กรณีศึกษาของระบบวัดคุมนิรภัย
Study Case of Safety Instrumented System: SIS

จารุวัฒน์ เพ็งระวะ
บดินทร์ สุทัศน์

เนื้อหานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต
สาขาวิชาวิศวกรรมการวัดคุม
ภาควิชาวิศวกรรมการวัดคุม คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2557

กรณีศึกษาของระบบวัดคุมนิรภัย
Study Case of Safety Instrumented System: SIS

จารุวัฒน์ เพ็งระวะ
บดินทร์ สุทัศน์

เนื้อหานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต
สาขาวิชาวิศวกรรมการวัดคุม
ภาควิชาวิศวกรรมการวัดคุม คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2557

Study Case of Safety Instrumented System: SIS

JARUVAT PENGRAVA
BADIN SUTHAT

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
BACHELOR OF ENGINEERING IN INSTRUMENTATION ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
ACADEMIC YEAR 2014

ปริญญานิพนธ์ปีการศึกษา 2557
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองปริญญานิพนธ์

.....

หัวข้อปริญญานิพนธ์	กรณีศึกษาของระบบวัดคุมนิรภัย Study Case of Safety Instrumented System: SIS			
นักศึกษาผู้จัดทำ	จารุวัฒน์	เพ็งระวะ	**รหัสนักศึกษา**	54010190
	บดินทร์	สุทัศน์	**รหัสนักศึกษา**	54010724
ปริญญาตรี	วิศวกรรมศาสตร์บัณฑิต			
สาขาวิชา	วิศวกรรมการวัดคุม			
ปีการศึกษา	2557			

อาจารย์ผู้ควบคุมปริญญานิพนธ์	ลายมือชื่อ
รองศาสตราจารย์สักรียา ชิตวงศ์	

หัวข้อปริญญานิพนธ์	กรณีศึกษาของระบบวัดคุมนิรภัย Study Case of Safety Instrumented System: SIS		
นักศึกษาผู้จัดทำ	จารุวัฒน์ เพ็งระวะ	รหัสนักศึกษา	54010190
	บดินทร์ สุทัศน์	รหัสนักศึกษา	54010724
ปริญญาตรี	วิศวกรรมศาสตรบัณฑิต		
สาขาวิชา	วิศวกรรมการวัดคุม		
ปีการศึกษา	2557		

บทคัดย่อ

โครงงานนี้เป็นการศึกษาขั้นตอนการออกแบบระบบวัดคุมนิรภัย (Safety Instrumented System: SIS) โดยดำเนินงานตามมาตรฐานสากล IEC 61508 และมาตรฐาน IEC 61511 ซึ่งแสดงความต้องการโดยรวมของระบบวัดคุมนิรภัย เพื่อให้เป็นไปตามข้อกำหนดของมาตรฐาน ซึ่งภายในโครงงานได้แสดงส่วนประกอบต่างๆของระบบวัดคุมนิรภัย การวิเคราะห์หาค่าความอันตรายของกระบวนการผลิต ความหมายของค่าระดับความปลอดภัย วิธีการหาค่าระดับความปลอดภัย และวิธีการออกแบบระบบวัดคุมนิรภัยตามวงรอบความปลอดภัยมาตรฐานสากล IEC-61511

Thesis Title	Study Case of Safety Instrumented System: SIS	
Authors	Mr. Jaruvat	Phengrava
	Mr. Badin	Suthat
Thesis Advisor	Assoc.Prof. Sakreya	Chitwong
Year	2014	

Abstract

This project studies about how to design Safety Instrumented System: SIS based on International Standards IEC 61508/61511. Which represents the needs of the overall Safety Instrumented System In order to comply with the standard. In this project, which has shown the various components of the Safety Instrumented System, Process Hazard Analysis, the definition of the Safety Integrity Level: SIL, how to determine SIL and how to design Safety Instrumented System follow by safety life cycle of International Standard IEC-61511.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี ขอขอบพระคุณ รศ.สักรียา ชิตวงศ์ ที่ให้คำแนะนำความรู้ คำปรึกษาและเอาใจใส่เป็นอย่างดี จึงทำให้ปริญญานิพนธ์นี้สำเร็จลุล่วงไปได้ด้วยดี คณะผู้จัดทำขอกราบขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณคณาจารย์ทุกท่านที่ให้การศึกษาและความรู้ เพื่อนำความรู้ที่ได้มาประยุกต์ใช้ในการทำปริญญานิพนธ์ฉบับนี้

สุดท้ายนี้ขอขอบพระคุณบิดา มารดา ของคณะผู้จัดทำทุกท่าน ผู้ที่มอบชีวิต การศึกษาและอนาคต ตลอดจนให้คำปรึกษาและความช่วยเหลือในด้านต่างๆและกำลังใจในการทำปริญญานิพนธ์ฉบับนี้ให้สำเร็จลุล่วงไปได้ด้วยดี

คณะผู้จัดทำหวังว่าปริญญานิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อผู้สนใจที่จะศึกษาและหากเกิดข้อผิดพลาดประการใดคณะผู้จัดทำขออภัยมา ณ โอกาสนี้ด้วย

คณะผู้จัดทำ

สารบัญ

หน้า

บทคัดย่อภาษาไทย I
บทคัดย่อภาษาอังกฤษ II
กิตติกรรมประกาศ III
สารบัญ IV
สารบัญตาราง VII
สารบัญรูปภาพ VIII

บทที่ 1 บทนำ 1
1.1 ที่มาและความสำคัญ 1
1.2 หลักการและเหตุผล 1
1.3 วัตถุประสงค์ 1
1.4 ขอบเขต 1
1.5 ประโยชน์ที่คาดว่าจะได้รับ 2

บทที่ 2 ทฤษฎีและหลักการที่เกี่ยวข้อง 3
2.1 คำนำ 3
2.2 มาตรฐานสากลของระบบวัดคุมนิรภัย 3
2.2.1 มาตรฐาน IEC-61508 4
2.2.2 มาตรฐาน IEC-61511 4
2.3 การออกแบบระบบวัดคุมนิรภัย 5
2.4 ฟังก์ชันวัดคุมนิรภัย (Safety Instrumented Function) 7
2.5 ค่าระดับความปลอดภัย (Safety Integrity Level) 8
2.5.1 Low demand mode 8
2.5.2 High demand mode 9
2.6 ส่วนประกอบของฟังก์ชันวัดคุมนิรภัย 9
2.6.1 อุปกรณ์การวัด (Sensing Element) 10
2.6.1.1 ชนิดของอุปกรณ์การวัด 10
2.6.1.2 รูปแบบเครื่องมือวัดในระบบนิรภัย 12
2.6.2 ตัวประมวลผล (Logic Solver) 15
2.6.3 อุปกรณ์สุดท้าย (Final Element) 16
2.7 การวิเคราะห์อันตรายของกระบวนการผลิต (Process Hazard Analysis) 17
2.8 ความเสี่ยง (Risk) 17
2.9 ความเสี่ยงที่ยอมรับได้ (Tolerable Risk Guideline) 18
2.10 การลดค่าความเสี่ยง (Risk reduction) 19
2.11 ชั้นการป้องกันในกระบวนการผลิต (Layer of Protection in Process) 21

สารบัญ (ต่อ)

หน้า

2.12 วิธีการหาค่า SIL ที่ต้องการ) 22
2.13 Layer Of Protection analysis (LOPA) 23
2.14 ผลประโยชน์ที่ได้จากระบบวัดคุมนิรภัย 25

บทที่ 3 การดำเนินงาน 26
3.1 คำนำ 26
3.2 การออกแบบระบบวัดคุมนิรภัยตามมาตรฐาน IEC-61511 26
3.2.1 ขั้นตอนการวิเคราะห์อันตรายในกระบวนการผลิต 27
3.2.2 ประเมินความอันตรายเพื่อกำหนดค่าระดับความปลอดภัย หรือค่า SIL 29
3.2.3 จัดทำรายละเอียดความต้องการของระบบวัดคุมนิรภัยทั้งหมด 33
3.2.3.1 การเลือกใช้งานเครื่องมือวัดในส่วนอินพุตหรือ (Sensor part) 35
3.2.3.2 การเลือกใช้งานตัวควบคุม (PLC) 36
3.2.3.3 การเลือกใช้งานวาล์วนิรภัย (Shut Down Valve) 36
3.2.4 ดำเนินการจัดทำระบบวัดคุมนิรภัยให้เป็นไปตามที่ได้ออกแบบ 38
3.3 สถาปัตยกรรมของระบบวัดคุมนิรภัย 39
3.3.1 องค์ประกอบของส่วนควบคุมในระบบวัดคุมนิรภัย 39
3.3.1.1 ตัวควบคุม (CPU 317F) 40
3.3.1.2 ตัวแปลงสัญญาณระหว่าง 4 – 20 mA และ Profibus DP 41
3.3.1.3 Analog Input Module 41
3.3.1.4 Digital Output Module 42
3.3.1.5 Program SIMATIC Manager 42
3.4 ขั้นตอนการเขียน Safety Program 1oo2DI Voting 43
3.4.1 การตั้งค่าคอนฟิกของระบบอัตโนมัติ (Automation System) 43
3.4.2 การสร้าง Safety Program โดยการตั้ง F-Runtime Group 43
3.4.3 โครงสร้างและการทำงานของฟังก์ชัน F_1oo2DI (FB190) 43
3.4.3.1 โครงสร้างของฟังก์ชัน F_1oo2DI (FB190) 43
3.4.3.2 การทำงานของฟังก์ชัน F_1oo2DI (FB190) 45
3..4.4 ดำเนินการเขียนฟังก์ชัน 1oo2DI Voting ตามที่ได้ทำการออกแบบไว้ 46
3.4.4.1 ทำการสร้าง Data Block (DB2) 46
3.4.4.2 เขียนโปรแกรมใน OB1 46
3.4.4.3 เขียนโปรแกรมใน FB1 (Safety Program) 50

บทที่ 4 การทดลองและผลการทดลอง 52
4.1 คำนำ 52
4.2 วิธีการทดสอบ Analog Input Module 52

4.3 วิธีการทดลอง 54
4.4 ผลการทดลอง 56
4.4.1 กรณีที่อินพุตทั้งสองตัวตรวจจับค่าได้เท่ากัน และมีค่าน้อยกว่าค่า Set Point 56
4.4.2 กรณีที่อินพุตทั้งสองตัวตรวจจับค่าได้เท่ากัน และมีค่ามากกว่าค่า Set Point 56
4.4.3 กรณีอินพุตตัวที่ 1 เกิดความผิดพลาดในการทำงาน 57
4.4.4 กรณีอินพุตตัวที่ 2 เกิดความผิดพลาดในการทำงาน 58

บทที่ 5 สรุปผลการทดลอง 59
5.1 สรุปผลการทดลอง 59
5.2 วิเคราะห์ปัญหาและข้อเสนอแนะ 59

บรรณานุกรม 60

ภาคผนวก 61

สารบัญตาราง

ตารางที่ **หน้า**

2.1 ค่าระดับความปลอดภัยอัตราการเกิดอันตรายต่ำ (Low Demand Mode) 8
2.2 ค่าระดับความปลอดภัยอัตราการเกิดอันตรายสูง (High Demand Mode) 9
2.3 ตารางแสดงจำนวนอุปกรณ์น้อยที่สุดที่ยอมให้เกิดความผิดพลาดได้ 11
2.4 Layer Of Protection Analysis (LOPA) 24
3.1 รายงานผลลัพธ์ของการวิเคราะห์ความเป็นอันตรายที่ท่อส่งทางน้ำขาเข้าบัฟเฟอร์แท็งก์ 28
3.2 รายงานผลลัพธ์ของการวิเคราะห์ความเป็นอันตรายที่ถังพักน้ำก่อนเข้าสู่กระบวนการ 28
3.3 รายงานผลลัพธ์ของการวิเคราะห์ความเป็นอันตรายที่ถังความดันใช้งาน 29
3.4 ความถี่ของเหตุการณ์ที่ยอมรับได้ 31
3.5 ตารางจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดของ IEC 61508 สำหรับอุปกรณ์ TYPE B 34
3.6 ตารางข้อมูลของ Sensor Part 35
3.7 ตารางข้อมูลของ Safety PLC 36
3.8 ตารางข้อมูลของ Shutdown Valve 37
3.9 ตารางแสดงคุณลักษณะทั่วไปของ CPU 317F 40
3.10 ตารางแสดงแสดงลักษณะทั่วไปของ IM 153-2 41
3.11 ตารางแสดงแสดงลักษณะทั่วไปของอนาล็อกอินพุตโมดูล 42
3.12 ตารางแสดงแสดงลักษณะทั่วไปของดิจิตอลเอาท์พุตโมดูล 42

สารบัญภาพ

รูปที่		หน้า
2.1	ความแตกต่างการใช้งานมาตรฐาน IEC61508 และ IEC 61511	3
2.2	การใช้งานมาตรฐาน IEC 61508 และ IEC 61511	5
2.3	IEC 61508 Safety Life Cycle	6
2.4	IEC 61511 Safety Life Cycle	6
2.5	ฟังก์ชันวัดคุมนิรภัย	9
2.6	ฟังก์ชันนิรภัยในระบบ SIS	10
2.7	อุปกรณ์การวัดแบบ 1oo1 Voting	13
2.8	อุปกรณ์การวัดแบบ 1oo2 Voting ในภาวะปรกติ	14
2.9	การทำงานของวาล์วนิรภัย	16
2.10	แผนภาพแสดงความเสี่ยง	17
2.11	ALARP	19
2.12	วิธีการลดความเสี่ยงในโรงงานอุตสาหกรรม	20
2.13	ฟังก์ชันการป้องกันความดันเกินบนแผนภาพกระบวนการผลิต	21
2.14	การทำงานของชั้นการป้องกันความดันเกิน	22
3.1	วงรอบความปลอดภัย (Safety Life Cycle) ของมาตรฐาน IEC 61511	26
3.2	แผนภาพ (P&ID) ของกระบวนการผลิต	27
3.3	จำนวนฟังก์ชันนิรภัยของการป้องกันถังความดันใช้งาน	30
3.4	Cause & Effect Diagram ของการป้องกันของชั้นกระบวนการผลิตระเบิด	30
3.5	ไดอะแกรม LOPA ของฟังก์ชันการบอกกันถังความดันใช้งาน (TK-002) ระเบิด	31
3.6	ไดอะแกรม LOPA ของฟังก์ชันการบอกกันถังความดันใช้งาน (TK-002) ระเบิด (หลังการคำนวณหาค่าต่างๆเรียบร้อยแล้ว)	32
3.7	แผนภาพ (P&ID) ของกระบวนการผลิตหลังมีการติดตั้งระบบวัดคุมนิรภัย	38
3.8	แผนภาพ FTA ของฟังก์ชันนิรภัย	38
3.9	สถาปัตยกรรมของระบบวัดคุมนิรภัย	40
3.10	ตัวควบคุม (CPU 317F)	40
3.11	ตัวแปลงสัญญาณระหว่าง 4 – 20 mA และ Profibus DP	41
3.12	Analog Input Module	41
3.13	Digial Output Module	42
3.14	ฟังก์ชันบล็อกของ F_1oo2DI (FB190)	44
3.15	Data บล็อกของฟังก์ชัน F_1oo2DI (FB190)	44
3.16	Timing Diagram การทำงานของฟังก์ชัน 1oo2DI	45
3.17	ข้อมูลที่อยู่ภายใน DB2	46
3.18	การใช้คำสั่ง Move เพื่อทำการย้ายข้อมูล อนาล็อก อินพุต ตัวที่ 1 มาเก็บไว้ในหน่วยความจำของตัวควบคุม (PLC)	46

3.19 การใช้คำสั่ง Move เพื่อทำการย้ายข้อมูลจาก อนาล็อก อินพุต ตัวที่ 2 มาเก็บไว้ในหน่วยความจำของตัวควบคุม (PLC) 47
3.20 การใช้งานฟังก์ชันอนาล็อก เสกล (FC105) เพื่อใช้เสกลค่าอนาล็อก อินพุต ตัวที่ 1 47
3.21 การใช้งานฟังก์ชันอนาล็อก เสกล (FC105) เพื่อใช้เสกลค่าอนาล็อก อินพุต ตัวที่ 2 48
3.22 ฟังก์ชัน Compare (น้อยกว่าหรือเท่ากับ) เพื่อทำการเปรียบเทียบระหว่างค่าอนาล็อกอินพุต ตัวที่ 1 กับค่า Set Point 48
3.23 ฟังก์ชัน Compare (น้อยกว่าหรือเท่ากับ) เพื่อทำการเปรียบเทียบระหว่างค่าอนาล็อกอินพุต ตัวที่ 2 กับค่า Set Point 49
3.24 คำสั่งปิดหรือเปิดวาล์ว 49
3.25 การใช้คำสั่ง Call เพื่อเรียกใช้งาน Safety Program 49
3.26 การย้ายค่าอินพุตปรกติ ตัวที่ 1 (OB1) มาอยู่ใน Safety Program 50
3.27 การย้ายค่าอินพุตปรกติ ตัวที่ 2 (OB1) มาอยู่ใน Safety Program 50
3.28 การเซตค่าพารามิเตอร์ภายในฟังก์ชัน F_1oo2DI (FB190) 51
3.29 การย้ายข้อมูลจากเอาท์พุตของฟังก์ชัน F_1oo2DI (FB190) ไปสั่งให้วาล์วปิดหรือเปิดภายในโปรแกรมปรกติ (OB1) 51
4.1 สถาปัตยกรรมในการต่อการทดลองใช้งานฟังก์ชัน 1oo2DI Voting 52
4.2 อุปกรณ์แปลงสัญญาณจากไฟ 0 – 10 VDC เปลี่ยนเป็นกระแส 4 – 20 mA 53
4.3 จ่ายกระแสให้กับตัวควบคุมอนาล็อก อินพุต โมดูล 53
4.4 หน้าต่างของ Variable Table 1 (VAT1) 54
4.5 ค่าพารามิเตอร์ที่สนใจในการทดลอง 54
4.6 กรณีที่อินพุตทั้งสองตัวตรวจจับค่าได้เท่ากัน และมีค่าน้อยกว่าค่า Set Point 56
4.7 กรณีที่อินพุตทั้งสองตัวตรวจจับค่าได้เท่ากัน และมีค่ามากกว่าค่า Set Point 57
4.8 **กรณีอินพุตตัวที่ 1 เกิดความผิดพลาด**ในการทำงาน 57
4.9 **กรณีอินพุตตัวที่ 2 เกิดความผิดพลาด**ในการทำงาน 58

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

โครงงานนี้จัดทำขึ้นเพื่อศึกษาหลักการและการทำงานของระบบวัดคุมนิรภัย (Safety Instrumented System : SIS) ตามมาตรฐาน IEC 61508 และ 61511 ทำความเข้าใจข้อกำหนดต่างๆ ของอุปกรณ์วัด ตัวควบคุม และอุปกรณ์สุดท้าย สำหรับระบบวัดคุมนิรภัย (Sensor, Logic solver and Final device) และสามารถออกแบบระบบวัดคุมนิรภัยให้สอดคล้องตามมาตรฐานอุตสาหกรรม IEC 61511

1.2 หลักการและเหตุผล

ปัจจุบันอุตสาหกรรมปีโตรเคมี อย่างเช่น โรงกลั่นน้ำมัน โรงแยกก๊าซ โรงงานเคมี เป็นต้น ได้มีการลงทุนและก่อตั้งขึ้นในประเทศไทยเป็นจำนวนมาก ตลอดจนแท่นขุดเจาะน้ำมันและก๊าซธรรมชาติในอ่าวไทย เนื่องจากอุตสาหกรรมดังกล่าวเป็นกระบวนการที่มีความเสี่ยงต่อการเกิดระเบิด การรั่วไหลของสารพิษ ซึ่งก่อให้เกิดความเสียหายต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมเป็นวงกว้าง เพื่อป้องกันและลดโอกาสจะเกิดเหตุการณ์ดังกล่าว จึงได้มีการนำเทคโนโลยีที่เรียกว่า “ระบบวัดคุมนิรภัย (Safety Instrumented System : SIS)” มาประยุกต์ใช้งาน ซึ่งเป็นองค์ความรู้ที่เกี่ยวข้องกับวิศวกรในระบบการวัดและควบคุม เพื่อให้การผลิตบัณฑิตทางวิศวกรรมการวัดคุมสอดคล้องกับความต้องการบุคลากรของภาคอุตสาหกรรมโครงงานนี้จึงได้ครอบ คลุมเนื้อหา ซึ่งประกอบด้วย การทำความเข้าใจเกี่ยวกับมาตรฐานสากล คือ IEC 61508 และ 61511 ศึกษาอุปกรณ์วัดและตัวควบคุมที่ใช้งานระบบวัดคุมนิรภัย ตลอดจนศึกษาขั้นตอน วิธีการคำนวณ และการออกแบบระบบวัดคุมนิรภัยตามมาตรฐานดังกล่าว

1.3 วัตถุประสงค์

1. เรียนรู้หลักการของระบบวัดคุมนิรภัย (Safety Instrumented System: SIS)
2. เรียนรู้มาตรฐาน IEC 61508 และ 61511
3. เข้าใจข้อกำหนดต่างๆ ของอุปกรณ์วัดสำหรับระบบวัดคุมนิรภัย (Sensor, Logic solver and Final element)
4. เข้าใจข้อกำหนดต่างๆ ของตัวควบคุมสำหรับระบบวัดคุมนิรภัย (Logic solver : SIL Controller)
5. สามารถออกแบบระบบวัดคุมนิรภัยตามมาตรฐานอุตสาหกรรม

1.4 ขอบเขต

ติดตั้ง และเซ็ตค่าพารามิเตอร์ต่างๆพร้อมกับทดสอบการใช้งานโปรแกรมสำหรับระบบวัดคุมนิรภัย

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. เข้าใจข้อกำหนดต่างๆ ของอุปกรณ์วัด ตัวควบคุม และอุปกรณ์สุดท้าย สำหรับระบบวัดคุมนิรภัยตามมาตรฐาน IEC 61508 และ 61511
2. สามารถเรียนรู้ เข้าใจหลักการ และออกแบบระบบวัดคุมนิรภัย
3. เข้าใจโครงสร้างของระบบควบคุมกระบวนการเชิงอุตสาหกรรมที่มีระบบวัดคุมนิรภัย
4. สามารถนำองค์ความรู้ที่ได้ไปประกอบอาชีพต่อไปในอนาคตหลังจบการศึกษา

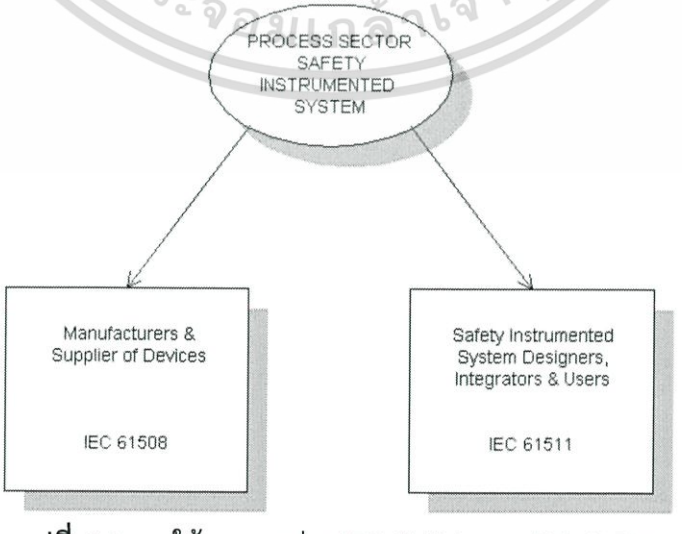
บทที่ 2
ทฤษฎีและหลักการที่เกี่ยวข้อง

2.1 คำนำ

สำหรับการทำงานเกี่ยวข้องกับระบบควบคุมและเครื่องมือวัดในอุตสาหกรรมกระบวนการผลิตชนิดต่างๆ รวมไปถึงอุตสาหกรรมปิโตรเคมี, อุตสาหกรรมการกลั่นน้ำมัน และอุตสาหกรรมเกี่ยวกับการแยกก๊าซธรรมชาติทั้งบนพื้นดินและแท่นการผลิตกลางทะเล ในปัจจุบันคงจะต้องมีความคุ้นเคยซึ่งอาจต้องทำงานหรือออกแบบรายละเอียดเกี่ยวกับเครื่องมือวัดในระบบนิรภัย ที่ต้องมีการดำเนินงานออกแบบให้อยู่ในระดับค่าระดับความปลอดภัย หรือค่า SIL (Safety Integrity Level) ซึ่งคำว่าค่าระดับความปลอดภัยนี้ จะมีความเกี่ยวข้องโดยตรงกับการทำงานในระบบการป้องกันอันตราย, ระบบนิรภัยต่างๆ, ระบบหยุดทำงานแบบฉุกเฉิน หรือ ระบบ ESD (Emergency Shutdown System) ในอุตสาหกรรมกระบวนการผลิตค่าระดับความปลอดภัย ได้ถูกกำหนดขึ้นโดยมาตรฐานสากล IEC 61508/61511 ซึ่งระบบ ESD หรือระบบนิรภัยต่างๆ (Safety Related System) จะถูกเรียกชื่อตามมาตรฐานสากล IEC 61508/61511 ว่าระบบ SIS (Safety Instrumented System) โดยมาตรฐาน IEC 61508 ได้ถูกรับรองให้ใช้งานประมาณปี 1998 ส่วนมาตรฐาน IEC 61511 ได้ถูกรับรองให้ใช้งานในภายหลังประมาณปี 2003 เพื่อเป็นแนวทางในการใช้งานกับอุตสาหกรรมกระบวนการผลิต

โดยโครงงานนี้เป็นการแสดงความต้องการโดยรวมของระบบนิรภัย เพื่อให้เป็นไปตามข้อกำหนดมาตรฐานสากล IEC 61508/61511 ซึ่งภายในบทความได้แสดงส่วนประกอบต่างๆที่อยู่ในระบบวัดคุมนิรภัย การวิเคราะห์หาค่าอันตรายของกระบวนการผลิต ความหมายของค่าระดับความปลอดภัย วิธีการหาค่าระดับความปลอดภัย และวิธีการออกแบบระบบวัดคุมนิรภัยตามวงรอบความปลอดภัยมาตรฐานสากล IEC-61511

2.2 มาตรฐานสากลของระบบวัดคุมนิรภัย



รูปที่ 2.1 การใช้งานระหว่าง IEC 61508 และ IEC 61511

จากรูปที่ 2.1 เป็นแนวทางในการใช้งานมาตรฐานสากลทั้งสองมาตรฐาน โดยถ้าผู้ใช้งานเป็นผู้ผลิตหรือผู้จำหน่ายอุปกรณ์ต่างๆ ที่จะนำไปใช้งานในระบบนิรภัย (Safety Related System) ต้องมีการผลิตหรือตรวจสอบตามข้อกำหนดในมาตรฐาน IEC 61508 เพื่อให้อุปกรณ์ที่ถูกผลิตออกมานั้นเป็นไปตามข้อกำหนดของมาตรฐานและถูกรับรองให้นำไปใช้ในระบบนิรนิรภัย (Certified Devices) แต่ถ้าเป็นผู้ใช้งานอุปกรณ์ที่ถูกผลิตมาตามข้อกำหนด หรือออกแบบระบบนิรภัยโดยรวม หรือนำอุปกรณ์ต่างๆ ไปใช้งานในระบบนิรภัยจะต้องทำตามข้อกำหนดในมาตรฐาน IEC 61511

2.2.1 มาตรฐาน IEC 61508

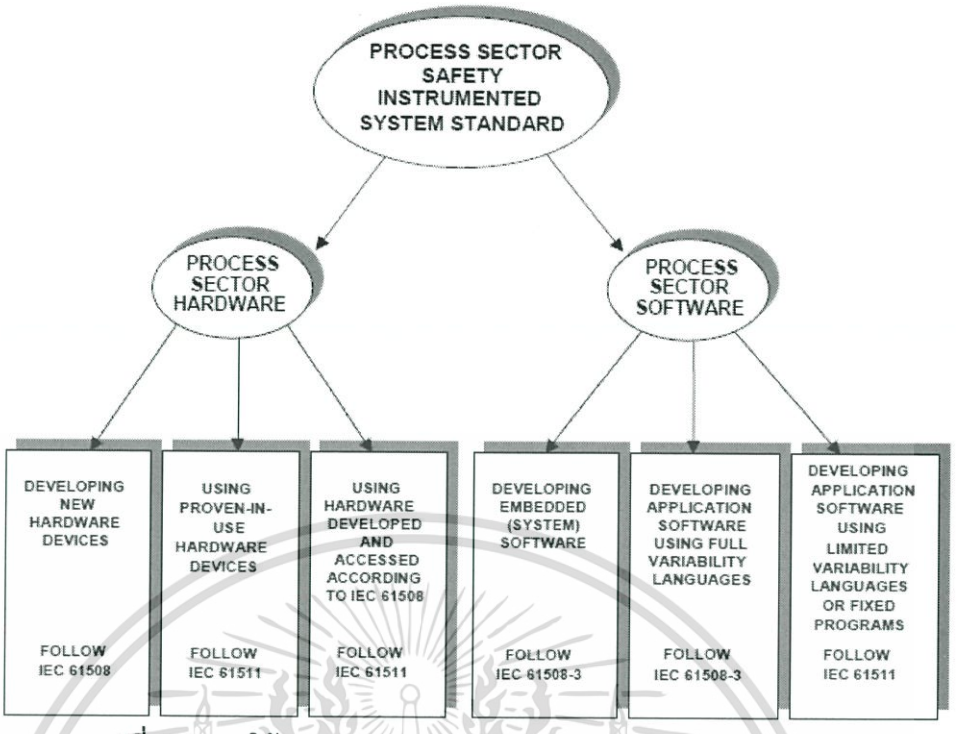
สำหรับผู้ผลิตอุปกรณ์ชิ้นส่วน (Hardware) หรือพัฒนาโปรแกรมขึ้นมาใหม่เพื่อนำไปใช้งานในระบบวัดคุมนิรภัย จะต้องดำเนินการให้เป็นไปตามมาตรฐาน IEC 61508 ซึ่งมาตรฐาน IEC 61508 นั้นจะเป็นมาตรฐานในการกำหนดรายละเอียดของระบบวัดคุมนิรภัยตั้งแต่ในขั้นตอนของการออกแบบกระบวนการผลิตจนถึงขั้นตอนการใช้งานระบบวัดคุมนิรภัย และใช้ในการกำหนดค่าระดับความปลอดภัยของฟังก์ชันนิรภัย (Safety Function) ซึ่งมาตรฐานนี้มีอยู่ด้วยกันทั้งหมด 7 ส่วน ดังนี้

- Part 1: General requirement
- Part 2: Requirements for electrical/electronic/programmable electronic safety-related system
- Part 3: Software requirement
- Part 4: Definitions and abbreviations
- Part 5: Example of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of part 2 and 3
- Part 7: Overview of techniques and measures

2.2.2 มาตรฐาน IEC 61511

สำหรับผู้ใช้งานระบบวัดคุมนิรภัยสำหรับอุตสาหกรรมกระบวนการผลิต (Process Industrial Sector) จะต้องดำเนินการให้เป็นไปตามมาตรฐาน IEC 61511 ซึ่งมาตรฐานนี้มีอยู่ 3 ส่วน ดังนี้

