วิธีการตรวจสอบค่าระดับความปลอดภัยของฟังก์ชั่นวัดคุมนิรภัยสำหรับวาล์วลดความดันในท่อส่งแก๊สโดยใช้วิธีการโมเดลมาร์คอฟ

SIL VERIFICATION OF SAFETY INSTRUMENTED FUNCTION FOR BLOCK VALVE IN GAS PIPLINE BY USING MARKOV MODEL METHODOLOGY

ปวริศา กองทอง

PAWARISA KONGTONG

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมการวัดคุม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2560

KMITL-2017-EN-M-060-093

วิธีการตรวจสอบค่าระดับความปลอดภัยของฟังก์ชั่นวัดคุมนิรภัยสำหรับวาล์วลดความดันในท่อส่งแก๊สโดยใช้วิธีการโมเดลมาร์คอฟ

SIL VERIFICATION OF SAFETY INSTRUMENTED FUNCTION FOR BLOCK VALVE IN GAS PIPLINE BY USING MARKOV MODEL METHODOLOGY

ปวริศา กองทอง

PAWARISA KONGTONG

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมการวัดคุม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2560

KMITL-2017-EN-M-060-093

SIL VERIFICATION OF SAFETY INSTRUMENTED FUNCTION FOR BLOCK VALVE IN GAS PIPLINE BY USING MARKOV MODEL METHODOLOGY

PAWARISA KONGTONG

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN INSTRUMENT ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2017

KMITL-2017-EN-M-060-093

คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ วิธีตรวจสอบค่าระดับความปลอดภัยของฟังก์ชั่นวัดคุมนิรภัยสำหรับวาล์วลดความดันในท่อส่งแก๊สโดยใช้วิธีการโมเดลมาร์คอฟ

Thesis Title SIL Verification of Safety Instrumented Function for Block Valve in Gas Pipline by using Markov Model Methodology

นักศึกษา นางสาวปวริศา กองทอง

รหัสประจำตัว 55611752

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมการวัดคุม

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.สักรียา ชิตวงศ์

หมายเลขวิทยานิพนธ์ KMITL-2017-EN-M-060-093

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.ฟูศักดิ์	ชีวสุวิทย์	
รศ.ดร.วิทยา	ทิพย์สุวรรณพร	
ผศ.ดร.พงษ์ชัย	นิลาศ	
รศ.ทรงชัย	วีระทวีมาศ	
รศ.สักรียา	ชิตวงศ์	

วัน / เดือน/ ปี ที่สอบ วันอังคารที่ 18 กรกฎาคม พ.ศ. 2560 เวลา 15.00-17.00 น.
สถานที่สอบ ณ อาคาร A ชั้น 5 ห้องประชุม 3

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร. คมสัน มาลีสี)
คณบดี คณะวิศวกรรมศาสตร์
วันที่ 18 กรกฎาคม พ.ศ. 2560

หัวข้อวิทยานิพนธ์	วิธีการตรวจสอบค่าระดับความปลอดภัยของฟังก์ชั่นวัดคุมนิรภัย สำหรับวาล์วลดความดันในท่อส่งแก๊สโดยใช้วิธีการโมเดลมาร์คอฟ
นักศึกษา	นางสาวปวริศา กองทอง
รหัสประจำตัว	5511752
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมการวัดคุม
พ.ศ.	2560
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.สักรียา ชิตวงศ์

บทคัดย่อ

ในงานวิจัยนี้เป็นการนำเสนอวิธีการในการคำนวณหาค่าระดับความปลอดภัย (Safety Integrity Level, SIL) ซึ่งมีความสำคัญในการออกแบบระบบนิรภัย ของระบบวาล์วลดความดันในท่อส่งก๊าซ โดยใช้วิธีโมเดลมาร์คอฟ (Markov Model) ซึ่งอ้างอิงตามมาตรฐานสากล IEC 61508 / 61511 เหตุผลในการนำวิธีการโมเดลมาร์คอฟมาใช้ ในงานวิจัยนี้ โมเดลมาร์คอฟเป็นวิธีการที่ใช้เวลาน้อยและมีความยืดหยุ่นมากกว่าวิธีการอื่นในการหาค่าระดับความปลอดภัย วิธีโมเดลมาร์คอฟนี้จะใช้วิธีการเชิงคุณภาพที่แสดงให้เห็นความน่าจะเป็นค่าเฉลี่ยของค่าความผิดพลาด (PFDavg) และเวลาในการซ่อมจากโมเดลมาร์คอฟที่จะใช้ปรับปรุงกระบวนการผลิตต่อไป

Thesis	SIL Verification of Safety Instrumented Function for Block Valve in Gas Pipeline by Using Markov Model Methodology
Student	Miss Pawarisa Kongtong
Student ID.	5511752
Degree	Master of Engineering
Program	Instrumentation Engineering
Year	2017
Thesis Advisor	Assoc. Prof. Sakriya Chitwong

ABSTRACT

This paper presents about methods methods of safety integrity level (SIL) verification which is significant to safety system design of block valve system in gas pipeline by using Markov Model method which refer to International standard IEC 61508/61511. The reason of using Markov Model method is that it takes less time and more flexible than other methods to determine SIL. This method uses a qualitative approach showing Average Probability of Failure (PFDavg) rate data and repairing time from model to implement in further process.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ได้ดำเนินการจนสำเร็จลุล่วงไปได้ เนื่องจากความกรุณาให้คำปรึกษา ความช่วยเหลือ ให้ความรู้ คำแนะนำ ชี้แนะแนวทางการแก้ไขปัญหา รวมทั้งยังสอนให้ข้าพเจ้ารู้จักคิดวิเคราะห์เพื่อแก้ไขปัญหาต่างๆ ตลอดจนให้ความรู้และประสบการณ์ที่ดีแก่ข้าพเจ้าจากรองศาสตราจารย์ สักรียา ชิตวงศ์ ซึ่งเป็นอาจารย์ผู้ควบคุมวิทยานิพนธ์ ข้าพเจ้ารู้สึกซาบซึ้งในความอนุเคราะห์จากท่านอาจารย์และขอกราบขอบพระคุณท่านอาจารย์เป็นอย่างสูง

ขอกราบขอบพระคุณคณาจารย์ภาควิชาวิศวกรรมการวัดคุม คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุก ๆ ท่านที่ได้ประสิทธิ์ประสาทวิชาให้กับข้าพเจ้า

ขอขอบคุณ คุณพรพัชรา ค่ำคูณ คุณฤทวัชร์ วินิจฉัยกุล คุณอานนท์ ศรีสุวรรณ คุณปณิธิ ลิปิสุนทร และคุณ เจษฎา จารุศะศิ ที่คอยให้คำปรึกษาและชี้แนะแนวทางในการทำงานวิจัย

ขอขอบคุณเพื่อน ๆ พี่ ๆ น้อง ๆ ทุกคนที่ทำให้ข้าพเจ้ารู้จักมิตรภาพดี ๆ ให้การช่วยเหลือเป็นกำลังใจ ให้ความห่วงใยและเข้าใจ จนทำให้ข้าพเจ้าสามารถผ่านพ้นอุปสรรค และปัญหาต่าง ๆ มาได้ด้วยดี

สำหรับคุณงามความดีอันใดที่เกิดจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบให้กับบิดามารดา ซึ่งเป็นที่รักและเคารพยิ่ง ตลอดจนครูอาจารย์ที่เคารพทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้และถ่ายทอดประสบการณ์ที่ดีให้แก่ข้าพเจ้า

ปวริศา กองทอง

สารบัญ

หน้า

บทคัดย่อภาษาไทย I
บทคัดย่อภาษาอังกฤษ II
กิตติกรรมประกาศ III
สารบัญ IV
สารบัญตาราง VII
สารบัญรูป IX

บทที่ 1 บทนำ 1
1.1 ความสำคัญของวิทยานิพนธ์ 1
1.2 วัตถุประสงค์ 2
1.3 ขอบเขตการวิจัย 2
1.4 ขั้นตอนของการศึกษา 2

บทที่ 2 ทฤษฎีที่เกี่ยวข้องที่เกี่ยวข้อง 3
2.1 ระบบวัดคุมนิรภัย 3
2.1.1 ระบบการควบคุมพื้นฐาน (Basic Process Control System, BPCS) 3
2.2 ระบบนิรภัย (Safety Related System) 5
2.3 มาตรฐานระบบวัดคุมนิรภัย 7
2.4 ระดับความปลอดภัย (Safety Integrity Level) หรือ SIL 9
2.5 การทนทานต่อความล้มเหลวของอุปกรณ์ 10
2.5.1 ระบบวัดคุมนิรภัย (Safety Instrumented System) 12
2.6 ความล้มเหลวในระบบนิรภัย (Failure in Safety System) 13
2.6.1 Random hardware failure 13
2.6.2 Systematic failure 13
2.7 ประเภทความล้มเหลวในระบบนิรภัย (Failure type in Safety system) 13
2.7.1 ความล้มเหลวนิรภัยตรวจจับได้ (Safe Detected Failure) 14
2.7.2 ความล้มเหลวนิรภัยตรวจจับไม่ได้ (Safe Undetected Failure) 14
2.7.3 ความล้มเหลวอันตรายตรวจจับได้ (Dangerous Detected Failure 14
2.7.4 ความล้มเหลวอันตรายตรวจจับไม่ได้ (Dangerous Detected Failure). 14
2.8 รูปแบบของอุปกรณ์วัดคุมนิรภัย (Sensing Element Architecture) 14
2.8.1 อุปกรณ์การวัดรูปแบบ 1oo1 (One out of One voting) 14
2.8.2 อุปกรณ์การวัดรูปแบบ 1oo2 (One out of Two Voting) 15
2.8.3 อุปกรณ์การวัดรูปแบบ 1oo3 (One out of Three Voting) 16
2.8.4 อุปกรณ์การวัดรูปแบบ 2oo3 (Two out of Three Voting) 17

สารบัญ (ต่อ)

หน้า

2.8.5 อุปกรณ์การวัดรูปแบบ 2oo2 (Two out of Two Voting) 18
2.9 แหล่งข้อมูลอัตราความล้มเหลวของอุปกรณ์ 19
2.9.1 ผู้ผลิต 19
2.9.2 คู่มือหรือฐานข้อมูลจากมาตรฐาน 20
2.10 โมเดลมาร์คอฟ 20
2.10.1 ประเภทโมเดลมาร์คอฟ (Markov Model Types) 21
2.11 เทคนิควิธีการมาร์คอฟ 22
2.12 ความล้มเหลวร่วมกันหรือ β (Common Cause Failure) 23
2.13 ค่าความล้มเหลวร่วมกัน β (Common Cause Failure) 23
2.13.1 การหาค่าความล้มเหลวร่วมกัน (Common Cause Failure) หรือค่า β,β_D 21

บทที่ 3 การดำเนินการศึกษางานวิจัย 33
3.1 ขอบเขตของการศึกษา 33
3.2 กรณีศึกษางานวิจัย 33
3.3 การประเมินโหมดความล้มเหลวที่สามารถเกิดขึ้นได้ของอุปกรณ์ในระบบ 32
3.4 อัตราความล้มเหลว (Failure Rate) ของอุปกรณ์ 36
3.4.1หาค่าอัตราความล้มเหลวร่วม (Common Cause Failure) 36
3.4.2 รายละเอียดข้อมูลของกรณีศึกษา 38
3.5 สร้างโมเดล มาร์คอฟ (Markov Model Construction) 38
3.5.1 สถานะระบบล้มเหลวนิรภัย (System Fail Safe State) 38
3.5.2 สถานะระบบล้มเหลวอันตรายตรวจจับได้ (System Fail Dangerous Detect) 39
3.5.3 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ (System Fail Dangerous Undetected State) 40
3.5.4 สถานะระบบล้มเหลวนิรภัยปกติตรวจจับได้ (System Fail Safety Detect Normal State) 41
3.5.5 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้44 45
3.5.6สถานะระบบล้มเหลวอันตรายตรวจจับได้ (System Fail Dangerous Detect Normal State) 49
3.5.7 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ (System Fail Dangerous Undetected Normal State) 52
3.6 การผสานสถานะโมเดลมาร์คอฟ 56
3.7 การหาค่าเฉลี่ยความผิดพลาดอันตรายของอุปกรณ์วัดคุมนิรภัย 57

สารบัญ (ต่อ)

หน้า

3.8 ผลจากการพิสูจน์ค่าระดับความปลอดภัยหาค่าเฉลี่ยความล้มเหลว 59
3.9 การพิจารณาการทนทานต่อความล้มเหลวของอุปกรณ์..... 59
3.91 พิจารณาวิธี Route 1_H ตามข้อกำหนดมาตรฐาน IEC61508 59
3.9 2 พิจารณาวิธี Route 2_H ตามข้อกำหนดมาตรฐาน IEC61508 60
3.9 3 พิจารณาตามข้อกำหนด Prior Use ใน มาตรฐาน IEC61511 60

บทที่ 4 การดำเนินการศึกษางานวิจัย..... 61
4.1 ผลการดำเนินการและวิจารณ์..... 61
4.2 ข้อเสนอแนะ..... 61

เอกสารอ้างอิง..... 62
ภาคผนวก ก..... 63
ประวัติผู้เขียน..... 69

สารบัญตาราง

ตารางที่ หน้า

2.1 ตารางค่าระดับความปลอดภัย ที่อัตราการเกิดเหตุการณ์อันตรายต่ำ 10
2.2 ตารางค่าระดับความปลอดภัย ที่อัตราการเกิดเหตุการณ์อันตรายสูง 10
2.3 ตารางจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาด 10
2.4 ตารางจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดตามมาตรฐาน IEC 61508 สำหรับ อุปกรณ์ Type A 10
2.5 ตารางจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดตามมาตรฐาน IEC 61508 สำหรับ อุปกรณ์ Type B 11
2.6 ตารางประเภทโมเดลมาร์คอฟ 21
2.7 วิธีการมาร์คอฟ 22
2.8 รายการที่ช่วยลดความล้มเหลวร่วม 24
2.9 Value of Z: programmable electronics 31
2.10 Value of Z-sensors or final elements 31
2.11 Calculation of β_{int} or β_{Dint} 32
2.12 Calculation of β or system with level of redundancy greater than 1oo2 32
3.1 แสดงโหมดความล้มเหลวของแต่ละอุปกรณ์ในฟังก์ชั่นนิรภัย 34
3.2 อัตราความล้มเหลวของอุปกรณ์ 35
3.3 อัตราความล้มเหลวร่วมของอุปกรณ์ 37
3.4 รายละเอียดข้อมูลของกรณีศึกษา 38
3.5 โหมดความล้มเหลวของอุปกรณ์ 38
3.6 โหมดความล้มเหลวของสถานะระบบล้มเหลวนิรภัย 39
3.7 สถานะระบบล้มเหลวอันตรายตรวจจับได้ 40
3.8 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ 41
3.9 สถานะระบบล้มเหลวนิรภัยปกติตรวจจับได้ 41
3.10 สถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับได้ 43
3.11 สถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับไม่ได้ 44
3.12 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ 45
3.13 สถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับ ได้ 46
3.14 สถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้ 48
3.15 สถานะระบบล้มเหลวอันตรายตรวจจับได้ 49
3.16 สถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับได้ 50
3.17 สถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้ 51
3.18 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ 52

สารบัญตาราง

ตารางที่ หน้า
3.19 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับได้..... 53
3.20 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้..... 55
3.21 ค่าระดับความปลอดภัยฟังก์ชั่นนิรภัยกรณีศึกษา 59
3.22 แสดงขอบเขตความสมบูรณ์ของอุปกรณ์ในระบบนิรภัยกรณีศึกษาด้วยวิธี route 1H 60

สารบัญรูป

รูปที่ หน้า

2.1 โครงสร้างระบบควบคุมพื้นฐาน 4

2.2 ฟังก์ชันการควบคุม 5

2.3 ระบบควบคุมพื้นฐานและระบบวัดคุมนิรภัย 6

2.4 การใช้งาน IEC 61508 และ IEC 61511 7

2.5 วงรอบความปลอดภัย (Safety Life Cycle) ของ IEC 61508 [5] 8

2.6 วงรอบความปลอดภัย (Safety Life Cycle) ของ IEC 61511 [7] 9

2.7 ฟังก์ชันวัดคุมนิรภัยในระบบวัดคุมนิรภัย 13

2.8 อุปกรณ์การวัดรูปแบบ 1oo1 15

2.9 อุปกรณ์การวัดรูปแบบ 1oo2 16

2.10 อุปกรณ์การวัดรูปแบบ 1oo3 17

2.11 อุปกรณ์การวัดรูปแบบ 2oo3 18

2.12 อุปกรณ์การวัดรูปแบบ 2oo2 19

2.13 สัญลักษณ์ของโมเดลมาร์คอฟ 20

2.14 ระบบโมเดลมาร์คอฟย้อนกลับไม่ได้ 21

2.15 ระบบโมเดลมาร์คอฟย้อนกลับได้ 21

3.1 แผนภาพกระบวนการของระบบวาล์วลดความดัน 34

3.2 สถานะระบบล้มเหลวนิรภัย 39

3.3 สถานะระบบล้มเหลวอันตรายตรวจจับได้ 40

3.4 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ 41

3.5 สถานะระบบล้มเหลวนิรภัยตรวจจับได้ 42

3.6 สถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับได้ 43

3.7 สถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับไม่ได้ 44

3.8 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ 46

3.9 สถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับได้ 47

3.10 สถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้ 48

3.11 สถานะระบบล้มเหลวอันตรายตรวจจับได้ 49

3.12 สถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับได้ 50

สารบัญรูป (ต่อ)

รูปที่ หน้า

3.13 สถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้ 52

3.14 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ 53

3.15 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับได้ 54

3.16 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้ 55

3.17 ผสานสถานะโมเดลมาร์คอฟ 56

3.18 เมตทริก P 57

3.19 การแทนค่า เมตทริก P 58

บทที่ 1
บทนำ

1.1 ความสำคัญของวิทยานิพนธ์

ในงานอุตสาหกรรมการผลิตต่างๆนั้นได้มีหลากหลายปัจจัยที่ใช้ในการผลิตเพื่อให้ได้ผลิตภัณฑ์ตามเป้าหมาย รวมไปถึงความต้องการด้านพลังงานที่มีแนวโน้มสูงขึ้น การนำก๊าซธรรมชาติซึ่งเป็นเชื้อเพลิงที่สามารถติดไฟ ลุกไหม้ และระเบิดมาใช้ในงานอุตสาหกรรมนั้น จำเป็นต้องใช้ระบบท่อที่สามารถนำก๊าซธรรมชาติไปสู่ผู้ใช้ได้อย่างปลอดภัยและเกิดการสูญเสียน้อยที่สุด ในระบบท่อส่งก๊าซจึงเป็นระบบที่เหมาะสม ซึ่งประเทศไทยได้นำระบบท่อส่งก๊าซธรรมชาติมาใช้เป็นเวลามากกว่า 25 ปี ในตลอดแนวเส้นทางของท่อส่งก๊าซธรรมชาติ มีก๊าซธรรมชาติบรรจุ อยู่เต็มตลอดแนวท่อ และมีการขนส่งตลอด 24 ชั่วโมง ใช้หลักการขนส่งจากแรงดันสูงสู่แรงดันต่ำ จึงต้องมีวาล์วลดความดันเพื่อลดแรงดัน ตามแนวเส้นทางวางท่อส่งก๊าซธรรมชาตินั้นต้องผ่านพื้นที่ เกษตรกรรม ชุนชน พื้นที่ข้างทางหลวง หากมีความมีความผิดพลาดใดๆ จากจะนำไปสู่อุบัติเหตุและเกิดอันตรายได้ ดังนั้นการศึกษาการประเมินความเสี่ยงของระบบวัดคุมนิรภัยสำหรับวาล์วลดความดันที่ใช้ในระบบท่อส่งก๊าซจึงมีความสำคัญอย่างมากเพื่อลดอุบัติภัยและผลกระทบที่จะเกิดขึ้นหากเกิดเหตุการณ์อันตราย

ในกระบวนการที่มีความเสี่ยงมีจำเป็นต้องมีควบคุมความเสี่ยงระบบวัดคุมนิรภัย (safety Instrumented System, SIS) เป็นส่วนสำคัญที่ช่วยในการป้องกันการเกิดอันตราย โดยได้มีการกำหนดค่าระดับความปลอดภัย (Safety Integrity Level, SIL) เพื่อเป็นแนวทางในการ ออกแบบ ติดตั้งหรือดำเนินการ รวมทั้งการบำรุงรักษา ซึ่งจะสามารถป้องกันหรือลดความรุนแรงผลกระทบที่อาจก่อให้เกิดความเสียหาย อาจมีสาเหตุมาจาก ความผิดพลาดของเครื่องมือวัดหรืออุปกรณ์ต่างๆในกระบวนการผลิต หรือความผิดพลาดของผู้ปฏิบัติงาน ความเสียหายที่เกิดขึ้นอาจจะทำให้เกิดอันตราย อาทิเช่น อันตรายต่อผู้ปฏิบัติงาน ความเสียหายต่ออุปกรณ์หรือต่อผลิตภัณฑ์ และส่งผลกระทบต่อสิ่งแวดล้อมในบริเวณนั้น

งานวิจัยเรื่องนี้ จึงมีจุดประสงค์ในการศึกษา วิธีการหาค่าระดับความปลอดภัย (SIL) โดยอ้างอิงตามมาตรฐานIEC 61511/611508 ใช้วิธีการหาค่าระดับความปลอดภัยด้วย โมเดลมาร์คอฟ ซึ่งวิธีการเหล่านี้จะให้ผลลัพธ์ที่ค่าเชิงปริมาณเป็นค่าทางคณิตศาสตร์ ทั้งนี้ William M. Goble Harry Cheddie [3] ได้กล่าวถึงวิธีการโมเดลมาร์คอฟว่าโมเดลมาร์คอฟนั้นมีวิธีการที่มีความยืดหยุ่นมากกว่าวิธีการอื่น แค่รูปแบบเดี่ยวของโมเดลมาร์คอฟสามารถแสดงให้เห็นถึงระบบการทนความผิดพลาดของการปฏิบัติการทั้งหมดรวมถึงโหมดความล้มเหลวอีกด้วย

1.2 วัตถุประสงค์

วิทยานิพนธ์ฉบับนี้มีวัตถุประสงค์ของการศึกษาดังต่อไปนี้

1. เพื่อศึกษาการหาค่าระดับความปลอดภัยของฟังก์ชันวัดคุมนิรภัยของระบบวัดคุมนิรภัยสำหรับวาล์วลดความดันที่ใช้ในระบบท่อส่งก๊าซ (กรณีศึกษาตัวอย่าง) และคำนวณหาค่าเฉลี่ยความล้มเหลวอันตรายโดยใช้วิธีการมาร์คอฟโมเดลใช้ตามมาตรฐานสากล International Electrotechnical Commission IEC 61508 และ IEC 61511

2. เพื่อปรับปรุงการวางแผนการทดสอบฟังก์ชันวัดคุมนิรภัยของของวาล์วลดความดันที่ใช้ในระบบท่อส่งก๊าซ

1.3 ขอบเขตการวิจัย

กรณีศึกษาฟังก์ชันวัดคุมนิรภัยของระบบท่อส่งแก๊สของโรงงานแห่งหนึ่ง รวบรวมทฤษฎีที่ใช้วิเคราะห์ค่าระดับความปลอดภัยเพื่อหาค่าระดับความปลอดภัยโดยใช้วิธีโมเดลมาร์คอฟ

1.4 ขั้นตอนของการศึกษา

วิทยานิพนธ์ฉบับนี้มีขั้นตอนของการศึกษาดังต่อไปนี้

1. บทที่ 1 เป็นการกล่าวถึง ความเป็นมาและความสำคัญของปัญหา วัตถุประสงค์ของการศึกษา การนำเสนอหลักการใหม่ของวิทยานิพนธ์ ขอบเขตวิทยานิพนธ์และรายละเอียดของวิทยานิพนธ์

2. บทที่ 2 เป็นการกล่าวถึง หลักการและทฤษฎีที่เกี่ยวข้องในการประเมินหาค่าระดับความปลอดภัย การคำนวณค่าความล้มเหลวอันตรายโดยวิธีโมเดลมาร์คอฟ

3. บทที่ 3 เป็นการนำเสนองานวิจัย วิธีการการหาค่าระดับความปลอดภัยและการคำนวณฟังก์ชันวัดคุมนิรภัยในกระบวนการผลิตที่ใช้เป็นกรณีศึกษา

4. บทที่ 4 เป็นบทสุดท้ายซึ่งจะกล่าวถึงสรุปผลการวิจัยและข้อเสนอแนะ ในส่วนสุดท้ายของวิทยานิพนธ์เป็นส่วนของภาคผนวก ประกอบไปด้วยบทความวิจัยที่ได้รับการตีพิมพ์และข้อมูลที่ใช้ในงานวิจัย ดังนี้

