบื้องต้นในการติดตั้ง

2) รูปแบบ 1oo2 (One out of Two) ใช้อุปกรณ์ 2 ตัวต่อแบบอนุกรม ใช้เป็นอุปกรณ์สำรอง 1 ตัว จะสามารถลดค่าความผิดพลาดอันตรายได้มากขึ้น แต่จะส่งผลต่อค่าความผิดพลาดนิรภัยมากขึ้น

3) รูปแบบ 1oo3 (One out of Three) ใช้อุปกรณ์ 3 ตัว ต่อแบบอนุกรม ใช้เป็นอุปกรณ์สำรอง 2 ตัว จะสามารถลดค่าความผิดพลาดอันตรายได้มากขึ้นกว่าเดิม ซึ่งจะส่งผลต่อค่าความผิดพลาดนิรภัยมากขึ้นเช่นกัน

4) รูปแบบ 2oo2 (Two out of Two) โดยรูปแบบนี้จะช่วยลดความผิดพลาดนิรภัย โดยใช้อุปกรณ์ 2 ตัว ต่อแบบขนาน เนื่องจากบางกระบวนการผลิตไม่ต้องการให้ระบบหยุดการทำงานโดยไม่เกิดเหตุขึ้น

5) รูปแบบ 2oo3 (Two out of Three) ใช้อุปกรณ์ 3 ตัว ต่อแบบอนุกรม และแบบขนาน ซึ่งจะสามารถลดค่าความผิดพลาดอันตรายได้ และช่วยลดค่าความผิดพลาดนิรภัยได้



ภาพที่ 6 รูปแบบพื้นฐานในการเชื่อมต่ออุปกรณ์

2.5 ความผิดพลาด (Failure Rate : λ)

ค่าความผิดพลาด พิจารณาจากอัตราความเสียหายของอุปกรณ์ต่อหนึ่งหน่วยเวลา โดยจะประเมินจากสถิติจำนวนอุปกรณ์ที่เสียหายในช่วงเวลาที่กำหนด หรือสามารถหาข้อมูลได้จากผู้ผลิต โดยแบ่งประเภทของความผิดพลาดได้ 2 ประเภท [1] ดังภาพที่ 7

1) ความผิดพลาดนิรภัย (Fail Safe : λ_S) หรือความปลอดภัยจากความผิดพลาด เป็นความผิดพลาดที่ไม่ส่งผลต่ออันตราย แต่จะส่งผลต่อการหยุดทำงานการผลิต แบ่งเป็น 2 ส่วน ได้แก่

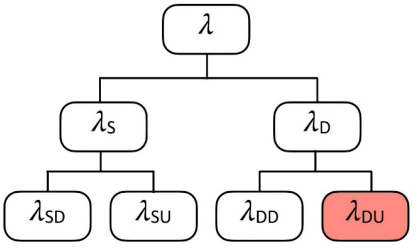
1.1) ความผิดพลาดนิรภัยที่ตรวจจับได้ (Safe Detected Failure : λ_{SD})

1.2) ความผิดพลาดนิรภัยที่ตรวจจับไม่ได้ (Safe Undetected Failure : λ_{SU})

2) ความผิดพลาดอันตราย (Fail Dangerous : λ_D) หรือความอันตรายจากความผิดพลาด เป็นความผิดพลาดที่ส่งผลต่ออุปกรณ์ไม่ทำงาน ก่อให้เกิดอันตรายต่อระบบ แบ่งเป็น 2 ส่วน ได้แก่

2.1) ความผิดพลาดอันตรายที่ตรวจจับได้ (Dangerous Detected Failure : λ_{DD})

2.2) ความผิดพลาดอันตรายที่ตรวจจับไม่ได้ (Dangerous Undetected Failure : λ_{DU}) เป็นความผิดพลาดที่อันตรายที่สุดเนื่องจากหากความผิดพลาดเกิดขึ้น และไม่มีการตรวจจับรายงาน มักจะเกิดจากความล้มเหลวในอุปกรณ์อย่างเงียบ ๆ



ภาพที่ 7 องค์ประกอบความผิดพลาด

2.6 ความผิดพลาดร่วม (Common Cause Failure : CCF)

ความผิดพลาดความล้มเหลวอุปกรณ์ที่เกิดจากสาเหตุร่วมกัน ซึ่งเกิดจากอุปกรณ์การเชื่อมต่อในรูปแบบต่าง ๆ การติดตั้งในบริเวณเดียวกัน หรือได้รับผลกระทบด้วยกัน เช่น อุณหภูมิ สภาพอากาศ จะส่งผลต่ออุปกรณ์โดยรอบตามความสัมพันธ์ โดยจะพิจารณาจากอัตราความผิดพลาดร่วมซึ่งสามารถหาได้จากค่าความสัมพันธ์ของอุปกรณ์ ตามมาตรฐาน IEC 61508-6 พิจารณาตามสมการที่ 10

2.7 ระยะเวลาในการออกแบบระบบนิรภัย

ระยะเวลาต่าง ๆ ดังภาพที่ 8 ที่นำมาพิจารณาการออกแบบระบบวัดคุมนิรภัย ประกอบไปด้วย

1) ระยะเวลาเฉลี่ยก่อนการเกิดความผิดพลาด (Mean Time To Failure: MTTF) ช่วงเวลาที่ใช้งานอุปกรณ์จนเกิดความผิดพลาดขึ้น หรือช่วงเวลาใช้งาน

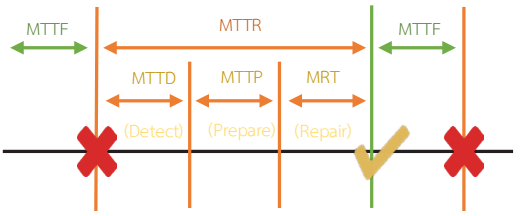
2) ระยะเวลาเฉลี่ยในการซ่อมแซมอุปกรณ์ (Mean Time To Restore: MTTR) ช่วงเวลาที่อุปกรณ์เกิดความผิดพลาดและซ่อมแซมจนสามารถใช้งานได้อีกครั้ง หรือช่วงเวลาซ่อมบำรุง