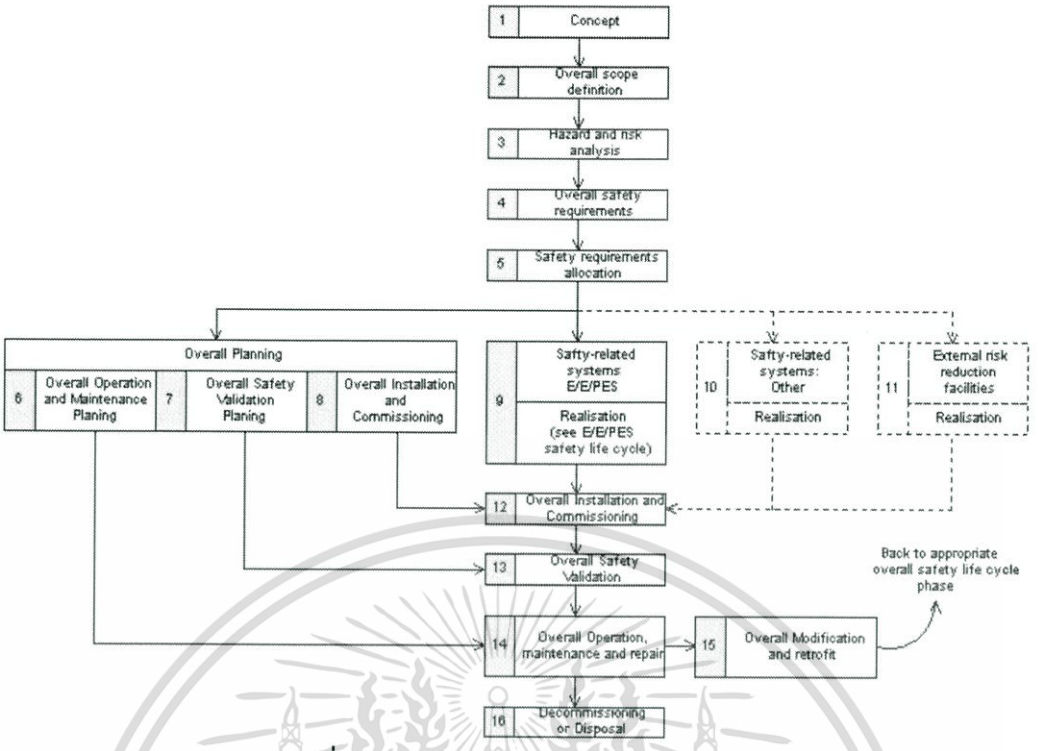
- Part 1: Framework, definitions, systems, hardware and software requirements
- Part 2: Guidelines for the application of IEC 61511-1
- Part 3: Guidance for the determination of the required safety integrity levels



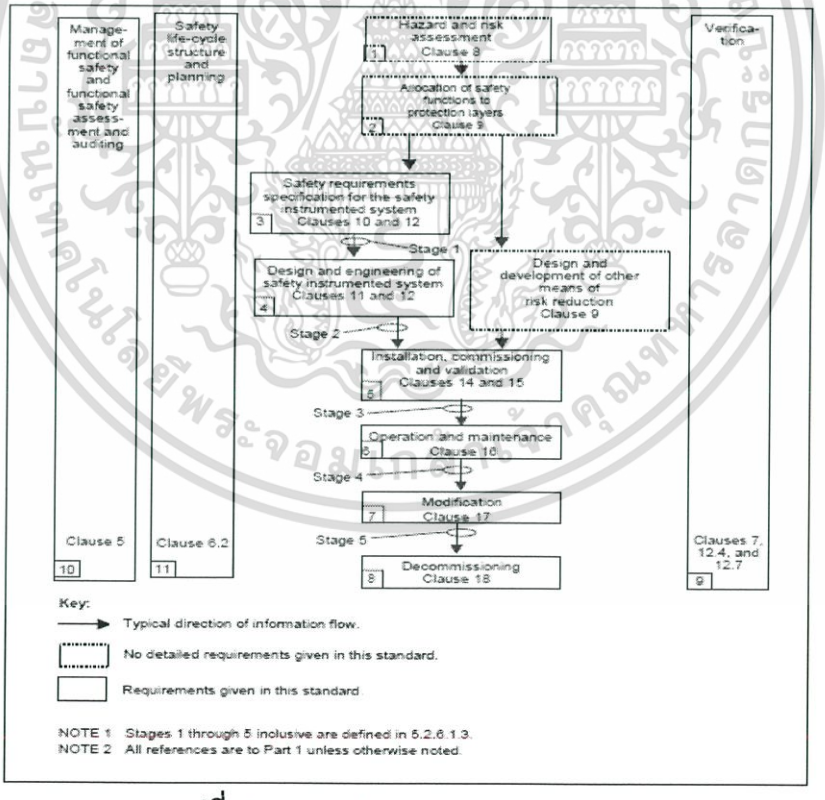
รูปที่ 2.2 การใช้งานมาตรฐาน IEC 61508 และ IEC 61511

2.3 การออกแบบระบบนิรภัย

เมื่อประมาณปี ค.ศ. 1998 คณะกรรมการ IEC (International Electro technical Commission) ได้นำเสนอมาตรฐาน IEC61508/61511 เพื่อใช้เป็นมาตรฐานในการออกแบบและใช้งานระบบนิรภัย ที่ประกอบด้วยอุปกรณ์ไฟฟ้า/อิเล็กทรอนิกส์/ระบบโปรแกรมทางอิเล็กทรอนิกส์ (Electrical/Electronics/Programmable Electronic System: E/E/PESs) ซึ่งระบบประมวลผลรูปแบบนี้จะถูกเรียกตามมาตรฐาน IEC-61508/61511 ว่า Safety Instrumented System หรือระบบ SIS หรือเป็นระบบที่คุ้นเคยกันดีในชื่อของ ระบบ ESD พื้นฐานของมาตรฐานทั้งสองจะเป็นไดอะแกรมที่เรียกว่า Safety Life Cycle สำหรับของมาตรฐาน IEC 61508 แสดงได้ดังรูปที่ 2.3 และมาตรฐาน IEC 61511 แสดงได้ดังรูปที่ 2.4



รูปที่ 2.3 IEC 61508 Safety Life Cycle



รูปที่ 2.4 IEC 61511 Safety Life Cycle

ลำดับขั้นการออกแบบตามวงรอบความปลอดภัยของมาตรฐาน IEC 61511 สามารถแสดงรายละเอียดในแต่ละเฟสได้ดังนี้

- เฟส 1 เป็นการวิเคราะห์หาความเป็นอันตรายที่อาจจะเกิดขึ้นในกระบวนการผลิต รวมไปถึงการประเมินผลกระทบต่อส่วนต่างๆ เมื่อมีเหตุการณ์อันตรายเกิดขึ้น
- เฟส 2 เมื่อทราบความเป็นอันตรายที่จะเกิดขึ้นในเฟส 1 แล้ว จะทำการจัดเตรียมฟังก์ชันนิรภัยต่างๆ ที่อยู่ในระบบวัดคุมนิรภัยและต้องทำการประเมินความเป็นอันตรายเพื่อนกำหนดค่าระดับความปลอดภัยหรือ ค่า SIL (Safety Integrity Level) ให้กับฟังก์ชันนิรภัยเหล่านี้เพื่อนำไปใช้เป็นข้อมูลในการออกแบบหรือเลือกใช้เครื่องมือวัด, ส่วนประมวลผลและอุปกรณ์สุดท้ายให้เหมาะสม
- เฟส 3 จัดทำรายละเอียดความต้องการของระบบวัดคุมนิรภัย (Safety Requirement Specification: SRS) เพื่อใช้ในการจัดส่งให้กับผู้ผลิตหรือผู้จำหน่ายอุปกรณ์ในส่วนต่างๆ เพื่อให้ผู้ผลิตหรือผู้จำหน่ายจัดทำอุปกรณ์ต่างๆ ได้ตรงตามความต้องการ
- เฟส 4 เป็นการดำเนินการจัดทำระบบวัดคุมนิรภัยให้เป็นไปตามความต้องการ โดยรายละเอียดในเฟสนี้จะเป็นการดำเนินของผู้ผลิตหรือผู้จำหน่ายในการจัดทำระบบนิรภัยให้ตรงกับความต้องการพร้อมทั้งการทดสอบการทำงานที่โรงงานผู้ผลิต จนถึงจัดส่งให้ผู้ใช้งานที่บริเวณโครงการก่อสร้าง และจะต้องมีการจัดเตรียมเอกสารแผนการติดตั้งและการใช้งานระบบอย่างชัดเจน
- เฟส 5 ทำการติดตั้งและทดสอบการทำงาน เป็นการดำเนินการติดตั้งระบบนิรภัยที่บริเวณการใช้งานให้เป็นไปตามข้อกำหนดของผู้ผลิตและทดสอบการทำงานร่วมกับกระบวนการผลิต
- เฟส 6 การใช้งานและการซ่อมบำรุง เป็นการใช้งานระบบนิรภัย สิ่งสำคัญต้องมีการจัดเตรียมการทดสอบการทำงานของฟังก์ชันนิรภัย เพื่อให้การทำงานเป็นไปตามรายละเอียดความต้องการ และเป็นการค้นหาความผิดพลาดอันตรายที่ระบบนิรภัยไม่สามารถตรวจสอบได้
- เฟส 7 การเปลี่ยนแปลงแก้ไขระบบนิรภัยหลังการใช้งาน จัดเตรียมขั้นตอนในการแก้ไขหรือเปลี่ยนแปลงระบบนิรภัยหลังจากที่มีการใช้งานผ่านไปแล้ว
- เฟส 8 การหยุดการทำงานเพื่อแก้ไขเพิ่มเติม เมื่อมีการเปลี่ยนแปลงใดๆ กับระบบนิรภัยจะต้องมีการจัดเตรียมแผนการหยุดทำงานระบบนิรภัยเพื่อดำเนินการ

2.4 ฟังก์ชันนิรภัย (Safety Function)

ความหมายของฟังก์ชันนิรภัยได้ถูกแสดงอยู่ในหัวข้อ 3.5.1 ของ IEC 61508-4 เป็นดังนี้ ฟังก์ชันนิรภัยเป็นฟังก์ชันที่ถูกจัดเตรียมไว้บนระบบนิรภัยชนิดต่างๆ ซึ่งมีจุดประสงค์ในการทำให้กระบวนการผลิตอยู่ในสภาวะปลอดภัยจากเหตุการณ์อันตรายที่กำหนดสำหรับตัวอย่างฟังก์ชันนิรภัยสำหรับอุปกรณ์ป้องกันอุณหภูมิเกิน โดยใช้เซนเซอร์อุณหภูมิติดตั้งไว้ในขดลวดของมอเตอร์ไฟฟ้า ในการสั่งหยุดการทำงานมอเตอร์ก่อนที่จะมีอุณหภูมิเกินจุดกำหนด ซึ่งจะเรียกว่าฟังก์ชันนิรภัย แต่ถ้ามีการจัดเตรียมฉนวนชนิดพิเศษที่สามารถทนอุณหภูมิสูงได้ ในลักษณะนี้จะไม่ใช่ฟังก์ชันนิรภัย (ถึงแม้ว่าจะเป็นการป้องกันอันตรายที่เหมือนกัน)

2.5 ค่าระดับความปลอดภัย SIL (Safety Integrity Level)

จากที่ได้กล่าวไปแล้วข้างต้น รูปแบบของระบบนิรภัยมีหลายรูปแบบให้ผู้ใช้งานได้เลือกใช้ โดยตัวแปรที่นำมากำหนดนั้นจะขึ้นอยู่กับค่าระดับความปลอดภัย หรือค่า SIL (Safety Integrity Level) ซึ่งจะใช้แสดงค่าเฉลี่ยความผิดพลาดอันตรายของฟังก์ชันนิรภัย หรือค่า PFD_{avg} (Average Probability of Failure on Demand) หรืออีกในความหมายหนึ่งจะเป็นค่าความเป็นไปได้เพียงใดที่ฟังก์ชันนิรภัยไม่สามารถทำงานได้ในเวลาที่ต้องการ ซึ่งมาตรฐานได้กำหนดค่าระดับความปลอดภัยของระบบนิรภัยได้เป็น 2 Mode ดังนี้

2.5.1 Low Demand Mode

ความหมายของ Low Demand Mode ได้ถูกแสดงอยู่ในหัวข้อ 3.5.12 ของ IEC 61508-4 เป็นดังนี้ ความถี่ของความต้องการบนระบบนิรภัยไม่มากกว่าหนึ่งครั้งต่อปีและไม่มากกว่าสองเท่าของความถี่ในการทดสอบการทำงาน โดยคาระดับความปลอดภัยได้ถูกแบ่งออกเป็น 4 ระดับตามมาตรฐาน IEC 61508-1 Table 2 ดังแสดงได้ในตารางที่ 2.1

ตารางที่ 2.1 ค่าระดับความปลอดภัยที่อัตราการเกิดอันตรายต่ำ (Low Demand Mode

ค่าระดับความปลอดภัย (Safety Integrity Level)	Low demand mode of operation (Average probability of a dangerous failure per hour)
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 $< 10^{-1}$

จากตารางที่ 2.1 จะเห็นว่าค่าระดับความปลอดภัย 4 จะมีผลรวมค่าเฉลี่ยความผิดพลาดอันตรายต่ำที่สุด และค่าระดับความปลอดภัย 1 จะมีผลรวมค่าเฉลี่ยความผิดพลาดอันตรายสูงที่สุด สำหรับฟังก์ชันควบคุมจะมีผลรวมค่าเฉลี่ยความผิดพลาดอันตรายสูงกว่าค่าระดับความปลอดภัย 1 หรืออาจเรียกว่า SIL 0 ซึ่งสามารถจัดเตรียมฟังก์ชันเหล่านี้ได้ในระบบควบคุมพื้นฐานทั่วไป (Basic Plant Control System: BPCS) ซึ่งในอุตสาหกรรมกระบวนการผลิตทั่วไปจะทำงานใน Mode นี้

สำหรับฟังก์ชันนิรภัยที่ทำงานใน Low Demand Mode อัตราความอันตราย (Hazard rate) ขึ้นอยู่กับอัตราความต้องการ (Rate on Demands) บนระบบนิรภัยและความเป็นไปได้ที่จะมีความผิดพลาดในการทำงานของระบบนิรภัยในฟังก์ชันนิรภัย แสดงได้ดังนี้

Hazard rate (h) = Demand rate (d) × Average probability of failure on demand (PFD_{avg})

ดังนั้นฟังก์ชันนิรภัยที่ทำงานใน Low Demand Mode ค่าระดับความปลอดภัย ถูกกำหนดจากค่าเฉลี่ยความเป็นไปได้ของความผิดพลาดในการทำหน้าที่ฟังก์ชันนิรภัย ค่านี้เป็นค่าที่ทำให้ค่าความเสี่ยงอยู่ในค่าที่ยอมรับได้ ดังนั้นค่า SIL ที่ต้องการสามารถหาได้จากอัตราความต้องการ (Demand rate) และอัตราความอันตราย (Hazard rate)

2.5.2 High Demand Mode

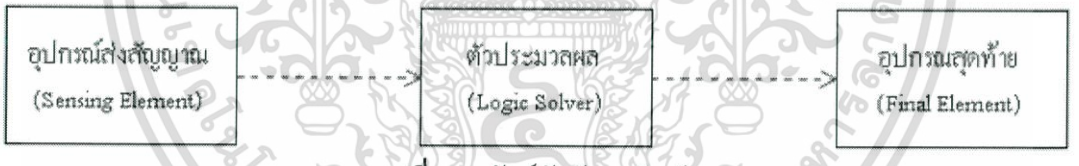
ความหมายของ High Demand Mode ได้ถูกแสดงอยู่ในหัวข้อ 3.5.12 ของ IEC 61508-4 เป็นดังนี้ ความถี่ของความต้องการบนระบบนิรภัยมากกว่าหนึ่งครั้งต่อปีและมากกว่าสองเท่าของความถี่ในการทดสอบการทำงาน โดยค่าระดับความปลอดภัยได้ถูกแบ่งออกเป็น 4 ระดับตามมาตรฐาน IEC 61508-1 Table 3 ดังแสดงได้ในตารางที่ 2.2

ตารางที่ 2.2 ค่าระดับความปลอดภัยที่อัตราการเกิดอันตรายสูง (High Demand Mode)

ค่าระดับความปลอดภัย (Safety Integrity Level)	Low demand mode of operation (Average probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

2.6 ส่วนประกอบของฟังก์ชันวัดคุมนิรภัย (Safety Instrumented Function: SIF)

ส่วนประกอบของฟังก์ชันวัดคุมนิรภัย หรือ Safety Instrumented Function (SIF) เป็นฟังก์ชันนิรภัยที่ถูกจัดเตรียมขึ้นด้วยเครื่องมือวัดทางอุตสาหกรรมชนิดต่างๆในระบบ SIS สำหรับ SIF ตามมาตรฐาน IEC 61508/61511 ประกอบไปด้วยส่วนหลักๆที่สำคัญอยู่ 3 ส่วน ดังแสดงในรูปที่ 2.5



รูปที่ 2.5 ฟังก์ชันวัดคุมนิรภัย

จากรูปที่ 2.5 ค่าระดับความปลอดภัยของฟังก์ชันวัดคุมนิรภัยสามารถหาได้จากผลรวมค่าเฉลี่ยความผิดพลาดอันตรายของทุก ๆ ส่วนรวมกัน เป็นสมการดังนี้

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

เมื่อ PFD_{AVG} = ผลรวมค่าเฉลี่ยความผิดพลาดอันตรายของฟังก์ชันวัดคุมนิรภัย

PFD_{SE} = ค่าเฉลี่ยความผิดพลาดอันตรายของอุปกรณ์ส่งสัญญาณ

PFD_{LS} = ค่าเฉลี่ยความผิดพลาดอันตรายของส่วนประมวลผล

PFD_{FE} = ค่าเฉลี่ยความผิดพลาดอันตรายของอุปกรณ์สุดท้าย

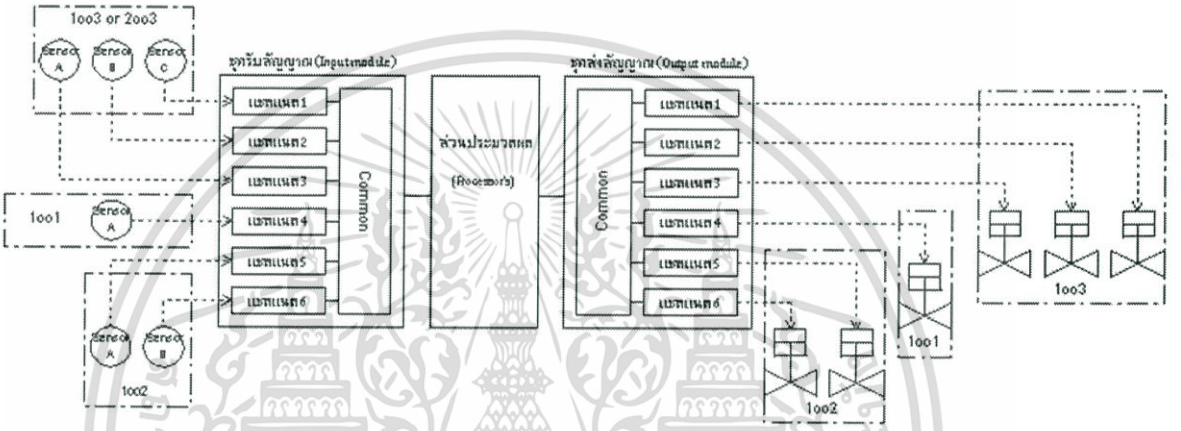
ดังนั้นเมื่อค่าระดับความปลอดภัยได้ถูกกำหนดให้กับฟังก์ชันนิรภัย โดยใช้วิธีการต่างๆตามมาตรฐาน IEC 61508/61511 แล้ว การออกแบบหรือการเลือกใช้อุปกรณ์ต่างๆ ในฟังก์ชันนิรภัยจะต้องมีค่าเฉลี่ยความผิดพลาดอันตรายอยู่ในขอบเขตของแต่ละค่าระดับความปลอดภัย

จากรายละเอียดที่ได้แสดงไปแล้วข้างต้น จะเห็นได้ว่าค่า SIL หรือค่าระดับความปลอดภัยไม่สามารถกำหนดได้จากอุปกรณ์เพียงส่วนเดียว แต่เกิดจากทั้ง 3 ส่วนร่วมกัน นั่นคือถ้าใช้ระบบ

ประมวลผลที่เป็นแบบ Safety PLC ที่ถูกรับรองที่ SIL 3 เป็นตัวประมวลผลรวม ไม่ได้หมายความว่าฟังก์ชันนิรภัยที่ต่อเข้ามายังส่วน

ประมวลผลนี้ทั้งหมดจะมีค่าระดับความปลอดภัยที่ SIL 3 ทุกฟังก์ชัน ต้องมีการพิจารณาค่าเฉลี่ยความผิดพลาดอันตรายของอุปกรณ์ส่วนอื่นๆร่วมด้วย

ระบบนิรภัยในอุตสาหกรรมกระบวนการผลิตจะมีฟังก์ชันนิรภัยอยู่หลายฟังก์ชันซึ่งจะถูกต่อเข้ากับส่วนประมวลผลรวมกันหรือแบ่งออกไปตามหน่วยการผลิตขึ้นอยู่กับการออกแบบ ในแต่ละฟังก์ชันอาจจะมีค่าระดับความปลอดภัยที่แตกต่างกันได้ แต่ค่าระดับความปลอดภัยของส่วนประมวลผลรวมต้องมีค่าเท่ากับค่าระดับความปลอดภัยสูงสุดของฟังก์ชันนิรภัย ตัวอย่างระบบ SIS สามารถแสดงได้ดังรูปที่ 2.6



รูปที่ 2.6 ฟังก์ชันนิรภัยในระบบ SIS

2.6.1 อุปกรณ์การวัด (Sensing Element)

เครื่องมือวัดในระบบวัดคุมนิรภัยจะถูกแบ่งตามการออกแบบ หลังจากที่มาตรฐานสากล IEC-61508 ได้ผ่านการรับรองให้มีการนำมาใช้งานกับการออกแบบระบบวัดคุมนิรภัยที่ใช้อุปกรณ์ที่มีชิ้นส่วนประเภท E/E/PEs จึงทำให้ผู้ผลิตเครื่องมือวัดได้ทำการผลิตเครื่องมือวัดเพื่อนำไปใช้งานกับระบบนิรภัยโดยเฉพาะ จากนั้นจึงให้ผู้ตรวจสอบอิสระ(Third party) ที่น่าเชื่อถือทำการตรวจสอบและรับรองให้ใช้งาน จะเรียกว่า Certified Instrumentation ส่วนเครื่องมือวัดที่มีใช้งานกันมาในระบบนิรภัยก่อนที่มาตรฐานนี้จะลองให้ใช้งานจะเรียกว่า Non-Certified Instrumentation ทั้งสองประเภทนี้สามารถนำไปใช้ในระบบนิรภัยได้

2.6.1.1 ชนิดของอุปกรณ์การวัด

- เครื่องมือวัดที่ผ่านการรับรอง (Certified Instrumentation)

อุปกรณ์ที่จะนำไปใช้ในระบบนิรภัยทั้งอุปกรณ์ที่ผ่านการทดสอบและได้รับการรับรองจากสถาบันที่เชื่อถือได้ว่าสามารถนำไปใช้กับระบบนิรภัยได้ และยังมีอุปกรณ์อีกหลายชนิดที่ยังไม่ได้รับการรับรองแต่ก็สามารถนำอุปกรณ์เหล่านั้นไปใช้ในระบบนิรภัยได้แต่จะต้องพิจารณาถึงรายละเอียดอัตราความผิดพลาดและชนิดของความผิดพลาด เพื่อความเชื่อถือได้ของข้อมูลสำหรับอุปกรณ์วัดที่จะนำมาใช้งานกับระบบวัดคุมนิรภัยแล้ว

มาตรฐาน IEC 61508 Part 2 ได้จัดตามตารางการจัดลักษณะรูปแบบของอุปกรณ์ในระบบควบคุมนิรภัยได้ 2 ตารางตามชนิดของอุปกรณ์ดังแสดงในรูปที่ 6 ซึ่งเป็นตารางสำคัญที่แสดงจำนวนอุปกรณ์น้อยที่สุดที่ยอมให้เกิดความผิดพลาดได้ (Minimum Hardware Fault tolerance: HFT) ในแต่ละรูปแบบของอุปกรณ์ในระบบวัดคุมนิรภัย ตารางทั้งสองแบ่งแยกคุณสมบัติของส่วนประกอบในอุปกรณ์ออกเป็น 2 ชนิดคือ อุปกรณ์ที่ประกอบด้วยส่วนประกอบชนิด A และอุปกรณ์ที่ประกอบด้วยส่วนประกอบชนิด B อุปกรณ์ที่ประกอบด้วยส่วนประกอบทั้ง 2 ชนิดนี้ถูกเรียกว่าระบบย่อย (Subsystem)

- อุปกรณ์ชนิด A (Type A)

  อุปกรณ์ที่เครื่องมือวัดที่จัดอยู่ในชนิดนี้มีส่วนประกอบของชิ้นส่วนพื้นฐานที่ใช้กันอยู่ทั่วไปอาทิเช่น ตัวทรานซิสเตอร์,ตัวต้านทาน และขดลวด เป็นต้น อุปกรณ์เหล่านี้สามารถใช้งานได้เป็นเวลานานและสามารถตรวจสอบการทำงานได้อย่างสมบูรณ์อุปกรณ์การวัดต่อเนื่องแบบทั่วไป (Conventional Analogue Transmitter) อุปกรณ์การวัดแบบหน้าสัมผัสอาทิเช่น สวิตช์ระดับ(Level Switch),สวิตช์ความดัน (Pressure Switch) และสวิตช์ตำแหน่ง(Position Switch) เป็นต้น อุปกรณ์เหล่านี้จัดอยู่ในอุปกรณ์ชนิดA

- อุปกรณ์ชนิด B (Type B)

  อุปกรณ์ที่เครื่องมือวัดที่จัดอยู่ในชนิดนี้เป็นอุปกรณ์ที่มีส่วนประกอบของชิ้นส่วน ที่ใช้เทคโนโลยีสมัยใหม่อาทิเช่น วงจรรวม (Integrated Circuit: IC) หรือไมโครโปรเซสเซอร์ (Microprocessor) เป็นต้น อุปกรณ์เหล่านี้ไม่สามารถใช้งานได้เป็นเวลานานและไม่สามารถตรวจสอบการทำงานได้อย่างสมบูรณ์

ตารางที่ 2.3 ตารางแสดงจำนวนอุปกรณ์น้อยที่สุดที่ยอมให้เกิดความผิดพลาดได้ (IEC 61508-2)

Table 2 - Hardware Safety integrity: architectural constraints on subsystems build from TYPE A components

Safe Failure Fraction (SFF)	Hardware fault tolerance (see note 2)		
	0 (see note 3)	1	2
< 60%	SIL 1	SIL 2	SIL 3
60% - 90%	SIL 2	SIL 3	SIL 4
90% - 99%	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Note 1 See explanation below for details on interpreting this table
Note 2 Hardware fault tolerance is the maximum number of faults in a subsystem, arising from random hardware failure, which can occur without leading to a undetected dangerous failure
Note 3 A hardware fault tolerance of zero means a single fault could cause an undetected dangerous failure

Table 3 - Hardware Safety integrity: architectural constraints on subsystems build from TYPE B components

Safe Failure Fraction (SFF)	Hardware fault tolerance (see note 2)		
	0 (see note 3)	1	2
< 60%	Not allowed	SIL 1	SIL 2
60% - 90%	SIL 1	SIL 2	SIL 3
90% - 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Note 1 See explanation below for details on interpreting this table
Note 2 Hardware fault tolerance is the maximum number of faults in a subsystem, arising from random hardware failure, which can occur without leading to a undetected dangerous failure
Note 3 A hardware fault tolerance of zero means a single fault could cause an undetected dangerous failure

จากตารางที่ 2.3 สามารถแสดงรายละเอียดของรูปแบบอุปกรณ์ใน Table2 และ Table3 ได้คือ

" 0 " หมายความว่า ใช้อุปกรณ์หนึ่งตัว ดังนั้นเมื่อตัวอุปกรณ์เกิดความผิดพลาดอันตรายจะทำให้ไม่มีอุปกรณ์ที่ยังสามารถทำงานได้ต่อไป ทำให้ระบบควบคุมนิรภัยไม่สามารถทำหน้าที่ได้อย่างถูกต้องต่อไปได้

" 1 " หมายความว่า ใช้อุปกรณ์สองตัวติดต่อกันให้มีการทำงานในรูปแบบอนุกรมดังนั้นเมื่ออุปกรณ์ตัวใดตัวหนึ่ง เกิดความผิดพลาดอันตราย แต่ยังคงมีอุปกรณ์ที่สองที่ยังคงทำงานได้ต่อไปจึงทำให้ระบบควบคุมนิรภัยสามารถทำงานได้อย่างถูกต้องตามฟังก์ชันนิรภัย

" 2 " หมายความว่า ใช้อุปกรณ์สามตัวต่อกันให้มีการทำงานในรูปแบบอนุกรม ดังนั้นเมื่ออุปกรณ์ตัวที่หนึ่งเกิดความผิดพลาดเสียหาย อุปกรณ์ตัวที่สองและตัวที่สามก็ยังสามารถทำงานได้ต่อไป ถึงแม้ว่าอุปกรณ์ตัวที่สองจะเกิดความผิดพลาดอันตราย อุปกรณ์ตัวที่สามก็ยังสามารถทำงานได้ต่อไป และระบบควบคุมนิรภัยก็ยังสามารถทำงานได้ต่อไปอย่างถูกต้อง

- เครื่องมือวัดที่ไม่ผ่านการรับรอง (Non-Certified Instrumentation)

อุปกรณ์เครื่องมือวัดส่วนใหญ่ที่จะใช้นำไปใช้เป็นอุปกรณ์วัด (Sensing Element) อาทิเช่น อุปกรณ์วัดความดัน(Pressure Transmitter) หรืออุปกรณ์วัดอุณหภูมิ(Temperature Transmitter) และอุปกรณ์สุดท้าย (Final Element) อาทิเช่น วาล์วนิรภัย(Shut Down Valve) ของระบบนั้น เป็นอุปกรณ์ที่ไม่ได้มีการรับรองเพื่อนำไปใช้ในระบบนิรภัยหรือเป็นอุปกรณ์ที่ใช้งานสำหรับควบคุมทั่วไป ดังนั้นจึงไม่สะดวกในการเลือกใช้งานและไม่สามารถแน่ใจได้ว่าอุปกรณ์นั้นมีความเชื่อมั่นในการทำงานได้เพียงใดในเวลาที่ต้องการ ดังนั้นการใช้งานและการผลิตจะต้องเป็นไปตามมาตรฐานโดยมาตรฐาน IEC 61508 ได้ผ่านการรับรองให้มีการใช้งานมาก่อน มาตรฐาน IEC 61511 โดย IEC 61508 เป็นมาตรฐานที่ใช้ในการออกแบบและจัดทำส่วนประมวลผลที่ประกอบไปด้วยระบบไฟฟ้าหรือระบบอิเล็คทรอนิคส์ที่สามารถโปรแกรมการทำงานได้ (Electrical/ Electronic/Programmable electronic system: E/E/PESs) ส่วน IEC 61511 จะเป็นมาตรฐานที่เกี่ยวข้องกับการใช้งานระบบนิรภัยในอุตสาหกรรมกระบวนการผลิต