ภาคผนวก ก บทความวิจัยที่ได้รับการตีพิมพ์

บทที่ 2
ทฤษฎีที่เกี่ยวข้องที่เกี่ยวข้อง

2.1 ระบบวัดคุมนิรภัย

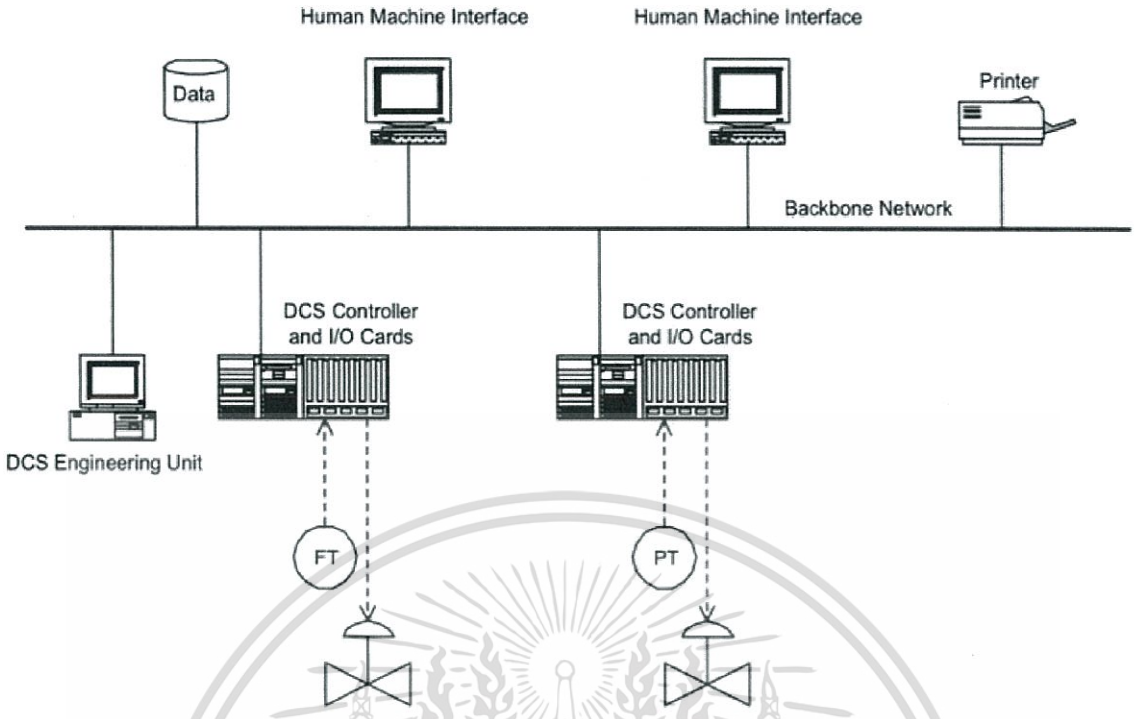
ในกระบวนการผลิตทางอุตสาหกรรม ต้องมีการการวัดและควบคุมตัวแปรในกระบวนการผลิต เพื่อให้ได้ผลิตภัณฑ์ตามที่ต้องการ ตัวแปรต่างๆและเครื่องมือวัดเป็นสาเหตุให้เกิดความเสี่ยงการเกิดเหตุการณ์อันตราย ความเสี่ยงที่จะเกิดขึ้น อาจจะเกิดอันตรายขึ้นกับสิ่งมีชีวิตหรือผู้ปฏิบัติงานเอง เกิดความเสียหายต่ออุปกรณ์ต่างๆในกระบวนการผลิต เกิดความสูญเสียต่อผลิตภัณฑ์ ส่งผลกระทบต่อสิ่งแวดล้ม หรือแม้กระทั่งต่อชื่อเสียงขององค์กร ดังนั้นการลดโอกาสเกิดเหตุการณ์อันตรายให้อยู่ในค่าที่ยอมรับได้ การออกแบบระบบวัดคุมนิรภัยของกระบวนการผลิตจึงมีความสำคัญอย่างมาก

2.1.1 ระบบการควบคุมพื้นฐาน (Basic Process Control System, BPCS)

ทวิช (2559) [1] ได้กล่าวไว้ว่า ในกระบวนการแต่ละอุตสาหกรรมจะต้องมีการวัดและควบคุมตัวแปรต่างๆทางกระบวนการ เพื่อทำการแสดงค่าและควบคุมตัวแปรต่างๆให้อยู่ในค่าที่ต้องการและเพื่อให้ผลิตภัณฑ์ที่ได้มีคุณสมบัติตามที่กำหนด ตัวแปรทางกระบวนการต่างๆเหล่านี้ ได้แก่ การไหล (Flow) ระดับของเหลว (Level) ความดัน (Pressure) อุณหภูมิ (Temperature)

ดังนั้นเพื่อให้บรรลุวัตถุประสงค์การควบคุมตัวแปรต่างๆเหล่านี้จึงต้องมีการจัดเตรียมระบบการวัดและควบคุมขึ้นในการกระบวนการผลิต โดยระบบการวัดและควบคุมจะประกอบไปด้วยฟังก์ชันการควบคุม (Control Function) หลายฟังก์ชันอุปกรณ์พื้นฐานที่สำคัญของฟังก์ชันการควบคุมจะมีอยู่ 3 ส่วนดังนี้

การวัด (Sensing Element)ตัวควบคุม (Controller) และ อุปกรณ์สุดท้าย (Final Element) โดยอุปกรณ์การวัดจะทำหน้าที่ในการเปลี่ยนตัวแปรจากกระบวนการให้เป็นสัญญาณไฟฟ้ามาตรฐาน เพื่อส่งค่าอินพุตของตัวควบคุมและไปแสดงค่าตัวแปรที่หน่วยแสดงผลของระบบควบคุมเพื่อให้ผู้ปฏิบัติงานสามารถสังเกตเห็นการเปลี่ยนแปลงและควบคุมตัวแปรต่างๆเหล่านี้ได้ จากนั้นตัวควบคุมจะทำการประมวลผลและส่งสัญญาณไฟฟ้าเอาต์พุตไปยังอุปกรณ์สุดท้ายที่เป็นวาล์วควบคุมเพื่อทำการปรับตัวแปรกระบวนการผลิตให้อยู่ในค่าที่ต้องการ ระบบการควบคุมพื้นฐานที่ใช้งานกันอย่างกว้างขวางสำหรับอุตสาหกรรมการผลิตในปัจจุบันคือระบบ DCS (Distributed Control System, DCS) ซึ่งสามารถแสดงตัวอย่างโครงสร้างพื้นฐานของระบบควบคุม (Control System Architecture) ได้ดังรูปที่ 2.1



รูปที่ 2.1 โครงสร้างระบบควบคุมพื้นฐาน

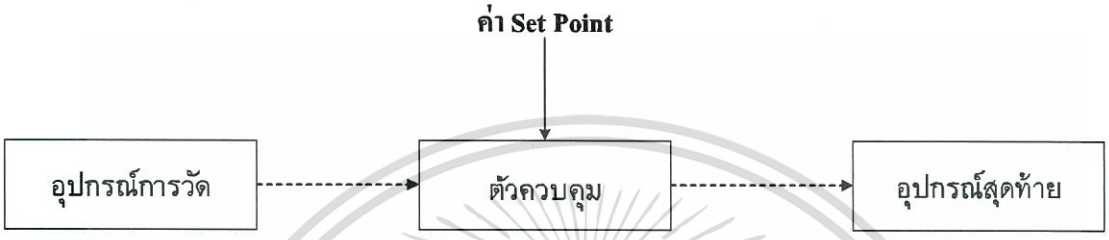
จากรูปที่ 2.1 ระบบการควบคุมพื้นฐาน จะเป็นระบบที่ใช้สำหรับควบคุมการทำงานกระบวนการผลิตโดยผ่านการอุปกรณ์เครื่องมือวัดและอุปกรณ์อื่นๆในกระบวนการผลิต เพื่อให้กระบวนการผลิตทำงานเป็นตามที่ต้องการหรือที่ได้ออกแบบไว้ จะมีส่วนประกอบหลักๆที่สำคัญดังต่อไปนี้

1. อุปกรณ์การวัด (Sensing Element) เป็นอุปกรณ์ที่ใช้เปลี่ยนตัวแปรจากกระบวนการผลิต (Process parameter) ให้เป็น สัญญาณไฟฟ้ามาตรฐาน 4 ถึง 20 มิลลิแอมแปร์ (mA.) ที่แรงดัน 24 โวลท์กระแสตรง (VDC.) หรือสัญญาณมาตรฐานชนิดอื่นๆ เพื่อส่งข้อมูลของตัวแปรต่างๆไปยังอุปกรณ์ควบคุม (Controller) และใช้แสดงค่าตัวแปรที่หน่วยแสดงผลของระบบควบคุม หน่วยแสดงผลอุปกรณ์การวัดพื้นฐานจะมีดังนี้ อุปกรณ์การวัดการไหล (Flow Transmitter) อุปกรณ์การวัดระดับของเหลว (Level Transmitter) อุปกรณ์การวัดความดัน (Pressure Transmitter) และอุปกรณ์การวัดอุณหภูมิ (Temperature Transmitter) อุปกรณ์นี้มีหลายชนิด ในการเลือกใช้จึงต้องเลือกใช้ให้เหมาสมกับสถานะและคุณสมบัติของไหลที่ต้องการวัดเพื่อให้ได้ข้อมูลที่ได้จากการวัดมีค่าความถูกต้องมากที่สุดและอุปกรณ์เหล่านั้นมีอายุการใช้งานที่นานขึ้น

2. ตัวควบคุม (Controller) เป็นส่วนที่ใช้ประมวลผลตัวควบคุม (Controller) ประกอบด้วยอุปกรณ์หลักๆ ดังนี้ แหล่งจ่ายพลังงาน (Power Supply Unit) ตัวประมวลผลกลาง (Central Processor Unit) ส่วนรับและส่งสัญญาณ (Input and Output Cards) ส่วนติดต่อสื่อสาร (Communication Port) และโปรแกรมในการควบคุม (Control Function Program) ตัวควบคุมจะทำการควบคุมตัวแปรจากกระบวนการผลิตให้อยู่ในค่าที่ต้องการ โดยการรับสัญญาณมาจากอุปกรณ์การวัดเพื่อมาทำการเปรียบเทียบกับค่าที่กำหนด (Set Point) และทำการประมวลผลจากนั้นจะส่งสัญญาณเอาต์พุตไปยังอุปกรณ์สุดท้ายเพื่อทำการปรับตัวแปรในกระบวนการ ตัวควบคุมในระบบการควบคุมพื้นฐานจะมีให้เลือกหลายชนิดขึ้นอยู่กับความต้องการในการควบคุม เช่น การ

ควบคุมแบบเปิดปิด (On-Off Control) การควบคุมแบบ PI (Proportional-Integral Control) การควบคุมแบบPD (Proportional-Derivative Control)) การควบคุมแบบ PID (Proportional-Integral-Derivative Control) เป็นต้น

3. อุปกรณ์สุดท้าย (Final Element) เป็นอุปกรณ์ที่ใช้สำหรับเปลี่ยนสัญญาณไฟฟ้ามาตรฐาน 4 ถึง 20 มิลลิแอมแปร์ (mA.) จากเอาต์พุตจากตัวควบคุมไปทำการควบคุมตัวแปรกระบวนการ เช่น อุปกรณ์สุดท้ายจะเป็น วาล์วควบคุม (Control Valve) ซึ่งจะทำการปิดเปิดของไหลตามสัญญาณเอาต์พุตจากตัวควบคุม



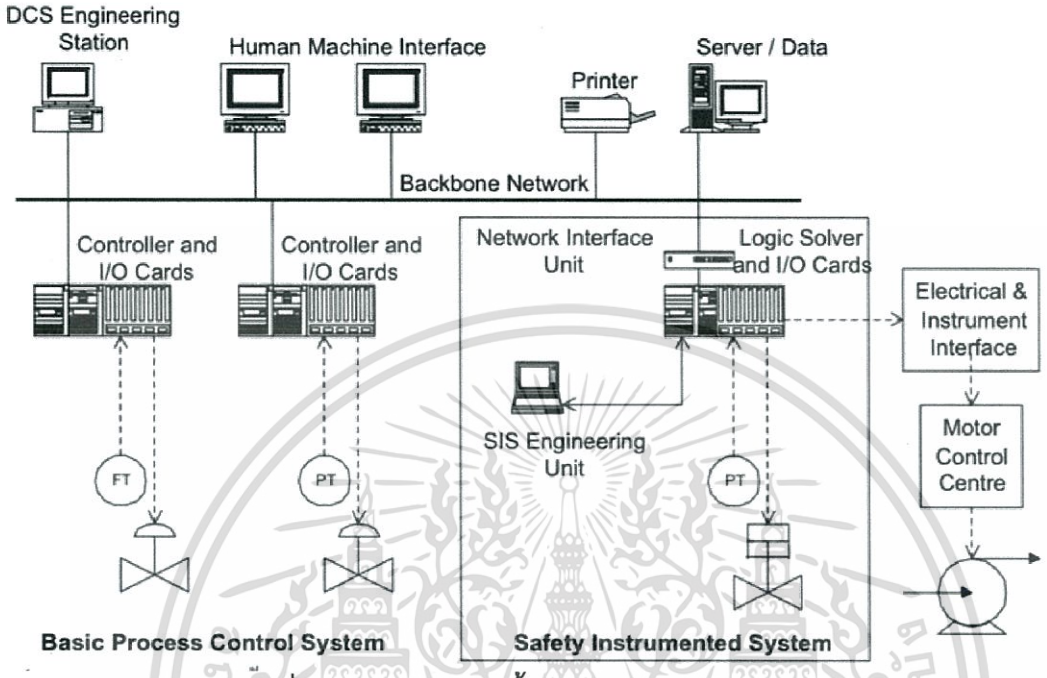
รูปที่ 2.2 ฟังก์ชันการควบคุม

2.2 ระบบนิรภัย (Safety Related System)

จากหัวข้อที่ผ่านมาเป็นการแสดงรายละเอียดการทำงานฟังก์ชั่นการควบคุมจะเห็นได้ว่าฟังก์ชั่นควบคุมสามารถทำการเปลี่ยนแปลงค่า Set point ได้ตามต้องการและอุปกรณ์การควบคุมที่เป็นวาล์วควบคุมจะมีการทำงานอยู่ตลอดเวลา มีการเคลื่อนที่ของก้านวาล์วบ่อยครั้งเพื่อปรับตัวแปรกกระบวนการให้อยู่ในค่าที่ต้องการ ซึ่งเมื่อมีใช้งานไปในระยะเวลานานๆอาจทำให้เกิดการสึกหรอหรือเกิดการติดขัดต่อการปิดเปิดหรืออาจปิดเปิดใช้ช้าลงหรืออาจเกิดความผิดปกติขึ้นในอุปกรณ์การวัดทำงานอ่านค่าไม่ถูกต้อง ซึ่งจะส่งผลให้ตัวแปรที่ต้องการควบคุมไม่สามารถควบคุมได้หรืออาจทำให้ค่าตัวแปรกระบวนการผลิตเหล่านี้มีค่าสูงเกินกว่าที่อุปกรณ์ทนได้หรืออาจเกิดการปฏิบัติงานที่ผิดพลาดโดยการใส่ค่า set point มากเกินไปหรือทำการสั่งเปิดปิดวาล์วไม่ถูกต้อง เหตุการณ์ต่างๆเหล่านี้อาจจะเป็นสาเหตุทำให้ค่าตัวแปรผิดไปจากค่าที่ต้องการได้ ถ้าค่าตัวแปรเหล่านี้มีค่าเกินกว่าจุดที่อุปกรณ์ต่างๆในกระบวนการผลิตจะทนได้ อาจทำให้เกิดการระเบิดหรือมีการรั่วไหลมายังภายนอก ถ้าของไหลมีความไวไฟ (Flammable) หรือมีความเป็นพิษ (Toxic) อาจทำให้เกิดการลุกไม้ หรืออาจทำให้เกิดอันตรายต่อผู้ปฏิบัติงานที่อยู่ในบริเวณนั้น เกิดความเสียหายต่อทรัพย์สินหรืออุปกรณ์ต่างๆหรือเกิดความเสียหายต่อสิ่งแวดล้มภายนอกได้ การป้องกันการเกิดเหตุการณ์เหล่านี้สามารถทำได้โดยการติดตั้งระบบป้องกัน (Protection System)หรือระบบนิรภัย (Safety System) เข้าไปในระบบควบคุมกระบวนการผลิต การป้องกันการเกิดเหตุการณ์เหล่านี้สามารถทำได้หลายวิธี ในขั้นตอนแรกอาจจะทำการออกแบบกระบวนการผลิตใหม่หรือออกแบบให้อุปกรณ์มีการทนความดันสูงกว่าความดันกระบวนการ หรือเลือกติดตั้งระบบนิรภัยชนิดต่างๆ เช่น การติดตั้งวาล์วนิรภัยทางกล (Pressure Relief Valve) หรือจัดเตรียมฟังก์ชั่นระบบวัดคุมนิรภัย (Safety Instrument System) เข้าไป เป็นต้น ในการพิจารณาว่าจะใช้เครื่องมือวัดชนิดใดนั้นจะขึ้นอยู่กับความเสี่ยง ความเหมาะสม ค่าความเชื่อมั่นในการทำงาน และค่าใช้จ่ายที่ต้องใช้

รายละเอียดของการเลือกใช้ฟังก์ชั่นนิรภัยที่ถูกจัดเตรียมบนระบบวัดคุมนิรภัยหรือ SIS (Safety Instrumented System) ที่มีส่วนประกอบของอุปกรณ์ทางไฟฟ้า ทางอิเล็กทรอนิกส์และโปรแกรม

ทางอิเล็กทรอนิกส์ (Electrical/ Electronic/ Programmable Electronic Systems) หรือระบบที่ใช้งานกันอย่างวางขวางเรียกว่า ระบบESD (Emergency Shutdown System) สามารถแสดงโครงสร้างระบบควบคุมพื้นฐานที่ได้มีการเพิ่มเติมระบบวัดคุมนิรภัยได้ดังรูปที่ 2.3



รูปที่ 2.3 ระบบควบคุมพื้นฐานและระบบวัดคุมนิรภัย

โดยระบบวัดคุมนิรภัยมีส่วนประกอบที่สำคัญดังต่อไปนี้

1. อุปกรณ์การวัด (Sensing Element) เป็นอุปกรณ์ที่ใช้วัดสภาวะของกระบวนการผลิตและเปลี่ยนตัวแปรต่างๆ ในกระบวนการผลิต (Process Parameter) ให้เป็นสัญญาณกระแสไฟฟ้ามาตรฐาน 4 ถึง 20 มิลลิแอมแปร์ (mA.) ที่แรงดัน 24 โวลท์กระแสตรง (VDC.) เพื่อส่งไปยังส่วนประมวลผล (Logic Solver) อุปกรณ์การวัดของระบบการควบคุมพื้นฐานมีดังนี้ อุปกรณ์การวัดการไหล (Flow Transmitter) อุปกรณ์การวัดระดับของเหลว (Level Transmitter) อุปกรณ์การวัดความดัน (Pressure Transmitter) และ อุปกรณ์การวัดอุณหภูมิ (Temperature Transmitter) แต่อุปกรณ์การวัดในระบบนิรภัยอาจมีมากว่าหนึ่งตัวขึ้นอยู่กับอัตราความล้มเหลว (Failure Rate)

2. ส่วนประมวลผล (Logic Solver) เป็นส่วนที่ใช้สำหรับประมวลผลโลจิกของระบบวัดคุมนิรภัย เพื่อใช้ในการควบคุมกระบวนการผลิตให้อยู่ในสภาวะปลอดภัยเมื่อเกิดความผิดปกติขึ้น โดยการรับสัญญาณอินพุตมาจากอุปกรณ์การวัดเพื่อมาทำการเปรียบเทียบกับค่าที่กำหนด (Set Point) และจากนั้นจะส่งเอาต์พุตแบบดิจิตอลไปยังอุปกรณ์สุดท้าย ส่วนประมวลผลจะประกอบด้วยอุปกรณ์หลัก ๆ ดังนี้

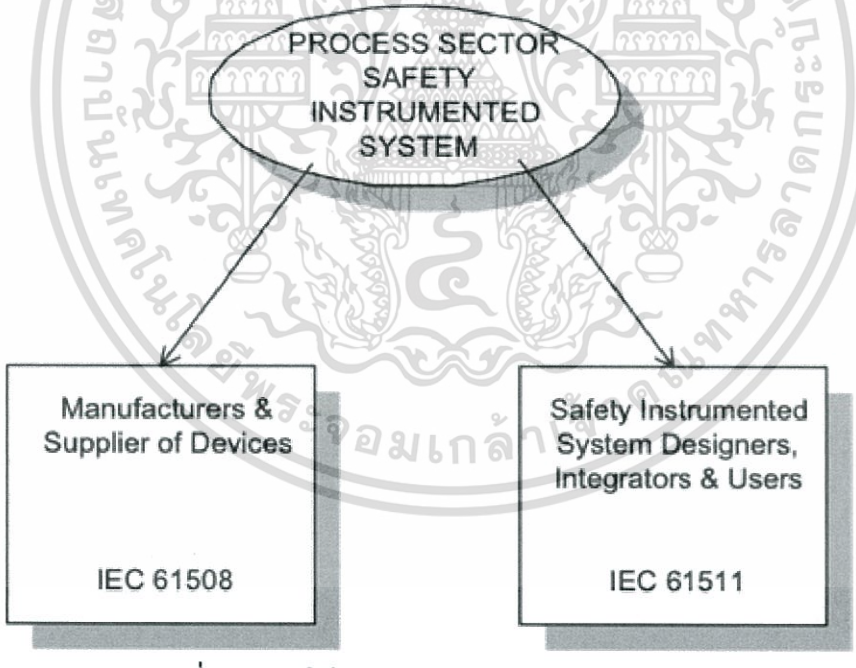
แหล่งจ่ายพลังงาน (Power Supply Unit) ตัวประมวลผลกลาง (Central Processor Unit) ส่วนรับและส่งสัญญาณ (Input and Output Cards) ส่วนติดต่อสื่อสาร (Communication Port) และโปรแกรมในการทำงาน

3. อุปกรณ์สุดท้าย (Final Element) เป็นอุปกรณ์ที่ใช้สำหรับเปลี่ยนสัญญาณไฟฟ้าจากส่วนประมวลผล ส่วนใหญ่จะเป็นสัญญาณไฟฟ้าแรงดัน 24 VDC ไปทำการปิดและเปิดอุปกรณ์สุดท้าย เช่น วาล์วนิรภัย (Shutdown Valve) หรือชุดควบคุมมอเตอร์ (Motor Control Center)

2.3 มาตรฐานระบบวัดคุมนิรภัย

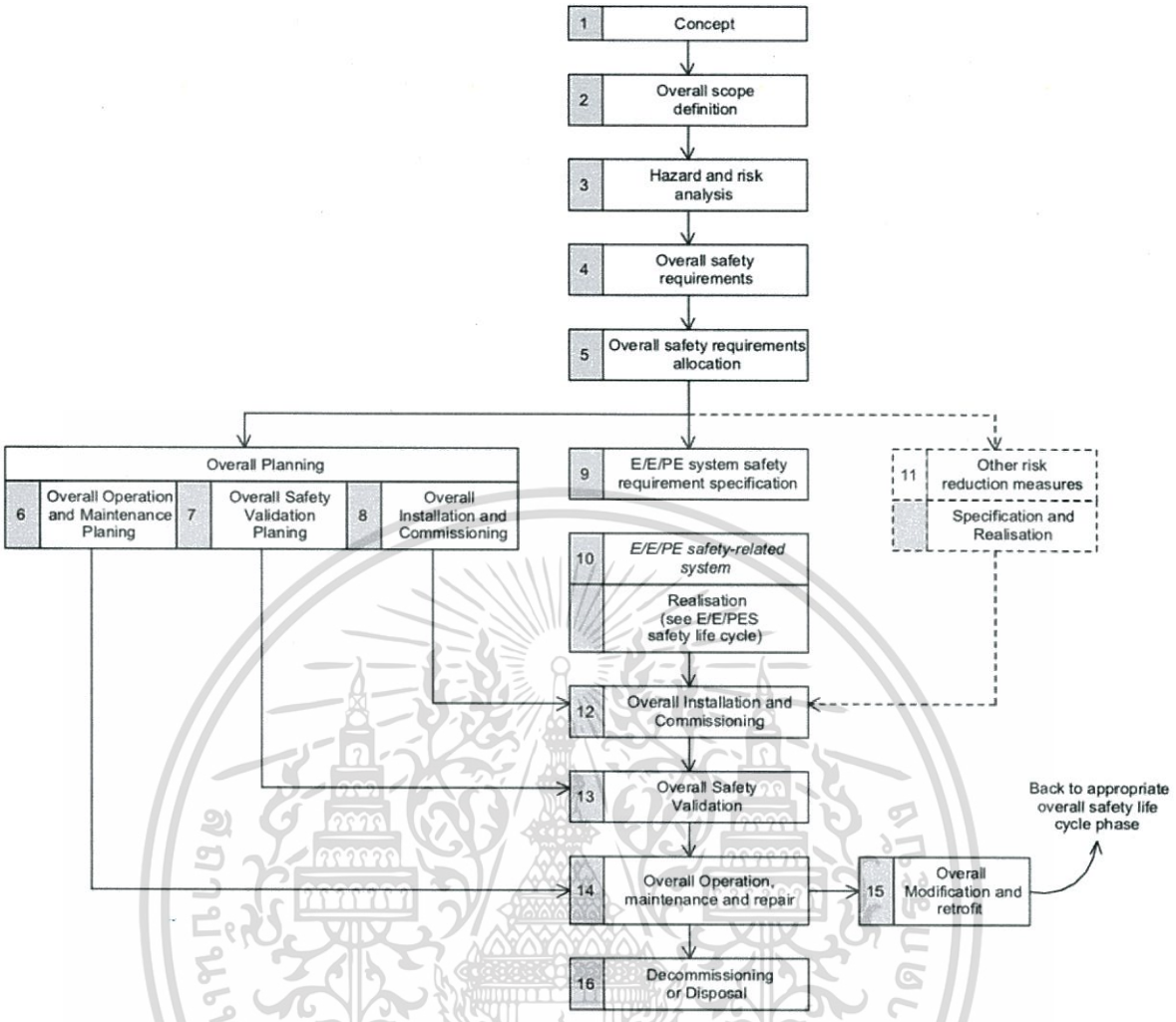
จากข้อผิดพลาดต่างๆที่เกิดขึ้นกับระบบวัดคุมนิรภัยตั้งแต่เริ่มต้นกำหนดในรายละเอียดสามารถที่จะทำการควบคุมได้ ทาง IEC (International Electrotechnical Commission) จึงได้จัดตั้งคณะกรรมการจากองค์กรต่างๆและผู้ที่มีส่วนเกี่ยวข้องกับระบบวัดคุมนิรภัยที่ครอบคลุมตั้งแต่ขั้นตอนการออกแบบไปจนถึงขั้นตอนการใช้งาน การซ่อมบำรุง และการปรับปรุงแก้ไขมาตรฐานที่ได้ผ่านการลงมติจากสมาชิกให้นำไปใช้งานนั้นคือมาตรฐาน IEC 61508 และ IEC 61511

มาตรฐาน IEC 61508 จะเป็นมาตรฐานในการกำหนดรายละเอียดของระบบนิรภัยตั้งแต่ขั้นตอนออกแบบกระบวนการผลิตอุปกรณ์ต่างๆ ไปจนถึงขั้นตอนการใช้งานและจะใช้การกำหนดค่าระดับความปลอดภัยคือค่า SIL (Safety Integrity Level) ของฟังก์ชั่นวัดคุมนิรภัย (Safety Function) ส่วนมาตรฐาน IEC 61511 จะเป็นมาตรฐานสำหรับผู้ใช้งานเพื่อเป็นแนวทางในการกำหนดรายละเอียดของระบบวัดคุมนิรภัยและการใช้งานอุปกรณ์ที่เป็นไปตามมาตรฐาน IEC 61508 และ IEC 61511 สามารถแสดงได้ดังรูป 2.4