2.1) MTTD (Mean Time To Detect) ระยะเวลาเฉลี่ยที่ใช้ในการตรวจจับความผิดปกติหรือระบุอันตรายที่เกิดขึ้น

2.2) MTTP (Mean Time To Prepare) ระยะเวลาเฉลี่ยที่ใช้ในการเตรียมพร้อมก่อนทำการซ่อมแซม

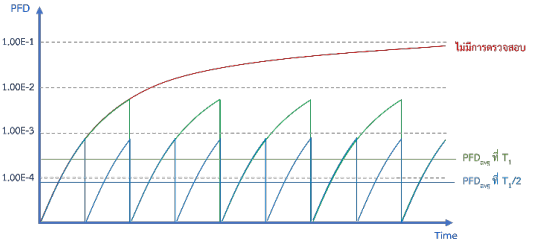
2.3) MRT (Mean Repair Time) ระยะเวลาเฉลี่ยที่ใช้ในการซ่อมแซมระบบให้กลับมาทำงานได้

3) ระยะเวลาเฉลี่ยระหว่างการเสียหาย (Mean Time Between Failure : MTBF) ช่วงเวลาตั้งแต่อุปกรณ์เกิดความล้มเหลวครั้งแรก จนถึงครั้งที่สอง



ภาพที่ 8 ระยะเวลาในการออกแบบระบบนิรภัย

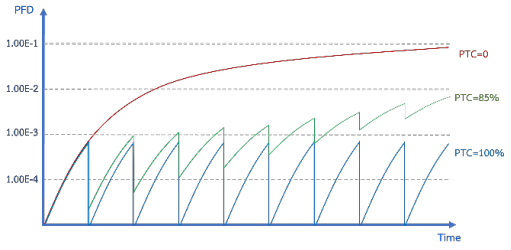
4) เวลาในการตรวจสอบ Proof test (Ti) ต่ออุปกรณ์ตามเวลาที่กำหนด เพื่อตรวจสอบความผิดพลาดในการทำงาน ซึ่งมีผลต่อระดับความปลอดภัยดังภาพที่ 9



ภาพที่ 9 เวลาในการตรวจสอบ Proof Test

2.8 การวัดความครอบคลุมของการทดสอบ (Proof Test Coverage : PTC)

การตรวจสอบอุปกรณ์ในระบบวัดคุมนิรภัย เพื่อตรวจสอบระบบและบำรุงรักษาอุปกรณ์ โดยการตรวจสอบอาจไม่สามารถตรวจสอบได้ครอบคลุมทั้งหมด เนื่องจากในระหว่างการตรวจสอบไม่สามารถหยุดกระบวนการ หรือไม่มีอุปกรณ์ในการตรวจสอบที่ครอบคลุม ซึ่งจะส่งผลต่อระดับอันตรายที่อาจเกิดขึ้น ดังภาพที่ 10



ภาพที่ 10 ระดับอันตราย และระยะเวลาแปรผันตามตามร้อยละการตรวจสอบครอบคลุม

2.9 ความน่าจะเป็นความล้มเหลว ต่อระยะเวลา (Probability of Failure on Demand : PFD)

พิจารณาตามค่าความน่าเชื่อถือ และค่าความผิดพลาดของอุปกรณ์ [1]

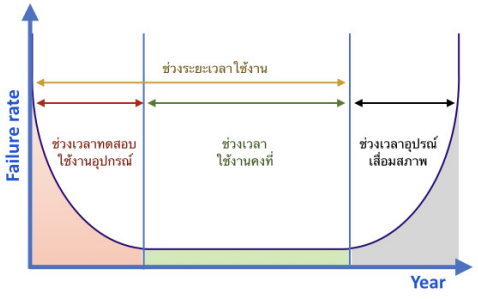
$$F(t) = 1-R(t) \quad (1)$$

เมื่อ F(t) คือ ค่าความผิดพลาด

R(t) คือ ค่าความน่าเชื่อถือ

โดยการกระจายความผิดพลาดของอุปกรณ์จะมีลักษณะเป็นกราฟรูปอ่างน้ำ โดยค่าความผิดพลาดจะแบ่งเป็น 3 ช่วง ดังภาพที่ 11

1) ช่วงทดสอบใช้อุปกรณ์
2) ช่วงระหว่างการใช้งาน
3) ช่วงเสื่อมสภาพของอุปกรณ์



ภาพที่ 11 กราฟระดับค่าความผิดพลาดต่อช่วงเวลาในการทำงาน [1]

ซึ่งจะพิจารณาความผิดพลาดในช่วงที่ 1 และ 2 เนื่องจากเป็นความเชื่อมั่นในระหว่างการทำงาน

$$R(t) = 1 - \lambda t \quad (2)$$

$$F(t) = \lambda t \quad (3)$$

จากสมการดังกล่าวสามารถหาค่าเฉลี่ยความน่าจะเป็นของความล้มเหลว โดยแบ่งเป็น 2 ประเภท

1) การคำนวณค่าความผิดพลาดอันตรายเฉลี่ยในระบบวัดคุมนิรภัย PFDavg ในระบบความเสี่ยงต่ำ

$$\mathrm{PFD_{avg}} = \frac{1}{T}\int_0^T \mathrm{PFD}\,dt = \frac{1}{T}\int_0^T F(t)dt \quad (4)$$