2.6.1.2 รูปแบบเครื่องมือวัดในระบบนิรภัย (Sensing Architecture)

เครื่องมือควบคุมแบบอนาลอก (Analogue transmitter) ได้รับการยอมรับและมีความเชื่อถือสูงในการนำไปใช้งานกับระบบควบคุมนิรภัย มากกว่าอุปกรณ์การวัดแบบหน้าสัมผัส (Switches) เนื่องจากอุปกรณ์การวัดแบบหน้าสัมผัสจะไม่สามารถทำการตรวจสอบความผิดพลาดแบบอัตโนมัติได้เหมือนกับอุปกรณ์การวัดแบบต่อเนื่อง ด้วยเหตุผลนี้อุปกรณ์การวัดแบบ

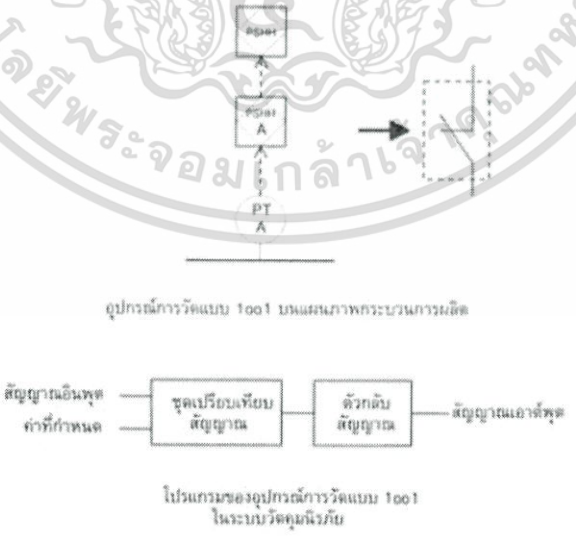
หน้าสัมผัสที่จะนำไปใช้งานในระบบควบคุมนิรภัยจึงมีการใช้งานที่ลดลงและเปลี่ยนมาใช้อุปกรณ์การวัดที่มีสัญญาณเอาต์พุตเป็นแบบอนาลอกแทน โดยใช้ร่วมกับตัวประมวลผลที่สามารถโปรแกรมการทำงานได้ เพื่อใช้ประโยชน์ที่ได้จากการเขียนโปรแกรมไปใช้ในการตรวจสอบการผิดพลาดของอุปกรณ์ รูปแบบพื้นฐานของอุปกรณ์การวัดแบบทั่วไปที่ใช้กันอย่างแพร่หลายในระบบควบคุมนิรภัยจะมีดังนี้

1. อุปกรณ์การวัดแบบ 1oo1 (One out of One voting)
2. อุปกรณ์การวัดแบบ 1oo2 (One out of One voting)
3. อุปกรณ์การวัดแบบ 1oo3 (One out of Three voting)
4. อุปกรณ์การวัดแบบ 2oo3 (Two out of Three voting)
5. อุปกรณ์การวัดแบบ 2oo2 (Two out of Two voting)

แต่ในส่วนของโครงงานที่ทำนี้จะขอยกตัวอย่างเพียง 2 กรณีเท่านั้น คือ การต่ออุปกรณ์การวัดแบบ 1oo1 (One out of One voting) และการต่ออุปกรณ์การวัดแบบ 1oo2 (One out of One voting)

- อุปกรณ์การวัดแบบ 1oo1 (One out of One voting)

รูปแบบนี้จะใช้อุปกรณ์การวัดเพียงตัวเดียวต่อกับระบบควบคุมนิรภัย ในการทำงานถ้าอุปกรณ์วัดค่าความผิดปกติได้หรือถึงจุดทำงานที่กำหนดไว้ ก็จะทำให้ระบบควบคุมนิรภัยทำงานทันที ซึ่งสามารถแสดงการเปรียบเทียบได้ในรูปสวิทช์ปกติเปิดหนึ่งตัว (ในสภาวะการทำงานหรือเมื่อจ่ายพลังงานให้กับอุปกรณ์จะทำให้สวิทช์อยู่ในตำแหน่งปิด) แต่ถ้าเกิดความผิดพลาดอันตรายขึ้นและระบบนิรภัยไม่สามารถตรวจสอบความผิดพลาดนั้นได้ จะทำให้กระบวนการผลิตเข้าสู่สภาวะอันตรายเพราะระบบควบคุมนิรภัยไม่สามารถทำงานได้ อุปกรณ์การวัดรูปแบบ 1oo1 และโปรแกรมการทำงาน แสดงได้ดังรูปที่ 2.7



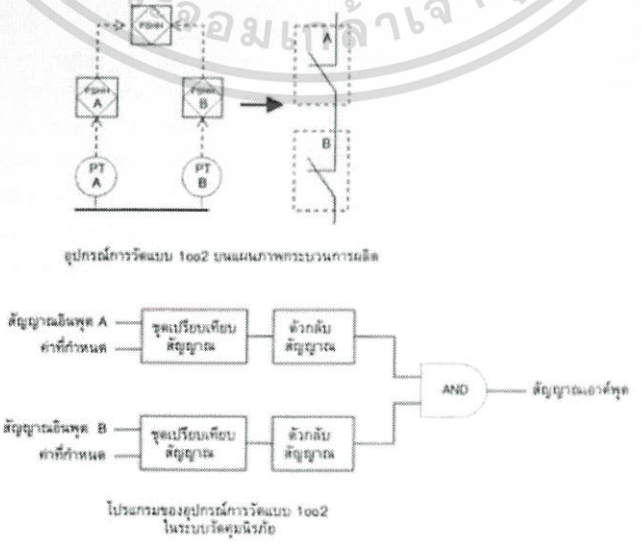
รูปที่ 2.7 อุปกรณ์การวัดแบบ 1oo1

ในการใช้งานอุปกรณ์การวัดรูปแบบ 1oo1 กับอุปกรณ์การวัดที่มีสัญญาณเอาต์พุตเป็นอนาลอก 4-20 mA ร่วมกับระบบประมวลผลที่

โปรแกรมการทำงานได้ จะต้องมีการเขียนโปรแกรมให้มีการทำงานในรูปแบบ 1oo1 ตัวโปรแกรมการทำงานหลักจะประกอบไปด้วยชุดเปรียบเทียบสัญญาณ (Comparator) กับค่าที่กำหนด และตัวกลับสัญญาณ (Inverter) ในสภาวะปกติค่าอินพุตจะมีค่าต่ำกว่าค่าที่กำหนด สัญญาณเอาต์พุตจากชุดเปรียบเทียบสัญญาณจะมีค่าเป็นศูนย์และเมื่อผ่านตัวกลับสัญญาณจะทำให้มีค่าเป็นหนึ่งหรือทำการจ่ายพลังงานไปยังอุปกรณ์สุดท้าย แต่ถ้าค่าสัญญาณอินพุตเพิ่มขึ้นอันเนื่องมาจากความผิดปกติของกระบวนการ อาทิเช่น เกิดความดันเพิ่มขึ้นหรือเกิดอุณหภูมิสูงขึ้น จนทำให้ให้สัญญาณอินพุตของชุดเปรียบเทียบสัญญาณมีค่ามากกว่าที่กำหนด จะทำให้สัญญาณเอาต์พุตของชุดเปรียบเทียบสัญญาณมีค่าเป็นหนึ่งและเมื่อผ่านตัวกลับสัญญาณจะทำให้สัญญาณเอาต์พุตมีค่าเป็นศูนย์หรือหยุดจ่ายพลังงานออกไปยังอุปกรณ์สุดท้าย ถ้าอุปกรณ์สุดท้ายเป็นวาล์วนิรภัยก็จะทำให้วาล์วปิด ซึ่งการทำงานแบบนี้จะเรียกว่า การทำงานแบบผิดพลาดนิรภัย (Fail Safe Design) คือเมื่อเกิดปัญหาการผิดพลาดใดๆกับระบบจะทำให้อุปกรณ์สุดท้ายหยุดทำงาน

- อุปกรณ์การวัดแบบ 1oo2 (One out of One voting) ในภาวะปรกติ

  รูปแบบนี้จะใช้อุปกรณ์การวัดสองตัวต่อกับระบบควบคุมนิรภัยให้มีการทำงานเป็นแบบอนุกรม ในการทำงานถ้าอุปกรณ์ตัวใดตัวหนึ่งวัดค่าความผิดปกติได้ หรือถึงจุดทำงานที่กำหนดไว้ก็จะทำให้ระบบควบคุมนิรภัยทำงานทันที ซึ่งสามารถแสดงในรูปสวิทช์ปกติเปิดสองตัวอนุกรมกัน (ในสภาวะทำงานหรือเมื่อจ่ายพลังงานให้อุปกรณ์สวิทช์จะทำงานในตำแหน่งปิด) แต่ถ้าเกิดความผิดพลาดอันตรายในตัวอุปกรณ์วัดตัวใดตัวหนึ่ง และระบบควบคุมนิรภัยไม่สามารถตรวจจับความผิดพลาดที่เกิดขึ้นนั้นได้ จะมีอุปกรณ์การวัดตัวที่สองทำงานต่อไปได้



รูปที่ 2.8 อุปกรณ์การวัดแบบ 1oo2

ในการใช้งานอุปกรณ์การวัดรูปแบบ 1oo2 กับอุปกรณ์การวัดที่มีสัญญาณเอาต์พุตเป็นอนาลอก 4-20 mA ร่วมกับระบบประมวลผลที่โปรแกรมการทำงานได้ จะต้องมีการเขียนโปรแกรมให้มีการทำงานในรูปแบบ 1oo2 ตัวโปรแกรมการทำงานหลักจะประกอบไปด้วยชุดเปรียบเทียบสัญญาณ (Comparator) กับค่าที่กำหนด และตัวกลับสัญญาณ (Inverter) สองชุดโดยสัญญาณอินพุตของชุดที่หนึ่งต่อกับอุปกรณ์การวัดตัวที่หนึ่งและสัญญาณอินพุตของชุดที่สองต่อกับอุปกรณ์การวัดตัวที่สอง จากนั้นนำสัญญาณที่ออกมาจากตัวกลับสัญญาณมาทำลอจิก AND และสัญญาณเอาต์พุตจะเป็นสัญญาณของลอจิก AND ในสภาวะปกติค่าสัญญาณอินพุตของทั้งสองค่าจะมีค่าต่ำกว่าที่กำหนด สัญญาณเอาต์พุตของชุดเปรียบเทียบสัญญาณจะมีค่าเป็นศูนย์และเมื่อผ่านตัวกลับสัญญาณจะมีค่าเป็นหนึ่งทำให้อินพุตของลอจิก AND มีค่าเป็นหนึ่งทั้งสองอินพุตทำให้สัญญาณเอาต์พุตของลอจิก AND มีค่าเป็นหนึ่งหรือทำการจ่ายพลังงานไปยังอุปกรณ์สุดท้ายสุดท้าย แต่ถ้าค่าสัญญาณอินพุตเพิ่มขึ้นอันเนื่องมาจากความผิดปกติของกระบวนการ อาทิเช่น เกิดความดันเพิ่มขึ้นหรือเกิดอุณหภูมิสูงขึ้นจนทำให้สัญญาณอินพุตของชุดเปรียบเทียบสัญญาณมีค่ามากกว่าที่กำหนด จะทำให้สัญญาณเอาต์พุตของชุดเปรียบเทียบสัญญาณมีค่าเป็นหนึ่งและเมื่อผ่านตัวกลับสัญญาณจะทำให้สัญญาณอินพุตของลอจิก AND มีค่าเป็นศูนย์ทั้งสองอินพุตเป็นผลทำให้สัญญาณเอาต์พุตมีค่าเป็นศูนย์หรือหยุดจ่ายพลังงานออกไปยังอุปกรณ์สุดท้าย ถ้าอุปกรณ์สุดท้ายเป็นวาล์วนิรภัย ก็จะทำให้วาล์วปิด แต่ถ้ามีอุปกรณ์การวัดตัวใดตัวหนึ่งเกิดความผิดพลาดอันตรายหรือไม่ตอบสนองต่อค่าการเปลี่ยนแปลงของกระบวนการผลิต ก็ยังมีอุปกรณ์วัดอีกตัวหนึ่งทำงานแทนได้ เนื่องมาจากลอจิก AND คือเมื่ออินพุตตัวใดตัวหนึ่งเป็นศูนย์ก็จะทำให้เอาต์พุตมีค่าเป็นศูนย์ด้วย

2.6.2 ตัวประมวลผล (Logic Solver)

ตัวประมวลผลเป็นส่วนประกอบหลักของระบบควบคุมนิรภัยสำหรับใช้ประมวลผลจากข้อมูลที่อ่านได้จากอุปกรณ์วัดและสั่งการไปยังอุปกรณ์สุดท้าย ดังนั้นส่วนประมวลผลจะต้องทำงานได้อย่างรวดเร็วและถูกต้อง เทคโนโลยีหลายๆแบบที่สามารถนำไปใช้ในการประมวลผลของระบบควบคุมนิรภัย การเลือกใช้ตัวแปรใดนั้นจะขึ้นอยู่กับตัวแปรต่างๆ อาทิเช่น ค่าระดับความเสี่ยงที่เกี่ยวข้องกับกระบวนการ, ขนาดของระบบ, ความสามารถในการนำไปใช้งานและความต้องการในการส่งผ่านข้อมูลต่างๆ

PLC เป็นส่วนประมวลผลที่สามารถนำไปประมวลผลที่สามารถนำไปประยุกต์ใช้งานในการควบคุมกระบวนการผลิตได้หลายประเภทและเป็นที่นิยมกันอย่างแพร่หลายในปัจจุบัน นอกจากนั้นแล้ว PLC ยังถูกนำไปใช้สำหรับการประมวลผลนิรภัยจะถูกเรียกว่า ส่วนประมวลผลสำหรับระบบนิรภัย (Safety PLC) ซึ่งเป็นส่วนประมวลผลที่ออกแบบมาพิเศษสำหรับระบบนิรภัยหรือ

ใช้ในการควบคุมแบบวิกฤต (Critical Control) ในการเลือกใช้ส่วนประมวลผลสำหรับระบบควบคุมนิรภัยแล้ว บ่อยครั้งจะพบคำถามว่า ทำไมไม่สามารถใช้ส่วนประมวลผลแบบทั่วไป (Conventional PLC) กับระบบนิรภัยได้หรืออะไรเป็นความแตกต่างของส่วนประมวลผลทั้งสอง

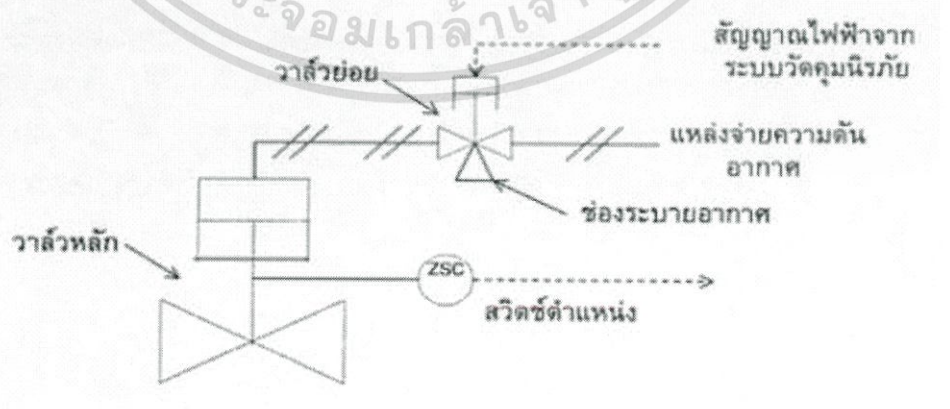
ส่วนประมวลผลสำหรับระบบนิรภัยจะถูกออกแบบเป็นอย่างพิเศษเพื่อให้บรรลุถึงจุดประสงค์ 2 ประการ คือ

1. ต้องไม่มีความผิดพลาดและถ้าหลีกเลี่ยงความผิดพลาดไม่ได้ต้องมีชุดทำงานสำรอง (Redundancy)
2. ความผิดพลาดต้องคาดคะเนได้หรือเป็นความผิดพลาดนิรภัย (Safe Failure)

ส่วนประมวลผลสำหรับระบบนิรภัยจะมีเทคนิคการออกแบบอุปกรณ์ (Hardware) และโปรแกรมการควบคุม (Software) อย่างพิเศษและมีหลายรูปแบบเพื่อให้มีความเชื่อมั่นในการทำงานได้สูง เช่น ระบบตรวจสอบความผิดพลาดภายในระบบเอง ซึ่งเป็นผลมาจากการทำงานร่วมกันระหว่างอุปกรณ์ต่างๆ กับโปรมแกรม, มีโปรแกรมการทำงานที่เชื่อถือได้, มีชุดการทำงานสำรองเมื่อชุดทำงานหลักเกิดความผิดพลาด และมีการรักษาความปลอดภัยเป็นพิเศษสำหรับการอ่านหรือเขียนข้อมูลผ่านช่องทางการสื่อสารแบบดิจิตอล (Communication port)

2.6.3 อุปกรณ์สุดท้าย (Final Element)

อุปกรณ์ด้านเอาต์พุตหรือหรืออุปกรณ์สุดท้ายของระบบควบคุมนิรภัย เป็นอุปกรณ์ที่ใช้กระทำกับกระบวนการเพื่อทำให้กระบวนการอยู่ในสภาวะที่ปลอดภัยเมื่อเกิดการผิดปกติขึ้น อุปกรณ์ที่มีการนำไปใช้งานส่วนใหญ่ คือ วาล์วนิรภัย (Shut Down Valve)วาล์วนิรภัย (Shut Down Valve) เป็นอุปกรณ์สุดท้าย (Final Element) ของระบบควบคุมนิรภัย (Safety Instrumented System: SIS) ที่มีการใช้งานในอุตสาหกรรม วาล์วนิรภัยจะถูกใช้เป็นตัวที่จะหยุดต้นเหตุของเหตุการณ์อันตรายหรือใช้เป็นตัวจำกัดขอบเขตของความเสียหาย โดยวาล์วนิรภัยจะเป็นวาล์วที่มีลักษณะการทำงานแบบวาล์วปิด - เปิดที่ถูกสั่งการมาจากระบบควบคุมนิรภัยด้วยสัญญาณไฟฟ้าไปยังวาล์วย่อย (Solenoid Valve) เพื่อใช้เปิดให้ความดันอากาศหรือน้ำมัน ไฮโดรริคไหลผ่านไปทำการปิด – เปิดวาล์วหลัก (Main Valve) ดังแสดงในรูปที่ 2.9



รูปที่ 2.9 การทำงานของวาล์วนิรภัย

2.7 การวิเคราะห์อันตรายกระบวนการผลิต (Process Hazard Analysis)

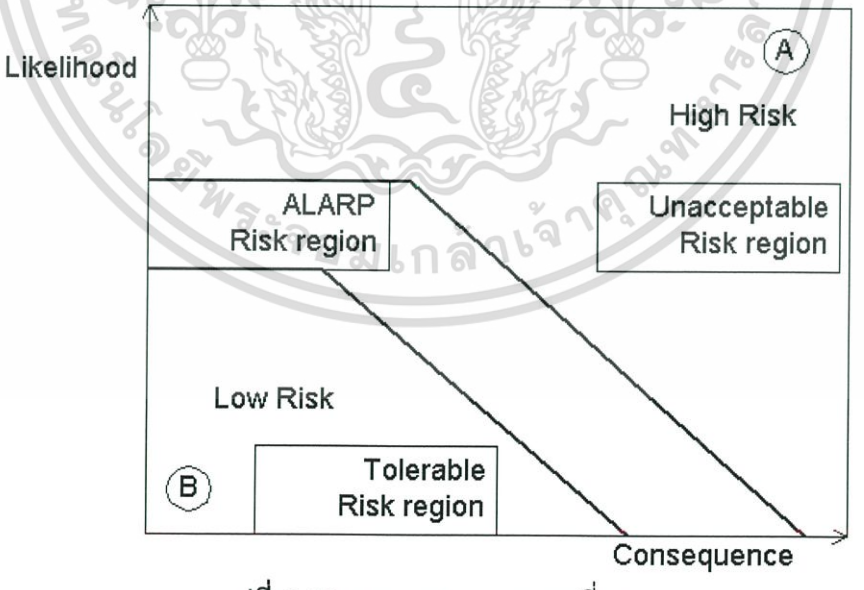
การวิเคราะห์อันตรายของกระบวนการผลิตจะเป็นขั้นตอนที่สำคัญในการกำหนดว่าจะต้องมีการจัดเตรียมฟังก์ชันนิรภัยตรงส่วนใดของกระบวนการผลิตและต้องมีจำนวนมากน้อยเพียงใดนั้น จะขึ้นอยู่กับผลลัพธ์ที่ได้จากการวิเคราะห์ความอันตรายของกระบวนการผลิต จะเป็นขั้นตอนที่ถูกกำหนดไว้ในมาตรฐาน IEC 61508 สำหรับวัตถุประสงค์ในการวิเคราะห์จะเป็นดังนี้

- ค้นหาแหล่งกำเนิดอันตรายหรือสาเหตุของอุบัติเหตุที่อาจเกิดขึ้นจากกระบวนการผลิต
- ค้นหาอันตรายที่แอบแฝงอยู่ในกระบวนการผลิต

สำหรับวิธีการที่รู้จักและใช้งานกันอย่างกว้างขวางจะเป็นวิธีการที่เรียกว่า HAZOP (Hazard and Operability) ในการทำ HAZOP จะทำการวิเคราะห์ตัวแปรกระบวนการทุกๆตัวที่สามารถเกิดขึ้นได้ในกระบวนการผลิตและจะดูผลกระทบที่ได้จากการเบี่ยงเบนไปของตัวแปรเหล่านั้น ถ้าผลกระทบจากการเบี่ยงเบน สามารถทำให้เกิดอันตรายกับสิ่งต่างๆได้ ทีมวิเคราะห์ก็จะแนะนำให้จัดเตรียมฟังก์ชันนิรภัยในการป้องกันอันตรายที่อาจจะเกิดขึ้น

2.8 ความเสี่ยง (Risk)

ความหมายของคำว่าความเสี่ยงหรือ Risk ซึ่งได้ถูกแสดงความหมายอยู่ในหัวข้อ 3.1.5 ของ IEC 61508-4 เป็นดังนี้ เป็นการรวมกันของความเป็นไปได้ของเหตุการณ์อันตรายกับความรุนแรงจากเหตุการณ์นั้น หรือกล่าวได้อย่างง่ายว่า ถ้าเหตุการณ์เกิดขึ้นได้บ่อยครั้งและมีความรุนแรงสูงก็จะมีความเสี่ยงสูง แต่ถ้าเหตุการณ์ไม่มีโอกาสเกิดขึ้นหรือเกิดขึ้นได้น้อยและไม่มีความรุนแรงก็จะมีความเสี่ยงต่ำ ค่าความเสี่ยงจึงสามารถแสดงในรูปแบบแผนภาพระหว่างความรุนแรงจากเหตุการณ์อันตรายและความเป็นได้ของเหตุการณ์อันตราย สามารถแสดงได้ดังรูปที่ 2.10



รูปที่ 2.10 แผนภาพแสดงความเสี่ยง

จากรูปที่ 2.10 จะเห็นได้ว่าที่จุด A จะมีค่าความเสี่ยงสูงเนื่องจากมีความรุนแรงจากเหตุการณ์อันตรายสูงและมีความเป็นไปได้ของการเกิดเหตุการณ์สูงเช่นเดียวกัน ซึ่งในจุดนี้จะจัดอยู่ในย่านที่เป็นความเสี่ยงที่ยอมรับไม่ได้ ส่วนที่จุด B จะมีค่าความเสี่ยงต่ำ เนื่องจากมีความรุนแรงจาก

เหตุการณ์อันตรายต่ำและมีความเป็นไปได้ของการเกิดเหตุการณ์ต่ำเช่นเดียวกัน ซึ่งในจุดนี้จัดอยู่ในย่านที่เป็นความเสี่ยงยอมรับได้และเป็นจุดที่ต้องการในการออกแบบอุตสาหกรรมกระบวนการผลิต ดังนั้นในการออกแบบกระบวนการผลิต เมื่อทำการวิเคราะห์ความอันตรายแล้วพบว่ามีค่าความเสี่ยงสูงเกินกว่าค่าที่ยอมรับได้ จะต้องหาวิธีการต่างๆ เพื่อมาทำให้ความเสี่ยงที่เกิดขึ้นลดลงมาอยู่ในระดับที่ยอมรับได้ ซึ่งวิธีการต่างๆ ได้ถูกแนะนำอยู่ในมาตรฐานนี้ จะกล่าวถึงในหัวข้อต่อไป

2.9 ค่าความเสี่ยงที่ยอมรับได้ (Tolerable Risk Guidelines)

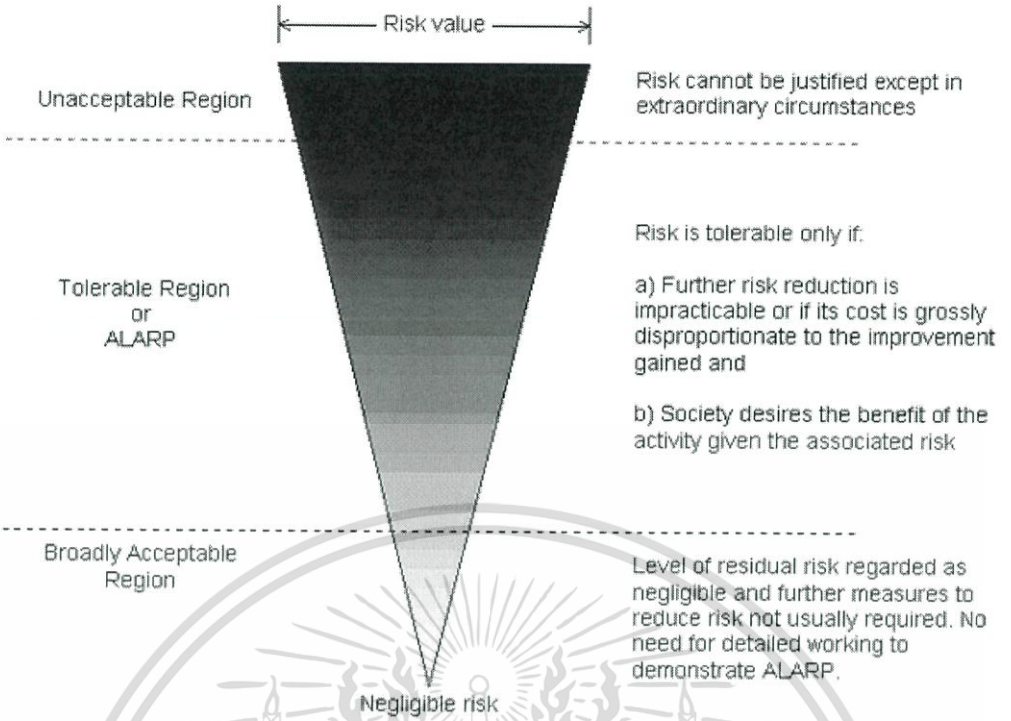
เมื่อได้ผ่านการวิเคราะห์อันตรายของกระบวนการผลิตแล้วพบว่ากระบวนการผลิตที่จะออกแบบก่อสร้างนั้นมีความเสี่ยงต่ออันตรายมากน้อยเพียงใด บริษัทหรือองค์กรต่าง ๆ มีหน้าที่ในการจำกัดความเสี่ยงในการดำเนินการ เพื่อเป็นความรับผิดชอบ, การปฏิบัติตามกฎหมายและเหตุผลทางธุรกิจ แต่การจัดทำโครงการเพื่อลดความเสี่ยงจะมีค่าใช้จ่ายที่เกิดขึ้นไม่ได้เป็นสัดส่วนกับผลประโยชน์ที่จะได้รับ จึงทำให้บริษัทหรือองค์กรต่าง ๆ ไม่อยู่ในตำแหน่งที่จะแข่งขันทางธุรกิจได้ นอกจากนั้นแล้วในบางประเทศระดับความเสี่ยงที่ยอมรับได้ถูกกำหนดโดยข้อบังคับ ดังเช่นในอเมริกา ยอมให้บริษัทหรือองค์กรต่าง ๆ กำหนดค่าระดับความเสี่ยงที่ยอมรับได้เอง การเลือกบรรทัดฐานความเสี่ยงที่ยอมรับได้ต้องถูกเลือกอย่างระมัดระวัง เพื่อให้มีความสมดุลทางด้านการแข่งขันทางธุรกิจ

จุดประสงค์ของระบบ SIS เพื่อลดความเสี่ยงของกระบวนการผลิตไปยังค่าความเสี่ยงที่ยอมรับได้ ค่า SIL จะแสดงค่าความเสี่ยงที่ลดลงทั้งหมดที่ระบบ SIS สามารถทำได้ การเลือกค่า SIL ของกระบวนการต้องการบรรทัดฐานที่ตัดสินใจว่ามีการเปลี่ยนแปลงจากความเสี่ยงที่คาดคะเนของกระบวนการผลิตไปยังค่าการลดความเสี่ยงที่ต้องการ มี 2 ขั้นตอนที่ต้องการในการจัดทำบรรทัดฐานความเสี่ยงที่ยอมรับได้ว่ามีความเหมาะสมเพียงใด ภาระหน้าที่การลดความเสี่ยงของอุปกรณ์เป็นดังนี้

ขั้นแรก ศึกษาความเสี่ยงของบุคคลที่ยอมรับได้

ขั้นที่สอง เปลี่ยนจำนวนและความรู้สึกเกี่ยวกับความเสี่ยงที่ยอมรับได้ไปเป็นแนวทางที่เป็นรูปธรรม

UK's HSE (Health and Safety Executive) ดำเนินการตามขั้นตอนที่เรียกว่า ALARP (As Low As Reasonably Practicable) วิธีนี้ได้แสดงว่ามีระดับความเสี่ยงที่ยอมรับไม่ได้ (Intolerable) ค่าความเสี่ยงที่ต่ำกว่าย่านที่ยอมรับไม่ได้จะเป็นย่าน ALARP ค่าความเสี่ยงที่อยู่ในย่าน ALARP เป็นค่าความเสี่ยงที่ยอมรับได้ ซึ่งเป็นค่าความเสี่ยงที่การลดความเสี่ยงทำไม่ได้ในทางปฏิบัติหรือมีค่าใช้จ่ายเป็นสัดส่วนที่ไม่เหมาะสมกับผลประโยชน์ที่ได้รับ ค่าความเสี่ยงที่ต่ำกว่าย่าน ALARP จะเป็นย่าน Broadly Acceptable ในย่านนี้เป็นค่าความเสี่ยงที่ต่ำที่สุดที่ไม่ต้องมีการพิจารณา สามารถแสดงไดอะแกรม ALARP ได้ดังรูปที่ 2.11