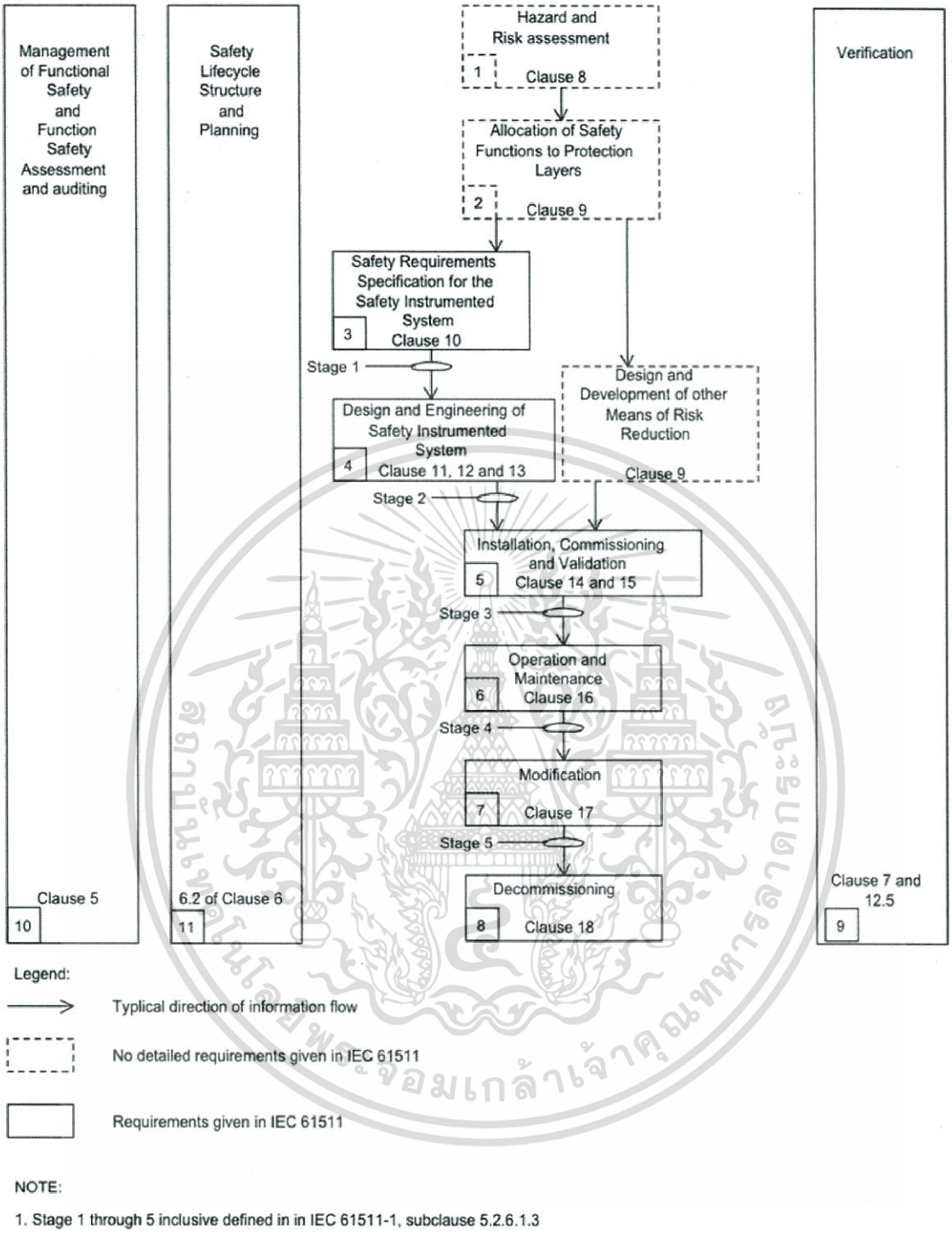


รูปที่ 2.4 การใช้งานIEC 61508 และ IEC 61511

มาตรฐาน IEC 61508และ IEC 61511 ได้กำหนดลำดับขั้นตอนสำหรับการออกแบบการเลือกใช้อุปกรณ์ต่างๆ การทดสอบ การซ่อมบำรุงและการปรับปรุงแก้ไขระบบวัดคุมนิรภัยที่มีส่วนประกอบของอุปกรณ์ทางไฟฟ้า ทางอิเล็กทรอนิกส์และโปรแกรมทางอิเล็กทรอนิกส์ (Electrical/ Electronic/ Programmable Electronic Systems) [4] ซึ่งลำดับขั้นตอนดังกล่าวจะเรียกว่าวงรอบความปลอดภัย (Safety Life Cycle) ดังแสดงในรูปที่ 2.5 และ 2.6



รูปที่ 2.5 วงรอบความปลอดภัย (Safety Life Cycle) ของ IEC 61508 [5]



รูปที่ 2.6 วงรอบความปลอดภัย (Safety Life Cycle) ของ IEC 61511 [7]

2.4 ระดับความปลอดภัย (Safety Integrity Level) หรือ SIL

ระบบวัดคุมนิรภัยจะถูกใช้งานในการทำหน้าที่ป้องกันหรือจำกัดขอบเขตความเสียหายของกระบวนการ อันเนื่องมาจากความผิดปกติของกระบวนการ ความผิดพลาดที่เกิดจากฟังก์ชันการควบคุมหรือความผิดพลาดที่เกิดขึ้นในระบบนิรภัยเอง ดังนั้นมาตรฐาน IEC 61508 จึงได้มีการกำหนดค่าเฉลี่ยความล้มเหลวอันตราย ของฟังก์ชันนิรภัยต่างๆที่อยู่ในระบบวัดคุมนิรภัย สำหรับนำไปใช้ในการป้องกันหรือจำกัดขอบเขตความเสียหาย ซึ่งค่าเฉลี่ยความล้มเหลวอันตรายจะเรียกว่า ค่าระดับ

ความปลอดภัยหรือ SIL ของฟังก์ชันนิรภัย (Safety Function) ในระบบวัดคุมนิรภัย โดยค่าระดับความปลอดภัยจะถูกแบ่งออกได้เป็น 4 ระดับตามช่วงค่าเฉลี่ยความล้มเหลวอันตรายช่วงละสิบเท่า ค่าระดับความปลอดภัยจะแสดงตามค่าเฉลี่ยความล้มเหลวอันตรายของอุปกรณ์ในเวลาที่ต้องการ (Average Probability of Failure on Demand) หรือ PFD_{avg} เวลาที่ต้องการเป็นสภาวะที่เกินจุดกำหนดความปลอดภัยของตัวแปรที่วัดได้จากกระบวนการผลิต ถ้าเวลาที่ต้องการเกิดขึ้น และระบบไม่สามารถทำงานได้ในเวลาที่กำหนดอันตรายจากเหตุการณ์นั้นจะเกิดขึ้น

ตารางที่ 2.1 ตารางค่าระดับความปลอดภัย ที่อัตราการเกิดเหตุการณ์อันตรายต่ำ [5]

ค่าระดับความปลอดภัย Safety Integrity Level (SIL)	Average probability of failure to perform its design function on demand (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

ตารางที่ 2.2 ตารางค่าระดับความปลอดภัย ที่อัตราการเกิดเหตุการณ์อันตรายสูง [5]

ค่าระดับความปลอดภัย Safety Integrity Level (SIL)	Average probability of failure to perform its design function on demand (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

2.5 การทนทานต่อความล้มเหลวของอุปกรณ์

IEC 61511-1 [11] ข้อย่อย 11.4 ได้แสดงความต้องการของจำนวนอุปกรณ์ต่ำสุด ที่ยอมให้เกิดความล้มเหลวขึ้น (Minimum Hardware Fault Tolerance) และยังคงทำให้ระบบสามารถทำงานตามฟังก์ชั่นนิรภัยที่ต้องการได้ถึงแม้ว่าความล้มเหลวจะเกิดขึ้นมากกว่า 1 ครั้ง ตามค่าระดับความปลอดภัย แสดงได้ตามตารางที่ 2.3

ตารางที่ 2.3 ตารางจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาด

Minimum Hardware Requirements according SIL	
SIL	Minimum HFT
1 (any mode)	0
2 (Low demand mode)	0
3 (High demand mode and Continuous mode)	1
4 (any mode)	1
5 (any mode)	2

จากตารางที่ 2.3 มาตรฐาน IEC 61511-1 ให้ผู้ออกแบบสามารถเลือกใช้ผลิตภัณฑ์ที่อยู่บนพื้นฐานข้อกำหนด Prior Use ตามมาตรฐาน IEC 61511-1: 2016 ข้อย่อย 11.5.3 จะต้องพิจารณาสิ่งต่างๆดังนี้

a) ต้องมีหลักฐานเพียงพอแสดงให้เห็นว่าอุปกรณ์มีความเหมาะสมกับการใช้งานในระบบวัดคุมนิรภัย
b) ต้องมีหลักฐาน ด้านคุณภาพในสิ่งต่างๆดังนี้
   - พิจารณาคุณภาพผู้ผลิต
   - มีการแสดงรายละเอียดของอุปกรณ์อย่างเพียงพอง
   - แสดงสมรรถนะการทำงานในสภาวะและสิ่งแวดล้มที่คล้ายคลึง
   - จำนวนและปริมาณประสบการณ์ในการทำงาน

ถ้าเป็นไปตามข้อกำหนดดังกล่าวข้างต้น สามารถเลือกใช้อุปกรณ์สำหรับฟังก์ชั่นนิรภัยได้ตามตารางที่ 2.3 นอกจากนั้นมาตรฐาน IEC 61511 ได้กำหนดทางเลือกให้กับผู้ใช้งานสามารถใช้ตารางอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดในมาตรฐาน IEC 61508 โดยแสดงตามตารางที่ 2.4 และ 2.5

ตารางที่ 2.4 ตารางจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดตามมาตรฐาน IEC 61508 สำหรับอุปกรณ์ Type A

Safe Failure Fraction of an Element	Hardware Fault Tolerance		
	0	1	2
<60%	SIL1	SIL2	SIL3
60%-<90%	SIL2	SIL3	SIL4
90%-<99%	SIL3	SIL4	SIL4
>-99%	SIL3	SIL4	SIL4

ตารางที่ 2.5 ตารางจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดตามมาตรฐาน IEC 61508 สำหรับอุปกรณ์ Type B

Safe Failure Fraction of an Element	Hardware Fault Tolerance		
	0	1	2
<60%	**Not Allowed**	**SIL1**	**SIL2**
60%-<90%	**SIL1**	**SIL2**	**SIL3**

ตารางที่ 2.5 ตารางจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดตามมาตรฐาน IEC 61508 สำหรับอุปกรณ์ Type B (ต่อ)

Safe Failure Fraction of an Element	Hardware Fault Tolerance		
	0	1	2
90%-<99%	SIL2	SIL3	SIL4
>-99%	SIL3	SIL4	SIL4

ตารางทั้งสองจะแบ่งแยกส่วนประกอบอุปกรณ์เป็น 2 ชนิดคือ อุปกรณ์ที่ประกอบไปด้วยส่วนประกอบชนิด A และส่วนประกอบชนิด B อุปกรณ์ที่ประกอบไปด้วยส่วนประกอบทั้ง 2 ชนิดนี้ถูกเรียกว่าระบบย่อย (Subsystem) โดยอุปกรณ์ทั้งสองชนิดสามารถแสดงรายละเอียดได้ดังนี้

อุปกรณ์ชนิด A (Type A)

เครื่องมือวัดที่ถูกจัดอยู่ในชนิดนี้เป็นอุปกรณ์ที่มีส่วนประกอบของชิ้นส่วนพื้นฐานที่ใช้กันอยู่ทั่วไป อาทิ เช่น ตัวทรานซิสเตอร์, ตัวคาแพซิสเตอร์, ตัวต้านทาน และขดลวด เป็นต้น อุปกรณ์เหล่านี้สามารถใช้งานได้เป็นเวลานานและสามารถทำการตรวจสอบการทำงานได้อย่างสมบูรณ์ อุปกรณ์การวัดต่อเนื่องแบบทั่วไป (Conventional Analogue Transmitter) อุปกรณ์การวัดแบบหน้าสัมผัส อาทิเช่น สวิตช์ระดับ (Level Switch) สวิตช์ความดัน (Pressure Switch) และสวิตช์ตำแหน่ง (Position Switch) เป็นต้น อุปกรณ์เหล่านี้จัดเป็นอุปกรณ์ชนิด A

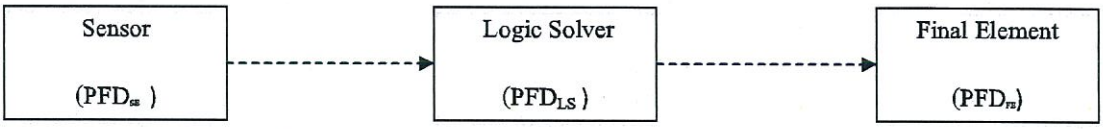
อุปกรณ์ชนิด B (Type B)

เครื่องมือวัดที่ถูกจัดอยู่ในชนิดนี้เป็นอุปกรณ์ที่มีส่วนประกอบของชิ้นส่วน ที่ใช้เทคโนโลยีสมัยใหม่ อาทิเช่น วงจรรวม (Integrated Circuit; IC) หรือไมโครโปรเซสเซอ (Microprocessor) เป็นต้น อุปกรณ์เหล่านี้ไม่สามารถใช้งานได้เป็นเวลานานและไม่สามารถทำการตรวจสอบการทำงานได้อย่างสมบูรณ์

2.5.1 ระบบวัดคุมนิรภัย (Safety Instrumented System)

ระบบวัดคุมนิรภัยสามารที่จะประกอบด้วยฟังก์ชั่นนิรภัยหรือ SIF (Safety Instrumented Functions) ทำหน้าที่ป้องกันอันตรายต่างๆตามที่กำหนด ฟังก์ชั่นนิรภัยจะประกอบไปด้วย 3 ส่วนดังนี้

อุปกรณ์การวัด (Sensing Element) ส่วนประมวลผล (Logic Solver) และอุปกรณ์สุดท้าย (Final Element) ซึ่งในแต่ละส่วนจะมีค่าความล้มเหลวอันตราย (Dangerous Failure) ของตัวเอง หลังจากค่าระดับความปลอดภัยหรือ SIL ได้ถูกกำหนดให้กับฟังก์ชั่นนิรภัยแล้วก็จะได้ผลรวมค่าเฉลี่ยความล้มเหลวอันตรายของฟังก์ชั่นนิรภัยตามรูป 2.7 จากนั้นนำค่าเฉลี่ยความล้มเหลวอันตรายของทุกๆส่วนในฟังก์ชั่นนิรภัยมารวมกัน ซึ่งผลลัพธ์ที่ได้จะต้องน้อยกว่าค่าเฉลี่ยความล้มเหลวอันตรายในระดับความปลอดภัยนั้น โดยสมการแสดงความล้มเหลวอันตรายได้ดังนี้



รูปที่ 2.7 ฟังก์ชันวัดคุมนิรภัยในระบบวัดคุมนิรภัย

$$PFD_{avg} = PFD_{SE} + PFD_{LS} + PFD_{FE} \quad (2.1)$$

เมื่อ

PFD_{avg} = ผลรวมค่าเฉลี่ยความล้มเหลวอันตรายของฟังก์ชันวัดคุมนิรภัย

PFD_{SE} = ค่าเฉลี่ยความล้มเหลวอันตรายของอุปกรณ์การวัด

PFD_{LS} = ค่าเฉลี่ยความล้มเหลวอันตรายของส่วนประมวลผล

PFD_{FE} = ค่าเฉลี่ยความล้มเหลวอันตรายของอุปกรณ์สุดท้าย

จากสมการที่ 2.1 จะเห็นได้ว่าการออกแบบสามารถทำได้โดยการเลือกใช้อุปกรณ์ในรูปแบบต่าง ๆ ทั้ง 3 ส่วน เพื่อให้ผลรวมค่าเฉลี่ยความล้มเหลวอันตรายมีค่าน้อยกว่าค่าเฉลี่ยความล้มเหลวอันตรายของค่าระดับความปลอดภัยที่ต้องการ

2.6 ความล้มเหลวในระบบนิรภัย (Failure in Safety System)

ความล้มเหลวที่เกิดขึ้นในส่วนต่างๆของระบบนิรภัยเมื่อเกิดขึ้นแล้วทำให้ระบบไม่สามารถทำงานหรือตอบสนองความผิดปกติที่ออกแบบไว้ได้ มาตรฐาน IEC 61508-4 ได้แสดงความล้มเหลวประเภทต่างๆดังนี้

1. Random hardware failure
2. Systematic failure

2.6.1 Random hardware failure

ความล้มเหลวในการทำงานของชิ้นส่วนหรืออุปกรณ์ต่างๆแบบนี้จะเกิดตามเวลาแบบสุ่ม (Random) เนื่องจากสาเหตุการเสื่อมสภาพทางกลไก จากการใช้งาน และ ความล้มเหลวประเภทนี้เกิดจากผลกระทบอื่นๆ เช่น การกัดกร่อน ความร้อน และการใช้งานนานๆ เนื่องจากความล้มเหลวเป็นแบบสุ่ม ข้อมูลทางสถิติสามารถหาได้จากการทดสอบและประวัติของประเภทความล้มเหลว ดังนั้นความน่าจะเป็นของความล้มเหลวแบบสุ่มนี้สามารถคำนวณได้

2.6.2 Systematic failure

ความล้มเหลวแบบระบบความล้มเหลวที่เกี่ยวข้องกับสาเหตุบางอย่างสามารถค้นหาได้ ซึ่งสามารถแก้ไขหรือตัดออกโดยการปรับเปลี่ยนออกแบบกระบวนการผลิต ขั้นตอนการดำเนินงานหรือปัจจัยอื่นๆที่เกี่ยวข้อง

2.7 ประเภทความล้มเหลวในระบบนิรภัย (Failure type in Safety system)

หลักการพื้นฐานในการออกแบบระบบนิรภัยเป็นการออกแบบหรือเลือกใช้อุปกรณ์ในส่วนต่างๆของระบบนิรภัย เพื่อทำให้ระบบมีโอกาสที่จะเกิดความล้มเหลวอันตรายอยู่ในค่าที่กำหนด ความล้มเหลวพื้นฐานสำคัญที่จะต้องพิจารณาในการออกแบบมีอยู่ 2 ประเภทคือ

2.7.1 ความล้มเหลวนิรภัยตรวจจับได้ (Safe Detected Failure)

ความล้มเหลวใดๆเมื่อเกิดขึ้นแล้วระบบนิรภัยตรวจจับได้ ซึ่งความล้มเหลวประเภทนี้จะเป็นความล้มเหลวที่เมื่อเกิดขึ้นแล้วทำให้ระบบนิรภัยทำงานหรืออาจจะส่งผลทำให้กระบวนการผลิตหยุดทำงานได้

2.7.2 ความล้มเหลวนิรภัยตรวจจับไม่ได้ (Safe Undetected Failure)

ความล้มเหลวใดๆเมื่อเกิดขึ้นแล้วระบบนิรภัยตรวจจับไม่ได้ ซึ่งความล้มเหลวประเภทนี้จะเป็นความล้มเหลวที่เมื่อเกิดขึ้นแล้วทำให้ระบบนิรภัยทำงานหรืออาจจะส่งผลทำให้กระบวนการผลิตหยุดทำงานได้แต่ผู้ใช้งานจะได้รู้ว่าเกิดความล้มเหลวนิรภัย

2.7.3 ความล้มเหลวอันตรายตรวจจับได้ (Dangerous Detected Failure)

ความล้มเหลวใดๆเมื่อเกิดขึ้นแล้วระบบนิรภัยตรวจจับได้ ซึ่งความล้มเหลวประเภทนี้จะเป็นความล้มเหลวที่เมื่อเกิดขึ้นแล้วจะขัดขวางทำให้ระบบนิรภัยไม่สามารถทำงานได้ในเวลาที่ต้องการ แต่ความล้มเหลวประเภทนี้สามารถตรวจจับได้และแก้ไขให้ระบบกลับมาทำงานได้ปกติ

2.7.4 ความล้มเหลวอันตรายตรวจจับไม่ได้ (Dangerous Detected Failure)

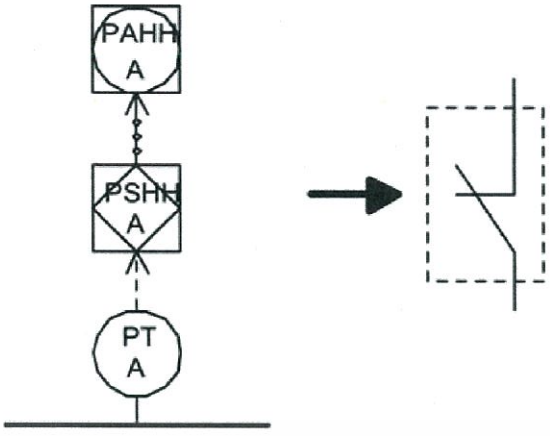
ความล้มเหลวใดๆเมื่อเกิดขึ้นแล้ว ระบบนิรภัยตรวจจับไม่ได้ ซึ่งความล้มเหลวประเภทนี้จะเป็นความล้มเหลวที่อันตรายที่สุดเมื่อเกิดขึ้นแล้วจะขัดขวางทำให้ระบบนิรภัยไม่สามารถทำงานได้ในเวลาที่ต้องการ แต่ความล้มเหลวประเภทนี้ไม่สามารถตรวจจับได้จึงไม่สามารถแก้ไขให้ระบบกลับมาทำงานได้ในช่วงเวลาปกติ

2.8 รูปแบบของอุปกรณ์วัดคุมนิรภัย (Sensing Element Architecture)

ในส่วนนี้ได้อธิบายถึงรูปแบบและลักษณะการทำงานต่างๆของอุปกรณ์การวัดของระบบประมวลผลและของอุปกรณ์สุดท้าย เพื่อที่สามารถเลือกใช้งานได้อย่างเหมาะสม รูปแบบพื้นฐานที่อุปกรณ์การวัดใช้กันอย่างแพร่หลายในระบบวัดคุมนิรภัยมี 5 รูปแบบดังนี้

2.8.1 อุปกรณ์การวัดรูปแบบ 1oo1 (One out of One voting)

รูปแบบนี้ใช้อุปกรณ์การวัดเพียงตัวเดียวต่อกับระบบวัดคุมนิรภัย ในการทำงานถ้าอุปกรณ์วัดค่าความผิดปกติได้หรือถึงจุดทำงานที่กำหนดไว้ก็จะทำให้ระบบวัดคุมนิรภัยทำงานทันที ซึ่งสามารถแสดงการเปรียบเทียบได้ในรูปสวิตช์ปกติเปิดหนึ่งตัว (ในสภาวะทำงานหรือเมื่อจ่ายพลังงานให้อุปกรณ์จะทำให้สวิตช์จะอยู่ในตำแหน่งปิด) แต่ถ้าเกิดความล้มเหลวอันตรายขึ้นและระบบวัดคุมนิรภัยไม่สามารถตรวจจับความผิดพลาดนั้นได้ จะทำให้กระบวนการผลิตเข้าสู่สภาวะอันตราย เพราะระบบวัดคุมนิรภัยไม่สามารถทำงานได้เป็นการทำงานแบบล้มเหลวนิรภัย (Fail Safe Design) คือเมื่อเกิดปัญหาการผิดพลาดใดๆกับระบบจะทำให้อุปกรณ์สุดท้ายหยุดทำงาน นอกจากนั้นแล้วอุปกรณ์การวัดในรูปแบบนี้ที่ไม่มีการตรวจสอบความผิดพลาดด้วยตัวเอง ดังนั้นเมื่อเกิดความล้มเหลวอันตรายขึ้นในอุปกรณ์ เช่น อุปกรณ์การวัดไม่ตอบสนองต่อการเปลี่ยนแปลงของค่าตัวแปรที่ต้องการวัดเป็นต้น ซึ่งจะเป็นสาเหตุทำให้กระบวนการผลิตเกิดความผิดปกติขึ้นจะทำให้ระบบวัดคุมนิรภัยไม่สามารถทำงานได้ในเวลาที่ต้องการ โดยความล้มเหลวอันตรายในอุปกรณ์ของรูปแบบนี้จะถูกตรวจพบเมื่อถึงเวลาในการทดสอบการทำงานของระบบนิรภัย อุปกรณ์การวัดรูปแบบ 1oo1 และโปรแกรมการทำงานแสดงในรูป 2.8



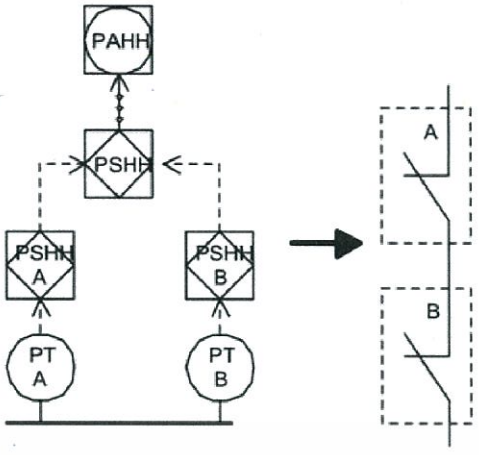
อุปกรณ์การวัดแบบ 1oo1 บนแผนภาพกระบวนการผลิต

โปรแกรมของอุปกรณ์การวัดแบบ 1oo1 ในระบบวัดคุมนิรภัย

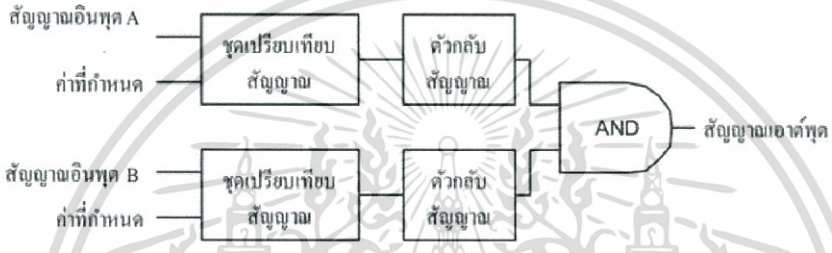
รูปที่ 2.8 อุปกรณ์การวัดรูปแบบ 1oo1

2.8.2 อุปกรณ์การวัดรูปแบบ 1oo2 (One out of Two Voting)