จากสมการที่ 4 พิจารณาสมการแต่ละรูปแบบพื้นฐานตามมาตรฐาน IEC 61508 ในระบบความเสี่ยงต่ำ [3]

$$PFD_{avg(1oo1)} = (\lambda_{DD}+ \lambda_{DU})t_{CE} \quad (5)$$

$$PFD_{avg(1oo2)} = 2((1- \beta_D)\lambda_{DD}+ (1- \beta)\lambda_{DU})^2 *t_{CE}\ t_{GE}+C_{CF} \quad (6)$$

$$PFD_{avg(1oo3)} = 6((1- \beta_D)\lambda_{DD} + (1- \beta)\lambda_{DU})^3 *t_{CE}\ t_{GE}\ t_{G2E}+C_{CF} \quad (7)$$

$$PFD_{avg(2oo2)} = 2(\lambda_{DD}+ \lambda_{DU})t_{CE} \quad (8)$$

$$PFD_{avg(2oo3)} = 6((1- \beta_D)\lambda_{DD}+ (1- \beta)\lambda_{DU})^2 *t_{CE}\ t_{GE}+C_{CF} \quad (9)$$

$$C_{CF} = \beta_D\lambda_{DD}\ MTTR+\beta\lambda_{DU}(PTC)(T_1/2+MRT) + \beta\lambda_{DU}(1-PTC)(T_2/2+MRT) \quad (10)$$

$$t_{CE} = (\lambda_{DU}/\lambda_D)(PTC)(T_1/2+MRT) + (\lambda_{DU}/\lambda_D)(1-PTC)(T_2/2+MRT) + (\lambda_{DD}/\lambda_D)MTTR \quad (11)$$

$$t_{GE} = (\lambda_{DU}/\lambda_D)(PTC)(T_1/3+MRT) + (\lambda_{DU}/\lambda_D)(1-PTC)(T_2/3+MRT) + (\lambda_{DD}/\lambda_D)MTTR \quad (12)$$

$$t_{G2E} = (\lambda_{DU}/\lambda_D)(PTC)(T_1/4+MRT) + (\lambda_{DU}/\lambda_D)(1-PTC)(T_2/4+MRT) + (\lambda_{DD}/\lambda_D)MTTR \quad (13)$$

2) การคำนวณค่าความผิดพลาดอันตรายในระบบวัดคุมนิรภัย PFH ในระบบความเสี่ยงสูง ซึ่งจะนำการหาค่าสูงสุดเฉลี่ยระยะเวลาตรวจสอบ

$$PFH_{avg} = \frac{PFD}{T} \quad (14)$$

จากสมการที่ 13 พิจารณาสมการแต่ละรูปแบบพื้นฐานตามมาตรฐาน IEC 61508 ในระบบความเสี่ยงสูง [3]

$$PFH_{avg(1oo1)} = \lambda_{DU} \quad (15)$$

$$PFH_{avg(1oo2)} = 2((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}) *((1-\beta)\lambda_{DU})t_{CE} + \beta\lambda_{DU} \quad (16)$$

$$PFH_{avg(1oo3)} = 6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})^2 *((1-\beta)\lambda_{DU})t_{CE}\, t_{GE} + \beta\lambda_{DU} \quad (17)$$

$$PFH_{avg(2oo2)} = 2\,\lambda_{DU} \quad (18)$$

$$PFH_{avg(2oo3)} = 6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}) *((1-\beta)\lambda_{DU})t_{CE} + \beta\lambda_{DU} \quad (19)$$

2.10 อัตราความผิดพลาดนิรภัย (Safe Failure Fraction : SFF)

อัตราความผิดพลาดนิรภัย หรืออัตราความน่าเชื่อถือของอุปกรณ์ที่จะไม่เกิดความผิดพลาดอันตรายที่ตรวจจับไม่ได้ โดยพิจารณาระดับค่า SIF ตามสมการที่ 20 เทียบกับระดับความเสี่ยงในกระบวนการอุตสาหกรรม ซึ่งแบ่งอุปกรณ์เป็น 2 ประเภท

1) อุปกรณ์ Type A อุปกรณ์เครื่องมือวัดพื้นฐาน เช่น ตัวต้านทาน ขดลวด คาปาซิเตอร์ ไดโอด ทรานซิสเตอร์ ไทริสเตอร์ เป็นต้น ซึ่งอุปกรณ์เหล่านี้สามารถใช้งานได้ระยะเวลานาน และสามารถตรวจสอบอุปกรณ์ได้

2) อุปกรณ์ Type B อุปกรณ์เครื่องมือวัดสมัยใหม่ มีส่วนประกอบชิ้นส่วนวงจรร่วม เช่น PLC Microprocesser Intergrate Circuit:IC เป็นต้น ซึ่งอุปกรณ์เหล่านี้ไม่สามารถใช้งานได้ระยะเวลานาน และไม่สามารถตรวจสอบอุปกรณ์ได้สมบูรณ์

$$SFF = \frac{\lambda_{DD}+\lambda_{SD}+\lambda_{SU}}{\lambda_{DD}+\lambda_{DU}+\lambda_{SD}+\lambda_{SU}} * 100 \quad (20)$$

การพิจารณาหาจำนวนอุปกรณ์สำรอง อุปกรณ์ทั้ง 2 ประเภท จะมีการพิจารณาที่แตกต่างกัน ดังนี้

ตารางที่ 4 จำนวนอุปกรณ์สำรองอัตราความผิดพลาดนิรภัยอุปกรณ์ชนิด Type A [3]

Safe Failure Fraction SFF	Hardware fault tolerance (Type A)		
	0	1	2
SFF < 60%	SIL 1	SIL 2	SIL 3
60% ≤ SFF <90%	SIL 2	SIL 3	SIL 4
90% ≤ SFF <99%	SIL 3	SIL 4	SIL 4
99% ≤ SFF	SIL 4	SIL 4	SIL 4

ตารางที่ 5 จำนวนอุปกรณ์สำรองอัตราความผิดพลาดนิรภัยอุปกรณ์ชนิด Type B [3]

Safe Failure Fraction SFF	Hardware fault tolerance (Type B)		
	0	1	2
SFF < 60%	X	SIL 1	SIL 2
60% ≤ SFF <90%	SIL 1	SIL 2	SIL 3
90% ≤ SFF <99%	SIL 2	SIL 3	SIL 4
99% ≤ SFF	SIL 3	SIL 4	SIL 4