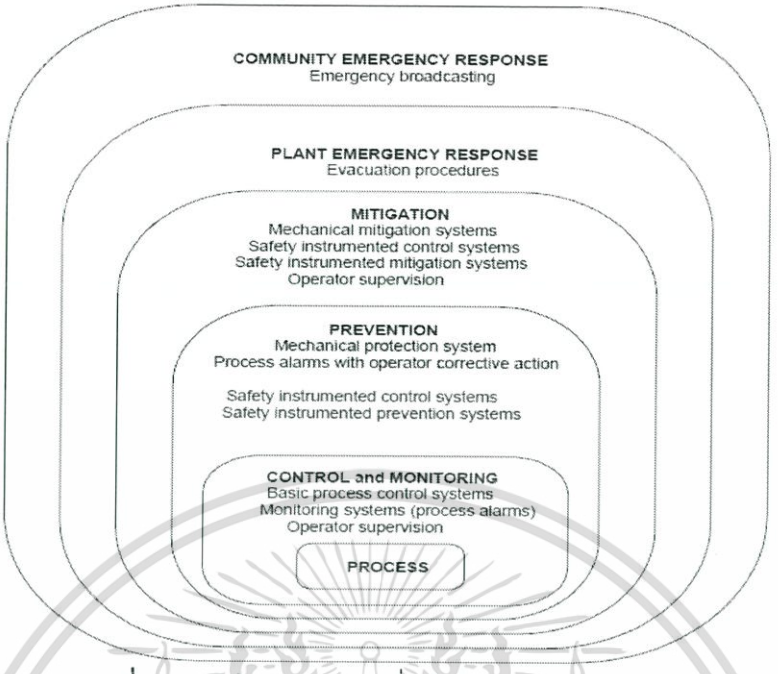


รูปที่ 2.11 ALARP

ค่าความเสี่ยงต่อการเสียชีวิตของตัวบุคคลสูงสุด เป็นค่าจำกัดสูงสุดของโอกาสในแต่ละปีที่กำหนดไว้สำหรับบุคคลมีโอกาสเสียชีวิต ถ้าค่าความเสี่ยงต่อการเสียชีวิตของตัวบุคคลสูงสุดมีค่าเท่ากับ 10E-3 ต่อปี หมายความว่ามีโอกาส 1 ใน 1000 ที่อาจจะเสียชีวิตในระยะเวลา 1 ปี ซึ่งค่านี้จะเป็นค่าสูงสุดที่สามารถยอมรับให้เกิดขึ้นในโรงงานอุตสาหกรรม บริษัทหรือองค์กรต่างๆใช้บรรทัดฐานค่าความเสี่ยงที่ยอมรับได้เป็นจำนวนที่ถูกแสดงค่าสูงสุดของการเสียชีวิตอยู่ในค่าระหว่าง 10E-3 ถึง 10E-6 ต่อปี

2.10 การลดค่าความเสี่ยง (Risk Reduction)

จากขั้นตอนการออกแบบระบบ SIS ในรูปที่ 2.3 และรูปที่ 2.4 มาตรฐานได้กำหนดให้มีการดำเนินการวิเคราะห์หาค่าความเสี่ยงที่จะเกิดเหตุการณ์อันตรายในกระบวนการผลิตที่ทำการออกแบบและต้องมีการประเมินผลกระทบที่จะเกิดขึ้นจากเหตุการณ์อันตราย ถ้าผลกระทบที่เกิดขึ้นส่งผลต่อบุคคล (Persons), สิ่งแวดล้อม และทรัพย์สินมีค่าต่างๆ (Equipment) หรือผลิตภัณฑ์ที่ได้ (Product) ต้องมีการทำการลดค่าความเสี่ยงต่อเหตุการณ์อันตรายเหล่านั้นให้อยู่ในค่าที่ยอมรับได้ (Accepted Level) ซึ่งค่าที่ยอมรับได้นั้นจะขึ้นอยู่กับข้อกำหนดของผู้ใช้งานหรือเจ้าของโรงงาน (Client) ว่าจะยอมรับค่าความเสี่ยงเหล่านี้ได้มากน้อยค่าไหน หรือข้อกำหนดทางกฎหมายของบริเวณก่อสร้างโครงการ ตัวอย่างข้อกำหนด เช่น ต้องมีความปลอดภัยต่อผู้ปฏิบัติการในโรงงาน, ต้องไม่มีของเสียรั่วไหลออกไปยังสิ่งแวดล้อมภายนอก หรือ กระบวนการผลิตต้องไม่หยุดการทำงานนานเกินไป เป็นต้น เมื่อได้ข้อกำหนดของค่าที่ยอมรับได้แล้ว ในช่วงการวิเคราะห์เหตุการณ์อันตรายและผลกระทบที่ตามมา ถ้ามีส่วนใดส่วนหนึ่งของกระบวนการผลิตที่อาจเกิดเหตุการณ์อันตราย และส่งผลต่อข้อกำหนดดังกล่าวข้างต้น ต้องทำการลดความเสี่ยงที่เกิดขึ้น วิธีการลดความเสี่ยงสามารถพบได้ในโรงงานอุตสาหกรรมแสดงได้ดังรูปที่ 2.12



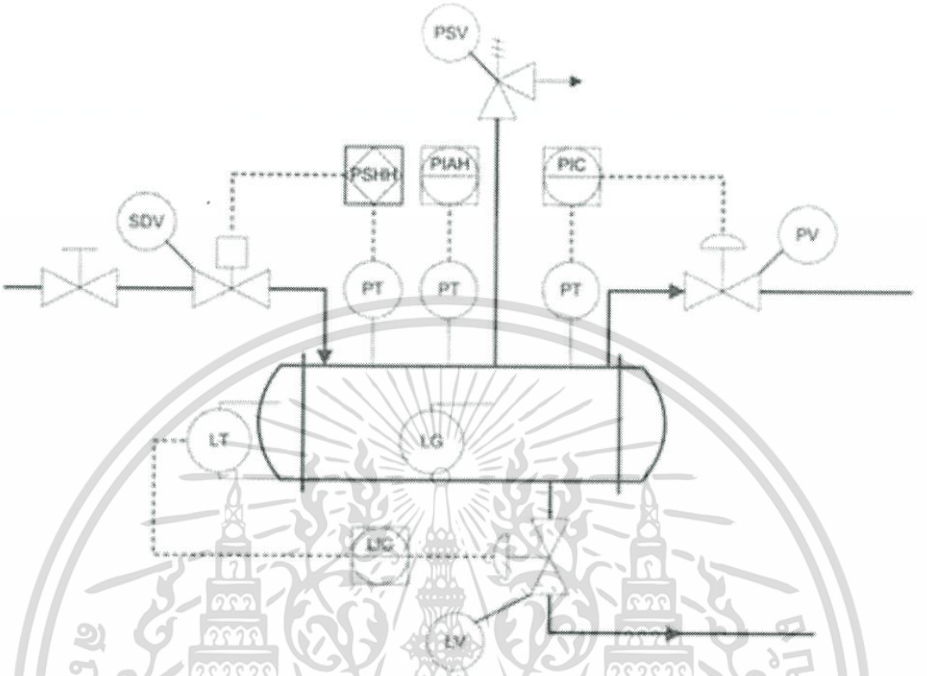
รูปที่ 2.12 วิธีการลดความเสี่ยงในโรงงานอุตสาหกรรม

จากแผนภาพในรูปที่ 2.12 จะเห็นได้ว่าวิธีการลดความเสี่ยงในโรงงานอุตสาหกรรมที่พบเห็นได้ทั่วไป จะเริ่มจากการออกแบบกระบวนการผลิตให้มีความปลอดภัยในการทำงาน และกระบวนการผลิตจะถูกควบคุมการทำงานด้วยระบบควบคุมกระบวนการผลิตพื้นฐาน (Basic Process Control System: BPCS) หรือระบบ DCS ซึ่งจะมีการจัดเตรียมสัญญาณเตือน (Alarm) เมื่อเกิดความผิดปกติขึ้นในกระบวนการผลิต จากนั้นผู้ปฏิบัติการที่ควบคุมกระบวนการผลิตจะทำการตอบสนอง (Response) ต่อสัญญาณเตือนเพื่อแก้ไขหรือยับยั้งความผิดปกติให้กลับสู่สภาวะปกติ

แต่ถ้าเกิดความผิดปกติในหลายส่วนหรือผู้ปฏิบัติการตอบสนองต่อความผิดปกติใช้เวลาเกินกว่าเวลาปลอดภัยของกระบวนการ (Process Safety Time) ก็จะเป็นหน้าที่ของระบบวัดคุมนิรภัย (Safety Instrumented System: SIS) ทำหน้าที่ป้องกันอันตรายไม่ให้เกิดขึ้นตามฟังก์ชันนิรภัยที่ได้ออกแบบไว้ ระบบ SIS อาจจะสั่งให้เครื่องจักรหยุดทำงาน, สั่งปิดหรือเปิดวาล์วนิรภัยตามจุดต่าง ๆ ในกระบวนการผลิต หรือถ้ามีการติดตั้งระบบนิรภัยทางกล เช่น วาล์วนิรภัยทางกล (Safety Relief Valve) เป็นต้น อุปกรณ์เหล่านี้ก็จะทำงานเมื่อถึงจุดที่กำหนดไว้ ถ้าเกิดมีเหตุการณ์อันตรายเกิดขึ้น อาทิเช่น เพลิงไหม้หรือสารเคมีรั่วไหล ระบบนิรภัยในส่วนยับยั้ง (Mitigation System) จะทำงานโดยการส่งสัญญาณเตือนความเป็นอันตรายของบริเวณที่สารเคมีรั่วไหล หรือสั่งเปิดระบบฉีดน้ำดับเพลิงในจุดที่เกิดไฟไหม้ แต่ถ้าเหตุการณ์อันตรายยังไม่สามารถควบคุมในอยู่ในขอบเขตที่กำหนดก็ต้องมีแผนการอพยพออกจากบริเวณมี่เกิดเหตุภายในโรงงาน หรือ ถ้าเหตุการณ์ลุกลาม อาจจะต้องแจ้งให้ชุมชนรอบๆ มีการอพยพให้ออกจากบริเวณ จะเห็นได้ว่าในการออกแบบโรงงานอุตสาหกรรมกระบวนการผลิตตามมาตรฐานสากลนี้จะต้องทำการพิจารณาการป้องกันหรือการลดความเสี่ยงต่อเหตุการณ์อันตรายที่อาจจะเกิดขึ้น ซึ่งระบบการป้องกันเหล่านี้จะเป็นทางเลือกให้ผู้ใช้งานสำหรับใช้ในการลดค่าความเสี่ยงลง

2.11 ชั้นการป้องกันในกระบวนการผลิต (Layer of protection in process)

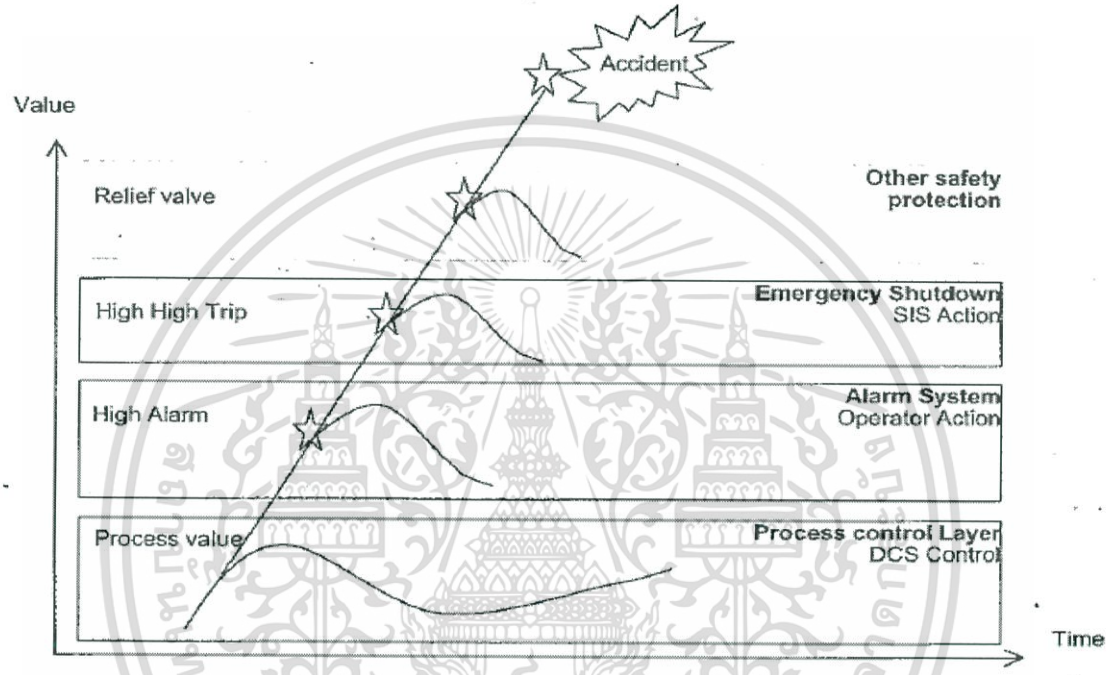
ตัวอย่างแสดงรายละเอียดชั้นการป้องกันความดันที่อาจจะเกิดขึ้นในกระบวนการผลิต ดังรูปที่ 2.13



รูปที่ 2.13 ฟังก์ชันการป้องกันความดันเกินบนแผนภาพกระบวนการผลิต

- การป้องกันชั้นที่ 1 เป็นระบบควบคุมพื้นฐาน ซึ่งจะทำการควบคุมความดันของกระบวนการผลิตให้อยู่ในค่าที่กำหนด แต่ถ้าเกิดความผิดพลาดบนส่วนใดส่วนหนึ่งของระบบควบคุมพื้นฐานจนทำให้ระบบไม่สามารถควบคุมค่าความดันให้อยู่ในค่าที่ต้องการได้ ก็จะทำให้ความดันในกระบวนการผลิตมีค่าสูงขึ้น จนไปถึงค่าความดันที่ตั้งไว้ในระบบสัญญาณเตือนซึ่งเป็นชั้นการป้องกันที่ 2 ก็จะเริ่มทำงาน
- การป้องกันชั้นที่ 2 ระบบจะส่งสัญญาณเตือนไปยังผู้ปฏิบัติงานที่ควบคุมการทำงานของกระบวนการผลิต ผู้ปฏิบัติงานก็จะทำการตอบสนองต่อสัญญาณเตือนโดยการสั่งการปิดหรือเปิดวาล์วในส่วนที่เกี่ยวข้อง ถ้าการตอบสนองนั้นถูกต้องและทันเวลาก็จะทำให้ความดันในกระบวนการผลิตลดลงมาอยู่ในค่าที่กำหนดหรือค่าที่ปลอดภัยได้ แต่ถ้าเกิดความผิดพลาดในการตอบสนองต่อสัญญาณเตือนหรือไม่สามารถตอบสนองได้ในเวลาที่กำหนดก็จะส่งผลทำให้ความดันในกระบวนการผลิตมีค่าสูงขึ้นไปอีก จนไปถึงค่าความดันที่ตั้งไว้ในระบบนิรภัยซึ่งเป็นชั้นการป้องกันที่ 3 ก็จะทำงาน
- การป้องกันชั้นที่ 3 ระบบนิรภัยก็จะสั่งปิดหรือเปิดวาล์วในส่วนที่เกี่ยวข้องเพื่อให้ความดันลดลงมาอยู่ในค่าที่ต่ำกว่าจุดที่ตั้งไว้ แต่ถ้าเกิดความผิดพลาดใดๆขึ้นในระบบนิรภัยแล้วทำให้ระบบนิรภัยไม่สามรถทำงานได้ทันเวลา ก็จะส่งผลทำให้ความดันในกระบวนการผลิตมีค่าสูงเพิ่มขึ้นมากไปอีก จนถึงจุดทำงานของวาล์วนิรภัยทางกล ซึ่งเป็นการป้องกันชั้นที่ 4

- การป้องกันชั้นที่ 4 วาล์วนิรภัยทางกลก็จะทำงานโดยการเปิดเพื่อระบายความดันออกไป ทำให้ความดันในระบบลดลงอยู่ในค่าที่ปลอดภัย แต่ถ้าเกิดความผิดพลาดที่ตัววาล์วนิรภัยจนทำให้ไม่สามารถทำงานได้ ความดันก็จะเพิ่มสูงขึ้นจนอุปกรณ์ในกระบวนการผลิตไม่สามารถจะทนความดันที่สูงมากค่านี้ได้หรือเกินกว่าค่าความดันที่ออกแบบของอุปกรณ์ จะทำให้เกิดการแตกร้าวของอุปกรณ์และเกิดการรั่วไหลออกไปยังภายนอก ซึ่งจะเป็นสาเหตุที่จะนำไปสู่เหตุการณ์อันตรายร้ายแรงได้ถ้าเป็นสารไวไฟหรือมีความดันสูงมากๆ การทำงานของชั้นการป้องกัน ได้ถูกแสดงได้ดังรูปที่ 2.14



รูปที่ 2.14 การทำงานของชั้นการป้องกันความดันเกิน

2.12 วิธีการหาค่า SIL ที่ต้องการ

มาตรฐาน IEC 61508 ได้แสดงวิธีการกำหนดค่า SIL ที่ต้องการเป็นดังนี้

- วิธีเชิงจำนวน (Quantitative Method)
- กราฟความเสี่ยง (Risk Graph) ซึ่งถูกแสดงในมาตรฐานนี้เป็นวิธีเชิงคุณภาพ (Qualitative Method)
- ตารางเหตุการณ์อันตราย (Hazard Event Severity Matrix) ซึ่งเป็นวิธีเชิงคุณภาพอีกวิธีหนึ่ง

มาตรฐาน IEC 61511 ได้แสดงวิธีการกำหนดค่า SIL ที่ต้องการเป็นดังนี้

- วิธี Semi-Quantitative (Semi-Quantitative method)
- วิธี Safety layer matrix ซึ่งถูกแสดงเหมือนวิธี Semi-Qualitative
- กราฟความเสี่ยงที่ถูกปรับเทียบแล้ว (Calibrated Risk Graph) ซึ่งถูกแสดงในมาตรฐานเป็นแบบวิธี Semi-Qualitative แต่ในบางผู้ใช้งานจะเป็นแบบวิธี Semi-Quantitative

- วิธีกราฟความเสี่ยง (Risk Graph) ถูกแสดงในรูปแบบวิธีเชิงคุณภาพ
- LOPA (Layer Of Protection Analysis)

สำหรับวิธีการที่มีความนิยมใช้ในการกำหนดค่า SIL มากที่สุดจะเป็นวิธี กราฟความเสี่ยงและ LOPA โดยเฉพาะอย่างยิ่งในส่วนของอุตสาหกรรมกระบวนการผลิต

การดำเนินการกำหนดค่าระดับความปลอดภัยหรืออาจเรียกว่าการประเมินความเสี่ยงจะดำเนินการประเมินผลกระทบต่อผู้ปฏิบัติงาน (Personal), ทรัพย์สิน (Asset), และสิ่งแวดล้อม (Environment) ว่ามีโอกาสเกิดเหตุการณ์อันตรายมากน้อยเพียงใดและผลกระทบมีความรุนแรงมากน้อยเพียงใด ถ้ามีโอกาสเกิดขึ้นสูงและมีความรุนแรงมาก ค่าระดับความปลอดภัยก็สูงตามไปด้วย หรือถ้ามีโอกาสเกิดขึ้นต่ำและมีความรุนแรงน้อย ค่าระดับความปลอดภัยก็จะต่ำ

สำหรับโครงการก่อสร้างใหม่ๆ คงไม่ใช่เรื่องยากที่จะดำเนินการตามขั้นตอนที่แสดงอยู่ในรูปที่ 2.3 และรูปที่ 2.4 ซึ่งจะเป็นลำดับขั้นตอนการทำงานที่ต้องดำเนินการอยู่แล้วในการออกแบบอุตสาหกรรมกระบวนการผลิต เพียงแต่เพิ่มลำดับขั้นตอนการประเมินความเสี่ยง เพื่อกำหนดค่าระดับความปลอดภัยให้กับฟังก์ชันนิรภัยที่ได้ถูกกำหนด หลังจากการขั้นตอนการทำ HAZOP สำหรับโครงการเก่าๆ หรือโรงงานอุตสาหกรรมกระบวนการผลิตที่ต้องการปรับปรุงระบบวัดคุมนิรภัยเก่า ให้เป็นไปตามข้อกำหนดตามมาตรฐานนี้ ก็ควรจะมีการประเมินความเสี่ยงของฟังก์ชันนิรภัยที่มีอยู่แล้วเพื่อกำหนดค่าระดับความปลอดภัยให้กับฟังก์ชันนิรภัยเหล่านั้น ก่อนที่จะดำเนินการออกแบบเพื่อปรับปรุงระบบ ซึ่งอาจมีความเป็นไปได้ที่ฟังก์ชันนิรภัยที่มีอยู่แล้วได้ถูกออกแบบไว้เกินกว่าหรือต่ำกว่าความต้องการ

2.13 Layer Of Protection Analysis (LOPA)

วิธี LOPA ถูกพัฒนาขึ้นโดย American Institute of Chemical Engineers สำหรับใช้เป็นวิธีการประเมินค่า SIL ที่ต้องการของฟังก์ชันนิรภัย

วิธี LOPA เป็นวิธีที่เริ่มจากจัดทำรายการของความอันตรายจากกระบวนการผลิตทั้งหมดตามการกำหนดโดย HAZOP หรือเทคนิคการกำหนดอันตรายอื่นๆโดยแสดงสาเหตุเริ่มต้น (Cause initiating) และชั้นการป้องกันหรือยับยั้งความอันตราย ซึ่งจะถูกวิเคราะห์ในรูปของ

- ผลกระทบ (Impact Event Description)
- ประมาณความรุนแรงของผลกระทบ (Severity Level)
- รายละเอียดของสาเหตุทั้งหมดทำให้เกิดผลกระทบ (Initiating Causes)
- ประมาณความถี่ของสาเหตุ (Initiation Likelihood)

จุดแข็งของวิธีการ LOPA นี้จะเป็นการจำแนกชั้นการป้องกันในภาคอุตสาหกรรมกระบวนการผลิต โดยปกติในการออกแบบจะจัดเตรียมการป้องกันเหตุการณ์อันตรายอยู่หลายๆชั้น ชั้นการป้องกันนี้จะจัดเตรียมโดยเทียบกับสาเหตุของการนำไปสู่เหตุการณ์อันตราย ชั้นการป้องกันที่มีอยู่ทั่วไปในอุตสาหกรรมการผลิตสามารถแสดงให้เห็นได้ดังตารางที่ 2.4

ตารางที่ 2.4 Layer Of Protection Analysis (LOPA)

#	1	2	3	4		5		6	7	8	9	10	11
					PROTECTION LAYERS								
	Impact event description F.3 F.14.1	Severity level F.4 F.14.1	Initiating cause F.5 F.14.2	Initiation likelihood F.6 F.14.3	General process design F.14.4	BPCS F.14.5	Alarms, etc. F.14.6	Additional mitigation, restricted access,F.8 F.14.7	IPL additional mitigation dikes, pressure relief F.9 F.14.8	Inter-mediate event likelihood F.10 F.14.9	SIF integrity level F.11 F.14.10	Mitigated event likelihood F.12 F.14.10	Notes
1	Fire from distillation column rupture	S	Loss of cooling water	0.1	0.1	0.1	0.1	0.1	PRV 01	10^{-1}	10^{-2}	10^{-3}	High pressure causes column rupture
2	Fire from distillation column rupture	S	Steam control loop failure	0.1	0.1		0.1	01	PRV 01	10^{-2}	10^{-2}	10^{-4}	Same as above
N													

IEC 3025/02

NOTE Severity Level E = Extensive; S = Serious; M = Minor.
Likelihood values are events per year, other numerical values are probabilities of failure on demand average.

- การออกแบบกระบวนการ (General Process Design) ดังตัวอย่างเช่น มีการออกแบบที่ลดโอกาสของการสูญเสียการเก็บกักไว้หรือการจุดระเบิด ถ้ามีการรั่วไหลสารไวไฟออกมา ซึ่งเป็นการลดโอกาสของการเกิดไฟไหม้หรือการระเบิด การออกแบบหรือเลือกใช้อุปกรณ์ไฟฟ้าที่ไม่เป็นตัวจุดประกายไฟ การกำหนดขั้นตอนในการถอดเปลี่ยนหรือซ่อมบำรุงอุปกรณ์ไฟฟ้าเหล่านี้
- ระบบควบคุมพื้นฐานหรือ BPCS (Basic Process Control System) ความผิดพลาดของฟังก์ชันควบคุมจะเป็นสาเหตุหลักๆของการเกิดอันตราย อย่างไรก็ตามอาจมีการออกแบบฟังก์ชันควบคุมอิสระซึ่งสามารถป้องกันผลกระทบได้และช่วยลดความถี่ของเหตุการณ์
- สัญญาณเตือน (Alarms) การจัดเตรียมสัญญาณซึ่งเป็นอิสระจากระบบควบคุมพื้นฐานและมีเวลาเพียงพอให้ผู้ปฏิบัติการตอบสนองต่อสัญญาณเตือนนั้น สามารถให้การไว้วางใจในสัญญาณเตือนสำหรับลดโอกาสการเกิดเหตุการณ์อันตราย
- การยับยั้ง, การจำกัดพื้นที่ (Mitigation, Restricted access) ถ้ามีเหตุการณ์เกิดขึ้นอาจมีการจำกัดการเข้าไปในพื้นที่อันตราย หรือการหลบหลีกออกจากพื้นที่อันตราย ซึ่งช่วยลดระดับความรุนแรงจากเหตุการณ์ได้

- ชั้นการป้องกันอิสระ (Independent Protection Layers) จำนวนบรรทัดฐานในการออกแบบต้องมีความเหมาะสม โดยเป็นชั้นการป้องกันที่มีตัวแปรลดความเสี่ยง ≥ 100 วาล์วนิรภัยทางกลและ Bursting Disk เป็นอุปกรณ์ที่มีคุณสมบัติเหมาะสม ซึ่งอุปกรณ์เหล่านี้จะต้องสามารถลดความเสี่ยงต่ออันตรายได้อย่างเหมาะสม เช่น อัตราการไหล
- ของวาล์วนิรภัยทางกลต้องลดความดันได้ทันเวลา หรือถ้าปล่อยระบบเผาทิ้ง (Flare System) ระบบต้องสามารถรองรับปริมาณการไหลได้ เป็นต้น

2.14 ผลประโยชน์ที่ได้จากระบบนิรภัย

จุดประสงค์ของระบบนิรภัยถูกออกแบบมาเพื่อใช้ในการแสดงสภาวะเหตุการณ์อันตรายและดำเนินการไปตามโปรแกรมที่ได้ถูกจัดเตรียมไว้ ทั้งในการป้องกันความเป็นอันตรายจากเหตุการณ์ที่เกิดขึ้น หรือยับยั้งผลกระทบที่จะเกิดขึ้นตามมา นอกเหนือจากนี้แล้วระบบนิรภัยยังมีส่วนที่เกี่ยวข้องกับการควบคุมกระบวนการผลิต หลังจากที่ได้ติดตั้งเข้าไปในระบบการควบคุมแล้วผลลัพธ์ที่ได้จากระบบนิรภัยจะเป็นดังนี้

- ระบบนิรภัยไม่ได้มีผลทำให้ผลิตภัณฑ์ที่ได้จากกระบวนการเพิ่มขึ้น
- ระบบนิรภัยไม่ได้ทำให้ประสิทธิภาพการทำงานของกระบวนการเพิ่มขึ้น
- ระบบนิรภัยสามารถประหยัดรายได้จากการสูญเสียผลิตภัณฑ์ได้
- ระบบนิรภัยสามารถลดค่าใช้จ่ายความเสี่ยง (Risk Cost) ได้

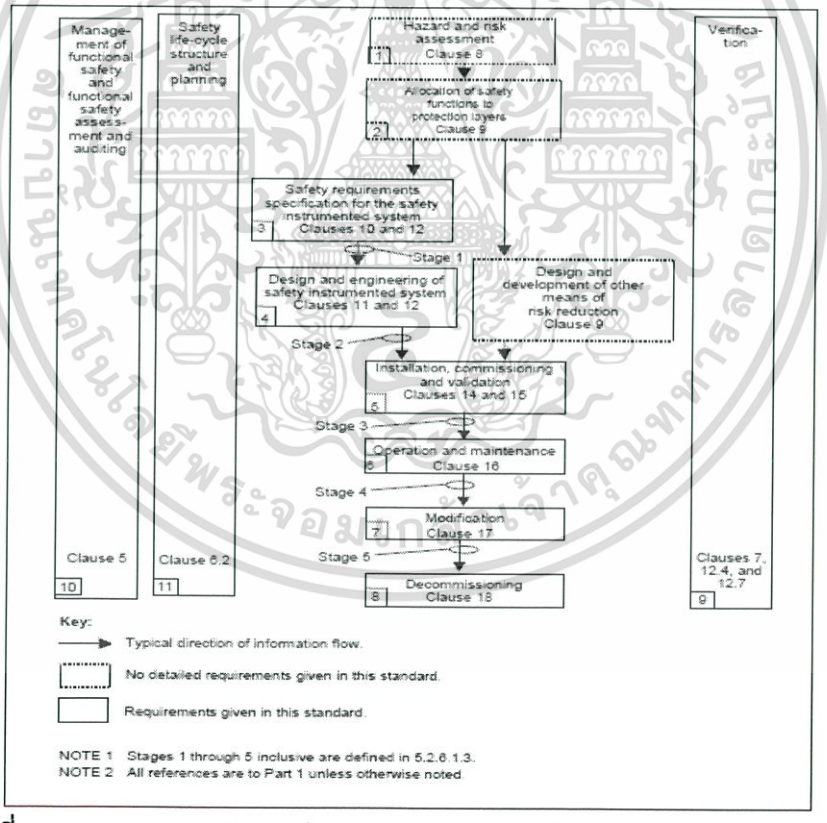
บทที่ 3
วิธีการดำเนินงาน

3.1 คำนำ

วิธีการดำเนินงานของโครงงานนี้เป็นกรณีสมมติการศึกษาวิธีการออกแบบระบบวัดคุมนิรภัย หรือ Safety Instrumented System: SIS โดยอ้างอิงตามมาตรฐาน IEC-61508 และมาตรฐาน IEC-61511 ซึ่งประกอบด้วย การวิเคราะห์หาสาเหตุความเป็นอันตรายของกระบวนการผลิต การประเมินหาค่าความปลอดภัยหรือ Safety Integrity Level: SILที่เหมาะสมกับกระบวนการการผลิตนั้น พร้อมทั้งออกแบบฟังก์ชันนิรภัยสำหรับช่วยลดความเป็นอันตรายของกระบวนการการผลิตให้อยู่ในค่าความปลอดภัยที่กำหนด

3.2 การออกแบบระบบวัดคุมนิรภัย

ในโครงงานนี้จัดทำการออกแบบระบบวัดคุมนิรภัยตามวงรอบความปลอดภัย (Safety Life Cycle) ของมาตรฐาน IEC-61511 ซึ่งจะมีขั้นตอนในการดำเนินงานเป็นไปดังรูปที่ 3.1