รูปแบบนี้ใช้อุปกรณ์การวัดรูปแบบ 1oo2 ใช้อุปกรณ์การวัดสองตัวต่อกับระบบวัดคุมนิรภัย ให้มีการทำงานเป็นแบบอนุกรม ในการทำงานถ้าอุปกรณ์ตัวใดตัวหนึ่งวัดค่าความผิดปกติได้หรือถึงจุดทำงานที่กำหนดไว้ก็จะทำให้ระบบวัดคุมนิรภัยทำงานทันที ซึ่งสามารถแสดงในรูปสวิทช์ปกติเปิดสองตัวต่ออนุกรมกัน (ในสภาวะทำงานหรือเมื่อจ่ายพลังงานให้อุปกรณ์จะทำให้สวิตช์จะอยู่ในตำแหน่งปิด) แต่ถ้าเกิดความล้มเหลวอันตรายในตัวอุปกรณ์การวัดตัวใดตัวหนึ่ง และระบบวัดคุมนิรภัยไม่สามารถตรวจจับความผิดพลาดที่เกิดขึ้นนั้นได้ จะมีอุปกรณ์การวัดตัวที่สองยังคงทำหน้าที่ต่อไปได้ รูปแบบนี้ระบบวัดคุมนิรภัยจะไม่สามารถตรวจสอบความผิดพลาดของอุปกรณ์เหล่านี้ได้ด้วยตัวเอง ในการทำงานจะมีการลงมติจากหนึ่งในสอง ดังนั้นเมื่ออุปกรณ์ทั้งสองตัวเกิดความล้มเหลวอันตรายขึ้น เช่น อุปกรณ์การวัดไม่ตอบสนองต่อการเปลี่ยนแปลงของค่าที่ต้องการวัด เป็นต้น ซึ่งจะทำให้กระบวนการผลิตเข้าสู่สภาวะอันตรายเพราะเมื่อกระบวนการผลิตเกิดความล้มเหลวอันตรายเพียงตัวเดียวจะยังคงเหลืออุปกรณ์อีกหนึ่งตัวทำงานในรูปแบบ 1oo1 โดยความล้มเหลวอันตรายของรูปแบบนี้จะสามารถตรวจพบได้เมื่อถึงเวลาในการทดสอบการทำงานของระบบวัดคุมนิรภัยสามารถแสดงการลดรูปแบบการทำงานหลังจากอุปกรณ์เกิดความผิดพลาดขึ้น อุปกรณ์การวัดรูปแบบ 1oo2 และโปรแกรมการทำงานแสดงในรูป 2.9



อุปกรณ์การวัดแบบ 1oo2 บนแผนภาพกระบวนการผลิต

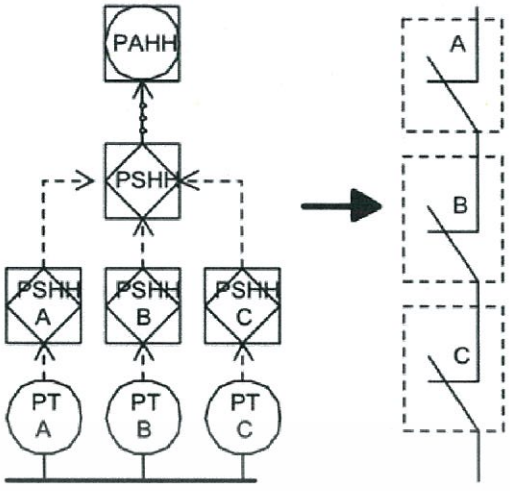


โปรแกรมของอุปกรณ์การวัดแบบ 1oo2 ในระบบวัดคุมนิรภัย

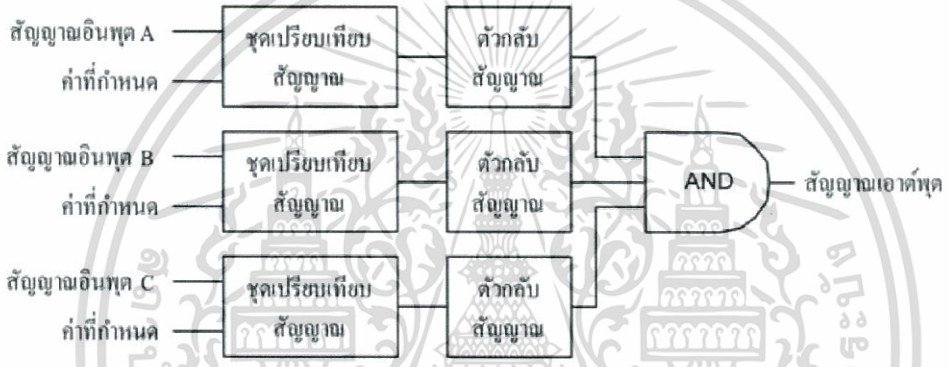
รูปที่ 2.9 อุปกรณ์การวัดรูปแบบ 1oo2

2.8.3 อุปกรณ์การวัดรูปแบบ 1oo3 (One out of Three Voting)

รูปแบบนี้ใช้อุปกรณ์การวัดรูปแบบ 1oo3 ใช้อุปกรณ์การวัดสามตัวต่อกับระบบวัดคุมนิรภัย ให้มีการทำงานเป็นแบบอนุกรมในการทำงานถ้าอุปกรณ์การวัดตัวใดตัวหนึ่งวัดค่าความผิดปกติได้หรือถึงจุดทำงานที่กำหนดไว้ก็จะทำให้ระบบวัดคุมนิรภัยทำงานทันที ซึ่งสามารถแสดงในรูปสวิตช์ปกติเปิดสามตัวต่ออนุกรมกัน (ในสภาวะทำงานหรือเมื่อจ่ายพลังงานให้อุปกรณ์ จะทำให้สวิตช์จะอยู่ในตำแหน่งปิด) แต่ถ้าเกิดความล้มเหลวอันตรายในตัวอุปกรณ์การวัดตัวที่หนึ่งหรือตัวที่สอง และระบบวัดคุมนิรภัยไม่สามารถตรวจจับความผิดพลาดนั้นได้ จะมีอุปกรณ์ตัวที่สองหรือตัวที่สามยังคงทำหน้าที่ต่อไปได้ในรูปแบบ 1oo2 หรือ 1oo1 แต่ในรูปแบบนี้จะมีโอกาสให้เกิดการทำงานแบบไม่เป็นจริง (False Tip) ได้สูงเนื่องจากมีจำนวนอุปกรณ์มากกว่ารูปแบบอื่นๆ อุปกรณ์การวัดรูปแบบ 1oo3 และโปรแกรมการทำงานแสดงในรูป 2.10



อุปกรณ์การวัดแบบ 1oo3 บนแผนภาพกระบวนการผลิต



โปรแกรมของอุปกรณ์การวัดแบบ 1oo3 ในระบบวัดคุมนิรภัย

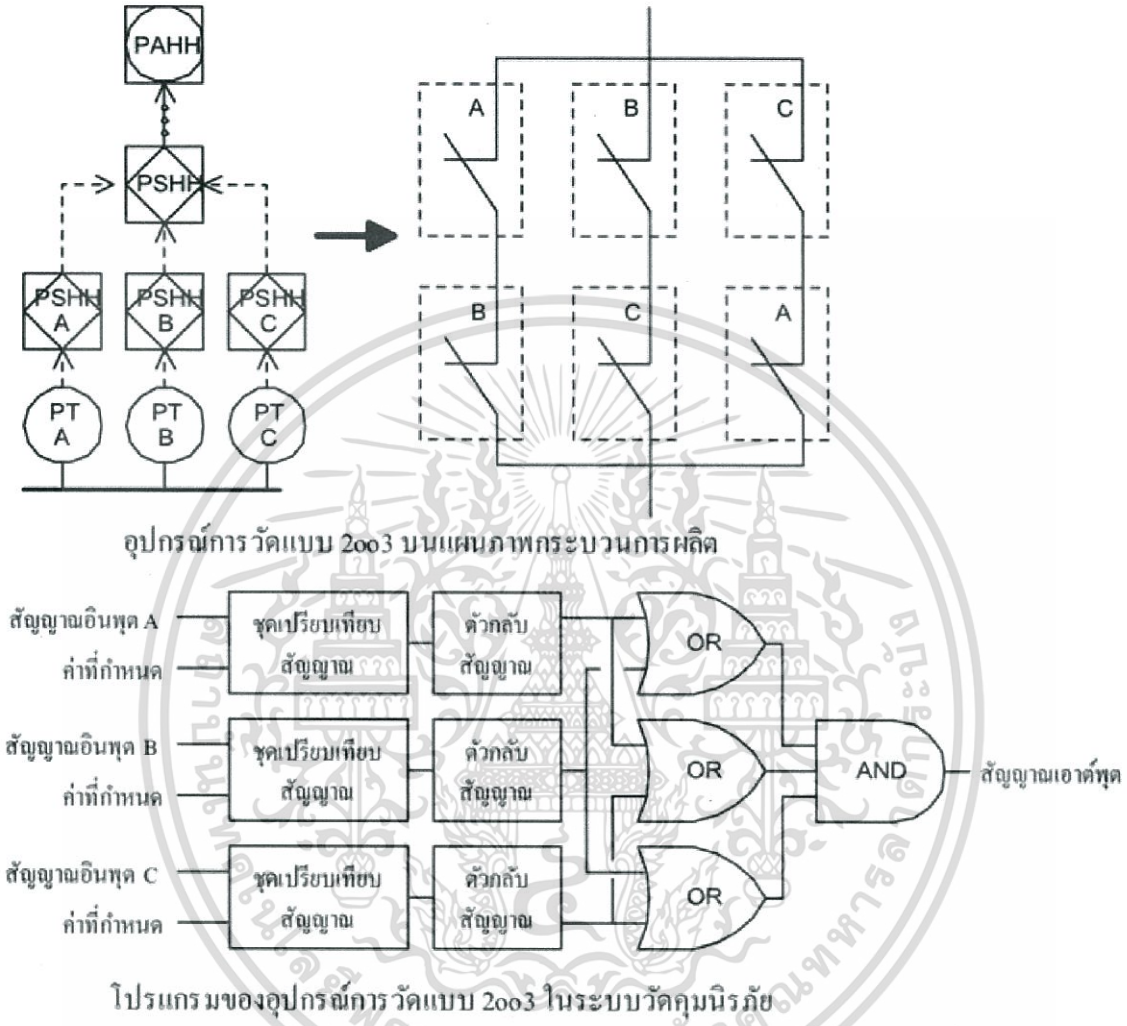
รูปที่ 2.10 อุปกรณ์การวัดรูปแบบ 1oo3

2.8.4 อุปกรณ์การวัดรูปแบบ 2oo3 (Two out of Three Voting)

รูปแบบนี้ใช้อุปกรณ์การวัดแบบ 2oo3 ใช้อุปกรณ์การวัดสามตัวต่อกับระบบวัดคุมนิรภัยให้มีการทำงานเป็นแบบลงมติ (Voting) จากสองในสามรูปแบบนี้ระบบวัดคุมนิรภัยจะทำงานก็ต่อเมื่ออุปกรณ์การวัดสองตัววัดค่าความผิดปกติได้ ซึ่งสามารถแสดงในรูปสวิตช์ปกติเปิดสามตัวโดยสวิตช์สองตัวต่ออนุกรมกันสามชุดจากนั้นนำมาต่อขนานกัน (ในสภาวะทำงานหรือเมื่อจ่ายพลังงานให้อุปกรณ์จะทำให้สวิตช์จะอยู่ในตำแหน่งปิด) แต่ถ้าเกิดความล้มเหลวอันตรายในอุปกรณ์การวัดตัวใดตัวหนึ่งและระบบวัดคุมนิรภัยไม่สามารถตรวจจับความผิดพลาดนั้นได้ จะมีอุปกรณ์ตัวที่สองและตัวที่สามยังคงทำหน้าที่ต่อไปได้ในรูปแบบ 2oo2 แต่ในรูปแบบนี้จะมีความเชื่อมั่นในการทำงานน้อยกว่าในรูปแบบ 1oo3 ในรูปแบบ 2oo3 ระบบวัดคุมนิรภัยสามารถตรวจสอบความผิดพลาดของอุปกรณ์ได้ด้วยตนเอง โดยการเปรียบเทียบค่าการวัดที่ได้จากอุปกรณ์การวัดทั้งสามตัวซึ่งสามารถทำให้ทราบได้ว่าอุปกรณ์ตัวใดเกิดความผิดพลาดขึ้นและถ้า

อุปกรณ์ตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายก็สามารถซ่อมแซมได้ทันที แต่ถ้าอุปกรณ์ตั้งแต่สองตัวขึ้นไป (A & B, B & C, หรือ A & C) เกิดความล้มเหลวอันตรายขึ้น อาทิเช่น อุปกรณ์การวัดไม่ตอบสนองต่อการเปลี่ยนแปลงของค่าที่ต้องการวัดจะทำให้กระบวนการผลิตเข้าสู่สภาวะอันตราย เพราะเมื่อกระบวนการผลิตเกิดความผิดปกติขึ้นจะทำให้ระบบวัดคุมนิรภัยไม่สามารถทำงาน

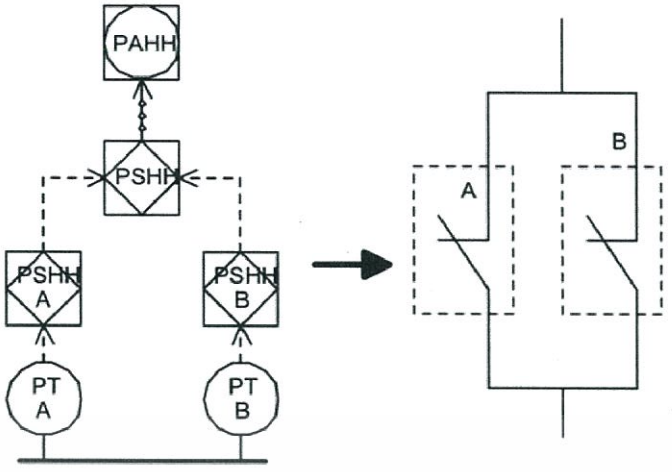
ได้ แต่ถ้าอุปกรณ์เพียงตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายขึ้น ระบบจะเปลี่ยนการทำงานไปเป็นรูปแบบ 2oo2 (Two out of Two Voting) สามารถแสดงการลดรูปแบบการทำงานหลังจากอุปกรณ์เกิดความผิดพลาดขึ้น อุปกรณ์การวัดรูปแบบ 2oo3 และโปรแกรมการทำงานแสดงในรูป 2.11



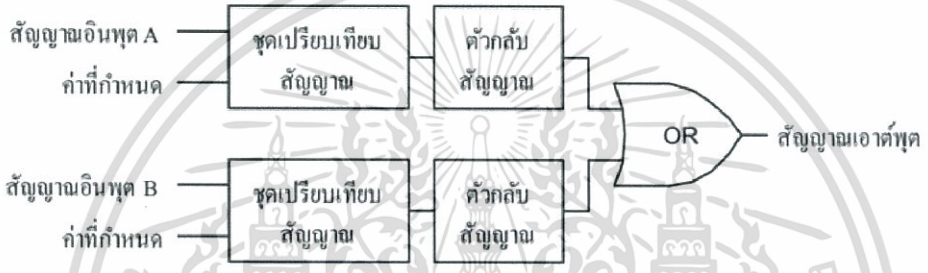
รูปที่ 2.11 อุปกรณ์การวัดรูปแบบ 2oo3

2.8.5 อุปกรณ์การวัดรูปแบบ 2oo2 (Two out of Two Voting)

อุปกรณ์การวัดแบบ 2oo2 ใช้อุปกรณ์สองตัวต่อกับระบบวัดคุมนิรภัยให้มีการทำงานเป็นแบบขนาน รูปแบบนี้ระบบวัดคุมนิรภัยจะทำงานก็ต่อเมื่ออุปกรณ์การวัดสองตัววัดค่าความผิดปกติได้ ซึ่งสามารถแสดงได้ในรูปสวิตช์ปกติเปิดสองตัวต่อขนานกัน(ในสภาวะทำงานหรือเมื่อจ่ายพลังงานให้อุปกรณ์จะทำให้สวิตช์จะอยู่ในตำแหน่งปิด) แต่ถ้าเกิดความผิดพลาดในตัวอุปกรณ์ที่ทำให้เกิดอันตรายบนอุปกรณ์ตัวใดตัวหนึ่ง และระบบวัดคุมนิรภัยไม่สามารถตรวจจับความผิดพลาดนั้นได้ จะทำให้ระบบวัดคุมนิรภัยไม่สามารถทำหน้าที่ได้อย่างถูกต้องต่อไปได้ เพราะการทำงานในรูปแบบนี้ต้องการอุปกรณ์ทั้งสองตัวในการทำงาน ในรูปแบบนี้จะมีการทำงานคล้ายกันกับในรูปแบบ 1oo1 แต่ในรูปแบบนี้จะมีค่าความพร้อมใช้งาน (Availability) สูงกว่าแบบ 1oo1 อุปกรณ์การวัดรูปแบบ 2oo2 และโปรแกรมการทำงานแสดงในรูป 2.12



อุปกรณ์การวัดแบบ 2oo2 บนแผนภาพกระบวนการผลิต



โปรแกรมของอุปกรณ์การวัดแบบ 2oo2 ในระบบวัดคุมนิรภัย

รูปที่ 2.12 อุปกรณ์การวัดรูปแบบ 2oo2

2.9 แหล่งข้อมูลอัตราความล้มเหลวของอุปกรณ์

ข้อมูลอัตราความล้มเหลวของอุปกรณ์หรือ Failure rate ของเครื่องมือวัดและควบคุมที่ใช้ในฟังก์ชั่นนิรภัยจะมีความสำคัญสำหรับใช้ในขั้นตอนตรวจสอบค่าระดับความปลอดภัย เพื่อใช้ยืนยันว่าผู้ใช้งานเลือกใช้เครื่องมือวัดและควบคุมในฟังก์ชั่นนิรภัยเหมาะกับค่าระดับความปลอดภัยที่ได้กำหนดไว้โดยสามารถหาได้จาก 2 แหล่งข้อมูลดังนี้

2.9.1 ผู้ผลิต

จากข้อกำหนดของมาตรฐานให้ผู้ผลิตต้องจัดเตรียมข้อมูลให้แก่ผู้ใช้งานอุปกรณ์ต่างๆเป็นไปตามข้อกำหนดมาตรฐานและควรมีการตรวจสอบรับรองจากสถาบันอิสระ ข้อมูลควรประกอบด้วยสิ่งต่างๆดังนี้

1. ความสามารถในระดับความปลอดภัยต่าง ๆ
2. โหมดความล้มเหลว (Failure Mode) และอัตราความล้มเหลวสภาวะการทำงานที่กำหนด
3. ข้อจำกัดทางด้านสิ่งแวดล้มเพื่อไม่ให้อัตราความล้มเหลวเกินกว่าที่ประมาณไว้
4. ข้อกำหนดหรือรายละเอียดในกรทดสอบการทำงานหรือซ่อมบำรุง
5. อัตราวินิจฉัยความล้มเหลว (Diagnostic Coverage)
6. คู่มือความปลอดภัย (Safety Manual)

2.9.2 คู่มือหรือฐานข้อมูลจากมาตรฐาน

ในบางครั้งข้อมูลผู้ผลิตอาจไม่ครบถ้วนเนื่องจากเป็นเครื่องมือวัดและควบคุมที่ไม่ได้ถูกออกแบบให้เป็นไปตามข้อกำหนดของมาตรฐาน IEC 61511/61508 ก็อาจใช้คู่มือหรือฐานข้อมูลที่ได้มีการเก็บรวบรวมได้ตัวอย่างต่อไปนี้

1. IEC 61709 (2011) : Electronic components-Reliability-Reference condition for failure rate and Stress model for convertion [7]

2. OREDA (2009) : Offshore Reliability Data [8]

3. SINTEF (2013a) : Reliability Data for Safety Instrumented System, PDS data Handbook [9]

4. Exida (2007) : Safety Equipment Handbook [10]

2.10 โมเดลมาร์คอฟ

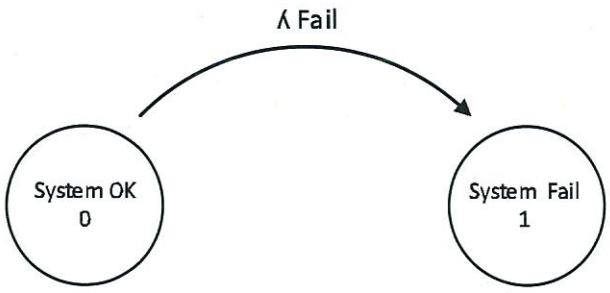
โมเดลมาร์คอฟ คือโมเดลที่ใช้เพื่อหาค่าความน่าจะเป็น (Probability)อีกเทคนิคหนึ่งในการคำนวณค่าระดับความปลอดภัยที่จะเกิดขึ้นในการเกิดสถานะ (State) สถานะใดสถานะหนึ่งประกอบด้วยสถานะและการเปลี่ยนสถานะ (Transition) โดย สถานะแทนการทำงานของอุปกรณ์และการเปลี่ยนแปลงจากสถานะหนึ่งไปยังอีกสถานะหนึ่งนั้นเป็นค่าความผิดพลาด (Failure rate) หรือความน่าจะเป็นของการซ่อมแซมของอุปกรณ์ (Restore rate) แสดงในรูป 2.13

รูปที่ 2.13 สัญลักษณ์ของโมเดลมาร์คอฟ

ที่มา William M. (2005) [3]

ระบบของโมเดลมาร์คอฟที่เกิดจากความล้มเหลวของสถานะของอุปกรณ์นั้นมีอยู่ 2 ระบบ คือ

1. โมเดลมาร์คอฟที่สามารถย้อนกลับไม่ได้เมื่อเกิดการเปลี่ยนแปลงสถานะที่เกิดจากการล้มเหลวของอุปกรณ์ไปอีกสถานะหนึ่งอุปกรณ์จะไม่สามารถย้อนกลับมายังสถานะเดิมได้



รูปที่ 2.14 ระบบโมเดลมาร์คอฟย้อนกลับไม่ได้

2. โมเดลมาร์คอฟที่สามารถย้อนกลับได้ เมื่อเกิดการเปลี่ยนแปลงสถานะที่เกิดจากการล้มเหลวของอุปกรณ์ไปอีกสถานะหนึ่งอุปกรณ์จะสามารถย้อนกลับมายังสถานะเดิมได้

รูปที่ 2.15 ระบบโมเดลมาร์คอฟย้อนกลับได้

2.10.1 ประเภทโมเดลมาร์คอฟ (Markov Model Types)

ประเภทโมเดลมาร์คอฟถูกแบ่ง 4 ประเภทโดยมาจาก 2 สาเหตุหลักคือ เวลาและสถานะ ดังต่อไปนี้ สถานะต่อเนื่อง (continuous states) สถานะไม่ต่อเนื่อง(discrete states) เวลาต่อเนื่อง (continuous time) และ เวลาไม่ต่อเนื่อง(discrete time).