3. ผลการดำเนินงาน

โปรแกรมคำนวณจะแบ่งเป็น 3 ส่วน ตามลำดับ ดังภาพที่ 12 และหน้าต่างการใช้งานดังภาพที่ 13

1) การคำนวณระดับความเสี่ยงในอุตสาหกรรม แบ่งเป็น 3 วิธี LOPA, Matrix และ Graph

2) การคำนวณข้อมูลเพิ่มเติม

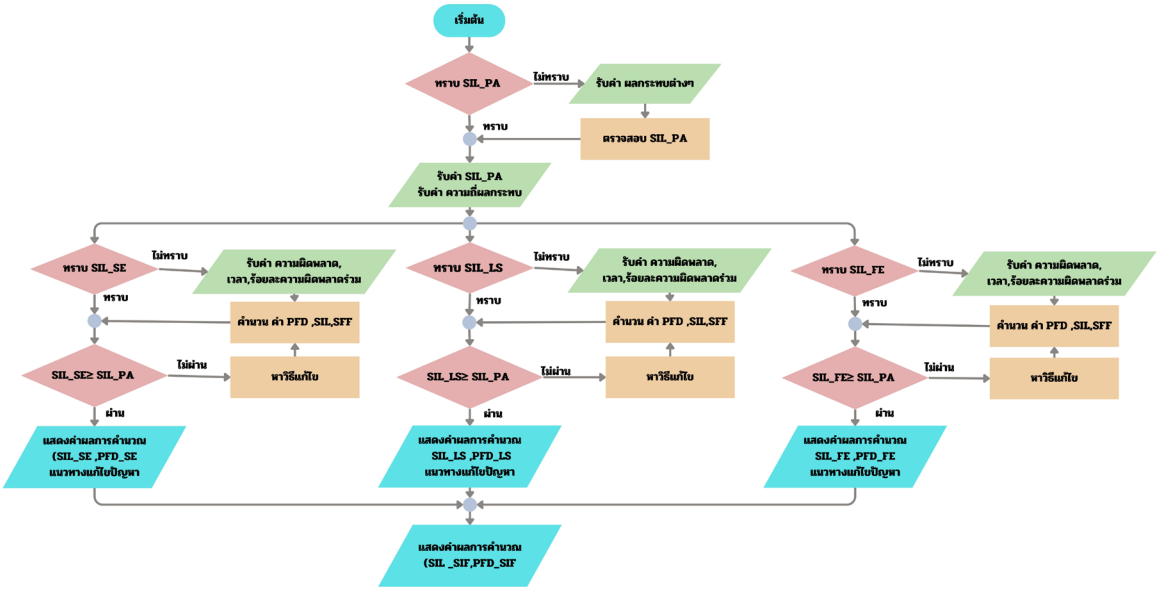
2.1) ค่าร้อยละอัตราความผิดพลาดร่วม

2.2) ค่าความผิดพลาดของอุปกรณ์ระบบประมวลผล ให้ค่าความผิดพลาดในแต่ละอุปกรณ์ย่อย

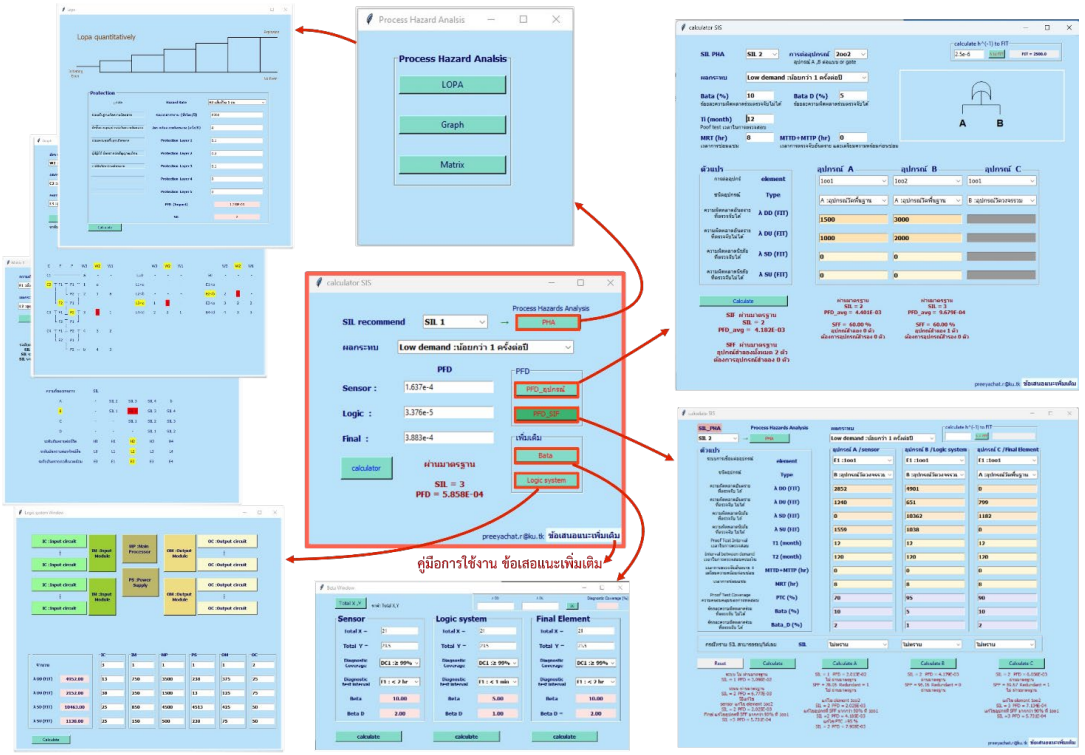
3) การประมวลผล

3.1) ระดับฟังก์ชันวัดคุมนิรภัย (SIF)

3.2) อัตราความผิดพลาดนิรภัย (SFF)