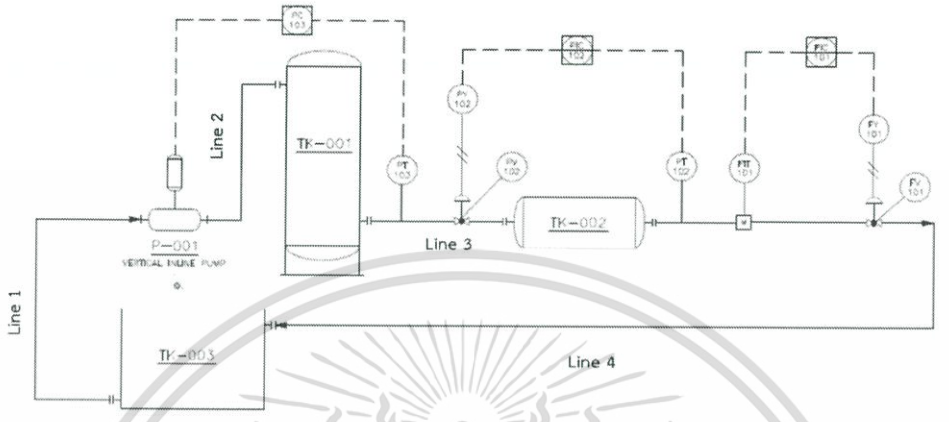


รูปที่ 3.1 วงรอบความปลอดภัย (Safety Life Cycle)ของมาตรฐาน IEC-61511

โดยในโครงงานจะดำเนินการตั้งแต่ขั้นตอนที่ 1 (Hazard and risk assessment) ถึงขั้นตอนที่ 4 (Design and Engineering of Safety Instrumented System) เท่านั้น เนื่องจากในการดำเนินงานจัดทำโครงงานนี้ไม่ได้มีการติดตั้งฟังก์ชันนิรภัยจริงเข้าไปในกระบวนการผลิต

3.2.1 ขั้นตอนการวิเคราะห์ความเป็นอันตรายในกระบวนการผลิต (Hazard and risk assessment)

ในขั้นตอนนี้เป็นการวิเคราะห์หาความเป็นอันตรายที่อาจจะเกิดขึ้นในกระบวนการผลิต รวมไปถึงการประเมินผลกระทบต่อส่วนต่างๆ เมื่อมีเหตุการณ์อันตรายเกิดขึ้น



รูปที่ 3.2 P&ID ของกระบวนการผลิต

จากแผนผังแสดงรายละเอียดเกี่ยวกับกระบวนการผลิตและอุปกรณ์ควบคุมต่างๆ (P&ID) จะเป็นกระบวนการของการวัดและควบคุมอัตราการไหลของน้ำและความดัน โดยใช้วิธีการควบคุมแบบคาสเคด ซึ่งกระบวนการเป็นการควบคุมอัตราการไหลหรือความดัน โดยใช้ความสัมพันธ์ระหว่างอัตราการไหลและความดันในการสั่งเปิดหรือปิดวาล์วควบคุม โดยกระบวนการจะเริ่มต้นจากปั๊มน้ำสูบออกจากถังเก็บน้ำ (Storage Tank: TK-003) ไปพักเก็บไว้ที่ถังพักน้ำ (Buffer Tank: TK-001) ที่จ่ายให้กับกระบวนการ แล้วจึงส่งน้ำให้ไหลเวียนภายในกระบวนการ และไหลกลับคืนไปยังถังเก็บน้ำใหม่อีกครั้ง โดยกระบวนการนั้นจะดำเนินการเช่นนี้ไปเรื่อยๆ จากนั้นทำการวิเคราะห์หาความเป็นอันตรายของกระบวนการผลิต (P&ID) ว่าต้องมีการจัดเตรียมฟังก์ชันนิรภัยตรงส่วนใดบ้างของกระบวนการผลิตนั้น และจะต้องมีชั้นการป้องกันจำนวนมากน้อยเพียงใดเพื่อที่ทำให้กระบวนการผลิตยังคงอยู่ได้อย่างปลอดภัย เมื่อมีความผิดพลาดเกิดขึ้นโดยขึ้นอยู่กับผลลัพธ์ที่ได้จากการทำการวิเคราะห์หาความเป็นอันตรายของกระบวนการผลิต ซึ่งการวิเคราะห์ความเป็นอันตรายนั้นมีหลากหลายวิธีในมาตรฐาน IEC-61508 และ IEC-61511 โดยในโครงงานนี้จะนำเสนอโดยใช้วิธี Hazard and Operability Studied (HAZOP) เป็นวิธีในการวิเคราะห์หาวามเป็นอันตรายของกระบวนการผลิตซึ่งผลจากการดำเนินงานนั้น สามารถสรุปการวิเคราะห์หาความเป็นอันตรายของกระบวนการโดยใช้วิธี Hazard and Operability Studied (HAZOP) ได้ดังตารางต่อไปนี้

ตารางที่ 3.1 รายงานผลลัพธ์ของการวิเคราะห์ความเป็นอันตรายที่ท่อส่งทางน้ำขาเข้าบัฟเฟอร์แท็งก์ ผลของการวิเคราะห์หาความเป็นอันตรายที่จะเกิดขึ้นในกระบวนการผลิต

Project: การควบคุมความดันภายในถังความดันใช้งาน			Node: Line 2	หน้า: 1
Node Description: ท่อส่งทางน้ำเข้าบัฟเฟอร์แท็งก์				
GUIDEWORD	สาเหตุ	ผลกระทบ	การป้องกัน	ข้อเสนอแนะ
1. การไหลมากไป	การทำงานของ Inverter ควบคุม Pump (P-001) ทำงานผิดพลาด	ทำให้ระดับน้ำภายในบัฟเฟอร์แท็งก์ (TK-001) มีระดับสูงขึ้น จนเป็นสาเหตุให้บัฟเฟอร์แท็งก์นั้นเกิดการระเบิดได้		1. ควรมีการติดตั้งระบบสัญญาณเตือนเมื่อมีอัตราการไหลภายในท่อ Line 2 มากเกินไป (Flow Alarm High: FAH)
2. การไหลน้อยไป	1. การทำงานของ Inverter ควบคุม Pump (P-001) ทำงานผิดพลาด 2. มีสิ่งแปลกปลอมเข้าไปอุดตันภายในท่อ Line2	ไม่มีผลกระทบ		

ตารางที่ 3.2 รายงานผลลัพธ์ของการวิเคราะห์ความเป็นอันตรายที่ถังพักน้ำก่อนเข้าสู่กระบวนการ ผลของการวิเคราะห์หาความเป็นอันตรายที่จะเกิดขึ้นในกระบวนการผลิต(ต่อ)

Project: การควบคุมความดันภายในถังความดันใช้งาน			Node: TK-001	หน้า: 2
Node Description: ถังพักน้ำก่อนเข้าสู่กระบวนการ (Buffer Tank)				
GUIDEWORD	สาเหตุ	ผลกระทบ	การป้องกัน	ข้อเสนอแนะ
3. ความดันสูงไป	1. ฟังก์ชันควบคุมความดันทำงานผิดพลาด 2. มีสิ่งแปลกปลอมเข้าไปอุดตันภายในท่อ Line 3 3. การทำงานของ Inverter ควบคุม Pump (P-001) ทำงานผิดพลาด 4. วาล์ว PV-102 เกิดการทำงานผิดพลาด	ทำให้ความดันภายในบัฟเฟอร์แท็งก์ (TK-001) มีความดันสูงขึ้น จนเป็นสาเหตุให้บัฟเฟอร์แท็งก์นั้นเกิดการระเบิดได้		2. ควรมีการติดตั้งระบบสัญญาณเตือนเมื่อมีความดันภายใน บัฟเฟอร์แท็งก์สูงมากเกินไป (Pressure Alarm High: PAH) 3. ควรมีการติดตั้งระบบสัญญาณเตือนเมื่อมีระดับน้ำภายในบัฟเฟอร์แท็งก์สูงมากเกินไป (Level Alarm High: LAH) 4. ควรมีการติดตั้ง Pressure relief Valve ภายในบัฟเฟอร์แท็งก์ (TK-001)
4. ความดันต่ำไป	1. ฟังก์ชันควบคุมความดันทำงานผิดพลาด 2. มีสิ่งแปลกปลอมเข้าไปอุดตันภายในท่อ Line 3 3. การทำงานของ Inverter ควบคุม Pump (P-001)ทำงานผิดพลาด	ไม่มีผลกระทบ		
5. ระดับน้ำสูงไป	2. มีสิ่งแปลกปลอมเข้าไปอุดตันภายในท่อ Line 3	ทำให้ระดับน้ำภายในบัฟเฟอร์แท็งก์ (TK-001) มีระดับสูงขึ้น จนเป็นสาเหตุให้บัฟเฟอร์แท็งก์นั้นเกิดการระเบิดได้		
6. ระดับน้ำต่ำไป	1. การทำงานของ Inverter ควบคุม Pump	ไม่มีผลกระทบ		

ตารางที่ 3.3 รายงานผลลัพธ์ของการวิเคราะห์ความเป็นอันตรายที่ถังความดันใช้งาน
ผลของการวิเคราะห์หาความเป็นอันตรายที่จะเกิดขึ้นในกระบวนการผลิต(ต่อ)

Project: การควบคุมความดันภายในถังความดันใช้งาน			Node: TK-002	หน้า: 3
Node Description: ถังความดันใช้งาน				
GUIDEWORD	สาเหตุ	ผลกระทบ	การป้องกัน	ข้อเสนอแนะ
7. ความดันสูงไป	1.ฟังก์ชันควบคุมความดันทำงานผิดพลาด 2. ฟังก์ชันควบคุมอัตราการไหลทำงานผิดพลาด 3. มีสิ่งแปลกปลอมเข้าไปอุดตันภายในท่อ L4 4. วาล์ว PV-101 เกิดการทำงานผิดพลาด 5. การทำงานของ Inverter ควบคุม Pump (P-001)	ทำให้ความดันภายในถังความดันใช้งาน (TK-002) มีค่าสูงขึ้น จนเป็นสาเหตุให้ถังความดันใช้งานนั้นเกิดการระเบิดได้		5. ควรมีการติดตั้งระบบ SIS เข้าไปในระบบ เพื่อป้องกันการระเบิดของถังความดันใช้งาน 6. ควรมีการติดตั้ง Pressure Relief Valve ภายในถังความดันใช้งาน(TK-002)
8. ความดันต่ำไป	1. ฟังก์ชันควบคุมอัตราการไหลทำงานผิดพลาด 2. ฟังก์ชันควบคุมอัตราการไหลทำงานผิดพลาด 3.การทำงานของ Inverter ควบคุม Pump (P-001)	ไม่มีผลกระทบ		

ในบทความนี้จะพิจารณาความอันตรายในส่วนของถังความดันใช้งานเท่านั้น โดยถังความดันใช้งานจะถูกออกแบบที่ความดันต่ำกว่าความดันออกแบบของท่อทางด้านเข้า ซึ่งจากรายงานผลลัพธ์ของการวิเคราะห์ความเป็นอันตรายของถังความดันใช้งาน นั้นสามารถสรุปความเป็นอันตรายของกระบวนการได้คือ เกิดขึ้นมาจากฟังก์ชันควบคุมความดันที่เป็นตัวส่งสัญญาณให้ Inverter ควบคุม Pump (P-001) ทำงานผิดพลาด และการทำงานที่ปลอดภัยของกระบวนการผลิตนี้ Inverter จะต้องสั่งให้ Pump (P-001) ปั๊มน้ำออกมาด้วยค่าที่ไม่เกินค่าที่ถูกกำหนดไว้

หลังจากผ่านการวิเคราะห์ความเป็นอันตราย (Process Hazard Analysis) จะพบว่าเมื่อ Inverter ควบคุม Pump (P-001) ทำงานผิดพลาด ทำให้ความดันในท่อส่งสูงขึ้นและเป็นผลให้ความดันภายในถังความดันใช้งาน (TK-002) มีค่าสูงขึ้นตามไปด้วย จนเป็นสาเหตุให้ถังความดันใช้งานนั้นเกิดการระเบิดได้ ฝ่ายความปลอดภัยได้ทำการวิเคราะห์ความอันตรายจากผลกระทบที่เกิดขึ้นจากการระเบิดของถังความดันใช้งาน สามารถแสดงผลกระทบได้ดังนี้

- มูลค่าความเสียหาย 1 ล้านบาท
- เกิดการบาดเจ็บ 2.67 คน
- เกิดอุบัติเหตุทำให้เสียชีวิต 1.12 คน

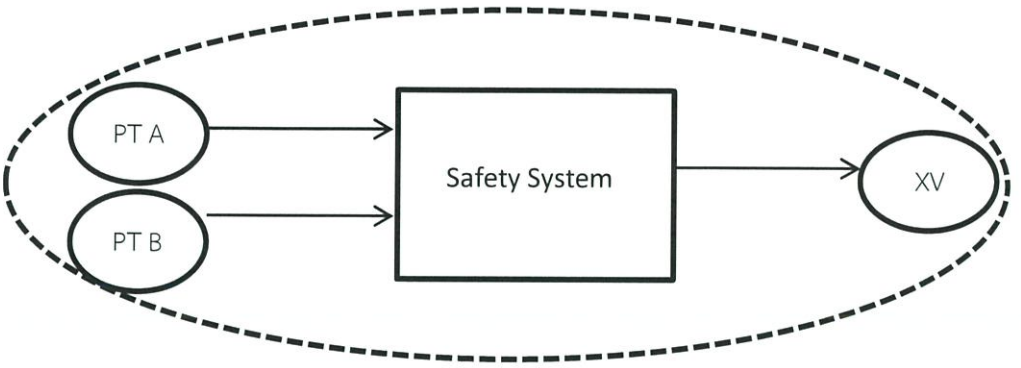
3.2.2 ประเมินความอันตรายเพื่อกำหนดค่าระดับความปลอดภัยหรือค่า SIL (Allocation of Safety Function to Protection Layers)

จากการวิเคราะห์ความอันตรายในเฟสที่ 1 ได้มีการจัดเตรียมฟังก์ชันนิรภัยเป็นดังนี้

- ปิดวาล์วสำหรับการเติมน้ำเข้ากระบวนการผลิต เมื่อความดันสูงกว่าค่าที่กำหนด

โดยการออกแบบฟังก์ชันนิรภัยเพื่อป้องกันความดันเกินภายในถังความดันใช้งาน (TK-002) ได้มีการจัดเตรียมฟังก์ชันนิรภัยได้ดังรูปที่ 3.3

SIF 1



รูปที่ 3.3 จำนวนฟังก์ชันนิรภัยของการป้องกันถังความดันใช้งาน (TK-002) ระเบิด

โดยปกติแล้วฟังก์ชันนิรภัยจะถูกแสดงรายละเอียดการทำงานอยู่ในเอกสารที่เรียกว่า Cause & Effect Diagram ซึ่งจะเป็นเอกสารที่แสดงความสัมพันธ์ระหว่างสัญญาณอินพุตและเอาต์พุต และใช้เป็นเอกสารที่แสดงจำนวนฟังก์ชันนิรภัยทั้งหมดที่ต้องการในกระบวนการผลิต และเป็นข้อมูลสำคัญสำหรับเขียนโปรแกรมการทำงานของระบบนิรภัยแสดงได้ดังรูปที่ 3.4

	การกระทำ	ปิด
	ผลกระทบ	XV- Tank-002 feed
สาเหตุ		
Tank-002 Pressure High High		x

รูปที่ 3.4 Cause & Effect Diagram ของการป้องกันกระบวนการผลิตระเบิด

ข้อมูลต่างๆของอุปกรณ์และกระบวนการมีดังนี้

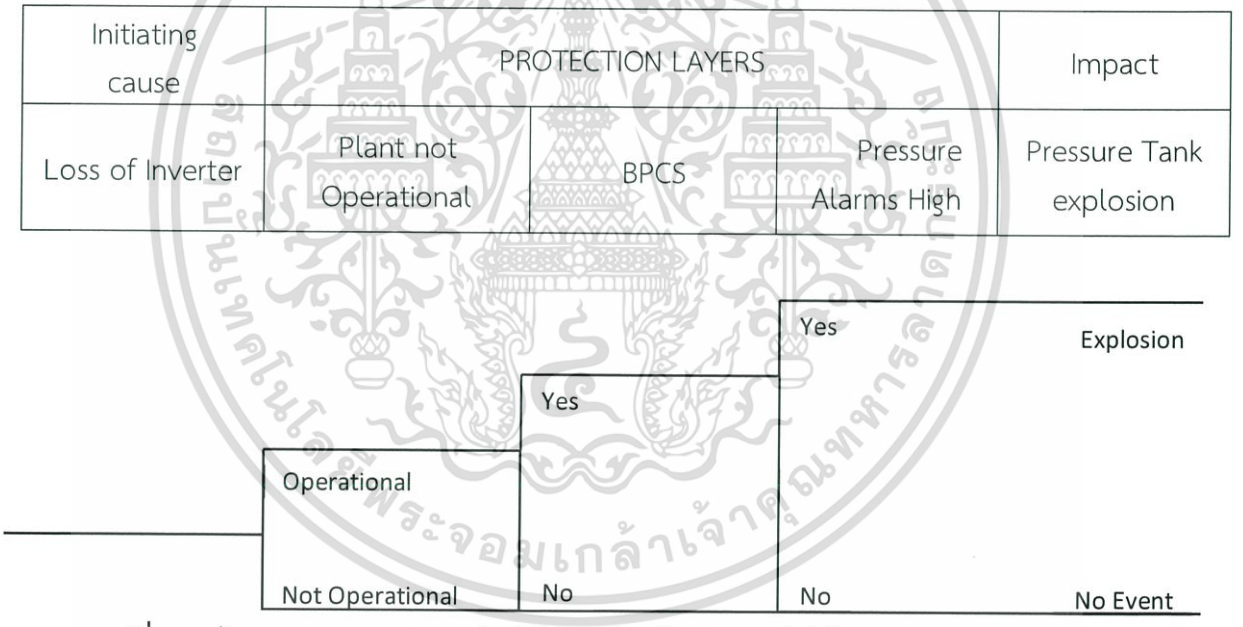
- อินเวอร์เตอร์เกิดความผิดพลาด 0.01 (IEC 61511-3 Annex F Table F4)
- ระบบควบคุมพื้นฐานทำงานผิดพลาด 0.1 (IEC 61511-3 Annex F Table F3)
- ผู้ปฏิบัติการผิดพลาดต่อสัญญาณเตือน 0.3 (IEC 61511-3 Annex F Table F3)

โดยได้มีการกำหนดอัตราความถี่ของเหตุการณ์ที่ไม่ต้องการ อยู่บนพื้นฐานความถี่ของเหตุการณ์ที่ยอมรับได้ เป็นดังตารางที่ 3.4

ตารางที่ 3.4 ความถี่ของเหตุการณ์ที่ยอมรับได้

Even Type	Tolerable Event Frequency
Fatalities Unlikely	1.0×10^{-3}
Fatalities likely	1.0×10^{-4}
Multiple Fatalities Unlikely	1.0×10^{-6}

ในขั้นตอนแรกต้องกำหนดรายละเอียดไดอะแกรม LOPA ขึ้นโดยแสดงรายละเอียดสาเหตุเริ่มต้นของเหตุการณ์อันตรายที่ได้มาจากการวิเคราะห์ความอันตรายและชั้นการป้องกันทั้งหมดที่ได้จัดเตรียมไว้ลงในไดอะแกรม LOPA แสดงได้ดังรูป 3.5



รูปที่ 3.5 ไดอะแกรม LOPA ของฟังก์ชันการป้องกันถังความดันใช้งาน (TK-002) ระเบิด

จากรูปที่ 3.5 จะแสดงให้เห็นว่า สาเหตุเริ่มต้นของเหตุการณ์อันตรายในกระบวนการผลิตจะเกิดขึ้นจากฟังก์ชันควบคุมความดันที่เป็นตัวส่งสัญญาณให้ Inverter ควบคุม Pump (P-001) ทำงานผิดพลาด จากนั้นจะเข้าสู่ชั้นการป้องกันชั้นแรก Plant not Operational การทำงานของกระบวนการผลิตซึ่งจะมีรูปแบบทำงานที่ไม่ต่อเนื่อง โดยในชั้นนี้จะช่วยลดความเสี่ยงระหว่างที่กระบวนการผลิตกำลังทำงานและเนื่องจากกระบวนการผลิตทำงานแบบไม่ต่อเนื่อง ถ้ากระบวนการผลิตไม่ทำงานก็จะไม่มีอันตรายใดๆเกิดขึ้น แต่ถ้ากระบวนการผลิตยังทำงานแล้วมีความผิดพลาดเกิดขึ้น ก็จะมีระบบป้องกันจากเครื่องมือวัดในระบบควบคุมพื้นฐาน ส่งสัญญาณเตือนความผิดปกติต่างๆไปยังผู้ปฏิบัติงาน จากนั้นผู้ปฏิบัติงานก็จะทำการวิเคราะห์ และตอบสนองต่อสัญญาณ

เตือน (Pressure Alarm High) ถ้าตอบสนองได้อย่างถูกต้องและทันเวลาก็จะไม่มีเหตุการณ์อันตรายเกิดขึ้น แต่ถ้าผู้ปฏิบัติงานบกพร่องต่อสัญญาณเตือน หรือตอบสนองไม่ทันต่อเวลาที่ต้องการก็จะทำให้เหตุการณ์อันตรายเกิดขึ้น เนื่องมาจากการระเบิดของถังความดันใช้งาน (TK-002)

เนื่องจากขั้นตอนการทำงานของกระบวนการผลิตเป็นแบบไม่ต่อเนื่อง ซึ่งทำให้ความถี่ของเหตุการณ์อันตรายที่ไม่ต้องการจะมีค่าลดลง ในขณะที่กระบวนการผลิตหยุดทำงานและต้องมีการนำไปพิจารณาในไดอะแกรม LOPA โดยข้อกำหนดในการทำงานของกระบวนการผลิตเป็นดังนี้

เวลาที่กระบวนการผลิตทำงาน = 5 ครั้ง/ปี x 6 สัปดาห์/ครั้ง x 7 วัน/สัปดาห์ x 24 ชม.

= 5040 ชั่วโมงการทำงานของกระบวนการ/ปี

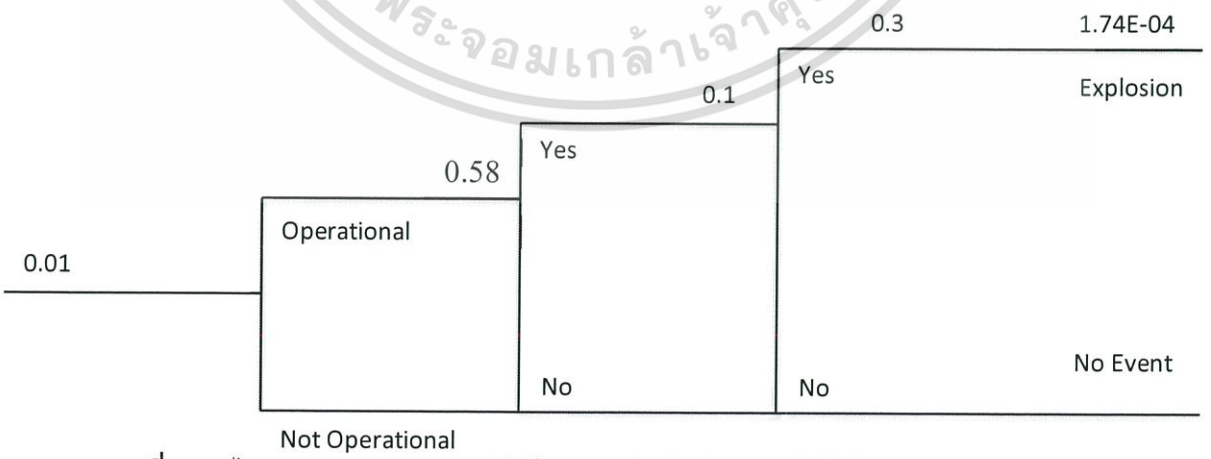
$$\text{อัตราส่วนการทำงานกระบวนการ} = \frac{\text{ชั่วโมงการทำงานของกระบวนการ}}{\text{ชั่วโมงการทำงานในหนึ่งปี}}$$

$$= \frac{5040}{8760}$$

$$= 0.58$$

นำค่าต่างๆ ที่ได้มาใส่ลงในไดอะแกรม LOPA ได้ดังนี้

Initiating cause	PROTECTION LAYERS			Impact
Loss of Inverter	Plant not Operational	BPCS	Pressure Alarms High	Pressure Tank explosion



รูปที่ 3.6 ไดอะแกรม LOPA ของฟังก์ชันการป้องกันถังความดันใช้งาน (TK-002) ระเบิด (หลังการคำนวณหาค่าต่างๆเรียบร้อยแล้ว)

จากไดอะแกรม LOPA จะได้ความถี่ของเหตุการณ์ที่ไม่ต้องการเป็นดังนี้

$$F = F_A \times P_1 \times P_2 \times P_3 \quad (3.1)$$
$$= 0.01 \times 0.58 \times 0.1 \times 0.3$$
$$= 1.74E\text{-}04 \text{ ครั้งต่อปี}$$

จากนั้นต้องมีความถี่ของเหตุการณ์ที่ยอมรับได้จากตารางที่ 3.4 ซึ่งถูกกำหนดขึ้นให้ใช้สำหรับกระบวนการผลิต โดยเทียบจากความสูญเสียที่เกิดขึ้นจะเป็นดังนี้

ถ้ามีเหตุการณ์เกิดขึ้นจะมีความสูญเสียหรือบาดเจ็บเท่ากับกับ 1.12 คน ซึ่งจะอยู่ในกลุ่มของ Multiple Fatalities likely ของส่วนค่าที่ยอมรับได้จากตารางที 3.4 จะได้ค่าความถี่เหตุการณ์ที่ยอมรับได้จะมีค่าเท่ากับ 1.0E-06 และจะพบว่าอัตราการเกิดเหตุการณ์อันตรายที่จะเกิดขึ้นจากไดอะแกรม LOPA จะมีค่าเท่ากับ1.74E-04 ซึ่งจะพบว่ามีค่ามากกว่าค่าที่ยอมรับได้ ดังนั้นจึงต้องการจัดเตรียมฟังก์ชันนิรภัยบนระบบนิรภัยเพื่อใช้สำหรับในการทำให้ความเสี่ยงต่อเหตุการณ์อันตรายมีค่าลดลง ค่าเฉลี่ยความผิดพลาดอันตรายหรือค่า PFD_{avg} ของฟังก์ชันนิรภัยที่ต้องการสำหรับลดความเสี่ยงให้อยู่ในค่าที่กำหนดจะเป็นดังนี้

$$PFD_{avg} = \text{Hazard Rate / Demand rate} \quad (3.2)$$
$$= 1.0E\text{-}06 \,/\, 1.74E\text{-}04$$
$$= 5.75E\text{-}03$$

และ
$$RRF = 1 / PFD_{avg} \quad (3.3)$$
$$= 174$$

จากตารางตัวแปรลดค่าความเสี่ยงของระบบ SIS ที่ค่าระดับความปลอดภัยต่างๆ อาจกล่าวได้ว่าต้องการระบบนิรภัยที่ค่าระดับความปลอดภัย SIL 2 ของฟังก์ชันนิรภัย เพื่อใช้ในการลดความเสี่ยงให้อยู่ในค่าที่ต้องการ โดยระบบ SIS ที่ค่า SIL 2 จะมีการลดความเสี่ยงอยู่ระหว่าง 100 ถึง 1000

3.2.3 จัดทำรายละเอียดความต้องการของระบบวัดคุมนิรภัยทั้งหมด (Safety Requirement Specification : SRS)

ฟังก์ชันนิรภัยสำหรับกระบวนการผลิตนี้จะเป็นการป้องกันไม่ให้ถังความดันใช้งาน (TK-002) ในกระบวนการเกิดการระเบิดถ้าค่าความดันสูงกว่าค่าที่กำหนดและได้กำหนดการทำงานของฟังก์ชันนิรภัยในรายละเอียดความต้องการ (Safety Requirement Specification: SRS) ในการประเมินความเสี่ยงและผลกระทบเพื่อกำหนดค่าระดับความปลอดภัยให้กับฟังก์ชันนิรภัยจะได้ระดับ SIL 2 ดังนั้นในการออกแบบและเลือกใช้อุปกรณ์ต้องมีค่าเฉลี่ยความผิดพลาดอันตรายรวมของฟังก์ชันนิรภัยต้องอยู่ระหว่าง 0.01 ถึง 0.001 โดยผู้ออกแบบจะต้องเลือกใช้อุปกรณ์ต่างๆ ให้เป็นไปตามมาตรฐาน IEC 61508 และมาตรฐาน IEC 61511 ดังข้อมูลในตารางต่อไปนี้

ตารางที่ 3.5 ตารางจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดของ IEC 61508 สำหรับอุปกรณ์ TYPE B

Safe failure fraction (SFF)	Hardware fault tolerance		
	0	1	2
< 60%	Not allowed	SIL 1	SIL 2
60%-90%	SIL 1	SIL 2	SIL 3
90% - 99%	SIL 2	SIL 3	SIL 4
>99%	SIL 3	SIL 4	SIL4

โดยในการออกแบบฟังก์ชันนิรภัยต้องทราบค่าตัวแปร 2 ตัวแปร ที่นำมาใช้ในการออกแบบฟังก์ชันนิรภัยคือค่า Safe failure fraction (SFF) และค่า Average Probability of failure on Demand (PFD_{avg})

1. Safe failure fraction (SFF) หาได้จากสูตร

$$SFF = \frac{\lambda_{SD}+\lambda_{SU}+\lambda_{DU}}{\lambda_{SD}+\lambda_{SU}+\lambda_{DD}+\lambda_{DU}} \quad (3.4)$$

โดยที่

λ_{SD} = ความผิดพลาดนิรภัยตรวจจับได้

λ_{SU} = ความผิดพลาดนิรภัยตรวจจับไม่ได้

λ_{DD} = ความผิดพลาดอันตรายตรวจจับได้

λ_{DU} = ความผิดพลาดอันตรายตรวจจับไม่ได้

2. Average Probability of failure on Demand (PFD_{avg}) หาได้จากสูตร

$$PFD_{AVG}(1oo1) = (\lambda_{DU}+\lambda_{DD})t_{CE} \quad (3.5)$$

$$PFD_{AVG}(1oo2) = 2\left[\left(1-\beta_D\right)\lambda_{DD}+\left(1-\beta\right)\lambda_{DU}\right](t_{CE}t_{GE}) + \beta\lambda_{DU}MTTR+\beta\lambda_{DU}\left(\frac{T_1}{2}+MRT\right) \quad (3.6)$$

โดยที่

λ_{DU} = ความผิดพลาดอันตรายตรวจจับไม่ได้

λ_{DD} = ความผิดพลาดอันตรายตรวจจับได้

β_D = ค่าความผิดพลาดร่วมตรวจจับได้ (5%)

β = ค่าความผิดพลาดร่วม (10%)

$$= \beta=2x\beta_D \quad (3.7)$$

MTTR = เวลาเฉลี่ยในการคืนค่า

MTR = เวลาเฉลี่ยที่ใช้ในการซ่อมแซม

t_{CE} = เวลาเฉลี่ยที่ลดลงของแต่ละรูปแบบ

$$=\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MRT\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR \quad (3.8)$$

t_{GE} = เวลาเฉลี่ยที่ลดลงของแต่ละกลุ่ม

$$= \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3}+MRT\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR \qquad (3.9)$$

T_1 = เวลาทดสอบการทำงาน (1ปี=8760ชั่วโมง)

3.2.3.1 การเลือกใช้งานเครื่องมือวัดในส่วนอินพุตหรือ Sensor part

เลือกพิจารณา 2051 4-20mA Hart Pressure Transmitter Coplanar Differential & Coplanar Gage ข้อมูลดังตารางที่ 3.6

ตารางที่ 3.6 ตารางข้อมูลของ Sensor Part (ดูรายละเอียดในภาคผนวก ก)

IEC 61508 Failure Rates in FIT[1]

Route 1_H Table

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
2051 4-20mA HART Pressure Transmitter: Coplanar Differential & Coplanar Gage	0	84	258	32	91%
2051 4-20mA HART Pressure Transmitter: Coplanar Absolute, Inline Gage & Absolute	0	94	279	41	90%

Route 2_H Table[2]

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
2051 4-20mA HART Pressure Transmitter: Coplanar Differential & Coplanar Gage	0	84	258	32
2051 4-20mA HART Pressure Transmitter: Coplanar Absolute, Inline Gage & Absolute	0	94	279	41
2051 Flowmeter based on 1195, 405, or 485 Primaries				
2051 4-20mA HART Flowmeter Series[3]	0	92	258	41
2051 Level Transmitter: (w/o additional Seal)				
2051 4-20mA HART Pressure Transmitter: Coplanar Differential & Coplanar Gage	0	84	258	67
2051 4-20mA HART Pressure Transmitter: Coplanar Absolute, Inline Gage & Absolute	0	94	279	75
2051 Transmitter with Remote Seals[4]				

หาค่า t_{CE} และค่า t_{GE} ได้จากสมการที่ 3.8 และ 3.9 ตามลำดับ

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MRT\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$= \frac{32}{290}\left(\frac{8760}{2}+8\right)+\frac{258}{290}8$$

$$= 491.12 \text{ h}$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3}+MRT\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$= \frac{32}{290}\left(\frac{8760}{3}+8\right)+\frac{258}{290}8$$

$$= 329.31 \text{ h}$$

หาค่า PFD_{AVG} (1oo2) จากสมการที่ (3.6) ดังนี้

$$PFD_{AVG} = 2\left[\left(1-\beta_D\right)\lambda_{DD}+\left(1-\beta\right)\lambda_{DU}\right](t_{CE}t_{GE}) + \beta\lambda_{DU}MTTR+\beta\lambda_{DU}\left(\frac{T_1}{2}+MRT\right)$$

$$= 2\left(\left(1-0.05\right)\frac{258}{10^9}+\left(1-0.1\right)\frac{32}{10^9}\right)^2 491.12x329.31) + 0.05x8x\frac{258}{10^9} + 0.1x\frac{32}{10^9}\left(\frac{8760}{2}+8\right)$$

$$= 1.41 \times 10^{-5}$$

หาค่า SFF จากสมการที่ 3.4 ดังนี้

$$SFF = \frac{\lambda^{SD}+\lambda^{SU}+\lambda^{DD}}{\lambda^{SD}+\lambda^{SU}+\lambda^{DD}+\lambda^{DU}}$$

$$= \frac{0+84+258}{0+84+258+32}$$

$$= 0.91 \text{ หรือ } 91\%$$

ในส่วนของ Sensor เมื่อพิจารณาค่า SFF และ PFD_{AVG} แล้วเลือกใช้อุปกรณ์ที่ใช้ในฟังก์ชันนิรภัยที่ระดับ SIL 3 จะต้องมีจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดเท่ากับ 1 หรือต้องใช้อุปกรณ์ 2 ตัวในรูปแบบ 1oo2 (One out of two voting)

3.2.3.2 การเลือกใช้งานตัวควบคุม (PLC)

เลือกพิจารณา Safety PLC SIMATIC S7-300 CPU317F-2 PN/DP ข้อมูลดังตารางที่ 3.7

ตารางที่ 3.7 ตารางข้อมูลของ Safety PLC (ดูรายละเอียดในภาคผนวก ก)

Probabilities of Failure

Below are the values for the CPU 317F-2 PN/DP probabilities of failure:

	Operation in Low Demand Mode low demand mode (average probability of failure on demand)	Operation in High Demand or Continuous Mode high demand/continuous mode (probability of a dangerous failure per hour)	Proof-test interval
F-compatible CPU 317F-2 PN/DP 6ES7317-2FK13-0AB0	4.76E-05	1.09E-09	10 years

ในส่วนของตัวควบคุม (PLC) ซึ่งจะใช้ค่า PFD_{avg} (Average Probability of failure on Demand) = 4.76×10^{-5} ซึ่งจะใช้ในฟังก์ชันนิรภัยที่ระดับ SIL 3 และออกแบบให้มีจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดเท่ากับ 0 หรือต้องใช้อุปกรณ์ 1 ตัวในรูปแบบ 1oo1 (One out of One voting)

3.2.3.3 การเลือกใช้งานวาล์วนิรภัย (Shut Down Valve)

จะเลือกพิจารณา Solenoid Valve 8314 with PVST ดังตารางที่ 3.8

ตารางที่ 3.8 ตารางข้อมูลของ Solenoid Valve (ดูรายละเอียดในภาคผนวก ก)

IEC 61508 Failure Rates

For valves used in a final element assembly, SIL must be verified for the specific application using the following failure rate data.