ตารางที่ 2.6 ตารางประเภทโมเดลมาร์คอฟ

State Space	Time	Application
Continuous	Continuous	Not in Reliability Analysis
Continuous	Discrete	Not in Reliability Analysis
Discrete	Continuous	Analytical Solutions
Discrete	Discrete	Numerical Solutions

1. สถานะปกติ (Regular State)

โมเดลมาร์คอฟที่จะมีสถานะคงที่ ซึ่งโมเดลมาร์คอฟที่จะเรียกว่าเป็นสถานะปกติ หรือสถานะ Ergotic ก็ต่อเมื่อเกิดความล้มเหลวแล้วสถานะมีการเปลี่ยนไปไปยังสถานะอื่น

2. สถานะดูดซึม (Absorbing State)

โมเดลมาร์คอฟที่เข้าไปสู่สถานะใดสถานะหนึ่งในเวลาหนึ่งและไม่สามารถเปลี่ยนไปสู่สถานะอื่นๆได้ในอนาคต หรือกล่าวได้ว่าถ้าเข้าไปสู่สถานะใดแล้วจะต้องอยู่ในสถานะนั้นตลอดไป จะเรียกสถานะนั้นว่าสถานะดูดซึม หรือสถานะ Non-ergotic

2.11 เทคนิควิธีการมาร์คอฟ

วิธีการในการหาค่าความน่าจะเป็นด้วยวิธีมาคอร์ฟมีหลากหลายวิธี การเลือกใช้งานจึงขึ้นอยู่กับข้อจำกัดของระบบที่ต้องการหาความน่าจะเป็น โดยแสดงในตาราง 2.4

ตารางที่ 2.7 วิธีการมาร์คอฟ

	Ergotic (Regular) Homogeneous	Non-ergotic (Absorbing) Homogeneous	Ergotic (Regular) Non-homogeneous	Non-ergotic (Absorbing) Non-homogeneous
Steady state probability solution via linear equations	Steady State Solution	Not Applicable	Not Applicable	Not Applicable
Time dependent analyticial solutions via differential equations	Continuous Time Solution	Continuous Time Solution	Not Applicable	Not Applicable
Numerical solution for state probability via matrix multiplication	Discrete Time Solution	Discrete Time Solution	Discrete Time Solution	Discrete Time Solution
Analytical / Numerical solution to mean time to first failure via matrix subtraction and inversion	Discrete Time Solution	Discrete Time Solution	Not Applicable	Not Applicable

2.12 ความล้มเหลวร่วมกันหรือ β (Common Cause Failure)

อุปกรณ์เครื่องมือวัดในฟังก์ชันนิรภัยในบางรูปแบบจะมีจำนวนอุปกรณ์ที่มากกว่าหนึ่งตัว ในการติดตั้งอุปกรณ์การวัดเหล่านี้จะถูกติดตั้งอยู่ในสภาวะแวดล้มเดียวกัน ดังนั้นจึงมีโอกาสที่อุปกรณ์ที่มากว่าหนึ่งตัวและมีคุณสมบัติที่เหมือนกันจะเกิดความล้มเหลวร่วมกัน สำหรับอุปกรณ์หรือชิ้นส่วนที่เหมือนกันสามารถแสดงสมการอัตราความล้มเหลวอิสระและความล้มเหลวร่วมกันได้ดังสมการที่ 2.2 และสมการที่ 2.3

$$\lambda_{DD(c)} = \beta_D \lambda_{DD}; \lambda_{DD(i)} = (1-\beta)\lambda_{DD} \quad (2.2)$$

$$\lambda_{DD(c)} = \beta_D \lambda_{DU}; \lambda_{DD(i)} = (1-\beta)\lambda_{DU} \quad (2.3)$$

โดย

λ_{DD} หมายถึง อัตราความล้มเหลวอันตรายร์ หน่วย ครั้ง/ชั่วโมง หรือ ครั้ง/ปี

$\lambda_{DD(c)}$ หมายถึง อัตราความล้มเหลวอันตรายร่วมกัน หน่วย ครั้ง/ชั่วโมง หรือ ครั้ง/ปี

β หมายถึง ความล้มเหลวร่วมกัน

2.13 ค่าความล้มเหลวร่วมกัน β (Common Cause Failure)

ค่าความล้มเหลวร่วมกัน หรือค่า β, β_D มาตรฐาน IEC 61508-6 Annex D ได้แสดงแนวทางในการคำนวณหาค่า β และ β_D สำหรับอุปกรณ์เครื่องมือวัดกับอุปกรณ์สุดท้ายและส่วนประมวลผลที่แยกออกจากกัน เป็นตัวแปรความล้มเหลวร่วมกันสำหรับความล้มเหลวอันตรายตรวจจับไม่ได้ (Undetectable dangerous failure) เป็นตัวแปรความล้มเหลวร่วมกันสำหรับความล้มเหลวอันตรายตรวจจับได้ (Detectable dangerous failure)

2.13.1 การหาค่าความล้มเหลวร่วมกัน (Common Cause Failure) หรือค่า β, β_D

มาตรฐาน IEC 61508-6 Annex D ได้แสดงแนวทางในการคำนวณหาค่า β และ β_D สำหรับอุปกรณ์เครื่องมือวัดกับอุปกรณ์สุดท้ายและส่วนประมลผลที่แยกออกจากกัน

β เป็นตัวแปรความล้มเหลวร่วมกันสำหรับความล้มเหลวอันตรายตรวจจับไม่ได้ (Undetectable dangerous failure)

β_D เป็นตัวแปรความล้มเหลวร่วมกันสำหรับความล้มเหลวอันตรายตรวจจับได้ (Detectable dangerous failure)

ในการออกแบบที่จะทำให้ค่าความเป็นไปได้ของการเกิดความล้มเหลวร่วมกันต่ำสุดสิ่งแรกต้องพิจารณาการป้องกันเหตุการณ์ที่จะเกิดขึ้น การจัดทำแบบแผนและออกแบบที่เหมาะสมในระบบนิภัยสามารถช่วยลดค่า β ที่นำมาใช้ในการประเมิน

ตารางที่ 2.6 ได้แสงตารางของตาราง D.1 ในมาตรฐาน IEC 61508-6 Annex D ได้แสดงค่าจำนวนที่เกี่ยวข้องที่อยู่บนพื้นฐานการตัดสินใจทางวิศวกรรม (Engineering Judgment) ซึ่งเป็นตัวแทนสำหรับแต่ละรายการที่ช่วยลดความล้มเหลวร่วม เนื่องจากอุปกรณ์เครื่องมือวัดกับอุปกรณ์สุดท้ายจะมีการดำเนินการติดตั้งที่แตกต่างจากส่วนประมวลผมที่เป็นระบบอิเลคทรอนิคส์แบบโปรแกรมการทำงานได้ จึงต้องมีการแยกตารางทั้งสองระบบออกจากกัน

ตารางที่ 2.8 รายการที่ช่วยลดความล้มเหลวร่วม

Item	Logic subsystem		Sensor and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Separation / segregation				
Are all signal cables for the channels routed separately at all positions?	1.5	1.5	1	2
Are the logic subsystem channels on separate printed-circuit boards?	3	1	-	-
Are the logic subsystem chanels in separate cabinets?	2.5	0.5	-	-
If the sensors/final elements have Dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?	-	-	2.5	1.5
If the Sensors/final elements have dedicated control electronics, is the electronics for each channel indoors and inseparate cabinets?	-	-	2.5	0.5
Diversity/redundancy				
Do the channels employ different electrical technologies for example, one electronic or programmable electronic and the other relay?	7,0			
Do the channels employ different electronic technologies for example, one electronic, the other programmable electronic?	5,0			

ตารางที่ 2.8 รายการที่ช่วยลดความล้มเหลวร่วม (ต่อ)

Item	Logic subsystem		Sensor and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Do the devices employ different physical principles for the sensing elements for example, pressure and temperature, vane anemometer and Doppler transducer, etc?			7,5	
Do the devices employ different electrical principles/designs for example, digital and analogue, different manufacturer (not re-badged) or different technology?			5,5	
Do the channels employ enhanced redundancy with MooN architecture, where N > M + 2	2,0	0,5	2,0	0,5
Do the channels employ enhanced redundancy with MooN architecture, where N = M + 2	1,0	0,5	1,0	0,5
Is low diversity used, for example hardware diagnostic tests using the same technology?	2,0	1,0		
Is medium diversity used, for example hardware diagnostic tests using different technology?	3,0	1,5		
Were the channels designed by different designers with no communication between them during the design activities?	1,0	1,0		
Are separate test methods and people used for each channel during commissioning?	1,0	0,5	1,0	1,0
Is maintenance on each channel carried out by different people at different times?	2,5		2,5	

ตารางที่ 2.8 รายการที่ช่วยลดความล้มเหลวร่วม (ต่อ)

Item	Logic subsystem		Sensor and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Complexity/design/application/maturity/experience				
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes?	0,5	0,5	0,5	0,5
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	0,5	1,0	1,0	1,0
Is there more than 5 years experience with the same hardware used in similar environments?	1,0	1,5	1,5	1,5
Is the system simple, for example no more than 10 inputs or outputs per channel?		1,0		
Are inputs and outputs protected from potential levels of over-voltage and over-current?	1,5	0,5	1,5	0,5
Are all devices/components conservatively rated (for example, by a factor of 2 or more)?	2,0		2,0	
Assessment/analysis and feedback of data				
Have the results of the failure modes and effects analysis or fault-tree analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?		**3,0**		**3,0**

ตารางที่ 2.8 รายการที่ช่วยลดความล้มเหลวร่วม (ต่อ)

Item	Logic subsystem		Sensor and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Were common cause failures considered in design reviews with the results fed back into the design? (Documentary evidence of the design review activity is required.)		3,0		3,0
Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)	0,5	3,5	0,5	3,5
Procedures/human interface				
Is there a written system of work to ensure that all component failures (or degradations) are detected, the root causes established and other similar items inspected for similar potential causes of failure?		1,5		1,5
Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?	1,5	0,5	2,0	1,0

ตารางที่ 2.8 รายการที่ช่วยลดความล้มเหลวร่วม (ต่อ)

Item	Logic subsystem		Sensor and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Are procedures in place to ensure that: maintenance (including adjustment or calibration) of any part of the independent channels is staggered, and, in addition to the manual checks carried out following maintenance, the diagnostic tests are allowed to run satisfactorily between the completion of maintenance on one channel and the start of maintenance on another?	1,5	0,5	2,0	1,0
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.) intended to be independent of each other, are not to be relocated?	0,5	0,5	0,5	0,5
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0,5	1,0	0,5	1,5
Does the system have low diagnostic coverage (60 % to 90 %) and report failures to the level of a field-replaceable module?	0,5			
Does the system have medium diagnostics coverage (90 % to 99 %) and report failures to the level of a field-replaceable module?	1,5	1,0		

ตารางที่ 2.8 รายการที่ช่วยลดความล้มเหลวร่วม (ต่อ)

Item	Logic subsystem		Sensor and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Does the system have high diagnostics coverage (>99 %) and report failures to the level of a field-replaceable module?	2,5	1,5		
Does the system diagnostic tests report failures to the level of a field-replaceable module?			1,0	1,0
Competence/training/safety culture				
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures?	2,0	3,0	2,0	3,0
Have maintainers been trained (with training documentation) to understand the causes and consequences of common cause failures?	0,5	4,5	0,5	4,5
Environmental control				
Is personnel access limited (for example locked cabinets, inaccessible position)?	0,5	2,5	0,5	2,5
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3,0	1,0	3,0	1,0
Are all signal and power cables separate at all positions?	2,0	1,0	2,0	1,0

ตารางที่ 2.8 รายการที่ช่วยลดความล้มเหลวร่วม (ต่อ)

tem	Logic subsystem		Sensor and final elements	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Environmental testing				
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10,0	10,0	10,0	10,0

NOTE 1 A number of the items relate to the operation of the system, which may be difficult to predict at design time. In these cases, the designers should make reasonable assumptions and subsequently ensure that the eventual user of the system is made aware of, for example, the procedures to be put in place in order to achieve the designed level of safety integrity. This could be by including the necessary information in the accompanying documentation.

NOTE 2 The values in the X and Y columns are based on engineering judgement and take into account the indirect as well as the direct effects of the items in column 1. For example, the use of field-replaceable modules leads to

– repairs being carried out by the manufacturer under controlled conditions instead of (possibly incorrect) repairs beingmade under less appropriate conditions in the field. This leads to a contribution in the Y column because the potential for systematic (and, hence, common cause) failures is reduced;

– a reduction in the need for on-site manual interaction and the ability quickly to replace faulty modules, possibly on-line, so increasing the efficacy of the diagnostics for identifying failures before they become common-cause failures. This leads to a strong entry in the X column.

ตารางที่ 2.9 Value of Z: programmable electronics

Diagnostic Coverage	Diagnostic test interval			
	Less than 1 min	Between 1 min and 5 min	Between 2 Days and one week	Greater than 5 min
≥ 99%	2	1.5	1	0
≥ 90%	1.5	1	0.5	0
≥ 60%	1	0.5	0	0

ตารางที่ 2.10 Value of Z-sensors or final elements

Diagnostic Coverage	Diagnostic test interval			
	Less than 2 hr	Between 2 hr and two days	Between 2 Days and one week	Greater than one week
≥ 99%	2	1.5	1	0
≥ 90%	1.5	1	0.5	0
≥ 60%	1	0.5	0	0

การใช้ค่าในตาราง 2.6 ต้องมีการสืบหารายการที่นำมาใช้ในระบบและรวมค่าที่ได้ของ X_{LS} และ Y_{LS} สำหรับส่วนประมวลผล และ X_{SF} และ Y_{SF} สำหรับอุปกรณ์เครื่องมือวัดกับอุปกรณ์สุดท้าย ค่าที่รวมกันจะเป็นค่า X และ Y ตามลำดับ

ตารางที่ 2.6 และ 2.7 อาจจะถูกใช้ในการกำหนดค่าตัวแปร Z เปอร์เซ็นต์การวินิจฉัยความล้มเหลว โดยค่า S จะสามารถคำนวณได้จากสมการดังนี้

$$S = X+Y \text{ (เพื่อใช้หาค่า } \beta_{int}) \quad (2.5)$$

$$S_D = X(Z+1) + Y \text{ (เพื่อใช้หาค่า } \beta_{Dint}) \quad (2.6)$$

ค่า S และ SD จะเป็นค่าที่ถูกใช้ในตารางที่ 2.8 เพื่อหาค่า β_{int} หรือ β_{Dint} ตามต้องการ อย่างไรก็ตามค่า β ที่ได้จากตารางที่ 4 เป็นค่าความล้มเหลวร่วมกันที่เกี่ยวข้องกับฟังก์ชันนิรภัยในรูปแบบ 1002 เท่านั้น ถ้าเป็นรูปแบบ MooN ค่า β ต้องถูกคูณด้วยตัวแปรคงที่ในตารางที่ D.5 เพื่อให้ได้ค่า β สุดท้าย

ตารางที่ 2.11 Calculation of β_{int} or β_{Dint}

Score (S or S_D)	Corresponding value of βin_t หรือ $\beta_{D\ int}$ for the :	
	Logic Sub System	Sensor or final elements
120 or above	0.50 %	1%
70 to 120	1%	2% 0.5
45 t0 70	2%	5%
Less than 45	5%	10%

NOTE 1 : The maximum levels of $\beta_{D\ int}$ shown in this table are lower than would normally be used, reflecting the use of the techniques specified elsewhere in this standard for the reduction in the probability of systematic failures as a whole, and of common cause failures as a result of this.

NOTE 2 :Values of $\beta_{D\ int}$ lower than 0,5 % for the logic subsystem and 1 % for the sensors would be difficult to justify.

ตารางที่ 2.12 Calculation of β or system with level of redundancy greater than 1oo2

MooN		N			
		2	3	4	5
M	1	β_{int}	0.5 β_{int}	0.3 β_{int}	0.2 β_{int}
	2	-	1.5 β_{int}	0.6 β_{int}	0.4 β_{int}
	3	-	-	1.75 β_{int}	0.8 β_{int}
	4	-	-	-	2 β_{int}

บทที่ 3
การดำเนินการศึกษางานวิจัย

3.1 ขอบเขตของการศึกษา

วิทยานิพนธ์ฉบับนี้มีขั้นตอนของการศึกษาดังต่อไปนี้

1. ศึกษาข้อมูลการวิจัยที่เกี่ยวข้องกับการหาค่าระดับความปลอดภัยของฟังก์ชันวัดคุมนิรภัย

2. ศึกษาและหาตำแหน่งอุปกรณ์วัดคุมที่เป็นฟังก์ชันวัดคุมนิรภัยจากแผนภาพกระบวนการของระบบท่อส่งแก๊ส (Piping and Instrument Flow Diagram, P&I) ดังแสดงในรูปที่ 3.1

3. สร้างโมเดลจากสถานะความล้มเหลวของอุปกรณ์ในระบบเป็นโมเดลมาร์คอฟ

4. หาค่าระดับความปลอดภัยของอุปกรณ์วัดคุมนิรภัยของฟังก์ชันวัดคุมนิรภัย

3.2 กรณีศึกษางานวิจัย

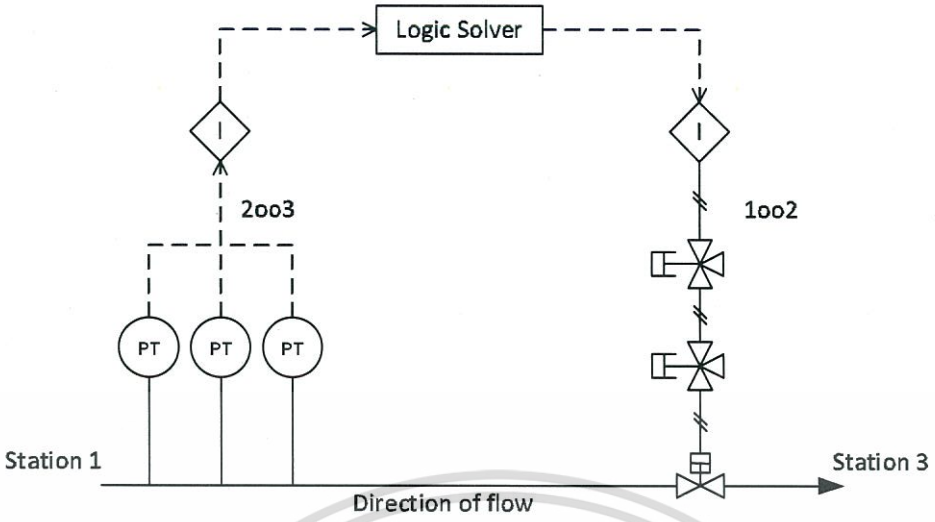
ในงานวิจัยนี้ฟังก์ชันวัดคุมนิรภัยของวาล์วลดความดันตามรายละเอียดในรูปที่ 3.1 การควบคุมกระบวนการได้ตั้งข้อสมมติฐานว่า รับก๊าซธรรมชาติจากสถานีจ่ายก๊าซที่ 1 เพื่อจ่ายก๊าซไปที่สถานี 3 ซึ่งควบคุมโดยมีอุปกรณ์วัดความดัน 3 ตัว โดยมีรูปแบบการทำงานแบบเลือกตั้ง 2oo3 เพื่อส่งสัญญาณควบคุม โดยเมื่ออุปกรณ์ 2 ใน 3 ทำงานหมายความว่าจะมีการส่งสัญญาณไปที่ส่วนประมวลผลระบบวัดคุมนิรภัย ในกรณีที่ความดันเกินจะส่งสัญญาณเพื่อไปสั่งอุปกรณ์ตัวสุดท้ายคือวาล์วลดความดัน หน้าที่วาล์วลดความดันทำงานเพื่อปิดก๊าซที่ไหลเข้า วัดคุมนิรภัยของกระบวนการนี้ประกอบไปด้วย

1. อุปกรณ์วัดความดัน (Presser Transmitter) ทำการวัดความดันท่อส่งก๊าซและส่งสัญญาณไปที่ตัวประมวลผลโดยมีรูปแบบการติดตั้งทำงานแบบเลือกตั้ง 2oo3

2. ตัวประมวลผล (Logic Solver) ทำการประมวลผลสัญญาณจากอุปกรณ์วัดความดันและส่งสัญญาณออกไปที่วาล์วควบคุมความนิรภัย.

3. วาล์วลดความดัน (Block Valve) เป็นอุปกรณ์สุดท้าย (Final Element) ของระบบวัดคุมนิรภัยวาล์วลดความดันจะถูกใช้เป็นตัวที่จะหยุดต้นเหตุของเหตุการณ์อันตรายหรือใช้เป็นตัวจำกัดขอบเขตความเสียหายที่อาจจะเกิดขึ้นโดยทำการปิดท่อส่งก๊าซที่จ่ายไปยังท่อฝั่งขาออก

4. วาล์วย่อย (Solenoid Valve) ทำการรับสัญญาณไฟฟ้าจากระบบวัดคุมนิรภัยเพื่อใช้เปิดปิดให้ความดันอากาศผ่านไปทำการปิดเปิดวาล์วลดความดัน (Block Valve) และโดยมีรูปแบบการติดตั้งทำงานแบบเลือกตั้ง 1oo2



รูปที่ 3.1 แผนภาพกระบวนการของระบบวาล์วลดความดัน

3.3 การประเมินโหมดความล้มเหลวที่สามารถเกิดขึ้นได้ของอุปกรณ์ในระบบ

พิจารณากรณีศึกษาจากรูปที่ 3.1 ในขณะที่กระบวนการอยู่ในสภาวะปกติ ความดันจะอยู่ในระดับปกติอุปกรณ์วัดความดันวัดความดันอยู่ในระดับปกติ (Normal) วาล์วลดความดัน อยู่ในสถานะมีความพร้อมใช้งาน (Availability) ซึ่งหากมีความดันเกินเกิดขึ้นวาล์วลดความดันซึ่งทำงานแบบไม่มีความดันอากาศวาล์วปิด (Air Failure Close) ถ้ากรณีที่เกิดความผิดพลาด เช่น อุปกรณ์วัดความดันทำงานผิดปกติ อุปกรณ์ประมวลผลไม่ส่งสัญญาณหรือวาล์วไม่สามารถปิดได้ กรณีนี้ที่ระบบนิรภัยไม่สามารถทำงานได้เกิดความล้มเหลวอันตราย เพราะฟังก์ชั่นนิรภัยไม่สามารถทำงานก่อนเกิดเหตุการณ์อันตรายได้

ตารางที่ 3.1 แสดงโหมดความล้มเหลวของแต่ละอุปกรณ์ในฟังก์ชั่นนิรภัย

สถานะ	รายละเอียดของการเปลี่ยนแปลงสถานะ	สถานะหลังเกิดความล้มเหลวของอุปกรณ์
0, OK	สถานะเริ่มต้น ไม่มีอุปกรณ์ล้มเหลว	-
9 FS	สถานะ ความล้มเหลวนิรภัย	FS
10 FD Detected	สถานะ ความล้มเหลวอันตรายตรวจจับได้	FDD
11, FD	สถานะ ความล้มเหลวอันตรายตรวจจับไม่ได้	FDU
1	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวนิรภัยแบบตรวจจับได้ แต่ระบบยังสามารถทำงานได้	IS
2	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวนิรภัยแบบตรวจจับไม่ได้ แต่ระบบยังสามารถทำงานได้	IS

ตารางที่ 3.2 แสดงโหมดความล้มเหลวของแต่ละอุปกรณ์ในฟังก์ชั่นนิรภัย (ต่อ)

สถานะ	รายละเอียดของการเปลี่ยนแปลงสถานะ	สถานะหลังเกิดความล้มเหลวของอุปกรณ์
3	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายแบบตรวจจับได้ แต่ระบบยังสามารถทำงานได้	IS
	ระบบประมวลผลเกิดความล้มเหลวอันตรายแบบตรวจจับได้.	FDD
	วาล์วย่อยตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายแบบตรวจจับได้ แต่ระบบยังสามารถทำงานได้	IS
	วาล์วตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายแบบตรวจจับได้ แต่ระบบยังสามารถทำงานได้	FDD
4	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายแบบตรวจจับไม่ได้ แต่ระบบยังสามารถทำงานได้	IS
	ระบบประมวลผลเกิดความล้มเหลวอันตรายแบบตรวจจับไม่ได้.	FDU
	วาล์วย่อยตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายแบบตรวจจับไม่ได้ แต่ระบบยังสามารถทำงานได้	IS
	วาล์วตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายแบบตรวจจับไม่ได้ แต่ระบบยังสามารถทำงานได้	FDU
5	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวนิรภัยแบบตรวจจับได้	IS
	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายแบบตรวจจับได้	IS
6	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวนิรภัยแบบตรวจจับได้	IS
	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายแบบตรวจจับไม่ได้	IS
7	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวนิรภัยแบบตรวจจับไม่ได้	IS
	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายแบบตรวจจับได้	IS
8	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวนิรภัยแบบตรวจจับไม่ได้	IS
	อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายแบบตรวจจับไม่ได้	IS

3.4 อัตราความล้มเหลว (Failure Rate) ของอุปกรณ์

หาอัตราความล้มเหลว (Failure Rate) ของอุปกรณ์แต่ละตัวโดยที่อัตราล้มเหลวอุปกรณ์จะมาจากผู้ผลิตของอุปกรณ์นั้น

ตารางที่ 3.2 อัตราความล้มเหลวของอุปกรณ์

อุปกรณ์	อัตราความล้มเหลวต่อ 9 ชั่วโมง (Failure per 10^9 hours , FITS)			
	อัตราความล้มเหลวอันตรายแบบตรวจจับไม่ได้ (Fail Dangerous Undetected) λ^{DU}	อัตราความล้มเหลวอันตรายแบบตรวจจับไม่ได้ (Fail Dangerous Detected) λ^{DD}	อัตราความล้มเหลวนิรภัยแบบตรวจจับไม่ได้ (Fail Safe Undetected) λ^{SU}	อัตราความล้มเหลวนิรภัยแบบตรวจจับได้ (Fail Safe detected) λ^{SD}
อุปกรณ์วัดความดัน	600	150	200	200
ตัวประมวลผล	125	2375	75	7425
วาล์วย่อย	585	500	1010	1010
วาล์ว	2270	1070	700	700

3.4.1 หาค่าอัตราความล้มเหลวร่วม (Common Cause Failure)

เนื่องจากอุปกรณ์วัดความดัน (presser Transmitter) และวาล์วย่อย (Solenoild Valve) เป็นอุปกรณ์ที่มีอยู่ในระบบมากกว่าหนึ่งตัวและถูกติดตั้งอยู่สภาวะสิ่งแวดล้อมเดียวกันทั้งหมด ดังนั้นจึงมีโอกาสเกิดความล้มเหลวร่วมกัน อุปกรณ์วัดความดันและวาล์วย่อยจึงมีค่าความล้มเหลวร่วมและนำมาคำนวณค่าความล้มเหลวของอุปกรณ์ ซึ่งในฟังก์ชั่นนิรภัยอุปกรณ์กรวัดความดันมีค่าอัตราความล้มเหลวร่วม 2% วาล์วย่อย 5% ดังแสดงต่อไปนี้

$$\lambda^{SD} = \lambda^{SDC}+\lambda^{SDN}$$

เมื่อ

$$\lambda^{SDC} = \beta\lambda^{SD} \quad (3.1)$$

และ

$$\lambda^{SDN} = (1-\beta)\lambda^{SD} \quad (3.2)$$

$$\lambda^{SU} = \lambda^{SUN}+\lambda^{SUC}$$

เมื่อ

$$\lambda^{SUC} = \beta\lambda^{SU} \quad (3.3)$$

และ

$$\lambda^{SUN} = (1-\beta)\lambda^{SU}$$

$$\lambda^{DD} = \lambda^{DDN}+\lambda^{DDC}$$

เมื่อ

$$\lambda^{DDC} = \beta\lambda^{DD} \quad (3.4)$$

และ

$$\lambda^{DDN} = (1-\beta)\lambda^{DD} \quad (3.5)$$

$$\lambda^{DU} = \lambda^{DUN}+\lambda^{DUC}$$

เมื่อ $$\lambda^{DUC} = \beta\lambda^{DU} \quad (3.6)$$

และ $$\lambda^{DUN} = (1-\beta)\lambda^{DU} \quad (3.7)$$

โดยที่ผลการหาอัตราความล้มเหลวร่วมของฟังก์ชั่นวัดคุมนิรภัยแสดงได้ดังตารางที่ 3.3

ตารางที่ 3.3 อัตราความล้มเหลวร่วมของอุปกรณ์

อุปกรณ์	β	อัตราความล้มเหลวต่อชั่วโมง								%SFF
		SDC	SUC	SDN	SUN	DDC	DUC	DDN	DUN	
อุปกรณ์วัดความดัน	2%	4E-09	4E-09	2E-07	2E-07	3E-09	1E-08	1E-07	6E-07	60%
ตัวประมวลผล	-	-	-	7E-06	8E-08	2E-06	1E-07	-	-	99 %
วาล์วย่อย	5%	5E-08	5.05 E-08	1E-06	1E-06	3E-08	3E-08	5E-07	6E-07	72.10 %
วาล์ว	-	-	-	7E-07	7E-07	1E-06	2E-06	-	-	30.9%