ภาพที่ 12 การออกแบบโปรแกรมวัดคุมนิรภัย

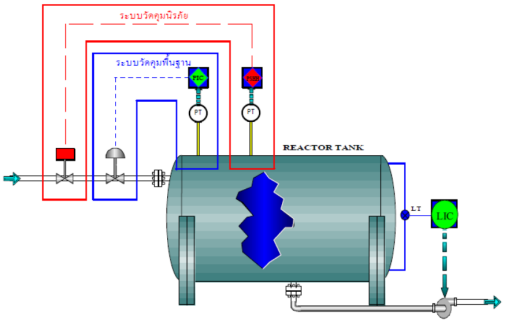


ภาพที่ 13 โปรแกรมคำนวณระบบวัดคุมนิรภัย

4. ตัวอย่างการคำนวณ

4.1 การหาค่าระดับความเสี่ยงในกระบวนการอุตสาหกรรม

ระบบการฆ่าเชื้อในโรงงานอุตสาหกรรม โดยก๊าซคลอรีน ซึ่งต้องควบคุมแรงดันในถังบรรจุสารเคมี มีความเสี่ยงสูงของการระเบิดและการรั่วไหลของสารเคมีอันตราย หากสูดดมหรือสัมผัสสารโดยตรงจะส่งผลให้เกิดอาการหายใจติดขัด วิงเวียนศีรษะ กัดกร่อนดวงตา ผิวหนัง และทางเดินหายใจ ซึ่งคลอรีนมีจุดเดือดต่ำที่ต้องรักษาแรงดันและควบคุมอัตราการไหล ดังภาพที่ 14 [6]



ภาพที่ 14 กระบวนการควบคุมการไหลและแรงดัน [6]

1) ความผิดพลาดที่อาจจะเกิดขึ้น

1.1) พนักงานควบคุมผิดพลาด 0.07 ครั้งต่อปี

1.2) มอเตอร์ขัดข้อง 0.3023 ครั้งต่อปี

1.3) อุปกรณ์วัดแรงดันชำรุด 0.6321 ครั้งต่อปี

1.4) สวิตช์ควบคุมผิดพลาด 0.1307 ครั้งต่อปี

1.5) เวลาที่กระบวนการผลิตทำงาน 8,760 ชั่วโมงต่อปี

2) อันตรายที่อาจจะเกิดขึ้น

2.1) อัตราการจากการเกิดเหตุการณ์ เกิดขึ้น 10 ปีต่อครั้ง (W2)

2.2) ผลกระทบต่อชีวิตคน หากเกิดเหตุส่งผลให้มีผู้เสียชีวิต 1 คน และผู้บาดเจ็บ 10 คน (C2)

2.3) ระยะเวลาในบริเวณอันตราย ผู้ปฏิบัติงานต้องอยู่มากกว่าครึ่งวัน (F2)

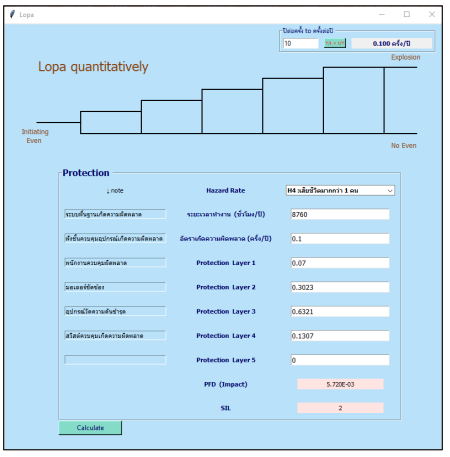
2.4) การหลีกเลี่ยงจากบริเวณอันตรายสามารถหลีกเลี่ยงเหตุการณ์ที่จะเกิดขึ้นได้ (P1)

2.5) เกิดความสูญเสียต่อทรัพย์สินจำนวนมากและต้องหยุดกระบวนการผลิตเป็นเวลาสั้นๆ (L3)

2.6) ความเสียหายต่อสิ่งแวดล้อม กระทบต่อสิ่งแวดล้อมชั่วคราวแต่ออกไปภายนอกขอบเขต (E3)

4.1.1 การคำนวณด้วยวิธี LOPA

พิจารณาค่าระยะเวลาในการทำงาน และโอกาสที่จะเกิดความผิดพลาดในแต่ละส่วนที่อาจจะเกิดขึ้น เช่น พนักงานควบคุมผิดพลาด มอเตอร์ขัดข้อง อุปกรณ์วัดแรงดันชำรุด สวิตช์ควบคุมผิดพลาด เป็นต้น

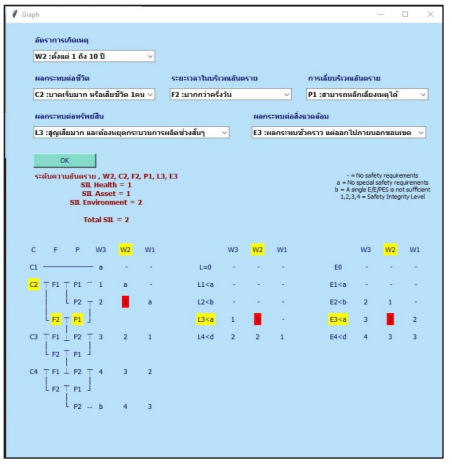


ภาพที่ 15 การคำนวณระดับอันตรายด้วยวิธี LOPA

จากการคำนวณโดยโปรแกรมค่าระดับอันตรายของระบบ มีค่าเท่ากับ SIL 2 ดังภาพที่ 15

4.1.2 การคำนวณด้วยวิธี Graph

พิจารณาจากค่าอัตราการเกิดเหตุ ผลกระทบต่อชีวิต ระยะเวลาในบริเวณอันตราย การหลีกเลี่ยงจากบริเวณที่เกิดเหตุ ความสูญเสียต่อทรัพย์สิน และความสูญเสียต่อสิ่งแวดล้อม