Failure rates for the Series 8314 Solenoid Valves in FIT*

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
8314	0 FIT	190 FIT	0 FIT	100 FIT	65.5%
8314 with PVST	0 FIT	190 FIT	99 FIT	1 FIT	99.7%

Applications

Series 8314 Solenoid	De-energize on trip, normally closed

จากตารางสามารถหาค่า PFD_{AVG} จากสมการที่ (3.5) ในส่วนของ Solenoid Valve ได้ดังนี้

$$PFD_{AVG} = (\lambda_{DU}+\lambda_{DD})t_{CE}$$

$$= \left(\frac{1}{10^9}+\frac{99}{10^9}\right) x484.85$$

$$= 4.84 \times 10^{-5}$$

และหาค่า *SFF* จากสมการที่ (3.4)

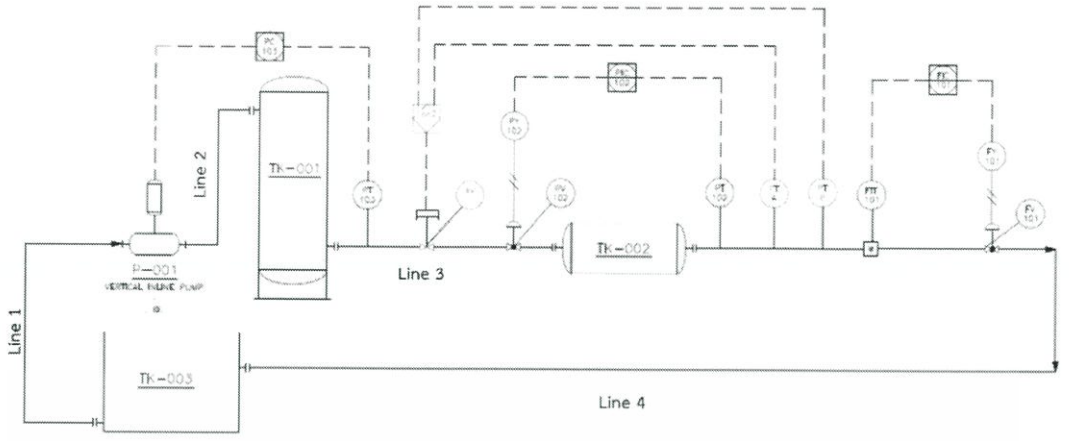
$$SFF = \frac{\lambda^{SD}+\lambda^{SU}+\lambda^{DD}}{\lambda^{SD}+\lambda^{SU}+\lambda^{DD}+\lambda^{DU}}$$

$$= \frac{0+190+99}{0+190+99+1}$$

$$= 0.9965 \text{ หรือ } 99.7\%$$

ในส่วนของ Solenoid valve เมื่อพิจารณาค่า SFF และ PFD_{AVG} แล้ว เลือกใช้อุปกรณ์ที่ใช้ในฟังก์ชันนิรภัยที่ระดับ SIL 3 จะต้องมีจำนวนอุปกรณ์ต่ำสุดที่ยอมให้เกิดความผิดพลาดเท่ากับ 0 หรือต้องใช้อุปกรณ์ 1 ตัวในรูปแบบ 1oo1 (One out of one voting)

ดังนั้น สรุปการเลือกใช้อุปกรณ์ต่างๆ ในฟังก์ชันนิรภัยตามข้อกำหนดของมาตรฐาน IEC 61508 และ IEC 61511 จึงสามารถแสดงฟังก์ชันนิรภัยบนแผนภาพกระบวนการควบคุมได้ดังรูปที่ 3.7

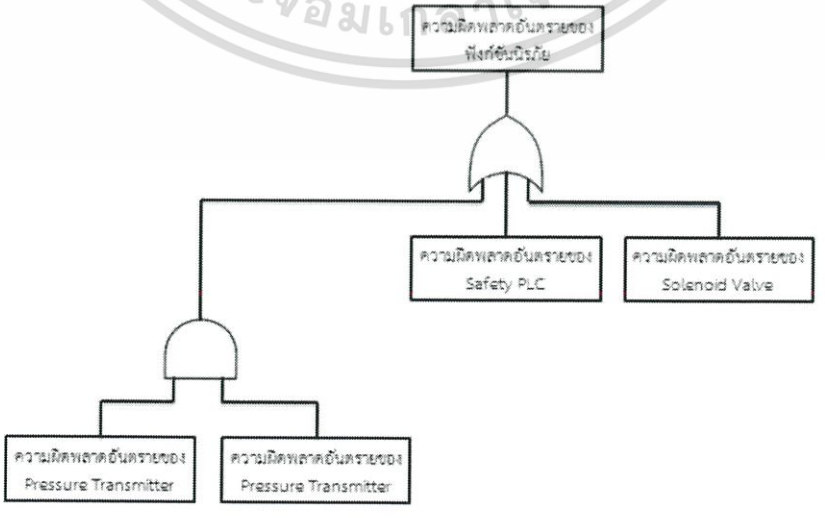


รูปที่ 3.7 แผนภาพ (P&ID) ของกระบวนการผลิตหลังมีการติดตั้งระบบวัดคุมนิรภัย

จากรูปที่ 3.7 เมื่อเกิดความผิดพลาดของฟังก์ชันควบคุมความดันจะเป็นสาเหตุให้เกิดความดันเกินในถังได้ จึงต้องมีการจัดเตรียมฟังก์ชันนิรภัยในการป้องกันความดันเกินในถัง จะเห็นว่าฟังก์ชันนิรภัยประกอบไปด้วยเครื่องมือวัดความดัน (Pressure Transmitter) ส่งสัญญาณไฟฟ้าไปยังส่วนประมวลผล เพื่อตรวจสอบค่าความดันที่อ่านได้จากกระบวนการผลิตว่ามีค่าสูงเกินกว่าค่าที่กำหนดหรือไม่ จากนั้นส่วนประมวลผลจะส่งสัญญาณเอาต์พุตไปยังวาล์วนิรภัย เพื่อสั่งปิดวาล์ว ในการหยุดแหล่งจ่ายของไหลที่จะเข้ามาในถัง

3.2.4 ดำเนินการจัดทำระบบวัดคุมนิรภัยให้เป็นไปตามที่ได้ออกแบบไว้ (Design and Engineering of Safety Instrumented System)

ในขั้นตอนนี้จะคำนวณหาค่าเฉลี่ยความผิดพลาดอันตรายของอุปกรณ์ที่เลือกว่าอยู่ในช่วงของค่าความปลอดภัยหรือไม่ จะใช้ Fault Tree analysis จากฟังก์ชันนิรภัยที่แสดงอยู่บนแผนภาพ FTA ได้ดังรูปที่ 3.8



รูปที่ 3.8 แผนภาพ FTA ของฟังก์ชันนิรภัย

โดยในการหาค่าเฉลี่ยความผิดพลาดอันตรายของฟังก์ชันนิรภัยจะต้องมีค่า Average Probability of failure on Demand หรือค่าเฉลี่ยความผิดพลาดอันตรายน้อยกว่าค่าเฉลี่ยความผิดพลาดอันตรายของกระบวนการผลิตโดยค่า Average Probability of failure on Demand ของกระบวนการผลิตอยู่ที่ 0.01-0.001 หรือที่ระดับ SIL 2

จากแผนภาพสามารถแสดงสมการค่าเฉลี่ยความผิดพลาดอันตรายของฟังก์ชันนิรภัยได้ดังนี้

PFD_{AVG} SIF = PFD_{AVG} Sensor + PFD_{AVG} PLC + PFD_{AVG} SDV

PFD_{AVG} SIF = ค่าเฉลี่ยความผิดพลาดอันตรายของฟังก์ชันนิรภัย

PFD_{AVG} Sensor = ค่าเฉลี่ยความผิดพลาดอันตรายของ Sensor part

PFD_{AVG} PLC = ค่าเฉลี่ยความผิดพลาดอันตรายของ Safety PLC

PFD_{AVG} SDV = ค่าเฉลี่ยความผิดพลาดอันตรายของ Solenoid Valve

จากตารางที่ 3.7, 3.8 และ 3.9 จะได้ค่า PFD_{AVG} (Average Probability of failure on Demand) ของแต่ละส่วนดังนี้

PFD_{AVG} Sensor = 1.41×10^{-5}

PFD_{AVG} PLC = 4.76×10^{-5}

PFD_{AVG} SDV = 4.84×10^{-5}

ดังนั้นจะได้ค่า

PFD_{AVG} SIF = $1.41 \times 10^{-5} + 4.76 \times 10^{-5} + 4.84 \times 10^{-5}$

= 1.1×10^{-4}

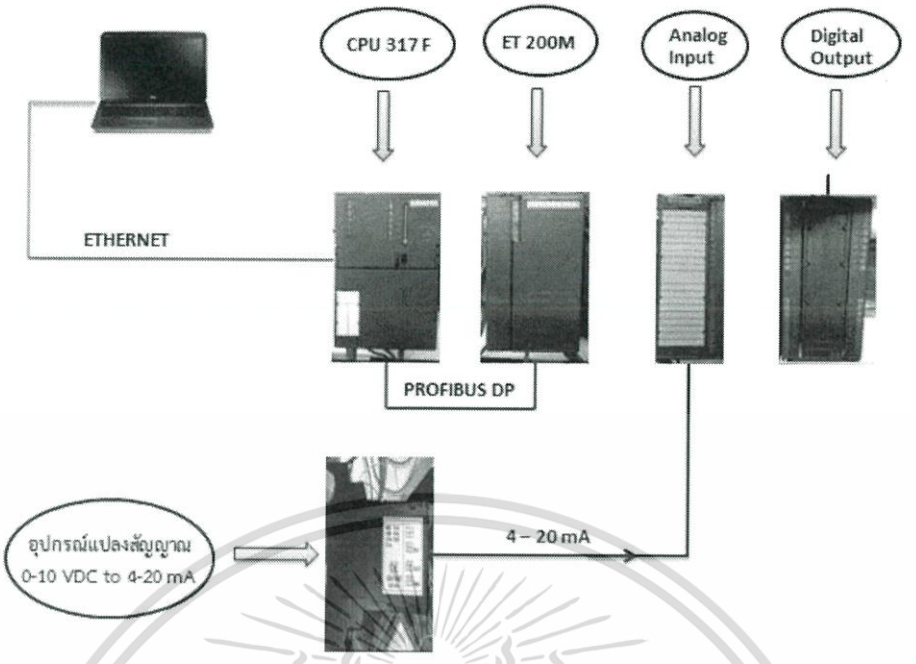
ค่าเฉลี่ยความผิดพลาดอันตรายของฟังก์ชันนิรภัยที่ทำการออกแบบจะมีค่า 6.25×10^{-4} ซึ่งมีค่าต่ำกว่าค่าที่ต้องการในระดับ SIL 2 (หรืออาจกล่าวได้ว่าอุปกรณ์และรูปแบบที่เลือกใช้สามารถนำไปใช้งานได้)

3.3 สถาปัตยกรรมของระบบวัดคุมนิรภัย (System Architecture of Safety Instrumented System)

สถาปัตยกรรมของระบบวัดคุมนิรภัยของกระบวนการบ่งบอกถึงอุปกรณ์ที่ใช้ควบคุมต่างๆซึ่งจะแสดงรายละเอียดเกี่ยวกับกระบวนการและเครือข่ายสื่อสารของระบบควบคุมการผลิต

3.3.1 องค์ประกอบของส่วนควบคุมในระบบวัดคุมนิรภัย

องค์ประกอบของส่วนควบคุมในระบบวัดคุมนิรภัยจะแสดงรายละเอียดของอุปกรณ์ภายในระบบทั้งหมด เช่น ตัวควบคุม (PLC), ตัวแปลงสัญญาณระหว่าง 4-20mA และ Profibus D/P, อนาล็อกอินพุตโมดูล และดิจิตอลเอาท์พุตโมดูล



รูปที่ 3.9 แสดงสถาปัตยกรรมของระบบวัดคุมนิรภัย

3.3.1.1 ตัวควบคุม (CPU317F)

เป็นส่วนประมวลผลและเชื่อมต่อกับอุปกรณ์ต่างๆโดยที่พอร์ตเชื่อมต่อประกอบด้วย พอร์ตโปรฟิบัสดีพี พอร์ตเอ็มพีไอ โดยในที่นี้เลือกใช้ตัวควบคุมของซีเมนส์ CPU317F รุ่น s7 300 หมายเลขรหัส 6ES7 317F-2FK13-0AB0 ดังรูปที่ดังรูปที่ 3.10 และตารางที่ แสดงลักษณะทั่วไปของ CPU317F

รูปที่ 3.10 ตัวควบคุม (CPU317F)

ตารางที่ 3.9 แสดงคุณลักษณะทั่วไปของ CPU317F

เวอร์ชันของตัวควบคุม	STEP 7 V5.4 SP2
อัตราการรับส่งข่อมูล	1.5 Mbps
ค่าระดับความปลอดภัยของตัวควบคุม	SIL 4

3.3.1.2 ตัวแปลงสัญญาณระหว่าง 4-20mAและดีพี (4-20mA/DP Coupler)

เป็นอุปกรณ์ที่ใช้แปลงสัญญาณระหว่างโปรฟีบัสดีพีที่อยู่ในด้านตัวควบคุมเป็นสัญญาณ 4-20 mA ที่อยู่ในด้านอุปกรณ์วัดระดับฟิลด์โดยในที่นี้เลือกใช้อุปกรณ์แปลงสัญญาณของซีเมนส์ ET200M รุ่น IM153-2 หมายเลขรหัส 6ES7 153-2BA02-0XB0 ดังรูปที่ 3.11 และตารางที่แสดงลักษณะทั่วไปของ IM153-2

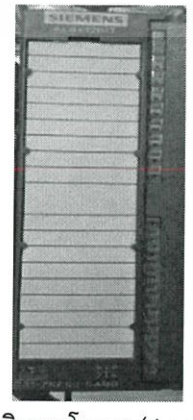
รูปที่ 3.11 ตัวแปลงสัญญาณระหว่าง 4-20mAและดีพี

ตารางที่ 3.10 แสดงคุณลักษณะทั่วไปของ IM153-2

Supply voltage	Rated value (DC) 24 V
อัตราการรับส่งข้อมูล	1.5 Mbps
BUS protocal	Profibus DP

3.3.1.3 อนาล็อกอินพุตโมดูล (Analog input Module)

เป็นอุปกรณ์ที่ใช้รับค่าสัญญาณไฟฟ้า 4 - 20 mA. จากอุปกรณ์วัดระดับฟิลด์ (Field Instrument) เพื่อส่งสัญญาณไปยังตัวแปลงสัญญาณต่อไป โดยในที่นี้ในที่นี้เลือกใช้อนาล็อกอินพุตโมดูลของซีเมนส์ AI หมายเลขรหัส 331-7KF02-0AB0 ดังรูปที่ 3.12 และตารางที่ 3.12 แสดงลักษณะทั่วไปของ**อนาล็อกอินพุตโมดูล**



รูปที่ 3.12 อนาล็อกอินพุตโมดูล (Analog input Module)

ตารางที่ 3.11 แสดงลักษณะทั่วไปของ**อนาล็อกอินพุตโมดูล**

การเชื่อมต่อสัญญาณ	ต่อสัญญาณแบบ 4 สาย
ช่วงของสัญญาณอินพุต	4 mA ถึง 20 mA
การตั้งค่าสัญญาณเตือน	channels 0 and 2

3.3.1.4 ดิจิตอลเอาท์พุตโมดูล (Digital output module)

เป็นอุปกรณ์ที่ส่งสัญญาณ Digital 0 หรือ 1 ตามลักษณะ Close or Open Switch เพื่อใช้สั่งในการเปิด-ปิด Shut down valve โดยในที่นี้ในที่นี้เลือกใช้ดิจิตอลเอาท์พุตโมดูลของซีเมนส์ DO รุ่น SM322หมายเลขรหัส 6ES7 322-1BL00-0AA0 ดังรูปที่ 3.13 และตารางที่ 3.13

รูปที่ 3.13 ดิจิตอลเอาท์พุตโมดูล (Digital output module)

ตารางที่ 3.12 แสดงลักษณะทั่วไปของ**ดิจิตอลเอาท์พุตโมดูล**

Supply voltage	Rated value (DC) 24 V
ค่าสัญญาณ 1 อ่านค่าที่	0.5 A
ค่าสัญญาณ 0 อ่านค่าที่	0.5 mA

3.3.1.5 โปรแกรม SIMATIC Manager

โปรแกรม SIMATIC Manager คือ เครื่องมือที่ใช้ในการออกแบบและจัดการการทำงานของระบบที่ได้ทำการออกแบบไว้ก่อนหน้านี้ โดยสามารถตั้งค่าการเชื่อมต่อทางด้านฮาร์ดแวร์ (hardware and network configuration tools) และการเลือกใช้ภาษาสำหรับการเขียนโปรแกรมควบคุม

โปรแกรมที่เป็นส่วนประกอบหลักๆของโปรแกรม SIMATIC MANAGER ได้แก่

- Configuring Network หรือ NetPro configuration tool คือ เครื่องมือที่ใช้กราฟิกในการแสดงการเชื่อมต่อของเอ็มพีไอ โปรฟิบัส และเครือข่ายย่อยอีเทอร์เน็ตทางอุตสาหกรรม เครื่องมือ

นี้จะแสดงให้เห็นถึงการเชื่อมต่อของแต่ละอุปกรณ์ และการสร้างการเชื่อมต่อของอุปกรณ์ด้วยกันเอง

- Hardware configuration คือ เครื่องมือสำหรับเพิ่มรายชื่ออุปกรณ์ทั้งหมดลงในระบบควบคุมและเพิ่มข้อมูลอุปกรณ์ทั้งหมดให้ผู้ปฏิบัติการสามมารถเข้าถึงทางโปรแกรมได้
- Ladder Diagram คือ Logic พื้นฐานที่ใช้ในการกำหนดคำสั่งให้กระบวนการให้เป็นไปตามที่ออกแบบไว้
- S7 Distributed Safety Program V.5.4 คือ เครื่องมือที่ใช้เขียนโปรแกรม Safety เพื่อใช้ออกแบบระบบวัดคุมนิรภัย โดยภายในตัวโปรแกรมจะมีฟังก์ชันบล็อกพิเศษ เช่น FB 190 F_1oo2D 1oo2 Evaluation with Discrepancy ที่ใช้สำหรับโปรแกรมการทำงานฟังก์ชัน One out of Two Voting ในการทำงานเพื่อป้องกันการเกิดความเป็นอันตรายของกระบวนการ

3.4 ขั้นตอนการเขียน Safety Program 1oo2DI Voting

หลังจากผ่านขั้นตอนการเลือกใช้งานฟังก์ชันระบบวัดคุมนิรภัยในเฟสที่ 3 (หัวข้อที่ 3.2.3) ตามการออกแบบมาตรฐาน IEC 61511 มาแล้วนั้น ในส่วนของขั้นตอนนี้ จะเป็นการเขียนโปรแกรมเพื่อใช้งานฟังก์ชันดังกล่าวให้เข้ากับเงื่อนไขที่ได้ออกแบบไว้ (1oo2 Voting) โดยขั้นตอนการเขียน Safety Program 1oo2 Voting (One out of Two Voting) นั้นมีรายละเอียดและขั้นตอนดังต่อไปนี้

3.4.1 ทำการการตั้งค่าคอนฟิกของระบบอัตโนมัติ (Automation System: AS)

ในขั้นตอนนี้จะเป็นการทำ Hardware Configuration, Network Configuration และวิธีการตั้งค่าพารามิเตอร์ตัวควบคุม (PLC) ให้สามารถทำงานได้ในการใช้งาน Safety Program ซึ่งได้อธิบายขั้นตอนการดำเนินงานไว้ในภาคผนวก ข.1, ภาคผนวก ข.2 และภาคผนวก ข.3 ตามลำดับ

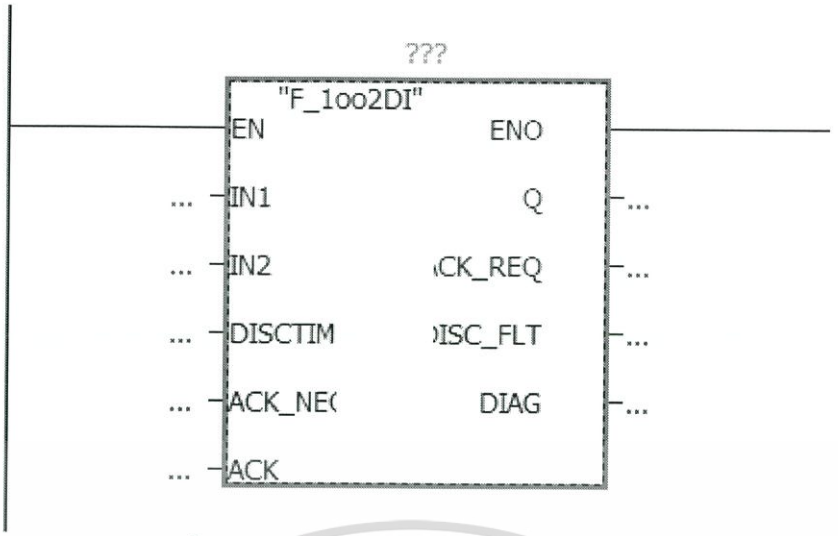
3.4.2 การสร้าง Safety Program โดยการตั้ง F-Runtime Group

ในการเขียน Safety Program นั้น จำเป็นต้องมีการสร้าง F-Runtime Group เพื่อกำหนดฟังก์ชัน Safety ในการทำงาน โดยรายละเอียดและขั้นตอนในการสร้าง F-Runtime Group นั้นได้ถูกแสดงไว้ในภาคผนวก ค

3.4.3 โครงสร้างและการทำงานของฟังก์ชัน F_1oo2DI (FB190)

3.4.3.1 โครงสร้างของฟังก์ชัน F_1oo2DI (FB190)

โครงสร้างของฟังก์ชัน F_1oo2DI (FB190) นั้นสามารดแสดงรายละเอียดได้ดังรูปที่ 3.14 และรูปที่ 3.15



รูปที่ 3.14 ฟังก์ชันบล็อกของ F_1oo2DI (FB190)

Address	Declaration	Name	Type	Initial value	Comment
0.0	in	IN1	BOOL	FALSE	SENSOR 1
0.1	in	IN2	BOOL	FALSE	SENSOR 2
2.0	in	DISCTIME	TIME	T#0MS	DISCREPANCY TIME
6.0	in	ACK_NEC	BOOL	TRUE	1=ACKNOWLEDGEMENT NECESSARY
6.1	in	ACK	BOOL	FALSE	ACKNOWLEDGEMENT
8.0	out	Q	BOOL	FALSE	OUTPUT
8.1	out	ACK_REQ	BOOL	FALSE	1=ACKNOWLEDGEMENT REQUEST
8.2	out	DISC_FLT	BOOL	FALSE	1=DISCREPANCY FAULT
9.0	out	DIAG	BYTE	B#16#0	SERVICE INFORMATION

รูปที่ 3.15 Data บล็อกของฟังก์ชัน F_1oo2DI (FB190)

จากรูปที่ 3.15 นั้นสามารถอธิบายค่าพารามิเตอร์ที่อยู่ภายในฟังก์ชัน F_1oo2DI (FB190) ได้ดังนี้

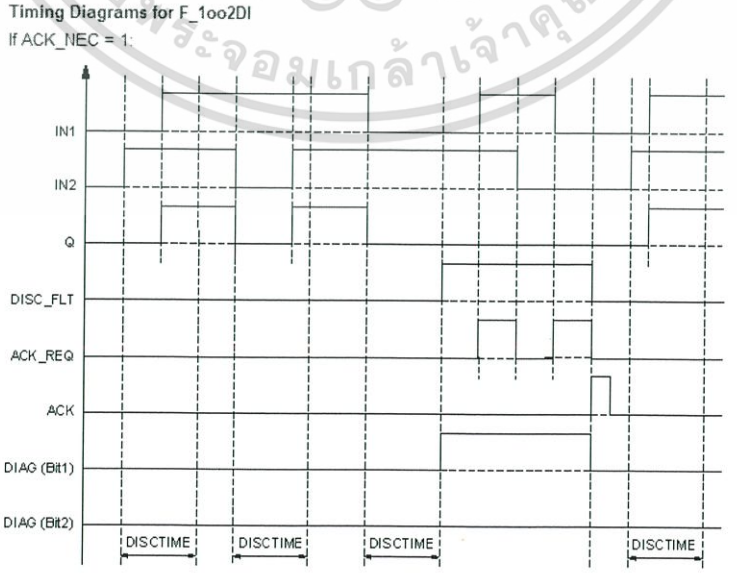
- IN1 คือ อินพุตตัวที่ 1 โดยมีชนิดข้อมูลเป็นแบบ บูลีน
- IN2 คือ อินพุตตัวที่ 2 โดยมีชนิดข้อมูลเป็นแบบ บูลีน
- DISCTIME คือ เวลาที่แสดงถึงความแตกต่างระหว่าง IN1 และ IN2 (โดยมีค่าอยู่ระหว่าง 0 ถึง 60 วินาที)
- ACK_NEC ถ้าเป็นลอจิก 1 หมายความว่าระบบนั้นมีการพิจารณาการตอบสนองต่อค่าความผิดพลาดที่เกิดขึ้นจากความแตกต่างของเวลา (discrepancy error)
- ACK คือ การตอบสนองต่อสัญญาณเตือนความผิดพลาดที่เกิดขึ้น (Acknowledgement)
- Q คือ เอาท์พุตของฟังก์ชัน โดยมีชนิดข้อมูลเป็นแบบ บูลีน
- ACK_REQ จะมีการแสดงสถานะก็ต่อเมื่อระบบเกิดความผิดพลาดขึ้นเท่านั้น (DISC_FLT มีค่าเท่ากับ 1) โดยถ้าเป็นลอจิก 1 หมายความว่า IN1 และ IN2 มีความเหมือนกันของสัญญาณที่เข้ามา และถ้าลอจิกเป็น 0 หมายความว่า IN1 และ IN2 มีความแตกต่างกันของสัญญาณที่เข้ามา

- DISC_FLT ถ้าเป็นลอจิก 0 จะหมายถึงว่ายังไม่มีความผิดพลาดเกิดขึ้นภายในระบบ และถ้าหากมีลอจิกเท่ากับ 1 หมายความว่าระบบนั้นเกิดความผิดพลาดแล้ว
- DIAG คือ Service information

3.4.3.2 การทำงานของฟังก์ชัน F_1oo2DI (FB190)