ค่าเฉลี่ยความล้มเหลวของระบบหาได้โดยนำเอาของค่าเฉลี่ยความล้มเหลวของของทั้ง 3 อุปกรณ์ในฟังก์ชันนิรภัยมารวมกัน คืออุปกรณ์วัดความดัน ตัวประมวลผล วาล์วย่อย และอุปกรณ์สุดท้าย (วาล์วนิรภัย) ดังแสดงในสมการที่ 3.1 และ 3.2

ค่าความล้มเหลวอันตราย

$$\lambda^{D} = \lambda^{DC}+\lambda^{D} \quad (3.8)$$

และ ค่าความล้มเหลวนิรภัย

$$\Lambda^{S} = \Lambda^{SC}+\Lambda^{SN} \quad (3.9)$$

3.4.2 รายละเอียดข้อมูลของกรณีศึกษา

รายละเอียดข้อมูลของกรณีศึกษาระยะรอบการทดสอบ (Test Interval , TI) 2 ปี และมีระยะเวลาการซ่อมแซม (Mean time to restore ,MTTR) 12 ชั่วโมง ในที่นี้จะหาค่าเฉลี่ยความล้มเหลวในโดยแทนค่าแสดงดังตาราง 3.4

ตารางที่ 3.4 รายละเอียดข้อมูลของกรณีศึกษา

TI	1,7520 ชั่วโมง
MTTR	12 ชั่วโมง
Shut down	24 ชั่วโมง

3.5 สร้างโมเดลมาร์คอฟ (Markov Model Construction)

นำข้อมูลที่ได้ไปหาค่าระดับความปลอดภัยของของฟังก์ชันวัดคุมนิรภัยโดยหาค่าความผิดพลาดอันตรายต่อช่วงระยะเวลาในการทดสอบการทำงานของอุปกรณ์วัดคุมนิรภัย (Probability of failure on demand, PFD) โดยใช้วิธีการวิเคราะห์โมเดลมาร์คอฟ (Markov Model) โดยสร้างแบบจากสถานะที่เปลี่ยนแปลงจากจากสถานะความผิดพลาดของอุปกรณ์ โดยมีสถานะเริ่มแรกจากสถานะ 0 เปลี่ยนแปลงไปยังสถานะอื่นๆเมื่อมีความล้มเหลวเกิดขึ้น

จากรายละเอียดการเปลี่ยนแปลงสถานะจากความล้มเหลวที่เกิดขึ้นในระบบจะสามารถจำแนกโหมดความล้มเหลว ของอุปกรณ์ในแต่ละสถานะ ได้ตามตารางที่ 3.5

ตารางที่ 3.5 โหมดความล้มเหลวของอุปกรณ์

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 2					SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	DUN
ตัวประมวลผล					SD	SU	DD	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU

3.5.1 สถานะระบบล้มเหลวนิรภัย (System Fail Safe State)

เมื่ออุปกรณ์ในระบบเกิดความล้มเหลวเป็นสาเหตุให้ระบบเกิดการเปลี่ยนจากสถานะที่ทำงานปกติไปยังสถานะความล้มเหลวนิรภัยคือสถานะหมายเลข 9 อัตราความล้มเหลวของอุปกรณ์ที่เกิดขึ้นแสดงตามตารางที่ 3.6

ตารางที่ 3.6 โหมดความล้มเหลวของสถานะระบบล้มเหลวนิรภัย

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	**SDC**	**SUC**	DDC	DUC	SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 2					SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	DUN
ตัวประมวลผล					**SD**	**SU**	DD	DU
วาล์วย่อย 1	**SDC**	**SUC**	DDC	DUC	**SDN**	**SUN**	DDN	DUN
วาล์วย่อย 2					**SDN**	**SUN**	DDN	DUN
วาล์ว					**SD**	**SU**	DD	DU

รูปที่ 3.2 สถานะระบบล้มเหลวนิรภัย

1. อัตราความล้มเหลวจากสถานะปกติไปยังสถานะระบบล้มเหลวนิรภัย

$$\lambda_{0,9} = 3/2\lambda_S{}^{SDC}+3/2\lambda_S{}^{SUC}+\lambda_L{}^{SD}+\lambda_L{}^{SU}+\lambda_{A1}{}^{SDC}+\lambda_{A1}{}^{SUC}+2\lambda_{A1}{}^{SDN}+2\lambda_{A1}{}^{SUN}+\lambda_{A2}{}^{SD}+\lambda_{A2}{}^{SU} \quad (3.10)$$

2. อัตราการซ่อมแซมของอุปกรณ์จากสถานะระบบล้มเหลวนิรภัยไปยังสถานะปกติ

$$\lambda_{9,0} = \mu_{SD} \quad (3.11)$$

3.5.2 สถานะระบบล้มเหลวอันตรายตรวจจับได้ (System Fail Dangerous Detect State)

เมื่ออุปกรณ์ในระบบเมื่อเกิดความล้มเหลวเป็นสาเหตุให้ระบบเกิดการเปลี่ยนจากสถานะที่ทำงานปกติไปยังสถานะความล้มเหลวอันตรายตรวจจับได้คือสถานะหมายเลข 10

ตารางที่ 3.7 สถานะระบบล้มเหลวอันตรายตรวจจับได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	**DDC**	DUC	SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 2					SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	DUN
ตัวประมวลผล					SD	SU	**DD**	DU
วาล์วย่อย 1	SDC	SUC	**DDC**	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	**DD**	DU

รูปที่ 3.3 สถานะระบบล้มเหลวอันตรายตรวจจับได้

1. อัตราความล้มเหลวจากสถานะปกติไปยังสถานะระบบอันตรายตรวจจับได้

$$\lambda_{0,10} = 3/2\lambda_S^{DDC}+\lambda_L^{DD}+\lambda_{A1}^{DDC}+\lambda_{A2}^{DD} \quad (3.12)$$

2. อัตราความล้มเหลวจากสถานะระบบอันตรายตรวจจับได้ ไปยังสถานะปกติ

$$\lambda_{10,0} = \mu_0 \quad (3.13)$$

3.5.3 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ (System Fail Dangerous Undetected State)

เมื่ออุปกรณ์ในระบบเมื่อเกิดความล้มเหลวเป็นสาเหตุให้ระบบเกิดการเปลี่ยนจากสถานะที่ทำงานปกติไปยังสถานะความล้มเหลวอันตรายตรวจจับไม่ได้คือสถานะหมายเลข 11

ตารางที่ 3.8 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	**DUC**	SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 2					SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	DUN
ตัวประมวลผล					SD	SU	DD	**DU**
วาล์วย่อย 1	SDC	SUC	DDC	**DUC**	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	**DU**

รูปที่ 3.4 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้

1. อัตราความล้มเหลวจากสถานะปกติไปยังสถานะระบบอันตรายตรวจจับไม่ได้

$$\lambda_{0,11} = 3\lambda_S^{DUC} + \lambda_L^{DU} + \lambda_{A1}^{DUC} + \lambda_{A2}^{DU} \qquad (3.14)$$

3.5.4 สถานะระบบล้มเหลวนิรภัยปกติตรวจจับได้ (System Fail Safety Detect Normal State)

เมื่ออุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวเป็นสาเหตุให้เกิดการเปลี่ยนไปยังสถานะความล้มเหลวนิรภัยตรวจจับได้ แต่ระบบยังสามารถทำงานได้

ตารางที่ 3.9 สถานะระบบล้มเหลวนิรภัยปกติตรวจจับได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	**SDN**	SUN	DDN	DUN
อุปกรณ์วัดความดัน 2					**SDN**	SUN	DDN	DUN

ตารางที่ 3.9 สถานะระบบล้มเหลวนิรภัยปกติตรวจจับได้ (ต่อ)

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 3					**SDN**	SUN	DDN	DUN
ตัวประมวลผล					SD	SU	DD	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU

รูปที่ 3.5 สถานะระบบล้มเหลวนิรภัยตรวจจับได้

1. อัตราความล้มเหลวจากสถานะปกติไปยังสถานะระบบล้มเหลวนิรภัยตรวจจับได้

$$\lambda_{0,1} = 3\lambda_S^{SDN} \tag{3.15}$$

2..อัตราความล้มเหลวจากสถานะระบบล้มเหลวนิรภัยตรวจจับไปยังสถานะปกติ

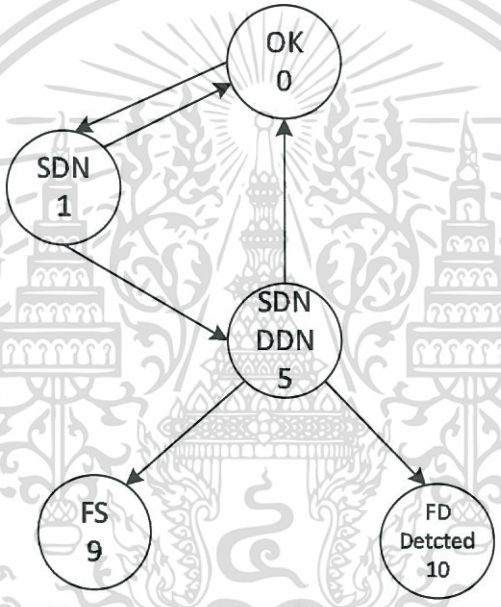
$$\lambda_{1,0} = \mu_0 \tag{3.16}$$

3.5.4.1 สถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับได้

ในกรณีที่อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวนิรภัยตรวจจับได้ระบบจะเปลี่ยนการทำงานอุปกรณ์ที่เหลืออีก 2 ตัว เป็นแบบ 1oo2 และเมื่ออุปกรณ์วัดความดันอีก 1 ใน 2 ตัวนั้น เกิดความล้มเหลวอันตรายตรวจจับได้ ระบบสามารถเข้าสู่สถานะล้มเหลวนิรภัยหรือล้มเหลวอันตรายตรวจจับตรวจจับได้

ตารางที่ 3.10 สถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	**DDN**	DUN
อุปกรณ์วัดความดัน 2					SDN	SUN	**DDN**	DUN
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	DUN
ตัวประมวลผล					SD	SU	DD	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU



รูปที่ 3.6 สถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับได้

1. อัตราความล้มเหลวจากสถานะความล้มเหลวนิรภัยตรวจจับได้ ไปยังสถานะระความล้มเหลวอันตรายตรวจจับได้

$$\lambda_{1,5} = 2\lambda_S^{DDN} \tag{3.17}$$

2. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับได้ไปยังสถานะปกติ

$$\lambda_{5,0} = \mu_0 \tag{3.18}$$

3. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับได้ไปยังสถานะระบบล้มเหลวนิรภัย

$$\lambda_{5,9} = \lambda_S{}^S \tag{3.19}$$

4. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับได้ไปยังสถานะระบบล้มเหลวอันตรายตรวจจับได้

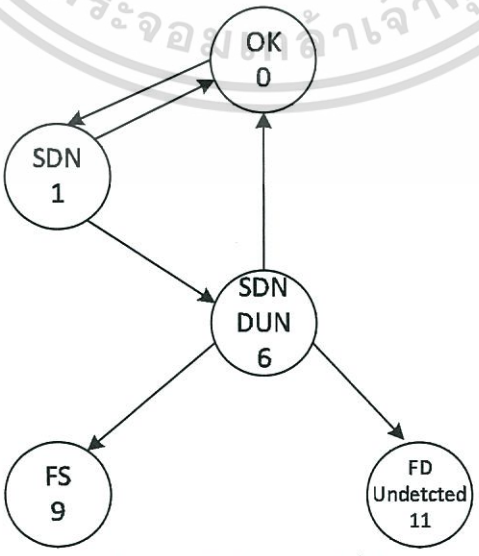
$$\lambda_{5,10} = \lambda_S{}^D \tag{3.20}$$

3.5.4.2 สถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับไม่ได้

ในกรณีที่อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวนิรภัยระบบจะเปลี่ยนการทำงานอุปกรณ์ที่เหลืออีก 2 ตัว เป็นแบบ 1oo2 และเมื่ออุปกรณ์วัดความดันอีก 1 ใน 2 ตัวนั้นเกิดความล้มเหลวอันตรายตรวจจับไม่ได้ ระบบสามารถเข้าสู่สถานะล้มเหลวนิรภัยหรือล้มเหลวอันตรายตรวจจับไม่ได้

ตารางที่ 3.11 สถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับไม่ได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	**DUN**
อุปกรณ์วัดความดัน 2					SDN	SUN	DDN	**DUN**
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	DUN
ตัวประมวลผล					SD	SU	DD	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU



รูปที่ 3.7 สถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับไม่ได้

1. ความล้มเหลวจากสถานะความล้มเหลวนิรภัยตรวจจับได้ ไปยังสถานะระบบความล้มเหลวอันตรายตรวจจับได้

$$\lambda_{1,6} = 2\lambda_S^{DUN} \tag{3.21}$$

2. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับไม่ได้ไปยังสถานะปกติ

$$\lambda_{6,0} = \mu_0 \tag{3.22}$$

3. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับได้ไปยังสถานะระบบล้มเหลวนิรภัย

$$\lambda_{6,9} = \lambda_S^{S} \tag{3.23}$$

4. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับได้และความล้มเหลวอันตรายตรวจจับได้ไปยังสถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้

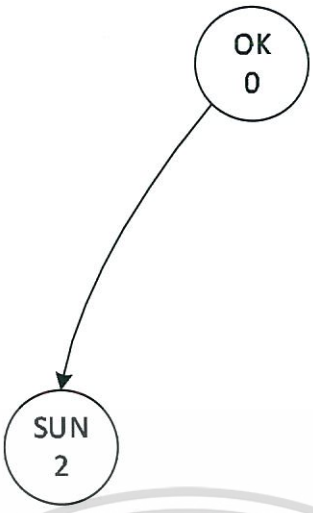
$$\lambda_{6,10} = \lambda_S^{DD} \tag{3.24}$$

3.5.5 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้

เมื่ออุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวเป็นสาเหตุให้ระบบเกิดการเปลี่ยนไปยังสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้ แต่ระบบยังสามารถทำงานได้

ตารางที่ 3.12 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	**SUN**	DDN	DUN
อุปกรณ์วัดความดัน 2					SDN	**SUN**	DDN	DUN
อุปกรณ์วัดความดัน 3					SDN	**SUN**	DDN	DUN
ตัวประมวลผล					SD	SU	DD	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU



รูปที่ 3.8 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้

1. อัตราความล้มเหลวจากสถานะปกติไปยังสถานะระบบล้มเหลวนิรภัยตรวจจับไม่ได้

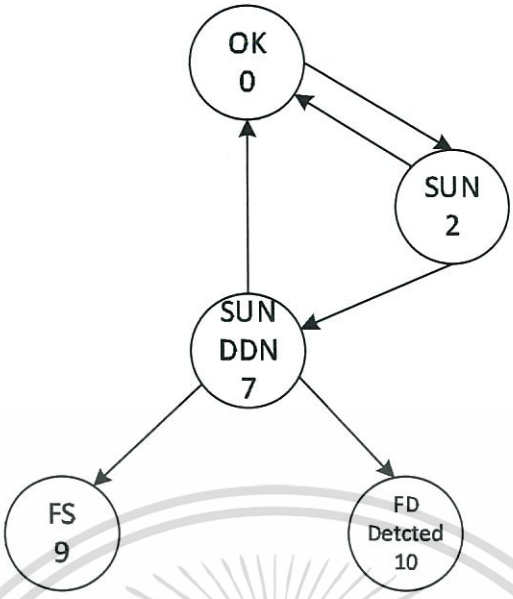
$$\lambda_{0,2} = 3\lambda_S^{SUN} \tag{3.25}$$

3.5.5.1 สถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับได้

ในกรณีที่อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดล้มเหลวนิรภัยแบบตรวจจับไม่ได้ระบบจะเปลี่ยนการทำงานอุปกรณ์ที่เหลืออีก 2 ตัวเป็นแบบ 1oo2 และเมื่ออุปกรณ์วัดความดันอีก 1 ใน 2 ตัวนั้นเกิดความล้มเหลวอันตรายตรวจจับได้ระบบสามารถเข้าสู่สถานะล้มเหลวนิรภัยหรือล้มเหลวอันตรายตรวจจับได้

ตารางที่ 3.13 สถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	**DDN**	DUN
อุปกรณ์วัดความดัน 2					SDN	SUN	**DDN**	DUN
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	DUN
ตัวประมวลผล					SD	SU	DD	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU



รูปที่ 3.9 สถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับได้

1. อัตราความล้มเหลวจากสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้ ไปยังสถานะความล้มเหลวอันตรายตรวจจับได้

$$\lambda_{2,7} = 2\lambda_S^{DDN} \tag{3.26}$$

2. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับได้ไปยังสถานะปกติ

$$\lambda_{7,0} = \mu_0 \tag{3.27}$$

3. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับได้ไปยังสถานะระบบล้มเหลวนิรภัย

$$\lambda_{7,9} = \lambda_S^{S} \tag{3.28}$$

4. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับได้ไปยังสถานะระบบล้มเหลวอันตรายตรวจจับได้

$$\lambda_{7,10} = \lambda_S^{D} \tag{3.29}$$

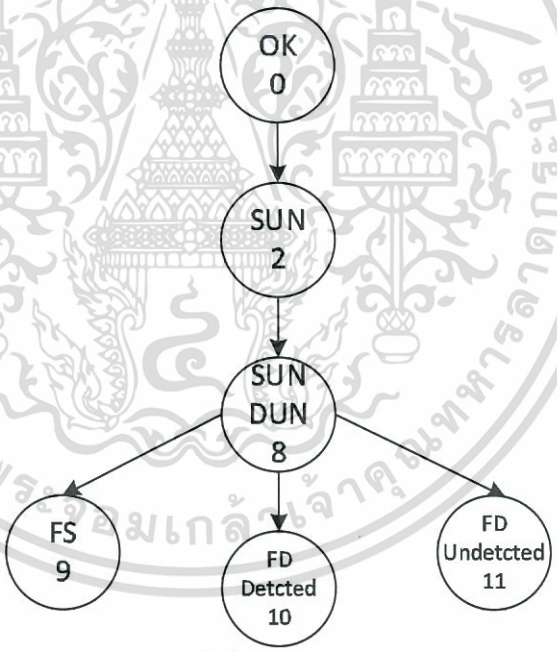
3.5.5.2 สถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้

ในกรณีที่อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวนิรภัยแบบตรวจจับไม่ได้ ระบบจะเปลี่ยนการทำงานอุปกรณ์ที่เหลืออีก 2 ตัว เป็นแบบ 1oo2 และเมื่ออุปกรณ์วัดความดันอีก 1 ใน 2

ตัวนั้นเกิดความล้มเหลวอันตรายตรวจจับไม่ได้ ระบบสามารถเข้าสู่สถานะล้มเหลวนิรภัยหรือสถานะล้มเหลวอันตรายตรวจจับไม่ได้

ตารางที่ 3.14 สถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 2					SDN	SUN	DDN	**DUN**
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	**DUN**
ตัวประมวลผล					SD	SU	DD	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU



รูปที่ 3.10 สถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้

1. อัตราความล้มเหลวจากสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้ ไปยังสถานะความล้มเหลวอันตรายตรวจจับไม่ได้

$$\lambda_{2,8} = 2\lambda_S^{DUN} \tag{3.30}$$

2. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้ไปยังสถานะระบบล้มเหลวนิรภัย

$$\lambda_{8,9} = \lambda_S^{S} \tag{3.31}$$

3. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้ไปยังสถานะระบบล้มเหลวอันตรายตรวจจับได้

$$\lambda_{8,10} = \lambda_S^{DD} \tag{3.32}$$

4. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้ไปยังสถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้

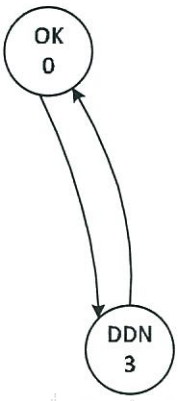
$$\lambda_{8,11} = \lambda_S^{DU} \tag{3.33}$$

3.5.6 สถานะระบบล้มเหลวอันตรายตรวจจับได้ (System Fail Dangerous Detect Normal State)

เมื่ออุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวเป็นสาเหตุให้เกิดการเปลี่ยนไปยังสถานะความล้มเหลวอันตรายตรวจจับได้ แต่ระบบยังสามารถทำงานได้

ตารางที่ 3.15 สถานะระบบล้มเหลวอันตรายตรวจจับได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	**DDN**	DUN
อุปกรณ์วัดความดัน 2					SDN	SUN	**DDN**	DUN
อุปกรณ์วัดความดัน 3					SDN	SUN	**DDN**	DUN
ตัวประมวลผล					SD	SU	**DD**	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	**DDN**	DUN
วาล์วย่อย 2					SDN	SUN	**DDN**	DUN
วาล์ว					SD	SU	**DD**	DU



รูปที่ 3.11 สถานะระบบล้มเหลวอันตรายตรวจจับได้

1. อัตราความล้มเหลวจากสถานะปกติไม่ได้ ไปยังสถานะความล้มเหลวอันตรายตรวจจับได้

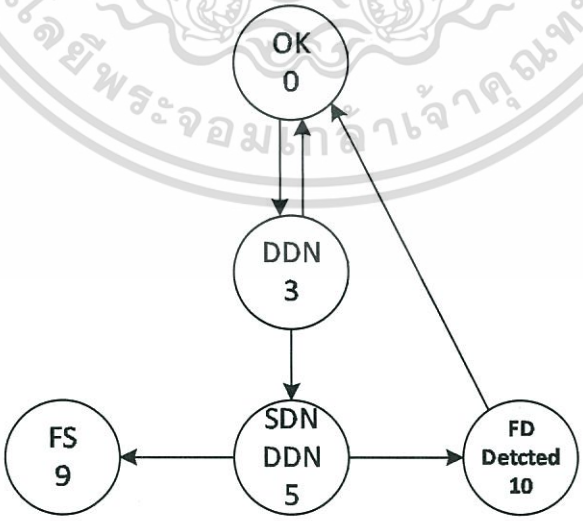
$$\lambda_{0,3} = 3\lambda_S^{DDN} + \lambda_L^{DD} + 2\lambda_{A1}^{DDN} + \lambda_{A2}^{DD} \quad (3.34)$$

3.5.6.1 สถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับได้

ในกรณีที่อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายตรวจจับได้ ระบบจะเปลี่ยนการทำงานอุปกรณ์ที่เหลืออีก 2 ตัว เป็นแบบ 1oo2 และเมื่ออุปกรณ์วัดความดันอีก 1 ใน 2 ตัวนั้นเกิดความล้มเหลวนิรภัยตรวจจับได้ ระบบสามารถเข้าสู่สถานะล้มเหลวนิรภัยหรือล้มเหลวอันตรายตรวจจับได้

ตารางที่ 3.16 สถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 2					**SDN**	SUN	DDN	DUN
อุปกรณ์วัดความดัน 3					**SDN**	SUN	DDN	DUN
ตัวประมวลผล					SD	SU	DD	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU



รูปที่ 3.12 สถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับได้

1. อัตราความล้มเหลวจากสถานะความล้มเหลวอันตรายตรวจจับได้ ไปยังสถานะความความล้มเหลวนิรภัยตรวจจับได้

$$\lambda_{3,5} = 2\lambda_S^{SDN} \quad (3.35)$$

2. อัตราความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับได้ไปยังสถานะระบบล้มเหลวนิรภัย

$$\lambda_{5,9} = \lambda_S^{S} \quad (3.36)$$

3. อัตราสถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับได้ไปยังสถานะระบบล้มเหลวอันตรายตรวจจับได้

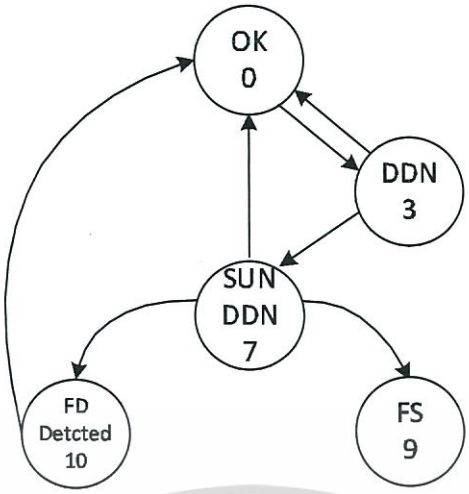
$$\lambda_{5,10} = \lambda_S^{D} \quad (3.37)$$

3.5.6.2 สถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้

ในกรณีที่อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายตรวจจับได้ ระบบจะเปลี่ยนการทำงานอุปกรณ์ที่เหลืออีก 2 ตัว เป็นแบบ 1oo2 และเมื่ออุปกรณ์วัดความดันอีก 1 ใน 2 ตัวนั้นเกิดความล้มเหลวนิรภัยตรวจจับไม่ได้ ระบบสามารถเข้าสู่สถานะล้มเหลวนิรภัยหรือล้มเหลวอันตรายตรวจจับไม่ได้

ตารางที่ 3.17 สถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	**DUN**
อุปกรณ์วัดความดัน 2					SDN	SUN	DDN	**DUN**
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	DUN
ตัวประมวลผล					SD	SU	DD	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU



รูปที่ 3.13 สถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้

1. อัตราความล้มเหลวจากสถานะความล้มเหลวอันตรายตรวจจับได้ ไปยังสถานะความความล้มเหลวนิรภัยตรวจจับได้

$$\lambda_{3,7} = 2\lambda_S^{SUN} \tag{3.38}$$

2. อัตราความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้ ไปยังสถานะระบบล้มเหลวนิรภัย

$$\lambda_{7,9} = \lambda_S^{S} \tag{3.39}$$

3. อัตราสถานะความล้มเหลวอันตรายตรวจจับได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้ไปยังสถานะระบบล้มเหลวอันตรายตรวจจับได้

$$\lambda_{7,10} = \lambda_S^{D} \tag{3.40}$$

3.5.7 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ (System Fail Dangerous Undetected Normal State)

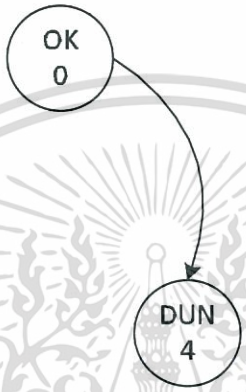
เมื่ออุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวเป็นสาเหตุให้เกิดการเปลี่ยนไปยังสถานะความล้มเหลวอันตรายตรวจจับไม่ได้ แต่ระบบยังสามารถทำงานได้