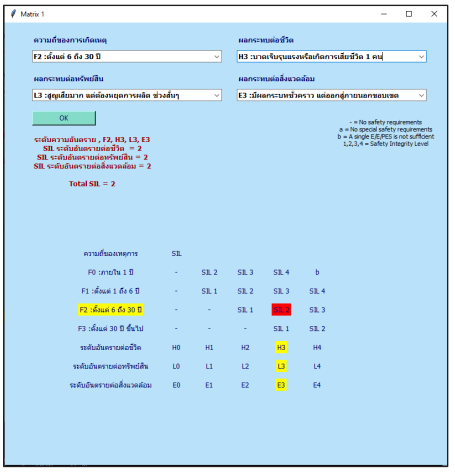


ภาพที่ 16 การคำนวณระดับอันตรายด้วยวิธี Graph

จากการคำนวณโดยโปรแกรมค่าระดับอันตรายของระบบ มีค่าเท่ากับ SIL 2 ดังภาพที่ 16

4.1.3 การคำนวณด้วยวิธี Matrix

พิจารณาจากค่าอัตราการเกิดเหตุ ผลกระทบต่อชีวิต ความสูญเสียต่อทรัพย์สิน และความสูญเสียต่อสิ่งแวดล้อม



ภาพที่ 17 การคำนวณระดับอันตรายด้วยวิธี Matrix

จากการคำนวณโดยโปรแกรมค่าระดับอันตรายของระบบ มีค่าเท่ากับ SIL 2 ดังภาพที่ 17 จะเห็นว่าแต่ละวิธีจะมีข้อดีข้อเสีย และวิธีที่เหมาะสมจะขึ้นอยู่กับบริบทและข้อมูลในการนำมาประเมินความเสี่ยง

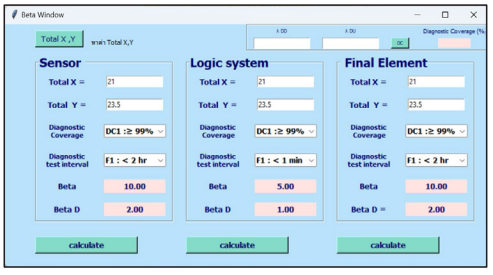
4.2 การคำนวณข้อมูลเพิ่มเติม

1) การคำนวณค่าอัตราความผิดพลาดร่วม (β) ตัวอย่างเช่น ระบบการฆ่าเชื้อในโรงงานอุตสาหกรรมโดยก๊าซคลอรีน ในพื้นที่ดังกล่าวมีความร้อน ซึ่งอาจจะส่งผลกระทบร่วมของอุปกรณ์ ตัวอย่างการคำนวณหาค่าอัตราความผิดพลาด [3] ดังตารางที่ 6

ตารางที่ 6 ตัวอย่างรายการค่า X และ Y อุปกรณ์อิเล็กทรอนิกส์ จากตารางความสัมพันธ์ มาตรฐาน IEC 61508-6

หมวดหมู่	ระบบมีการทดสอบการวินิจฉัยทีดี	
	X	Y
การแบ่งแยก	3.5	1.5
ความหลากหลายซ้ำซ้อน	2.00	1.00
เทคนิค ประสบการณ์	2.75	2.25
การวิเคราะห์ข้อมูล	0.25	4.75
การสัมผัสกับบุคคล	3.50	3.00
การฝึกอบรม วัฒนธรรม	1.25	3.75
การควบคุมสภาพแวดล้อม	2.75	2.25
การตรวจสอบสภาพแวดล้อม	5.00	5.00

กำหนดให้พิจารณาค่า Total X และ Total Y จากตารางความสัมพันธ์ ให้มีค่าเท่ากันทุกระบบและมีค่าระดับการวินิจฉัยที่ดี



ภาพที่ 18 พิจารณาที่ Good Diagnostic Test

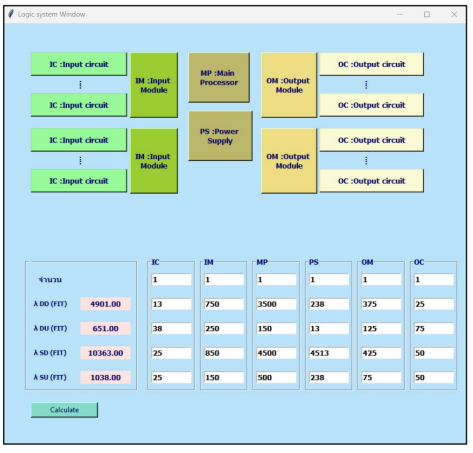
จากโปรแกรมจะช่วยในการคำนวณหาค่าอัตราความผิดพลาดร่วมของระบบ sensor และ Final Element ได้ค่า Bata = 10 % และ Bata D = 2% และ Logic system ค่า Bata = 5 % และ Bata D = 1 % ดังภาพที่ 18 ซึ่งการตรวจสอบแต่ละ

อุปกรณ์อาจมีค่า Total X และ Total Y ไม่เท่ากัน ขึ้นอยู่กับความสัมพันธ์ของการติดตั้ง และตรวจสอบระบบนั้น ๆ

2) การหาค่าอัตราความผิดพลาดรวมระบบ logic system กรณีผู้ผลิตให้ค่าความผิดพลาดแต่ละอุปกรณ์ภายใน เนื่องจากการต่อใช้งาน logic system ในแต่ละระบบฟังก์ชันวัดคุมนิรภัย อาจใช้งานหลายระบบฟังก์ชันวัดคุมนิรภัย และใช้งานบางช่อง ตัวอย่างการหาค่าความผิดพลาดรวมของระบบ logic system [7] ดังตารางที่ 7

ตารางที่ 7 ตัวอย่างจำนวนค่าความผิดพลาดในแต่ละอุปกรณ์ย่อยของระบบประมวลผล

อุปกรณ์	จำนวน	λ_{DD}	λ_{DU}	λ_{SD}	λ_{SU}
IC	1	13	38	25	25
IM	1	750	250	850	150
MP	1	3500	1500	4500	500
PS	1	238	13	4513	238
OM	1	375	125	425	75
OC	1	25	75	50	50