- กรณีที่ 1 อินพุต 1 (IN1) และ อินพุต 2 (IN2) มีค่าเท่ากับ 1 จะได้เอาท์พุต (Q) เท่ากับ 1
- กรณีที่ 2 อินพุต 1 (IN1) และ อินพุต 2 (IN2) มีค่าเท่ากับ 0 จะได้เอาท์พุต (Q) เท่ากับ 0
- กรณีที่ 3 อินพุต 1 (IN1) และ อินพุต 2 (IN2) มีค่าแตกต่างกัน โดยถ้าอินพุตทั้งสองมีค่าแตกต่างกันแล้วนั้น จะทำให้ฟังก์ชัน Discrepancy time (DISTIME) เริ่มจับเวลาทันที จากนั้นถ้า IN1 และ IN2 มีค่าแตกต่างกัน แต่ยังอยู่ในช่วงของเวลา DISCTIME ที่กำหนดไว้ระบบก็ยังสามารถทำงานได้ตามปรกติ (ไม่เกิด DISC_FLT) และจะทำให้เอาท์พุต (Q) มีค่าเท่ากับ 1
- กรณีที่ 4 อินพุต 1 (IN1) และ อินพุต 2 (IN2) มีค่าแตกต่างกัน โดยถ้าอินพุตทั้งสองมีค่าแตกต่างกันแล้วนั้น จะทำให้ฟังก์ชัน Discrepancy time (DISTIME) เริ่มจับเวลาทันที จากนั้นถ้า IN1 และ IN2 มีค่าแตกต่างกันเกินกว่าระยะเวลา DISCTIME ที่ได้กำหนดไว้ ระบบก็จะมีสัญญาณ Fault เกิดขึ้นภายในระบบ (DISC_FLT มีค่าท่ากับ 1) และจะทำให้เอาท์พุต (Q) มีค่าเท่ากับ 0

จากกระบวนการการทำงานทั้งหมดของฟังก์ชัน 1002DI (FB190) ที่ได้อธิบายมานั้น สามารถเขียน Timing Diagram การทำงานได้ดังรูปที่ 3.16



รูปที่ 3.16 Timing Diagram การทำงานของฟังก์ชัน 1oo2DI

3.4.4 ดำเนินการเขียนฟังก์ชัน 1oo2DI Voting ตามที่ได้ทำการออกแบบไว้

โดยในการออกแบบฟังก์ชัน 1oo2DI Voting นั้น ต้องการทำการออกแบบเพื่อไปสั่งงาน Shutdown Valve ที่มีรูปแบบการต่อใช้งานเป็น De-energize to trip

3.4.4.1 ทำการสร้าง Data Block2 (DB2)

ทำการสร้าง DB2 เพื่อใช้เป็นที่เก็บข้อมูลในการส่งถ่ายข้อมูลอินพุตหรือเอาท์พุตจากภายใน Safety Program (FB1) กับ Program ทั่วไป (OB1) ได้ ในกรณีที่ไม่ได้ใช้อุปกรณ์อินพุต (Input Module) และอุปกรณ์เอาท์พุต (Output Module) ที่เป็นอุปกรณ์ Safety Device จริง (โดยในโครงงานนี้ได้ใช้อุปกรณ์อนาล็อก อินพุต โมดูล และ ดิจิตอล เอาท์พุต โมดูล ที่ไม่ได้เป็นอุปกรณ์ Safety Device จริง) **โดยวิธีการสร้าง DB2 ทำได้คือ** คลิกที่ SIMATIC 300(1) **ใน** Project window > CPU 317F-2PN/DP > S7 Program(1) > Blocks > คลิกขวาพื้นที่ว่าง > Insert New Object > Data Block (โดยเราเลือกให้ DB2 นั้นเป็น F-DB) ดังรูปที่ 3.17

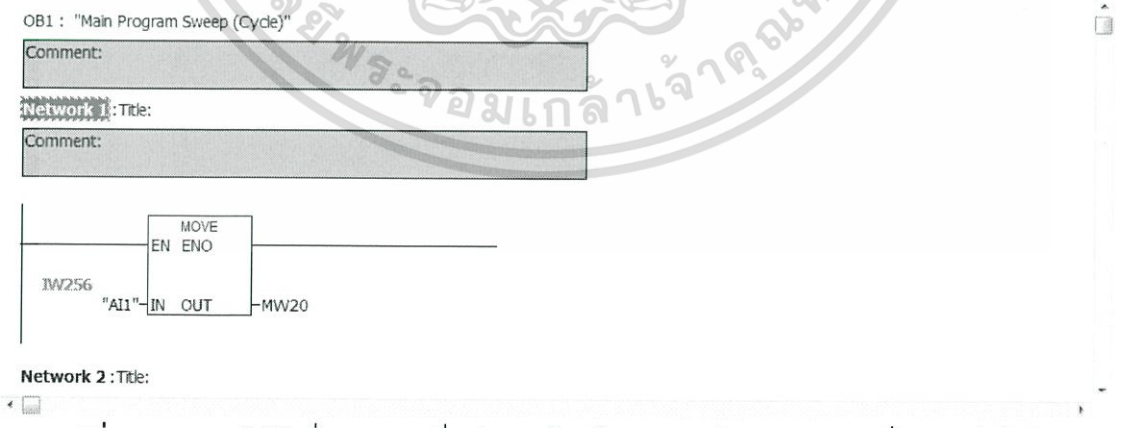
Address	Name	Type	Initial value	Comment
0.0		STRUCT		
+0.0	Out_Logic_Compare_AI1	BOOL	FALSE	Temporary placeholder variable
+0.1	Out_Logic_Compare_AI2	BOOL	FALSE	
+0.2	OUT_Logic_VALVE	BOOL	FALSE	
=2.0		END_STRUCT		

รูปที่ 3.17 ข้อมูลที่อยู่ภายใน DB2

3.4.4.2 เขียนโปรแกรมใน OB1

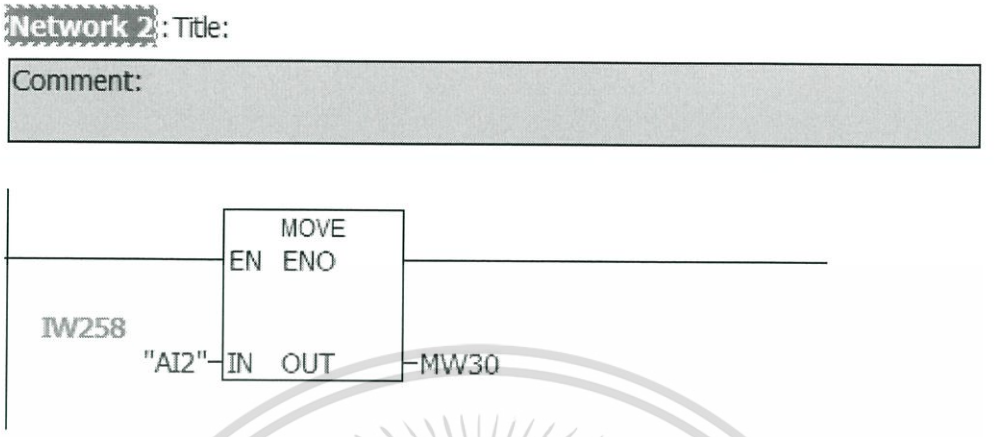
โดยเลือกดับเบิลคลิกที่ OB1 แล้วเขียนโปรแกรมดังนี้

Network 1: เป็นการเรียกใช้งานฟังก์ชัน Move เพื่อทำการย้ายข้อมูลจากอนาล็อก อินพุต ตัวที่ 1 มาเก็บไว้ในหน่วยความจำของตัวควบคุม (PLC) ที่ตำแหน่ง MW20 ดังรูปที่ 3.18



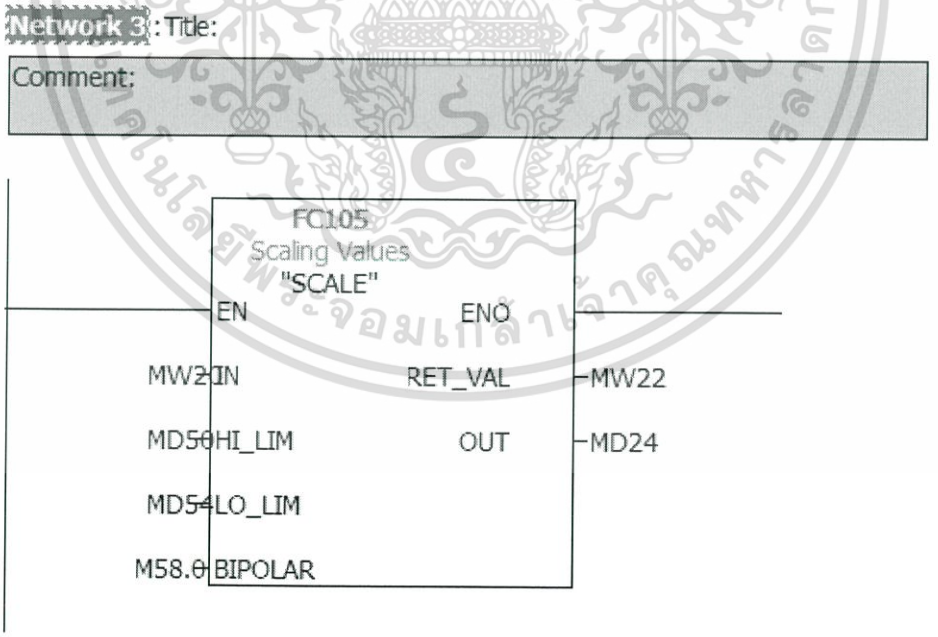
รูปที่ 3.18 การใช้คำสั่ง Move เพื่อทำการย้ายข้อมูล อนาล็อก อินพุต ตัวที่ 1 มาเก็บไว้ในหน่วยความจำของตัวควบคุม (PLC)

Network 2: เป็นการเรียกใช้งานฟังก์ชัน Move เพื่อทำการย้ายข้อมูลจากอนาล็อก อินพุต ตัวที่ 2 มาเก็บไว้ในหน่วยความจำของตัวควบคุม (PLC) ที่ตำแหน่ง MW30 ดังรูปที่ 3.19



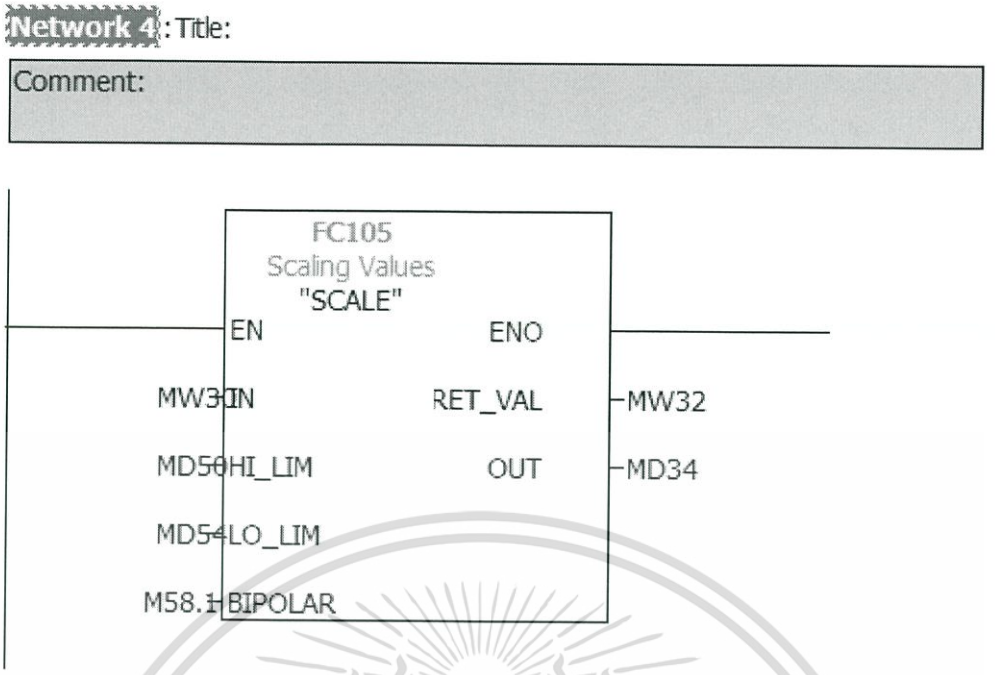
รูปที่ 3.19 การใช้คำสั่ง Move เพื่อทำการย้ายข้อมูลจาก อนาล็อก อินพุต ตัวที่ 2 มาเก็บไว้ในหน่วยความจำของตัวควบคุม (PLC)

Network 3: เป็นการเรียกใช้งานฟังก์ชันอนาล็อก สเกล (FC105) เพื่อทำการสเกลค่าอนาล็อก อินพุต ตัวที่ 1 ที่เข้ามา ให้อยู่ในช่วงที่ต้องการ (โดยในโครงงานนี้เป็นการสเกลค่าอนาล็อกอินพุตที่เข้ามาให้มีค่าอยู่ระหว่าง 0 ถึง 100%) ดังแสดงได้ดังรูปที่ 3.20



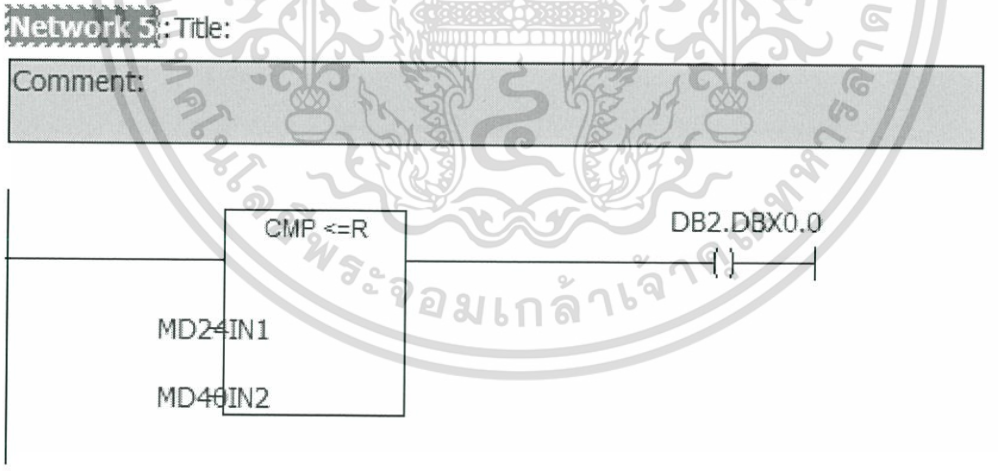
รูปที่ 3.20 การใช้งานฟังก์ชันอนาล็อก เสกล (FC105) เพื่อใช้เสกลค่าอนาล็อก อินพุต ตัวที่ 1

Network 4: เป็นการเรียกใช้งานฟังก์ชันอนาล็อก สเกล (FC105) เพื่อทำการสเกลค่าอนาล็อก อินพุต ตัวที่ 2 ที่เข้ามา ให้อยู่ในช่วงที่ต้องการ (โดยในโครงงานนี้เป็นการสเกลค่าอนาล็อกอินพุตที่เข้ามาให้มีค่าอยู่ระหว่าง 0 ถึง 100%) ดังแสดงได้ดังรูปที่ 3.21



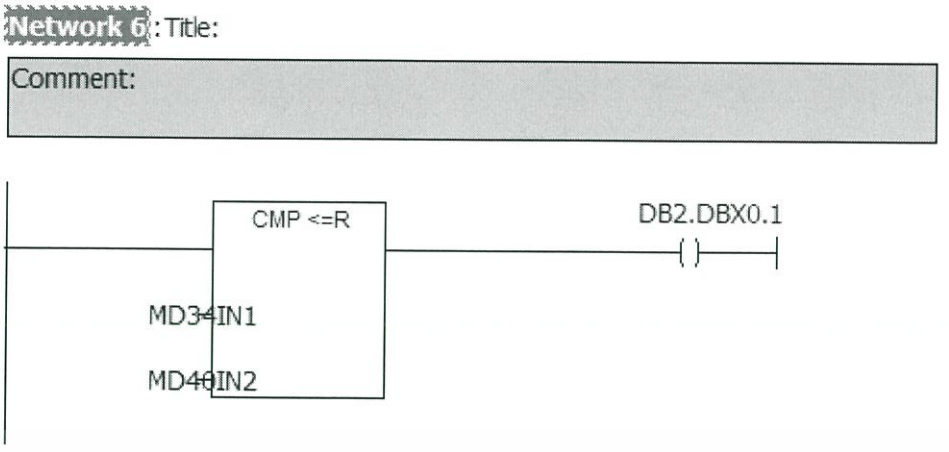
รูปที่ 3.21 การใช้งานฟังก์ชันอนาล็อก เสกล (FC105) เพื่อใช้เสกลค่าอนาล็อก อินพุต ตัวที่ 2

Network 5: เป็นการเรียกใช้งานฟังก์ชัน Compare (น้อยกว่าหรือเท่ากับ) เพื่อทำการเปรียบเทียบค่าอนาล็อก อินพุต ตัวที่ 1 (หลังจากเข้าฟังก์ชันสเกลแล้ว) กับค่า Set Point (โดยในโครงงานนี้ตั้งค่า Set Point เท่ากับ 80%) ดังรูปที่ 3.22



รูปที่ 3.22 ฟังก์ชัน Compare (น้อยกว่าหรือเท่ากับ) เพื่อทำการเปรียบเทียบระหว่างค่าอนาล็อก อินพุต ตัวที่ 1 กับค่า Set Point

Network 6: เป็นการเรียกใช้งานฟังก์ชัน Compare (น้อยกว่าหรือเท่ากับ) เพื่อทำการเปรียบเทียบค่าอนาล็อก อินพุต ตัวที่ 2 (หลังจากเข้าฟังก์ชันสเกลแล้ว) กับค่า Set Point (โดยในโครงงานนี้ตั้งค่า Set Point เท่ากับ 80%) ดังรูปที่ 3.23

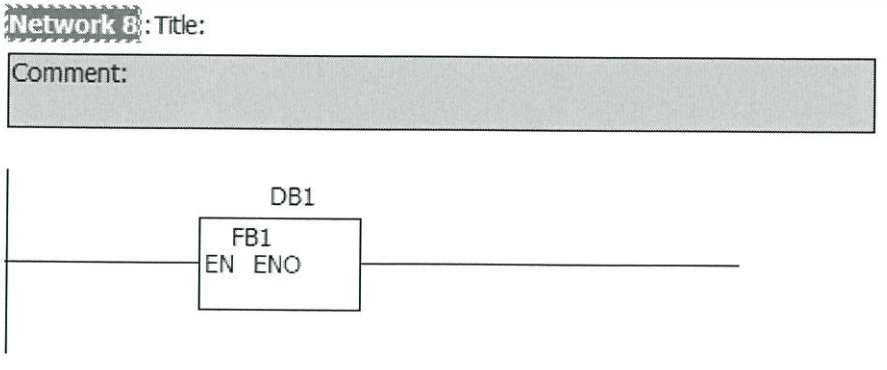


รูปที่ 3.23 ฟังก์ชัน Compare (น้อยกว่าหรือเท่ากับ) เพื่อทำการเปรียบเทียบระหว่างค่าอนาล็อกอินพุต ตัวที่ 2 กับค่า Set Point

Network 7: เป็นคำสั่งย้ายค่าเอาท์พุต ที่ได้จากฟังก์ชัน F_1oo2DI (FB190) มาเก็บไว้ใน DB2.DBX0.2 จากนั้นจึงนำเอาท์พุตจาก DB2.DBX0.2 มาเป็นคำสั่งเอาท์พุตสุดท้ายเพื่อไปทำการสั่ง ปิดหรือเปิดวาล์ว ดังรูปที่ 3.24

รูปที่ 3.24 คำสั่งปิดหรือเปิดวาล์ว

Network 8: เป็นการเรียกใช้งานคำสั่ง Call เพื่อเป็นคำสั่งเรียก Safety Program (FB1) ที่เราได้ทำการสร้าง F-Runtime Group ในขั้นตอนที่ 3.4.2 ดังรูปที่ 3.24

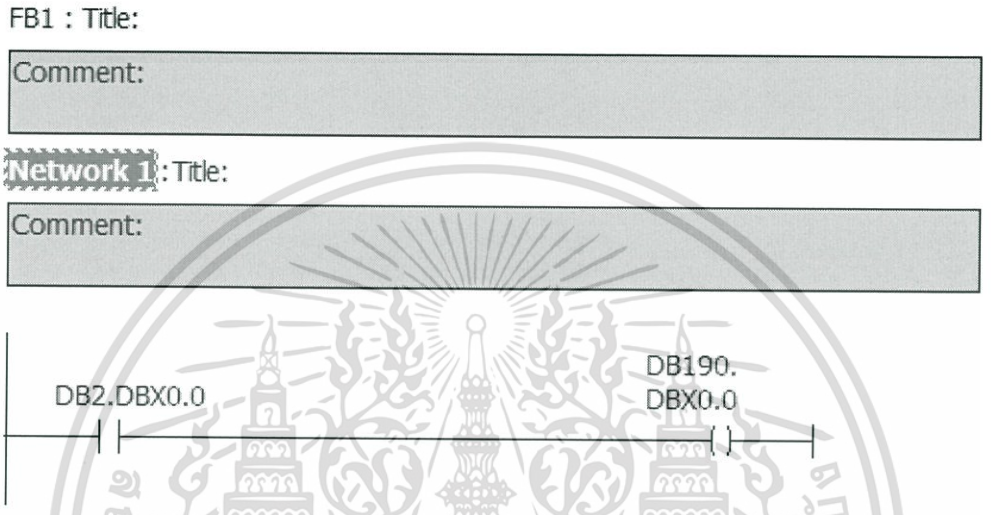


รูปที่ 3.25 การใช้คำสั่ง Call เพื่อเรียกใช้งาน Safety Program

3.4.4.3 เขียนโปรแกรมใน FB1 (Safety Program)

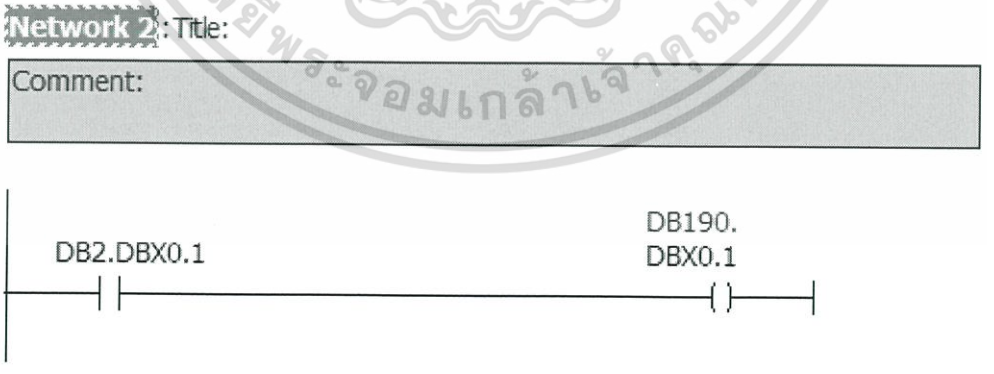
โดยเลือกดับเบิ้ลคลิกที่ FB1 แล้วเขียนโปรแกรมดังนี้

Network 1: เป็นการย้ายค่าอินพุตตัวที่ 1 จากโปรแกรมปรกติ (OB1) (หลังจากการทำการเปรียบเทียบกับค่า Set Point เรียบร้อยแล้ว) มาเก็บไว้ใน DB2.DBX0.0 เพื่อให้มาเป็นดิจิตอลอินพุตภายใน Safety Program (FB190) ดังรูปที่ 3.25



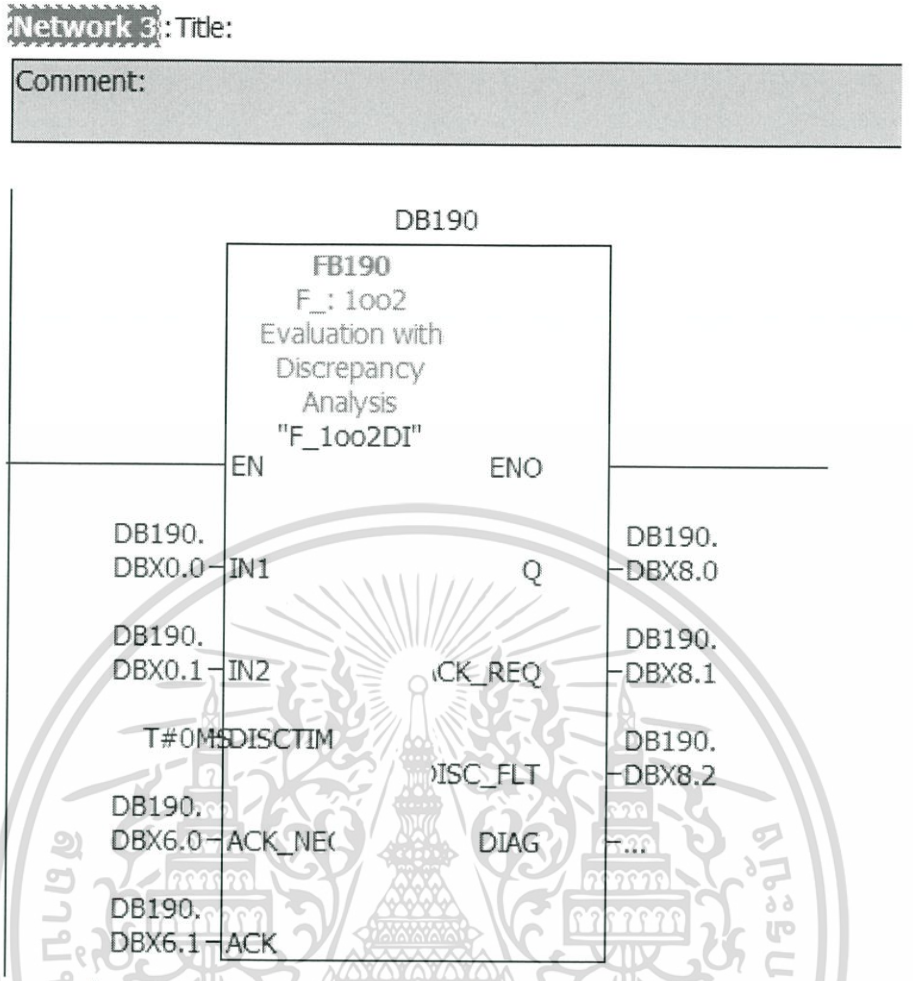
รูปที่ 3.26 การย้ายค่าอินพุตปรกติ ตัวที่ 1 (OB1) มาอยู่ใน Safety Program

Network 2: เป็นการย้ายค่าอินพุตตัวที่ 2 จากโปรแกรมปรกติ (OB1) (หลังจากการทำการเปรียบเทียบกับค่า Set Point เรียบร้อยแล้ว) มาเก็บไว้ใน DB2.DBX0.0 เพื่อให้มาเป็นดิจิตอลอินพุตภายใน Safety Program (FB190) ดังรูปที่ 3.26



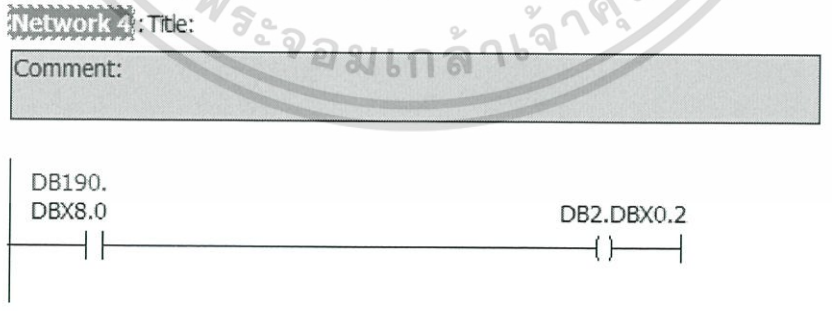
รูปที่ 3.27 การย้ายค่าอินพุตปรกติ ตัวที่ 2 (OB1) มาอยู่ใน Safety Program

Network 3: เรียกใช้งานฟังก์ชัน F_1oo2DI (Fb190) และเซตค่าพารามิเตอร์ต่างๆ ดังรูปที่ 3.27 โดยมีรายละเอียดของพารามิเตอร์ต่างๆภายในฟังก์ชัน ซึ่งได้ถูกอธิบายไว้ในหัวข้อ 3.4.3.1



รูปที่ 3.28 การเซตค่าพารามิเตอร์ภายในฟังก์ชัน F_1oo2DI (FB190)

Network 4: เป็นการนำเอาเอาท์พุตจากฟังก์ชัน F_1oo2DI (FB190) ไปเก็บไว้ใน DB2.DBX0.2 เพื่อนำไปใช้เป็นเอาท์พุตสั่งวาล์วให้ปิดหรือเปิดภายในโปรแกรมปรกติ (OB1)

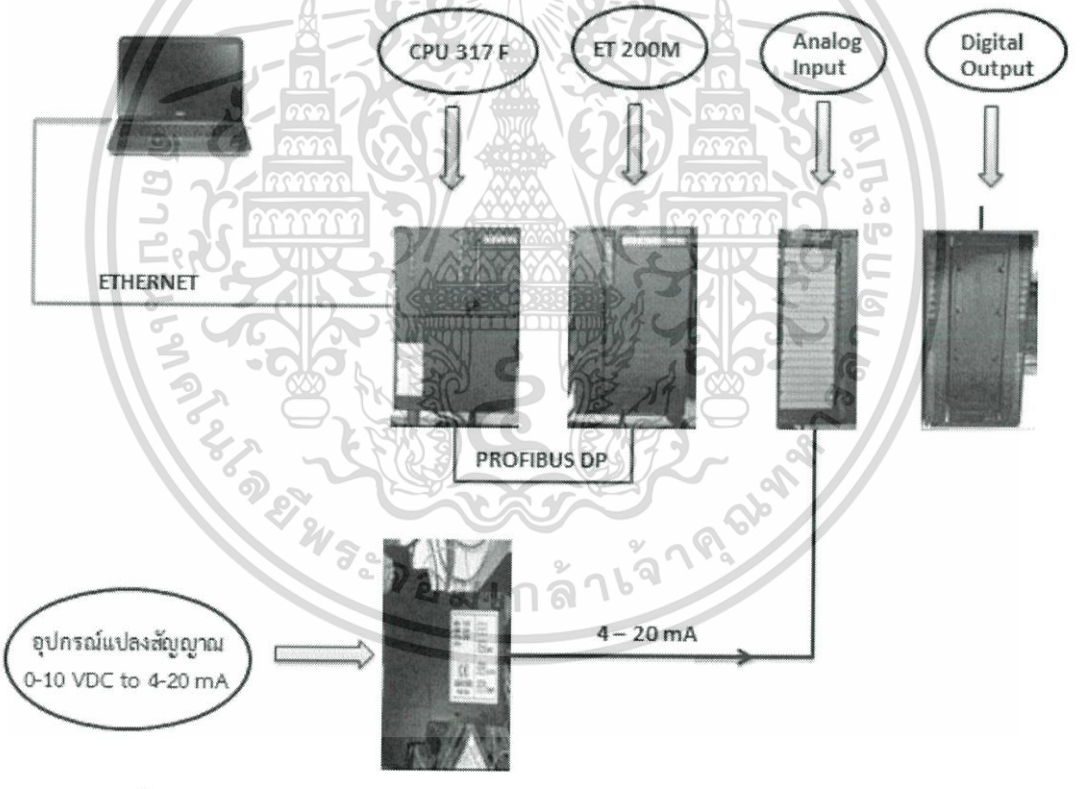


รูปที่ 3.29 การย้ายข้อมูลจากเอาท์พุตของฟังก์ชัน F_1oo2DI (FB190) ไปสั่งให้วาล์วปิดหรือเปิดภายในโปรแกรมปรกติ (OB1)