ตารางที่ 3.18 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	**DUN**
อุปกรณ์วัดความดัน 2					SDN	SUN	DDN	**DUN**
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	**DUN**

ตารางที่ 3.18 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้ (ต่อ)

อุปกรณ์	โหมดความล้มเหลว							
ตัวประมวลผล					SD	SU	DD	**DU**
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	**DUN**
วาล์วย่อย 2					SDN	SUN	DDN	**DUN**
วาล์ว					SD	SU	DD	**DU**



รูปที่ 3.14 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้

1. อัตราความล้มเหลวจากสถานะปกติไปยังสถานะความความอันตรายตรวจจับไม่ได้

$$\lambda_{0,4} = 3\lambda_S^{DUN} + \lambda_L^{DU} + 2\lambda_{A1}^{DUN} + \lambda_{A2}^{DU} \qquad (3.41)$$

3.5.7.1 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับได้

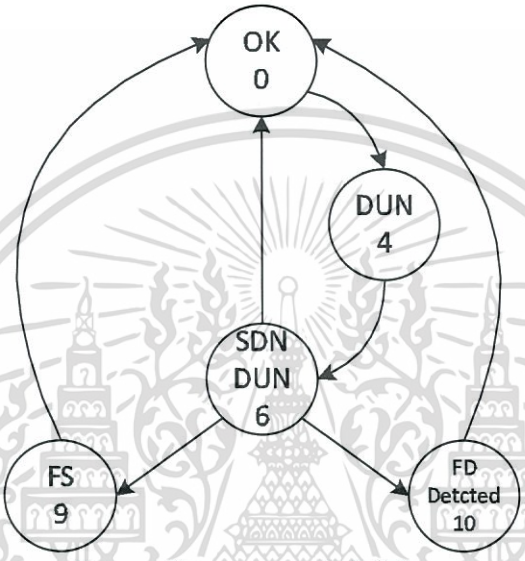
ในกรณีที่อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดอุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายตรวจจับไม่ได้ระบบจะเปลี่ยนการทำงานอุปกรณ์ที่เหลืออีก 2 ตัว เป็นแบบ 2oo2 และเมื่ออุปกรณ์วัดความดันเกิดความล้มเหลวนิรภัยตรวจจับได้ระบบสามารถเข้าสู่สถานะล้มเหลวนิรภัยหรือล้มเหลวอันตรายตรวจจับได้

ตารางที่ 3.19 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	**DUN**
อุปกรณ์วัดความดัน 2					SDN	SUN	DDN	**DUN**
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	DUN
ตัวประมวลผล					SD	SU	DD	DU

ตารางที่ 3.19 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับได้(ต่อ)

อุปกรณ์	โหมดความล้มเหลว							
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU



รูปที่ 3.15 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับได้

1. อัตราความล้มเหลวจากสถานะความล้มเหลวอันตรายตรวจจับไม่ได้ไปยังสถานะความล้มเหลวนิรภัยตรวจจับได้

$$\Lambda_{4,6} = 2\Lambda_S^{SDN} \tag{3.42}$$

2. อัตราความล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับได้ไปยังสถานะระบบล้มเหลวนิรภัย

$$\Lambda_{6,9} = \Lambda_S \tag{3.43}$$

3. อัตราสถานะความล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับได้ไปยังสถานะระบบล้มเหลวอันตรายตรวจจับได้

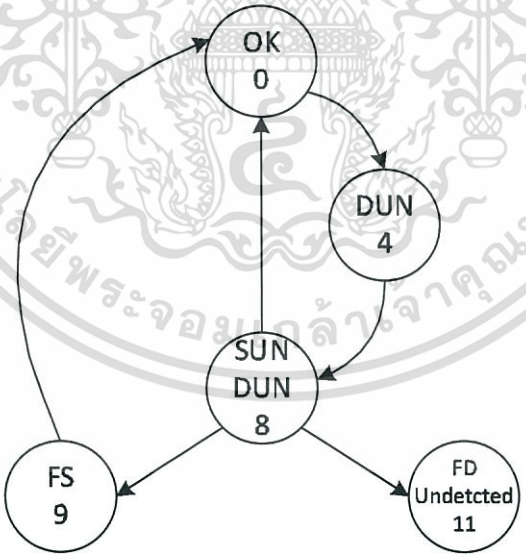
$$\Lambda_{6,10} = \Lambda_S^{DD} \tag{3.44}$$

3.5.7.2 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้

ในกรณีที่อุปกรณ์วัดความดันตัวใดตัวหนึ่งเกิดความล้มเหลวอันตรายตรวจจับไม่ได้ ระบบจะเปลี่ยนการทำงานอุปกรณ์ที่เหลืออีก 2 ตัว เป็นแบบ 2oo2 และเมื่ออุปกรณ์วัดความดันเกิดความล้มเหลวนิรภัยตรวจจับไม่ได้ระบบสามารถเข้าสู่สถานะล้มเหลวนิรภัยหรือล้มเหลวอันตรายตรวจจับไม่ได้

ตารางที่ 3.20 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้

อุปกรณ์	โหมดความล้มเหลว							
อุปกรณ์วัดความดัน 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
อุปกรณ์วัดความดัน 2					SDN	SUN	DDN	**DUN**
อุปกรณ์วัดความดัน 3					SDN	SUN	DDN	**DUN**
ตัวประมวลผล					SD	SU	DD	DU
วาล์วย่อย 1	SDC	SUC	DDC	DUC	SDN	SUN	DDN	DUN
วาล์วย่อย 2					SDN	SUN	DDN	DUN
วาล์ว					SD	SU	DD	DU



รูปที่ 3.16 สถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้และสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้

1. อัตราความล้มเหลวจากสถานะความล้มเหลวอันตรายตรวจจับไม่ได้ไปยังสถานะความล้มเหลวนิรภัยตรวจจับไม่ได้

$$\lambda_{4,8} = 2\lambda_S^{SUN} \tag{3.45}$$

2. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้ไปยังสถานะระบบล้มเหลวนิรภัย

$$\lambda_{8,9} = \lambda_S{}^{S} \tag{3.46}$$

3. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้ไปยังสถานะระบบล้มเหลวอันตรายตรวจจับได้

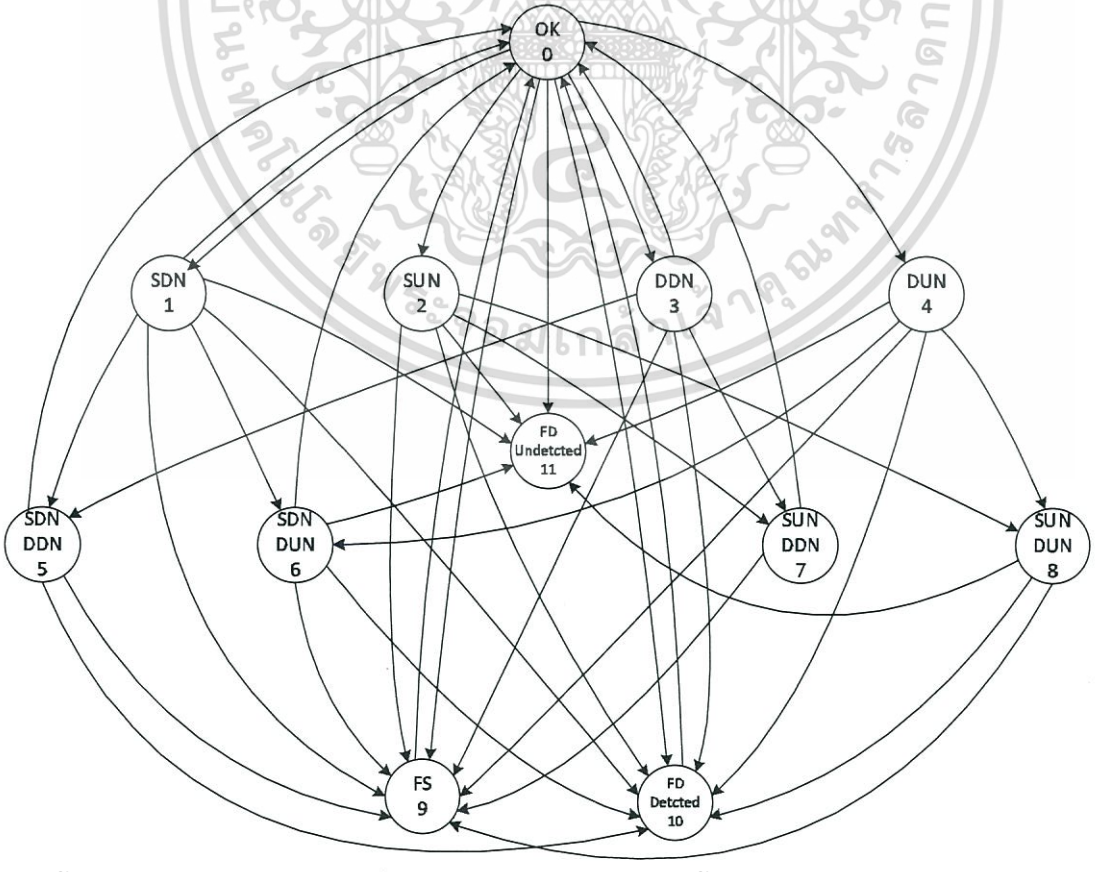
$$\lambda_{8,10} = \lambda_S{}^{DD} \tag{3.47}$$

4. อัตราความล้มเหลวจากสถานะระบบความล้มเหลวนิรภัยตรวจจับไม่ได้และความล้มเหลวอันตรายตรวจจับไม่ได้ไปยังสถานะระบบล้มเหลวอันตรายตรวจจับไม่ได้

$$\lambda_{8,11} = \lambda_S{}^{DU} \tag{3.48}$$

3.6 การผสานสถานะโมเดลมาร์คอฟ

เมื่อสร้างสถานะโมเดลมาร์คอฟครบทุกโหมดความล้มเหลวในระบบ ทุกสถานะที่สร้างขึ้นสามารถผสานเป็นหนึ่งโมเดลของฟังก์ชั่นนิรภัย แสดงตามรูปที่ 3.17



รูปที่ 3.17 ผสานสถานะโมเดลมาร์คอฟ

3.7 การหาค่าเฉลี่ยความผิดพลาดอันตรายของอุปกรณ์วัดคุมนิรภัย (PFDavg)

จากหัวข้อที่แล้วได้สร้างโมเดลมาร์คอฟและอัตราความล้มเหลวที่เกิดจากความล้มเหลวของอุปกรณ์ในแต่ละสถานะ ในหัวข้อนี้จะกล่าวถึงการหาค่าเฉลี่ยความล้มเหลว (PFD_{avg}) ของระบบวาล์วลดความดัน ในที่นี้ได้แสดงการหาค่าค่าเฉลี่ยความล้มเหลวโดยใช้วิธีการทรานซิชั่นเมตทริก (Transition Matrix) ของฟังก์ชั่นนิรภัยได้ตามเมตทริก P ในสมการ 3.42

$$P = \begin{bmatrix}
1-\Sigma & 3\lambda_S^{SDN} & 3\lambda_S^{SUN} & 3\lambda_S^{DuN}+\lambda_L^{DD}+2\lambda_{A1}^{DDN}+\lambda_{A2}^{DD} & 3\lambda_S^{DUN}+3\lambda_L^{DU}+\lambda_{A1}^{DUN}+\lambda_{A2}^{DU} & 0 & 0 & 0 \\
\mu_0 & 1-\Sigma & 0 & 0 & 0 & 2\lambda_S^{DDN} & 2\lambda_S^{DUN} & 0 \\
0 & 0 & 1-\Sigma & 0 & 0 & 0 & 0 & 2\lambda_S^{DDN} \\
\mu_0 & 0 & 0 & 1-\Sigma & 0 & 2\lambda_S^{DDN} & 0 & 2\lambda_S^{SUN} \\
0 & 0 & 0 & 0 & 1-\Sigma & 0 & 2\lambda_S^{SDN} & 0 \\
\mu_0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & 0 \\
\mu_0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 \\
\mu_0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\mu_{SD} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\mu_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix} \quad \ldots$$

$$\begin{bmatrix}
0 & \frac{3}{2\lambda_S^{SDC}}+\frac{3}{2\lambda_S}^{SUC}+\lambda_L^{SD}+\lambda_L^{SU}+\lambda_{A1}^{SDC}+\lambda_{A1}^{SUC}+2\lambda_{A1}^{SDN}+2\lambda_{A1}^{SUN}+\lambda_{A2}^{SD}+\lambda_{A2}^{SU} & \frac{3}{2\lambda_S}^{DDC}+\lambda_L^{DD}+\lambda_{A1}^{DDC}+\lambda_{A2}^{DD} & \frac{3}{2\lambda_S}^{DUC}+\lambda_L^{DU}+\lambda_{A1}^{DUC}+\lambda_{A2}^{DU} \\
0 & \lambda_S^{SDC}+2\lambda_S^{SDN} & \lambda_S^{DDC} & \lambda_S^{DUC} \\
2\lambda_S^{DUN} & 2\lambda_S^{SUC}+2\lambda_S^{SUN} & \lambda_S^{DDC} & \lambda_S^{DUC} \\
0 & \lambda_S^{SUC}+\lambda_S^{SDC}+\lambda_{A1}^{S} & \lambda_S^{DDC}+2\lambda_S^{DDN}+\lambda_{A1}^{DD} & 0 \\
2\lambda_S^{SUN} & \lambda_S^{SDC}+\lambda_S^{SUC}+\lambda_{A1}^{S} & \lambda_S^{DDC}+2\lambda_S^{DDN}+\lambda_{A1}^{D} & \lambda_S^{DUC}+2\lambda_S^{DUN}+\lambda_{A1}^{DU} \\
0 & \lambda_S^{S} & \lambda_S^{D} & 0 \\
0 & \lambda_S^{S} & \lambda_S^{DD} & 0 \\
0 & \lambda_S^{S} & \lambda_S^{D} & 0 \\
1-\Sigma & \lambda_S^{S} & \lambda_S^{DD} & 0 \\
0 & 1-\Sigma & 0 & 0 \\
0 & 0 & 1-\Sigma & 0 \\
0 & 0 & 0 & 0
\end{bmatrix}$$

รูปที่ 3.18 เมตทริก P

แทนค่าเฉลี่ยความล้มเหลว ในตารางที่ 3.3 แทนค่าในทรานซิชั่นเมตทริก P ได้ตามรูปที่ 3.19

$$P = \begin{bmatrix}
0.999996995 & 0.0000000588 & 0.0000000588 & 0.0000004836 \\
0.083333333 & 0.999999772 & 0 & 0 \\
0 & 0 & 0.999999812 & 0 \\
0.083333333 & 0 & 0 & 0.999999564 \\
0 & 0 & 0 & 0 \\
0.083333333 & 0 & 0 & 0 \\
0.083333333 & 0 & 0 & 0 \\
0.083333333 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0.041666667 & 0 & 0 & 0 \\
0.083333333 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix} \quad \ldots$$

$$\begin{bmatrix}
0.00000052705 & 0 & 0 & 0 \\
0 & 0.0000000294 & 0.0000001176 & 0 \\
0 & 0 & 0 & 0.0000000392 \\
0 & 0.0000000392 & 0 & 0.0000000392 \\
0.99999891 & 0 & 0.0000000392 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{bmatrix} \quad \cdots$$

$$\begin{bmatrix}
0 & 0.0000012851 & 0.00000034745 & 0.000000244225 \\
0 & 0.0000000792 & 0.0000000003 & 0.0000000012 \\
0.0000001176 & 0.0000000396 & 0.0000000003 & 0.0000000012 \\
0 & 0.00000010085 & 0.000000257 & 0 \\
0.0000000392 & 0.0000007508 & 0.0000000797 & 0.0000001773 \\
0 & 0.0000000407 & 0.000000075 & 0 \\
0 & 0.0000000407 & 0.000000015 & 0 \\
0 & 0.0000000407 & 0.000000075 & 0 \\
1 & 0.0000000407 & 0.000000015 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}$$

รูปที่ 3.19 การแทนค่าเมตทริก P

การหาค่าความล้มเหลวผิดพลาด จากเมตทริก P โดยใช้วิธีการสภาวะคงตัว (Steady State) ที่สถานะเริ่มต้นระยะทดสอบ เท่ากับศูนย์ (S^0) ไปจนถึงที่ระยะทดสอบของฟังก์ชั่นนิรภัยกรณีศึกษา 2 ปี หรือ 17850 ชั่วโมง ในที่นี้จะหาค่าเป็นตัวอย่าง ในระยะรอบทดสอบตั้งแต่ 0 ถึง 3 และ 17849 17850 ชั่วโมง ดังสมการที่ 3.49 และ 3.50

$$S^1 = S^0 \text{ x } P \tag{3.49}$$

$$S^n = S^{n-1} \text{ x } P \tag{3.50}$$

กำหนดให้ S^0= [1 0 0 0 0 0 0 0 0 0 0 0]

$S^1=S^0*P$

S^1=[1 0 0 0 0 0 0 0 0 0 0 0] x [P]

S^1=[0.999996995 0.000000059 0.000000059 0.000000484 0.000000527 0 ...
0 0 0 0.000001285 0.000000347 0.000000244]

$S^2= S^1$x[P]

S^2=[0.999996995 0.000000059 0.000000059 0.000000484 0.000000527 0 ...
0 0 0 0.000001285 0.000000347 0.000000244] x[P]

S^2= [0.99999411 0.000000118 0.000000118 0.000000967 0.000001054 0 ...
0 0 0 0.000002570 0.000000695 0.000000488]

$S^3 = S^2 x[P]$

$S^3 = [0.99999411 \quad 0.000000118 \quad 0.000000118 \quad 0.000000967 \quad 0.000001054 \quad 0 \quad \ldots$
$0 \quad 0 \quad 0 \quad 0.000002570 \quad 0.000000695 \quad 0.000000488] \times [P]$

$S^3 = [0.999991368 \quad 0.000000176 \quad 0.000000176 \quad 0.000001451 \quad 0.000001581 \quad 0 \quad \ldots$
$0 \quad 0 \quad 0 \quad 0.000003855 \quad 0.000001042 \quad 0.000000733]$

$S^{17519} = S^{17518} x[P]$

$S^{17519} = [253.8753094 \quad 0.0419136 \quad 0.0419182 \quad 0.3445170 \quad 0.3747899 \quad 0.0000412 \quad \ldots$
$0.0000549 \quad 0.0000412 \quad 0.0000549 \quad 0.9175227 \quad 0.1743848 \quad 0.1743848]$

$S^{17520} = S^{17519} x[P]$

$S^{17520} = [253.8753094 \quad 0.0419136 \quad 0.0419182 \quad 0.3445170 \quad 0.3747899 \quad 0.0000412 \quad \ldots$
$0.0000549 \quad 0.0000412 \quad 0.0000549 \quad 0.9175227 \quad 0.1743848 \quad 0.1743848] \times [P]$

$S^{17520} =$

$[253.96567039 \quad 0.04192852 \quad 0.04193316 \quad 0.34463963 \quad 0.37492328 \quad 0.00004125 \quad \ldots$
$0.00005492 \quad 0.00004124 \quad 0.00005492 \quad 0.91784930 \quad 0.24824567 \quad 0.17444683]$

3.8 ผลจากการพิสูจน์ค่าระดับความปลอดภัยหาค่าเฉลี่ยความล้มเหลว

เมื่อทำการพิสูจน์ประเมินผลค่าระดับความปลอดภัยที่ได้จากการประเมินความผิดปกติของอุปกรณ์ในฟังก์ชั่นวัดคุมนิรภัยพบว่า เมื่ออุปกรณ์ภายใต้การควบคุมทำงานอันใดอันหนึ่งหรือทั้งหมดได้ทำงานผิดพลาดค่าระดับความปลอดภัยของฟังก์ชันวัดคุมนิรภัย จะเห็นว่ามีค่าเฉลี่ยความล้มเหลวมีค่าเท่ากับ 0.17444683 ซึ่งอยู่ในค่าระดับความปลอดภัย SIL ตามตามรางที่ 3.22

ตารางที่ 3.21 ค่าระดับความปลอดภัยฟังก์ชั่นนิรภัยกรณีศึกษา

Current PFD_{avg}	SAFETY INTEGRITY LEVEL (SIL)	PFD_{avg}
	4	.0001 - .00001
	3	.001 - .0001
	2	.01 - .001
0.174446828	1	.1 - .01

3.9 การพิจารณาการทนทานต่อความล้มเหลวของอุปกรณ์

จากการการพิสูจน์ค่าระดับความปลอดภัยที่ได้กล่าวถึงไปใน**หัวข้อ**ที่ผ่านมาพบว่า ฟังก์ชั่นระบบวัดคุมนิรภัยมีค่าระดับความปลอดภัยอยู่ในค่าระดับ SIL 1 จึงแสดงให้เห็นว่าฟังก์ชั่นคุมนิรภัยนี้มีความสามารถป้องกันอันตรายที่เกิดจากการทำงานผิดพลาดของอุปกรณ์ได้ เมื่อผ่านการพิสูจน์ค่าระดับความปลอดภัยแล้ว ได้มีการการพิจารณาการทนทานต่อความล้มเหลวของอุปกรณ์ จากการพิจารณาความเหมาะสมของอุปกรณ์จากรายละเอียดข้อมูลของอุปกรณ์ที่กล่าวไว้ใน บทที่ 2 สรุปข้อมูลขอบเขตความสมบูรณ์ของกรณีศึกษามี 2 ข้อดังนี้

3.9.1 พิจารณาวิธี Route 1_H ตามข้อกำหนดมาตรฐาน IEC61508

การพิจารณาอยู่บนพื้นฐานความการทนทานต่อความล้มเหลวของอุปกรณ์ และค่าอัตราส่วนความล้มเหลวนิรภัย (SFF) ซึ่งในกรณีศึกษา ข้อกำหนดมาตรฐานเป็นอุปกรณ์แบบ เมื่อนำค่าไปเทียบ

กับตารางแสดงอุปกรณ์น้อยที่สุดที่ยอมให้เกิดความล้มเหลวได้สำหรับอุปกรณ์ ตามข้อกำหนดมาตรฐาน เมื่อพิสูจน์ค่าระดับความปลอดภัยที่ระดับ SIL1 จะสรุปได้ว่าค่าอัตราส่วนความล้มเหลวนิรภัยของอุปกรณ์ที่นำมาใช้งานในกรณีศึกษาได้ผลสรุปตามตารางที่ 3.22

ตารางที่ 3.22 แสดงขอบเขตความสมบูรณ์ของอุปกรณ์ในระบบนิรภัยกรณีศึกษาด้วยวิธี route 1_H

SIL I

อุปกรณ์	Type	ค่าอัตราส่วนความล้มเหลวนิรภัย (SFF)		จำนวนอุปกรณ์น้อยที่สุดที่ยอมให้เกิดความล้มเหลว (HFT)		
		ฟังก์ชั่นนิรภัย	IEC61508	ฟังก์ชั่นนิรภัย	IEC61508	
อุปกรณ์วัดความดัน	Type B	60%	<60%	2	10	ผ่านข้อกำหนด
ตัวประมวลผล		99 %	60%-<90%	0	0	ผ่านข้อกำหนด
วาว์ย่อย	Type A	72.10%	60%-<90%	1	0 (SIL3)	ผ่านข้อกำหนด
วาว์	Type A	30.9%	<60%	0	0	ผ่านข้อกำหนด

3.9.2 พิจารณาวิธี Route 2_H ตามข้อกำหนดมาตรฐาน IEC61508

การพิจารณาอยู่บนพื้นฐานความเชื่อมั่นของชิ้นส่วนจากข้อมูลสะท้อนกลับของผู้ใช้งาน จากข้อมูลความล้มเหลวของอุปกรณ์ของฟังก์ชั่นนิรภัยในกรณีศึกษาไม่ได้รับการรับรอง(certified) การพิจารณาด้วย Route 2_Hนี้จึงไม่เป็นได้ตามข้อกำหนดมาตรฐาน

3.9.3 พิจารณาตามข้อกำหนด Prior Use ใน มาตรฐาน IEC61511

เมื่อพิสูจน์ค่าระดับความปลอดภัยของฟังก์ชั่นนิรภัยในกรณีศึกษาที่ระดับ SIL1 อุปกรณ์ไม่มีหลักฐานเพียงพอที่จะแสดงให้เห็นว่าอุปกรณ์มีความเหมาะสมกับการใช้งานในระบบวัดคุมนิรภัย จึงไม่เป็นได้ตามข้อกำหนดมาตรฐาน

บทที่ 4
การดำเนินการศึกษางานวิจัย

4.1 ผลการดำเนินการและวิจารณ์

จากการการพิสูจน์ค่าระดับความปลอดภัยที่ได้กล่าวถึงไปในบทที่ผ่านมาพบว่า ฟังก์ชั่นระบบวัดคุมนิรภัยมีค่าระดับความปลอดภัยอยู่ในค่าระดับ SIL 1 จึงแสดงให้เห็นว่าฟังก์ชั่นคุมนิรภัยนี้สามารถป้องกันอันตรายที่เกิดจากการทำงานผิดพลาดของอุปกรณ์ได้ ซึ่งรูปแบบของฟังก์ชั่นวัดคุมนิรภัยที่ติดตั้งอยู่แล้วนั้นเพียงพอกับข้อกำหนดจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาด (HFT) จึงไม่จำเป็นต้องปรับปรุงหรือติดตั้งอุปกรณ์ในฟังก์ชั่นระบบวัดคุมนิรภัยเพิ่มเติม แต่ความเร็วในการทำงานของระบบนิรภัยจะต้องเร็วกว่าเวลาปลอดภัยของการผลิต (Process Safety Time)

ตามข้อกำหนด IEC 61508/61511 ในการออกแบบระบบนิรภัยตามมาตรฐานมีจึงควรออกแบบปรับปรุงให้ระบบนิรภัยต้องเป็นระบบที่ทำงานอิสระโดยแยกออกจากระบบควบคุมพื้นฐาน และต้องมีการออกแบบให้ทำงานเป็นแบบ Fail safe หรือแบบ De-energize to Trip และยังจะต้องจัดเตรียมระบบ Override หรือ เพื่อใช้ในการบำรุงหรือทดสอบการทำงาน รวมทั้งต้องมีการแสดงสถานะต่างๆอย่างชัดเจน

4.2 ข้อเสนอแนะ

ในการหาค่าระดับความปลอดภัยของระบบวัดคุมนิรภัย ควรหาอัตราความผิดพลาดอันตรายของอุปกรณ์นิรภัยจากผู้ผลิตที่ได้รับการรับรองจากสถาบันการตรวจสอบที่เชื่อถือได้และจากแหล่งข้อมูลที่เชื่อถือได้เป็นที่ยอมรับ หรือข้อมูลจากการเก็บประวัติของโรงงานเอง

การประเมินความเสี่ยงกระบวนการผลิตควรจะได้ข้อมูลจากพนักงานที่มีประสบการณ์สูงและควรมีพนักงานที่เกี่ยวข้องครบทุกด้าน เช่น วิศวกรเครื่องมือวัดและระบบควบคุม วิศวกรผู้ดูแลกระบวนการผลิต พนักงานควบคุมกระบวนการผลิต วิศวกรซ่อมบำรุง เป็นต้น ซึ่งจะทำให้ได้ผลการประเมินความเสี่ยงที่มีความน่าเชื่อถือ และควรมีการทำการทบทวนอีกครั้ง (Update & Review) หากมีการเปลี่ยนแปลงในกระบวนการผลิต

สำหรับการออกแบบฟังก์ชันวัดคุมนิรภัยจะต้องพิจารณาถึงความเหมาะสมของช่วงเวลาในการทดสอบ รูปแบบการทดสอบ รวมถึงรูปแบบการทำงานของอุปกรณ์การวัดซึ่งนอกจากพิจารณาด้านความเชื่อมั่นแล้วยังต้องคำนึงถึงความพร้อมใช้งาน ค่าใช้จ่าย และพื้นที่ในการติดตั้ง

เอกสารอ้างอิง

[1] ทวิช ชูเมือง. **การออกแบบระบบวัดคุมนิรภัย. กรุงเทพมหานคร.:** อุ๊คบี. 2559.