ภาพที่ 19 การหาค่าความผิดพลาด Logic system

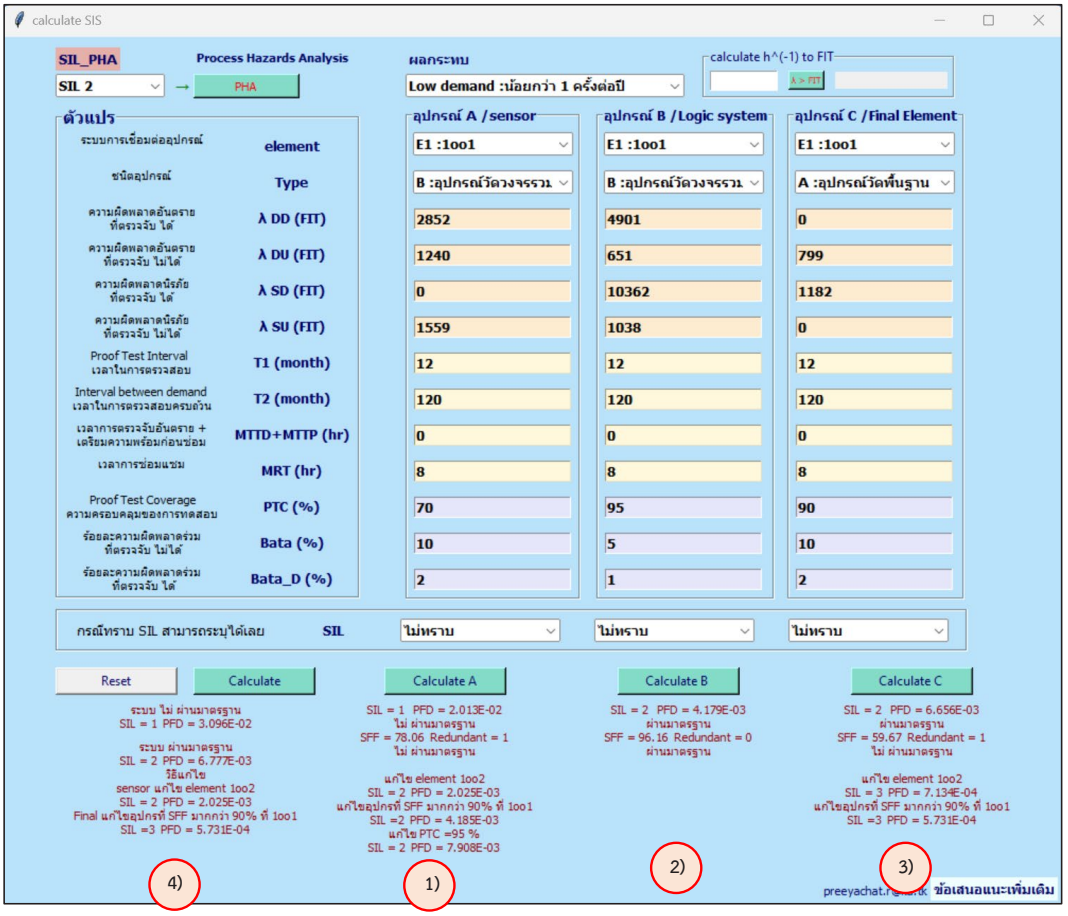
พิจารณาจำนวนและค่าความผิดพลาดในแต่ละอุปกรณ์ย่อย จากโปรแกรมจะช่วยในการคำนวณหาค่าความน่าจะเป็นที่จะเกิดความผิดพลาดอันตรายในแต่ละประเภทในหน่วย FIT ดังภาพที่ 19 โดยมีค่า λ_{DD} เท่ากับ 4,901 FIT λ_{DU} เท่ากับ 651 FIT λ_{SD} เท่ากับ 10,363 FIT และ λ_{SU} เท่ากับ 1,038 FIT

4.3 การคำนวณหาค่า SIF และ SFF

ตัวอย่างการคำนวณหาค่าระบบฟังก์ชันวัดคุมนิรภัย และอัตราค่าความผิดพลาดนิรภัย โดยจะพิจารณาระดับอันตรายจากกระบวนการฆ่าเชื้อในโรงงานอุตสาหกรรม โดยก๊าซคลอรีนอยู่ที่ SIL 2 มีค่าอัตราความผิดพลาดร่วมจากการคำนวณตามภาพที่ 19 และค่าความผิดพลาดในแต่ละอุปกรณ์ดังตารางที่ 8 โดยนำข้อมูลดังกล่าวลงสู่โปรแกรม

ตารางที่ 8 ตัวอย่างค่าความผิดพลาดอุปกรณ์ในกระบวนการ

รายละเอียดอุปกรณ์	Sensor	Safety PLC	Valae
element	1oo1	1oo1	1oo1
Type	B	B	A
λ_{DD}	2,852	4,091	0
λ_{DU}	1,240	651	799
λ_{SD}	0	10,363	1,182
λ_{SU}	1,559	1,038	0
T_1 (month)	12	12	12
T_2 (month)	120	120	120
MRT	8	8	8
PTC	70	95	90



ภาพที่ 20 การหาค่า SIF และ SFF

จากโปรแกรมจะช่วยคำนวณหาค่า SIL ดังภาพที่ 20 โดยพิจารณาค่าระดับอันตรายที่ SIL 2 ผลคำนวณ ดังนี้

1) ระบบ sensor มีการต่อแบบ 1oo1 เป็นอุปกรณ์ชนิด B มีอุปกรณ์ทั้งหมด 1 ตัว ค่า SFF มีค่าเท่ากับ 78.06 % ตามมาตรฐานต้องการอุปกรณ์สำรอง 1 ตัว และค่า PFDavg = 2.013E-2 ระดับความปลอดภัย SIL1

ดังนั้นระบบ Sensor มีค่า SFF และ SIL ไม่ผ่านมาตรฐาน โดยโปรแกรมจะแนะนำการแก้ไขเบื้องต้นโดยการเพิ่มเติมอุปกรณ์สำรองอีก 1 ตัว ต่อแบบ 1oo2 ส่งผลให้ระดับค่า SFF ผ่านมาตรฐาน และระดับความปลอดภัย เท่ากับ SIL2 ผ่านมาตรฐาน

2) ระบบ Logic system มีการต่อแบบ 1oo1 เป็นอุปกรณ์ชนิด B มีอุปกรณ์ทั้งหมด 1 ตัว ค่า SFF มีค่าเท่ากับ 96.16 % ตามมาตรฐานไม่ต้องการอุปกรณ์สำรอง และค่า PFDavg = 4.179E-3 ระดับความปลอดภัย SIL2

ดังนั้นระบบ Logic system มีค่า SFF และ SIL ผ่านมาตรฐาน

3) ระบบ Final Element มีการต่อแบบ 1oo1 เป็นอุปกรณ์ชนิด A มีอุปกรณ์ทั้งหมด 1 ตัว ค่า SFF มีค่าเท่ากับ 59.67 % ตามมาตรฐานต้องการอุปกรณ์สำรอง 1 ตัว และค่า PFDavg = 2.656E-3 ระดับความปลอดภัย SIL2

ดังนั้น ระบบ Final Element มีค่า SIL ผ่านมาตรฐาน แต่ SFF ไม่ผ่านมาตรฐาน โดยโปรแกรมจะแนะนำการแก้ไขเบื้องต้นโดยการ เพิ่มเติมอุปกรณ์สำรองอีก 1 ตัว ต่อแบบ 1oo2 ผ่านมาตรฐาน

4) ผลรวมค่า PFD_{avg} = 3.096E-2 ค่าระดับความปลอดภัยรวมเท่ากับ SIL 1 ซึ่งมีค่าน้อยกว่าระดับอันตราย โดยหากแก้ไขตามที่โปรแกรมแนะนำข้างต้น จะสามารถแก้ไขค่า PFDavg = 6.777E-3 ระดับความปลอดภัย SIL2 ผ่านมาตรฐาน

5. สรุปผลการศึกษา

การศึกษาได้พัฒนาโปรแกรมคอมพิวเตอร์ในการคำนวณระบบวัดคุมนิรภัย ตามมาตรฐาน IEC 61508/61511 เพื่อช่วยในการคำนวณหาค่าความเสี่ยงในกระบวนการอุตสาหกรรม จากตัวอย่างการคำนวณกระบวนการฆ่าเชื้อในโรงงานอุตสาหกรรมโดยก๊าซคลอรีนจะเห็นได้ว่าสามารถช่วยในการหาค่าระดับความเสี่ยง 3 วิธีพื้นฐาน LOPA, Matrix และ Graph ซึ่งสามารถคำนวณหาความเสี่ยงเท่ากับ SIL 2 โดยผู้ใช้งานสามารถเลือกใช้ได้ตามความเหมาะสม และการตรวจสอบระดับฟังก์ชันวัดคุมนิรภัย SIF พบว่าอุปกรณ์ มีค่าระดับ SIL และ SFF ไม่ผ่านมาตรฐาน และFinal Element มีค่า SFF ไม่ผ่านมาตรฐาน เช่นเดียวกับระดับ SIL ไม่ผ่านมาตรฐาน โดยโปรแกรมแนะนำให้เพิ่มอุปกรณ์สำรองของระบบและ Final Element อีกอย่างละ 1 ตัว ต่อแบบ 1oo2 จะส่งผลให้ ระดับ SIL และ SFF ผ่านมาตรฐาน จากตัวอย่างการคำนวณจะช่วยลดระยะเวลาการคำนวณ การตรวจสอบออกแบบระบบวัดคุมนิรภัย ลดความผิดพลาดจากการคำนวณ และช่วยหาแนวทางการแก้ไขปัญหาการออกแบบระบบวัดคุมนิรภัยดังกล่าว โดยสามารถดาวน์โหลดโปรแกรมใช้งานและเอกสารเพิ่มเติมได้ตาม QR-Code ดังภาพที่ 21

https://bit.ly/4b5CZ7r

ภาพที่ 21 QR Code โปรแกรมระบบวัดคุมนิรภัย

6. กิตติกรรมประกาศ

บทความนี้ได้รับการสนับสนุนจากโครงการปริญญาโท สาขาวิศวกรรมความปลอดภัย

7. เอกสารอ้างอิง

[1] ทวิช ชูเมือง (2548). ระบบวัดคุมนิรภัยในอุตสาหกรรมกระบวนการผลิต. กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

[2] ทวิช ชูเมือง (2551). การกำหนดค่าระดับความปลอดภัยสำหรับฟังก์ชันนิรภัย. กรุงเทพฯ :วีพริ้นท์.

[3] International Electrotechnical Commission .Functional safety of electrical/ electronic/programmable electronic safety-related systems ,IEC 61508,2010-04

[4] International Electrotechnical Commission .Functional safety – Safety instrumented systems for the process industry sector ,IEC 61511,2003-03

[5] Ronald J. WILLEY (2014). Layer of Protection Analysis .International Symposium on Safety Science and Technology, 84 : 12-22.

[6] ปิยวรรธน์ นิใจ (2559). การวิเคราะห์ความเสี่ยงของกระบวนการทำงานระหว่างคนกับหม้อต้มไอน้ำชีวมวล ในอุตสาหกรรมผลิตเส้นใยสังเคราะห์ โดยเทคนิควิเคราะห์ความผิดพลาดแบบแผนภูมิต้นไม้. วิทยานิพนธ์ปริญญาโท มหาวิทยาลัยเกษตรศาสตร์.

[7] William M. Goble Harry Cheddie (2005). Safety Instrumented Systems Verification: Practical Probabilistic Calculations ,NC :ISA Instrumentation Systems and Automation Society