[2] ทวิช ชูเมือง. **การกำหนดค่าระดับความปลอดภัยสำหรับฟังก์ชันนิรภัย,** กรุงเทพมหานคร : วีพริ้นท์. 2551.

[3] William M. Goble and Harry Cheddie, **"Safety Instrumented Systems Verification Practical Probabilistic Calculations"** ISA-The Instrumentation, Systems and Automation Society,. 2005

[4] International Electrotechnical Commission. "Functional safety Safety Instrumented Systems for the Process Industry Sector" **IEC-61511**, 2003.

[5] International Electrotechnical Commission. "Functional safety of Electrical / Electronics / Programmable Electronic Safety - Related System"**IEC-61508,** 2010.

[6] The Instrumentation Systems, and Automation Society. "Safety Instrumented Functions (SIF) Safety Integrity Level (SIL) Evaluation Techniques Part 4: Determining the SIL of a SIF via Markov Analysis" **ISA-TR84.00.02**, Part 4, 2002.

[7] International Electrotechnical Commission. "Electronic components-Reliability-Reference condition for failure rate and Stress model for convertion"**IEC-61709**, 2011.

[8] SINTEF and NTNU. "Offshore Reliability Data" **OREDA**, 2009

[9] SINTEF. **"Reliability Data for Safety Instrumented System, PDS data Handbook"** 2013

[10] Exida. **"Safety Equipment Handbook"**, 2005

[11] International Electrotechnical Commission. "Functional safety – Safety Instrumented Systems for the Process Industry Sector" **IEC-61511**, 2016.

[12] P Kongtong and S. Chitwong, "SIL Verification of Safety Instrumented System for Block Valve System in Gas Pipeline by Using Markov Model Methodology" Hongkong, **The International Multi Conference of Engineers and Computer Scientists 2017**, Vol II, pp.644-677.

ภาคผนวก ก
บทความวิจัยที่ได้รับการตีพิมพ์

บทความวิจัยที่ได้รับการตีพิมพ์ในวารสารทางวิชาการระดับนานาชาติในวิทยานิพนธ์นี้มีรายละเอียดดังต่อไปนี้

[12] P Kongtong and, S. Chitwong. "SIL Verification of Safety Instrumented System for Block Valve System in Gas Pipeline by Using Markov Model Methodology" The International Multi Conference of Engineers and Computer Scientists 2017, Vol II, pp.644 – 677.

SIL Verification of Safety Instrumented System for Block Valve System in Gas Pipeline by Using Markov Model Methodology

P. Kongtong and, S. Chitwong

Abstract—**This paper presents about methods for evaluation of safety integrity level (SIL) which is significant to reduce risk of failure of block valve in gas pipeline system by using Markov Model method which refer to International standard IEC 61508/61511. The reason of using Markov Model method is that it takes less time and more flexible than other methods to determine SIL. This method uses a qualitative approach showing Average Probability of Failure (PFDavg) rate data and repairing time from model to implement in further process.**

Index Terms—**, tracking, biomimetic, redundancy, degrees-of-freedom Safety Instrumented Systems, Safety Instrumented Functions, Safety Integrity Levels, Markov Models, Probability of Failure on Demand**

I. INTRODUCTION

SAFETY Instrumented Systems (SIS) are not new. It has long been the practices to fit protective systems to industrial process plant where there is a potential threat to life or the environment. In example, to increase of energy consumption, safety system design in process of natural gas, which is flammable fluid, has generally been more significant. Natural gas pipeline in Thailand have been serviced to supply natural gas to consumer for 24 hrs./day for more than 25 years. The high pressure natural gas transfer itself to lower pressure. Pressure control valves are basically used to reduce pressure to proper with each area application. The natural gas pipelines are mostly routed through area of agriculture, community or highway where any fault of safety system design may become disaster to life or property. For this reason, risk assessment for control loop of this pressure control valve is highly significant to be reviewed in order to avoid hazard.

For hazardous process, safety instrumented system is significantly used to control reliability and safety of process. "Safety Integrity Level (SIL)" is used to define target probability of failure on demand (PFD) of a Safety Instrument Function (SIF) which is a guideline for safety design, installation and also preventive maintenance included. Dangerous failure such as instrument failure could make a severity consequence to property, environment and human which route cause of failure possibly came from several reasons whether failure of process instrument.

II. VERIFICATION METHODOLOGY

The method for SIL having various methodologies can be used to verify the SIL of SIS. The methods divided into two types are qualitative and quantitative methods.

Qualitative methods such as risk matrix are evaluation based on experience or knowledge of expert team to estimate the consequence of a hazard. Quantitative methods such as LOPA (Layer of Protection Analysis), FTA (Fault Tree Analysis), Markov Model evaluation are based on numerical data and mathematical analysis.

III. CASE STUDY

A. Determination of Safety Instrumented Function

In this work, safety instrumented function of block valve system protects over pressure in gas pipeline. The process operation of the block valve is receiving natural gas from station 1 in order to transmit to station 3. This SIF consists of three pressure transmitters (PT) having a two out of tree voting configuration serving as the inputs to the logic solver system. The logic solver will then signal to block valves with two solenoid valve (SOV) having one out of two voting configuration to close, shutting off the flow into the pipeline shown in Fig. 1.

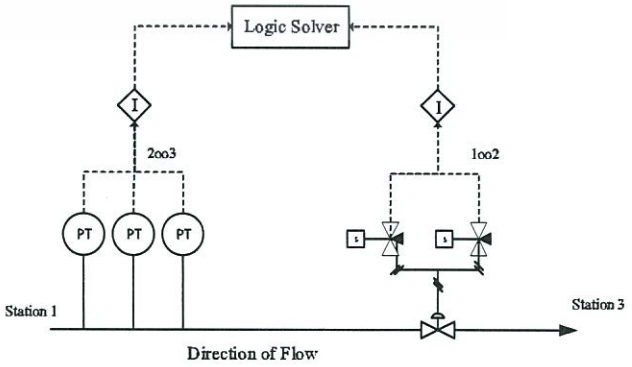


Fig. 1 Block Valve System

Manuscript received December 22, 2016; revised January 09, 2017.

Pawarisa Kongtong and Sakreya Chitwong are with the department of Instrumentation and Control Engineering, Faculty of Engineering, King Mongkut's Institute of technology Ladkrabang, Ladkrabang, Bangkok 10520 THAILAND. (e-mail : pawarisa.kt@hotmail.com, sakreya.ch@kmitl.ac.th).

IV. Units Evaluation Method

A. Markov Model

Markov model is a technique to calculate safety integrity level by state transition diagram. The diagram from state to another state will be presented transition failure mode of each component. The corresponding transition rates are indicated on the arrows or transition arch is shown in Fig. 2.

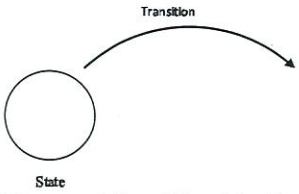


Fig. 2 Representation of Transition State

The two types of the system of Markov model are Restorable and Non-Restorable. Restorable shown in Fig. 3 the system containing state which can fail and can then be restore to initial state without necessary system failure. Non–Restorable shown in Fig. 4 is system containing state which can fail and cannot be restored to their up state without necessary system failure. The state transition diagram contains only transition direction towards system failure state.

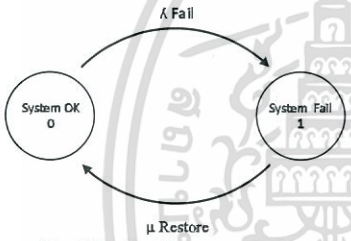


Fig. 3 Restorable component

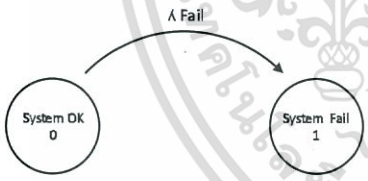


Fig. 4 Non- restorable component

B. State of Components

The state of a component is determined by list of the possible failure mode of each component to classify the degraded state (intermediate) and failure system states of block valve system. The initial state is a unique one which means no failure at all. The states are listed in Table I.

TABLE I, The State of a System

Components	Failure Mode	Resulting System State after a Single Failure
Pressure Sensor (S)	SD	Intermediate State
	SU	Intermediate State
	DD	Intermediate State
	DU	Intermediate State
Logic Solver (L)	S	Fail Safe
	D	Fail Dangerous
Solenoid Valve (A1)	SD	Fail Safe
	SU	Fail Safe
	DD	Intermediate State
	DU	Intermediate State
Block Valve (A2) +Actuator	S	Fail Safe
	D	Fail Dangerous

C. Probability of Failure

In block valve system, PFDavg is calculated by the state transition rates, repairs and restorations, which will be added into the models. Common cause failure can also be added into the calculation steps. It is capably simplified by a transition metric including failure modes of each component typically divided into four modes:

--Safe detected (SD)
--Safe undetected (SU)
--Dangerous detected (DD)
--Dangerous undetected (DU)

The λ parameter is the rate that the demand occurs.
The proof test interval (TI), the mean time to restore (MTTR), PFDavg defined as in Table II.

TABLE II, PFD Values of Component

Model Parameters	Pressure Transmitter	Logic Solver	Solenoid Valve	Valve +Actuator
λ^{SDC}	$4x10^{-10}$	-	5.05E x10-09	-
λ^{SUC}	$4x10^{-10}$	-	5.05E x10-09	-
λ^{SDN}	$1.96x10^{-8}$	$7.425 x10^{-07}$	9.595E x10-08	7 x10E-08
λ^{SUN}	$1.96 x10^{-8}$	$7.5 x10^{-09}$	9.595E x10-08	7E x10-08
λ^{DDC}	$3 x10^{-10}$	2.375x10-07	2.5E x10-09	1.07 x10E-07
λ^{DUC}	$1.2 x10^{-09}$	1.25E x10-08	2.925E x10-09	2.27E x10-07
λ^{DDN}	$1.47 x10^{-08}$	-	4.75E x10-08	-
λ^{DUN}	$5.88 x10^{-08}$	-	5.558E x10-08	-
SFF%	0.6	0.99	0.721	0.309
Test Interval (Hours)	17,520	17,520	17,520	17,520
MTTR (Hours)	12	12	12	12

D. Notation

PFD_{avg}	Average Probability of Failure on Demand
λ_S	Failure Rate of Sensor
λ_L	Failure Rate of Logic Solver
λ_{A1}	Failure Rate of Solenoid Valve
λ_{A1}	Failure Rate of Block Valve combines Actuator
λ^{SDC}	Safe Detected Common Cause Failure Rate
λ^{SUC}	Safe Undetected Common Cause Failure Rate
λ^{SUN}	Safe Undetected Normal Mode Failure Rate
λ^{SDN}	Safe detected Normal Mode Failure Rate.
λ^{DUN}	Dangerous Undetected Normal Mode Failure Rate
λ^{DUC}	Dangerous Undetected Common Cause Failure Rate
λ^{DDN}	Dangerous Detected normal mode failure rate
λ^{DDC}	Dangerous Detected Common Cause Failure Rate
μ_0	Restoration Rate
μ_{SD}	Restoration Rate for Shutdown

E. Calculating

Markov model illustrated in Fig. 5 is calculated by steady state probability solutions. The system has twelve states initial 0 to 11 and there are transition arcs of 41 between the states. It is assumed that system is operating in states 0.

ISBN: 978-988-14047-7-0
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Since twelve states exist, the P-matrix has a dimension of 12x12.

Each of the states from the Fig. 5 is identified by three units. State 0 represent system OK in fully operation. State 1, 2, 3 and 4 represent the system has firstly degrade (Intermediate State). State 5, 6, 7 and 8 represent the system has secondary degrade. State 9 represent system fail safe state. State 10 represent system fail dangerous undetected state. State 10 represent system fail dangerous detected.

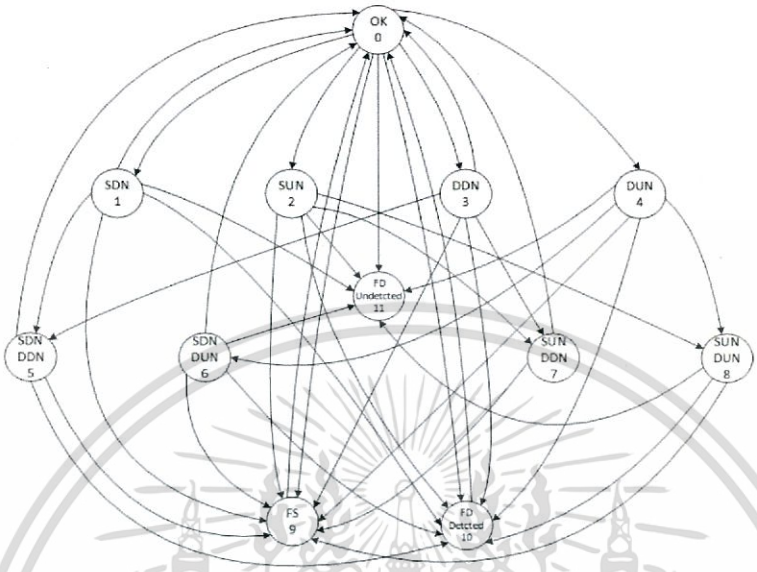


Fig. 5 Markov model of block valve system

$\Lambda_{0,0} = 1-(\Lambda_{0,1} + \Lambda_{0,2} \Lambda_{0,3} + \Lambda_{0,4} + \Lambda_{0,9+} \Lambda_{0,10+} \Lambda_{0,11})$
$\Lambda_{1,0} = \mu_0$
$\Lambda_{0,1} = 3\Lambda_S^{SDN}$
$\Lambda_{1,1} = 1-(\Lambda_{1,5} + \Lambda_{1,6} + \Lambda_{1,9} + \Lambda_{1,10} + \Lambda_{1,11})$
$\Lambda_{1,5} = 2\Lambda_S^{DDN}$
$\Lambda_{1,6} = 2\Lambda_S^{DUN}$
$\Lambda_{1,9} = \Lambda_S^{SC} + 2\Lambda_S^{SN}$
$\Lambda_{1,10} = \Lambda_S^{DDC}$
$\Lambda_{1,11} = \Lambda_S^{DUC}$
$\Lambda_{0,2} = 3\Lambda_S^{SUN}$
$\Lambda_{2,2} = 1-(\Lambda_{2,7} + \Lambda_{2,8} + \Lambda_{2,9} + \Lambda_{2,10} + \Lambda_{2,11})$
$\Lambda_{2,7} = 2\Lambda_S^{DDN}$
$\Lambda_{2,8} = 2\Lambda_S^{DUN}$
$\Lambda_{2,9} = \Lambda_S^{SUC} + 2\Lambda_S^{SUN}$
$\Lambda_{2,10} = \Lambda_S^{DDC}$
$\Lambda_{2,11} = \Lambda_S^{DUC}$
$\Lambda_{0,3} = 3\Lambda_S^{DDN} + \Lambda_L^{DD} + 2\Lambda_{A1}^{DDN} + \Lambda_{A2}^{DD}$
$\Lambda_{3,0} = \mu_0$
$\Lambda_{3,3} = 1-(\Lambda_{3,5} + \Lambda_{3,7} + \Lambda_{3,9} + \Lambda_{3,10})$
$\Lambda_{3,5} = 2\Lambda_S^{SDN}$
$\Lambda_{3,7} = 2\Lambda_S^{SUN}$
$\Lambda_{3,9} = \Lambda_S^{SUC} + \Lambda_S^{SDC} + \Lambda_{A1}^{S}$
$\Lambda_{3,10} = \Lambda_S^{DC} + 2\Lambda_S^{DN} + \Lambda_{A1}^{DD}$
$\Lambda_{0,4} = 3\Lambda_S^{DUN} + \Lambda_L^{DU} + 2\Lambda_{A1}^{DUN} + \Lambda_{A2}^{DU}$
$\Lambda_{4,4} = 1-(\Lambda_{4,6} + \Lambda_{4,8} + \Lambda_{4,9} + \Lambda_{4,10} + \Lambda_{4,11})$
$\Lambda_{4,6} = 2\Lambda_S^{SDN}$
$\Lambda_{4,8} = 2\Lambda_S^{SUN}$
$\Lambda_{4,9} = \Lambda_S^{SDC} + \Lambda_S^{SUC} + \Lambda_{A1}^{S}$
$\Lambda_{4,10} = \Lambda_S^{DDC} + 2\Lambda_S^{DDN} + \Lambda_{A1}^{DD}$
$\Lambda_{4,11} = \Lambda_S^{DUC} + 2\Lambda_S^{DUN} + \Lambda_{A1}^{DU}$
$\Lambda_{5,5} = 1-(\Lambda_{5,9} + \Lambda_{5,10})$
$\Lambda_{5,0} = \mu_0$
$\Lambda_{5,9} = \Lambda_S^{S}$
$\Lambda_{5,10} = \Lambda_S^{D}$
$\Lambda_{6,6} = 1-(\Lambda_{6,9} + \Lambda_{6,10})$
$\Lambda_{6,0} = \mu_0$
$\Lambda_{6,9} = \Lambda_S^{S}$
$\Lambda_{6,10} = \Lambda_S^{DD}$
$\Lambda_{7,7} = 1-(\Lambda_{7,9} + \Lambda_{7,10})$
$\Lambda_{7,0} = \mu_0$
$\Lambda_{7,9} = \Lambda_S^{S}$
$\Lambda_{7,10} = \Lambda_S^{D}$
$\Lambda_{8,8} = 1-(\Lambda_{8,9} + \Lambda_{8,10})$
$\Lambda_{8,9} = \Lambda_S^{S}$
$\Lambda_{8,10} = \Lambda_S^{DD}$
$\Lambda_{0,9} = 3\Lambda_S^{SDC} + 3\Lambda_S^{SUC} + \Lambda_L^{SD} + \Lambda_L^{SU} + \Lambda_{A1}^{SDC} + \Lambda_{A1}^{SUC} + 2\Lambda_{A1}^{SDN} + 2\Lambda_{A1}^{SUN} + \Lambda_{A2}^{SD} + \Lambda_{A2}^{SU}$
$\Lambda_{9,9} = 1$
$\Lambda_{0,10} = 3\Lambda_S^{DDC} + \Lambda_L^{DD} + \Lambda_{A1}^{DDC} + \Lambda_{A2}^{DD}$
$\Lambda_{10,10} = 1$
$\Lambda_{0,11} = 3\Lambda_S^{DUC} + \Lambda_L^{DU} + \Lambda_{A1}^{DUC} + \Lambda_{A2}^{DU}$
$\Lambda_{11,11} = 1$

The state of transition matrix is shown in Fig. 6

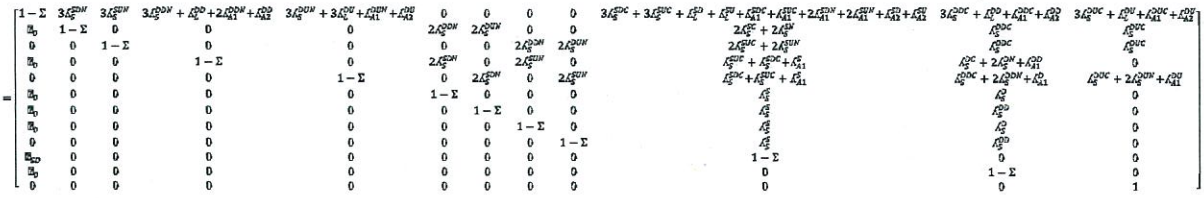


Fig. 6 Transition matrix of block valve system

Substituting the given failure rates and other parameter into the transition matrix is the P-matrix resulted in Fig. 7

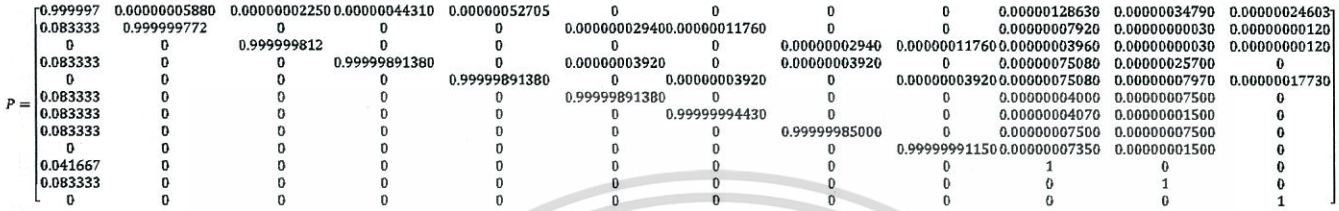


Fig. 7 Numeric transition matrix

V. Results

The transition matrix is calculated by the result of PFD_{avg} of 0.16413. The PFD_{avg} an achieved SIL level for low demand application is SIL 1 as Table III.

Due to SIL level being SIL1, no need to improve, but the enhanced design of the block valve design is a fail-close and solenoid valve de-energized to trip.

TABLE III, Safety Integrity Levels

Current PFD_{avg}	Safety Integrity Level (SIL)	PFD_{avg}
	4	.0001 - .00001
	3	.001 - .0001
	2	.01 - .001
0.16413	1	.1 - .01

Table V shows the PFD_{avg} with respect to change in test interval of the block valves. In this system, Fig. 8 shows a plot of probability of failure on demand as a function of operating time interval.

TABLE V, Results of PFD

ime Interval (Month)	3	6	9	12
PFD_{avg}	0.000593763	0.001565583	0.003537514	0.007770226
Time Interval (Month)	15	18	21	24
PFD_{avg}	0.016968965	0.037012553	0.080710488	0.17598927

VI. Conclusion

We proposed a method verifying the SIL which user can apply to other units in the requirements for verification SIF and implement to improve more thorough hazard and risk analysis to determine their needs more accurately.

The entire verification method will be obvious that the safety of operation reduces the risk. A loss, that will occur, can contribute to plan maintenance work, inspection, and to increase reliability.

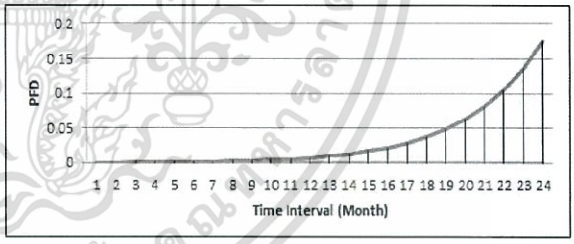


Fig. 8 Plot PFD as a function of operating time interval

References

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

[2] IEC-61508, "Functional safety of Electrical/electronic/programmable electronic safety-related systems," International Electrotechnical Commission, 2000.

[3] T. Chumuang, "Safety Instrumented System in Process Industrial Handbook," SE-EDUCATION, 2008 (in Thai).

[4] ISA-TR84.00.02-2002, "Safety Instrumented Functions (SIF)-Safety Integrity Level (SIL) Evaluation Techniques," The Instrumentation Systems and Automation Society, 2002.

[5] GeunWoong Yun, William J. Rogers, M. Sam Mannan, "*Journal of Loss Prevention in the Process Industries*," 22, 91–96, 2009.

[6] IEC-61165, "Application of Markov techniques, International Electrotechnical Commission, " 2006.

IAENG INTERNATIONAL ASSOCIATION OF ENGINEERS

International MultiConference of Engineers and Computer Scientists 2017

Hong Kong, 15-17 March, 2017

presents this

Best Student Paper Award of The 2017 IAENG International Conference on Electrical Engineering

to

P. Kongtong, and S. Chitwong

for the paper entitled

SIL Verification of Safety Instrumented System for Block Valve System in Gas Pipeline by Using Markov Model Methodology

Anna Lee, Assistant Secretary, IAENG
25 May 2017

ประวัติผู้เขียน

ชื่อ-นามสกุล	นางสาวปวริศา กองทอง
วัน เดือน ปีเกิด	10 พฤศจิกายน 2531 ที่จังหวัดอำนาจเจริญ
ที่อยู่	1458/64 เดอะนีซโมโน บางนา ถ.บางนา-ตราด แขวงบางนา เขตบางนา กรุงเทพฯ 10260
ประวัติการศึกษา	2553 วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมการวัดคุม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ประสบการณ์การทำงาน	
พ.ศ.2554-2555	ตำแหน่ง Sales Engineer บริษัท อัซบิล ไทยแลนด์ จำจัด
พ.ศ.2556-2558	ตำแหน่งวิศวกรเครื่องมือวัด บริษัท ไทยนิปปอนสตีลแอน์ซูมิคิน เอ็นจิเนียริ่ง แอนด์คอนตรัคชั่น จำกัด
ปัจจุบัน	ตำแหน่งวิศวกรเครื่องมือวัดและควบคุม บริษัท พีทีที แมนแทนแนนซ์ แอนด์เอ็นจิเนียริ่ง จำกัด