บทที่ 4
การทดลองและผลการทดลอง

4.1 คำนำ

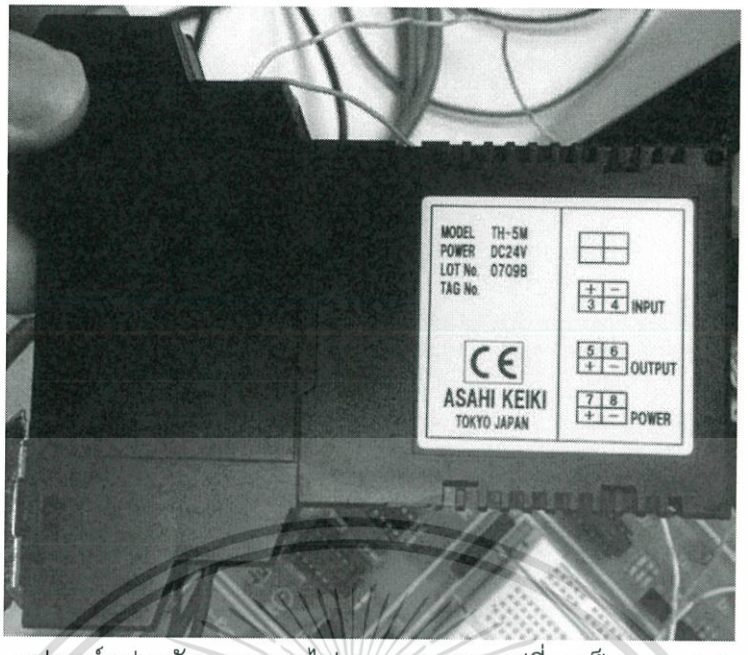
ในโครงงานนี้เป็นการทดลองและทดสอบใช้งาน Safety Program 1oo2DI Voting โดยในการออกแบบฟังก์ชัน 1oo2DI Voting นั้น ต้องการทำการออกแบบเพื่อไปสั่งงาน Shutdown Valve ที่มีรูปแบบการต่อใช้งานเป็น De-energize to trip โดยในการทดลอง เป็นการจำลองสัญญาณอินพุตจากอุปกรณ์วัด (Pressure Transmitter) ที่ได้ออกแบบมาในบทที่ 3 โดยการใช้อุปกรณ์แปลงสัญญาณจากไฟ 0 – 10 VDC เปลี่ยนเป็นกระแส 4 – 20 mA แล้วรับสัญญาณอินพุตเข้ามาผ่านอนาล็อก อินพุต โมดูล (Analog Output module) แล้วส่งเข้าฟังก์ชัน Safety Program 1oo2DI Voting ภายในตัวควบคุม (PLC) เพื่อนำสัญญาณเอาท์พุตจาก ดิจิตอล เอาท์พุต โมดูล (Digital Output module) สั่งปิดหรือเปิด Shut Down Valve ตามโปรแกรมที่ได้ออกแบบไว้ ดังรูปที่ 4.1



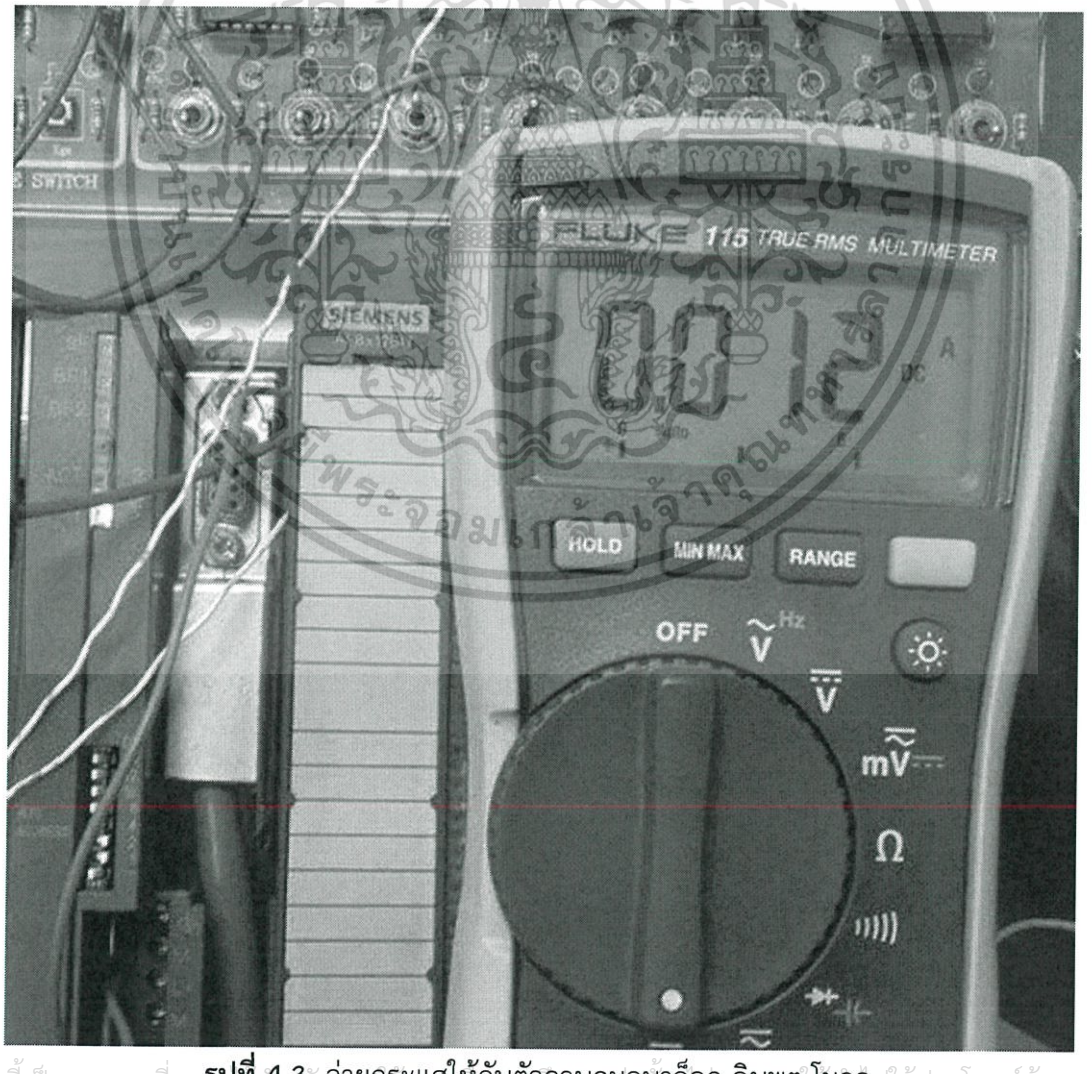
รูปที่ 4.1 สถาปัตยกรรมในการต่อการทดลองใช้งานฟังก์ชัน 1oo2DI Voting

4.2 วิธีการทดสอบอนาล็อกอินพุต โมดูล

การจ่ายกระแสฟ้าและวัดค่ากระแสไฟฟ้าให้กับตัวควบคุมอนาล็อกอินพุต โมดูล โดยอุปกรณ์แปลงสัญญาณไฟฟ้า 0 – 10 VDC เปลี่ยนเป็นกระแส 4 – 20 mA ดังในรูปที่ 4.2 สำหรับจ่ายกระแสให้กับตัวควบคุมอนาล็อก อินพุต โมดูล ดังรูปที่ 4.3



รูปที่ 4.2 อุปกรณ์แปลงสัญญาณจากไฟ 0 – 10 VDC เปลี่ยนเป็นกระแส 4 – 20 mA



รูปที่ 4.3 จ่ายกระแสให้กับตัวควบคุมอน้ำล็อก อินพุต โมดูล

4.3 วิธีการทดลอง

เนื่องจากในโครงงานนี้ไม่ได้มีการต่ออุปกรณ์อินพุต หรืออุปกรณ์เอาท์พุต (Field Instrument) เข้าไปจริงในการดำเนินงาน ดังนั้นในการที่จะดูผลการทดลองต่างๆนั้น จึงจำเป็นต้องดูในตาราง Variable Table (VAT) ภายในโปรแกรม SIMATIC Manager โดยวิธีการที่จะสร้างตาราง Variable Table (VAT) เพื่อมาดูค่าของตัวแปรหรือค่าพารามิเตอร์ต่างๆนั้น สามารถสร้างได้ตามวิธีการ ดังนี้

1. คลิกที่ SIMATIC 300(1) ใน Project window > CPU 317F-2PN/DP > S7 Program(1) > Blocks > คลิกขวาพื้นที่ว่าง > Insert New Object > Variable Table (VAT) จะได้ดังรูปที่ 4.4

VAT_1 -- Project\SIMATIC 300(1)\CPU 317F-2 PN/DP\S7 Program(1)

	Address	Symbol	Display format	Status value	Modify value
1					

รูปที่ 4.4 หน้าต่างของ Variable Table 1 (VAT1)

2. กำหนดค่าพารามิเตอร์ต่างๆที่สนใจในการทดลอง ดังรูปที่ 4.5

VAT_1 -- Project\SIMATIC 300(1)\CPU 317F-2 PN/DP\S7 Program(1)

	Address	Symbol	Display format	Status value	Modify value
1	IW 256	"AI1"	DEC		
2	IW 258	"AI2"	DEC		
3	MD 24		FLOATING_POINT		
4	MD 34		FLOATING_POINT		
5	MD 40		FLOATING_POINT		
6	MD 50		FLOATING_POINT		
7	MD 54		FLOATING_POINT		
8	DB2.DBX 0.0		BOOL		
9	DB2.DBX 0.1		BOOL		
10	DB190.DBX 0.0		BOOL		
11	DB190.DBX 0.1		BOOL		
12	DB190.DBX 6.0		BOOL		
13	DB190.DBX 6.1		BOOL		
14					
15	DB190.DBX 8.1		BOOL		
16	DB190.DBX 8.2		BOOL		
17	DB190.DBX 8.0		BOOL		
18	Q 0.0	"OUT_Valve"	BOOL		

รูปที่ 4.5 ค่าพารามิเตอร์ที่สนใจในการทดลอง

จากรูปที่ 4.5 นั้นสามารถอธิบายค่าพารามิเตอร์ที่อยู่ภายใน Variable Table 1 (VAT1) ได้ดังนี้

- IW 256 คือ ค่าอินพุต ตัวที่ 1 ที่เข้ามาในอนาล็อก อินพุต โมดูล
- IW 258 คือ ค่าอินพุต ตัวที่ 2 ที่เข้ามาในอนาล็อก อินพุต โมดูล
- MD 24 คือ ค่าอินพุต ตัวที่ 1 หลังจากผ่านฟังก์ชันสเกลอินพุต (ซึ่งจะมีค่าอยู่ระหว่าง 0 – 100 เปอร์เซ็นต์)
- MD 34 คือ ค่าอินพุต ตัวที่ 2 หลังจากผ่านฟังก์ชันสเกลอินพุต (ซึ่งจะมีค่าอยู่ระหว่าง 0 – 100 เปอร์เซ็นต์)
- MD 40 คือ Set Point (ซึ่งถูกกำหนดไว้ที่ 80%)
- MD 50 คือ ค่าสูงสุดของฟังก์ชันสเกลอินพุต (ซึ่งถูกกำหนดให้เท่ากับ 100)
- MD 54 คือ ค่าต่ำสุดของฟังก์ชันสเกลอินพุต (ซึ่งถูกกำหนดให้เท่ากับ 0)
- DB2.DBX 0.0 คือ เอาท์พุตโลจิกของอินพุตตัวที่ 1 ที่ผ่านฟังก์ชัน Compare เปรียบเทียบกับค่า Set Point
- DB2.DBX 0.1 คือ เอาท์พุตโลจิกของอินพุตตัวที่ 2 ที่ผ่านฟังก์ชัน Compare เปรียบเทียบกับค่า Set Point
- DB190.DBX 0.0 คือ อินพุตโลจิกตัวที่ 1 ของฟังก์ชัน 1oo2DI (FC 105)
- DB190.DBX 0.1 คือ อินพุตโลจิกตัวที่ 2 ของฟังก์ชัน 1oo2DI (FC 105)
- DB190.DBX 6.0 คือ ขา ACK_NEC ของฟังก์ชัน 1oo2DI (FC 105) โดยจะมีค่าเท่ากับ 1 เพราะในการทดลองเป็นการคิดที่มีการตอบสนองต่อค่าความผิดพลาดที่เกิดขึ้นจากความแตกต่างของเวลา (discrepancy error)
- DB190.DBX 6.1 คือ ขา ACK ของฟังก์ชัน 1oo2DI (FC 105) (เป็นส่วนของการตอบสนองต่อสัญญาณเตือนความผิดพลาดที่เกิดขึ้น: Acknowledgement)
- DB190.DBX 8.1 คือ ขา ACK_REQ ของฟังก์ชัน 1oo2DI (FC 105) จะมีการแสดงสถานะก็ต่อเมื่อระบบเกิดความผิดพลาดขึ้นเท่านั้น (DISC_FLT มีค่าเท่ากับ 1) โดยถ้าเป็นลอจิก 1 หมายความว่า IN1 และ IN2 มีความเหมือนกันของสัญญาณที่เข้ามา และถ้าลอจิกเป็น 0 หมายความว่า IN1 และ IN2 มีความแตกต่างกันของสัญญาณที่เข้ามา
- DB190.DBX 8.2 คือ ขา DISC_FLT ของฟังก์ชัน 1oo2DI (FC 105) ถ้าเป็นลอจิก 0 จะหมายถึงว่ายังไม่มีความผิดพลาดเกิดขึ้นภายในระบบ และถ้าหากมีลอจิกเท่ากับ 1 หมายความว่าระบบนั้นเกิดความผิดพลาดแล้ว
- DB190.DBX 8.0 คือ เอาท์พุตโลจิก ของฟังก์ชัน 1oo2DI (FC 105)
- Q 0.0 คือ เอาท์พุตโลจิกที่ส่งไปยัง ดิจิตอล เอาท์พุต โมดูล เพื่อสั่งงานไปยัง Shutdown Valve โดยถ้ามีค่าเท่ากับ 1 นั้น จะมีการจ่ายไฟไปให้กับ Shutdown Valve และถ้ามีค่าเท่ากับ 0 นั้น จะไม่มีการจ่ายไฟไปให้กับ Shutdown Valve

4.4 ผลการทดลอง

4.4.1 กรณีที่อินพุตทั้งสองตัวตรวจจับค่าได้เท่ากัน และมีค่าน้อยกว่าค่า Set Point

กรณีสมมติที่อุปกรณ์การวัด Pressure Transmitter ตัวที่ 1 และตัวที่ 2 ตรวจจับค่าได้ทั้งสองตัวเท่ากันและมีค่าอยู่ในระดับที่ต่ำกว่าค่า Set Point (Set Point มีค่าเท่ากับ 80%) โดยสมมติให้ Pressure Transmitter ทั้งสองตัวตรวจจับค่าได้เท่ากับ 12 mA หรือเท่ากับ 50% ดังแสดงได้ดังรูปที่ 4.6

VAT_1 -- @Project\SIMATIC 300(1)\CPU 317F-2 PN/DP\S7 Program(1) ONLINE

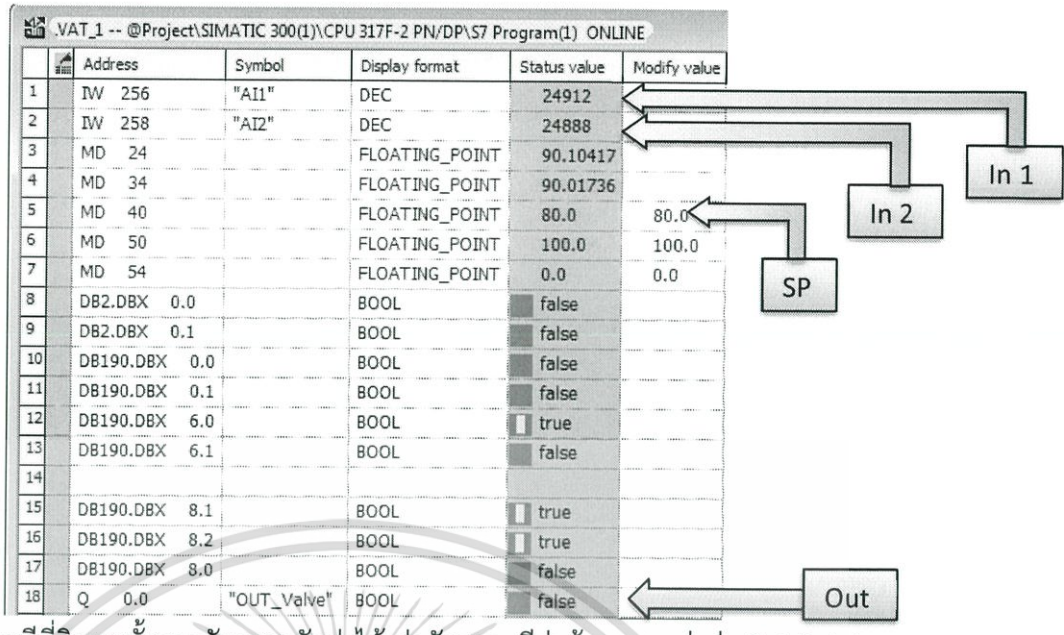
	Address	Symbol	Display format	Status value	Modify value
1	IW 256	"AI1"	DEC	13840	
2	IW 258	"AI2"	DEC	13816	
3	MD 24		FLOATING_POINT	50.05787	
4	MD 34		FLOATING_POINT	49.97107	
5	MD 40		FLOATING_POINT	80.0	80.0
6	MD 50		FLOATING_POINT	100.0	100.0
7	MD 54		FLOATING_POINT	0.0	0.0
8	DB2.DBX 0.0		BOOL	true	
9	DB2.DBX 0.1		BOOL	true	
10	DB190.DBX 0.0		BOOL	true	
11	DB190.DBX 0.1		BOOL	true	
12	DB190.DBX 6.0		BOOL	true	
13	DB190.DBX 6.1		BOOL	false	
14					
15	DB190.DBX 8.1		BOOL	false	
16	DB190.DBX 8.2		BOOL	false	
17	DB190.DBX 8.0		BOOL	true	
18	Q 0.0	"OUT_Valve"	BOOL	true	

In 1
In 2
SP
Out

รูปที่ 4.6 กรณีที่อินพุตทั้งสองตัวตรวจจับค่าได้เท่ากัน และมีค่าน้อยกว่าค่า Set Point

4.4.2 กรณีที่อินพุตทั้งสองตัวตรวจจับค่าได้เท่ากัน และมีค่ามากกว่าค่า Set Point

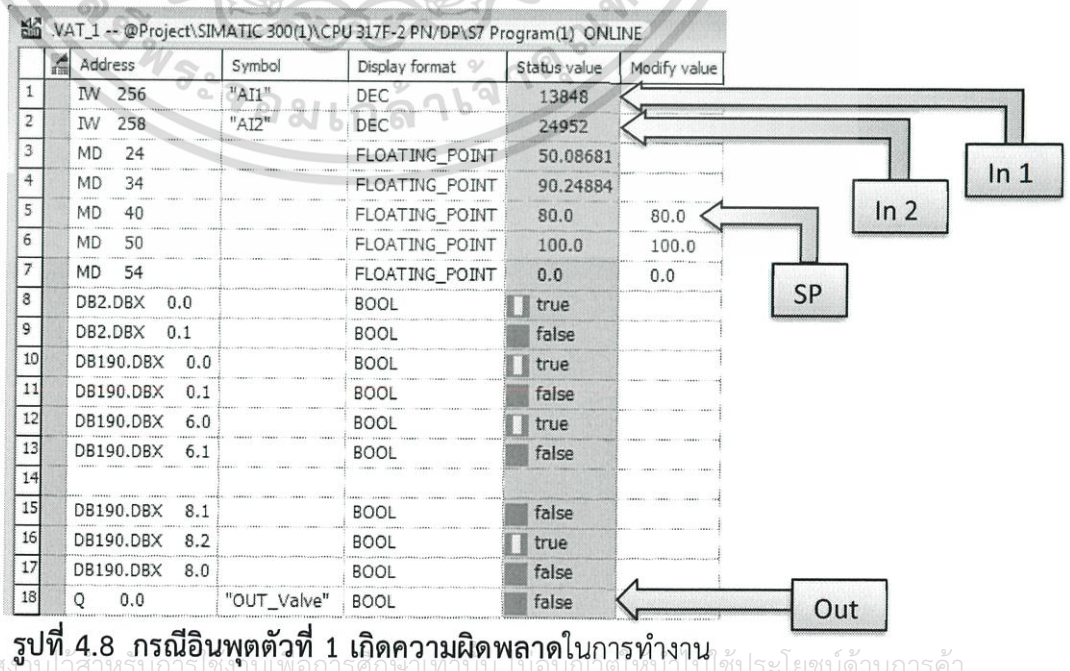
กรณีสมมติที่อุปกรณ์การวัด Pressure Transmitter ตัวที่ 1 และตัวที่ 2 ตรวจจับค่าได้ทั้งสองตัวเท่ากันและมีค่าอยู่ในระดับที่สูงกว่าค่า Set Point (Set Point มีค่าเท่ากับ 80%) โดยสมมติให้ Pressure Transmitter ทั้งสองตัวตรวจจับค่าได้เท่ากับ 18.4 mA หรือเท่ากับ 90% ดังแสดงได้ดังรูปที่ 4.7



รูปที่ 4.7 กรณีที่อินพุตทั้งสองตัวตรวจจับค่าได้เท่ากัน และมีค่าน้อยมากกว่าค่า Set Point

4.4.3 กรณีอินพุตตัวที่ 1 เกิดความผิดพลาดในการทำงาน

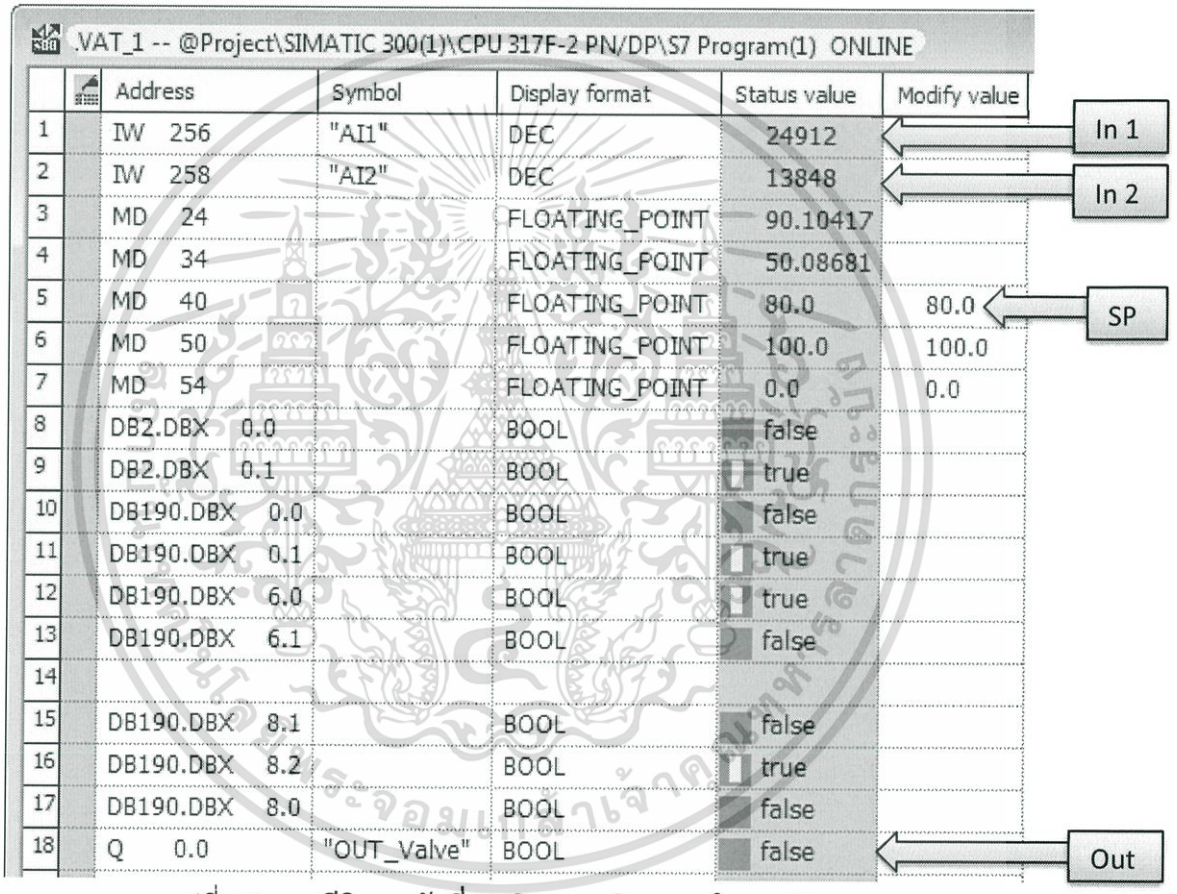
กรณีสมมติที่สมมติให้อุปกรณ์การวัด Pressure Transmitter ตัวที่ 1 เกิดความผิดพลาดในการทำงาน (อาจเกิดมาจากอุปกรณ์เกิดความเสียหาย หรือผิดพลาดในการตรวจจับค่า) โดยค่าที่ตรวจจับได้นั้นมีค่าต่ำกว่าค่า Set Point ที่กำหนด (Set Point มีค่าเท่ากับ 80%) โดยสมมติให้ Pressure Transmitter ตัวที่ 1 ตรวจจับค่าได้เท่ากับ 12 mA (หรือเท่ากับ 50%) และสมมติให้อุปกรณ์การวัด Pressure Transmitter ตัวที่ 2 ตรวจจับค่าได้ถูกต้องและมีค่าอยู่ในระดับที่มากกว่าค่า Set Point โดยสมมติให้ Pressure Transmitter ตัวที่ 2 ตรวจจับค่าได้เท่ากับ 18.4 mA หรือเท่ากับ 90% ดังรูปที่ 4.8



รูปที่ 4.8 กรณีอินพุตตัวที่ 1 เกิดความผิดพลาดในการทำงาน

4.4.4 กรณีอินพุตตัวที่ 2 เกิดความผิดพลาดในการทำงาน

กรณีสมมติที่สมมติให้อุปกรณ์การวัด Pressure Transmitter ตัวที่ 2 เกิดความผิดพลาดในการทำงาน (อุปกรณ์เกิดความเสียหาย หรือตรวจจับค่าได้ผิดพลาด) โดยค่าที่ตรวจจับได้นั้นมีค่าต่ำกว่าค่า Set Point ที่กำหนด (Set Point มีค่าเท่ากับ 80%) โดยสมมติให้ Pressure Transmitter ตัวที่ 2 ตรวจจับค่าได้เท่ากับ 12 mA (หรือเท่ากับ 50%) และสมมติให้อุปกรณ์การวัด Pressure Transmitter ตัวที่ 1 ตรวจจับค่าได้ถูกต้องและมีค่าอยู่ในระดับที่มากกว่าค่า Set Point โดยสมมติให้ Pressure Transmitter ตัวที่ 1 ตรวจจับค่าได้เท่ากับ 18.4 mA หรือเท่ากับ 90% ดังรูปที่ 4.9



	Address	Symbol	Display format	Status value	Modify value
1	IW 256	"AI1"	DEC	24912	
2	IW 258	"AI2"	DEC	13848	
3	MD 24		FLOATING_POINT	90.10417	
4	MD 34		FLOATING_POINT	50.08681	
5	MD 40		FLOATING_POINT	80.0	80.0
6	MD 50		FLOATING_POINT	100.0	100.0
7	MD 54		FLOATING_POINT	0.0	0.0
8	DB2.DBX 0.0		BOOL	false	
9	DB2.DBX 0.1		BOOL	true	
10	DB190.DBX 0.0		BOOL	false	
11	DB190.DBX 0.1		BOOL	true	
12	DB190.DBX 6.0		BOOL	true	
13	DB190.DBX 6.1		BOOL	false	
14					
15	DB190.DBX 8.1		BOOL	false	
16	DB190.DBX 8.2		BOOL	true	
17	DB190.DBX 8.0		BOOL	false	
18	Q 0.0	"OUT_Valve"	BOOL	false	

รูปที่ 4.9 **กรณีอินพุตตัวที่ 2 เกิดความผิดพลาดในการทำงาน**

บทที่ 5
สรุปผลการทดลอง

5.1 สรุปผลการทดลอง

โครงงานนี้ได้ทำการศึกษาและวิจัยขั้นตอนการออกแบระบบวัดคุมนิรภัย (Safety Instrumented System: SIS) โดยดำเนินงานตามมาตรฐาน IEC 61508 และมาตรฐาน IEC 61511 ด้วยการศึกษาขั้นตอนการออกแบบระบบวัดคุมนิรภัยของมาตรฐาน IEC 61511 (มาตรฐานสำหรับผู้ใช้งาน: User) ซึ่งในมาตรฐานนั้นมีด้วยกันอยู่ 8 ขั้นตอนด้วยกัน แต่ในโครงงานนี้ได้ดำเนินการจัดทำเพียง 4 ขั้นตอนเท่านั้น (ขั้นตอนที่ 1 ถึงขั้นตอนที่ 4) เนื่องมาจากในโครงงานนี้ไม่ได้มีการติดตั้งอุปกรณ์ความปลอดภัยจริงเข้าไปในกระบวนการ และได้ทำการออกแบบ Safety program แบบ 1oo2DI Voting เพื่อใช้ป้องกันการเกิดอันตรายที่จะเกิดขึ้นในกระบวนการผลิต

โดยการทดลองนั้น เริ่มตั้งแต่การตั้งค่าอุปกรณ์ควบคุม (PLC) และอุปกรณ์การเชื่อมต่อของระบบ รวมไปถึงการสร้างฟังก์ชันความปลอดภัย (Safety Program) เพื่อช่วยลดและป้องกันการเกิดอันตรายในกระบวนการผลิต และดำเนินการเขียน Safety program ให้สอดคล้องกับเงื่อนไขที่ต้องการ

5.2 วิเคราะห์ปัญหาและข้อเสนอแนะ

เนื่องจากการออกแบบระบบวัดคุมนิรภัย (Safety Instrumented System: SIS) การใช้โปรแกรมและการออกแบบฟังก์ชันความปลอดภัย (Safety Program) มีความซับซ้อนเป็นอย่างมาก และยังเป็นการศึกษาเฉพาะกลุ่มอีกด้วย ทำให้ต้องศึกษาทำความเข้าใจในระบบเป็นอย่างมาก ต้องศึกษาการใช้งานตัวควบคุม (PLC) ในโหมดความปลอดภัย (Safety Mode) และวิธีการเขียนฟังก์ชันความปลอดภัย (Safety Program) ให้ตรงกับการออกแบบใช้งาน ดังนั้นเวลาจะทำการปรับเปลี่ยนหรือกำหนดค่าเพื่อใช้งาน จะต้องดำเนินการทำให้สัมพันธ์กันเป็นเชิงวิศวกรรม เพื่อให้สามารถใช้งานได้จริงตามวัตถุประสงค์ นอกจากนี้ยังต้องสร้างความชำนาญและการปฏิบัติอย่างสม่ำเสมอก็จะทำให้การออกแบบและใช้งานฟังก์ชันความปลอดภัยมีความสมบูรณ์ยิ่งขึ้น

บรรณานุกรม

ทวิช ชูเมือง. 2551. **การกำหนดค่าระดับความปลอดภัยสำหรับฟังก์ชันนิรภัย**. กรุงเทพฯ : ดวงกมลสมัย จำกัด

ทวิช ชูเมือง. 2548. **ระบบวัดคุมนิรภัยในอุตสาหกรรมกระบวนการผลิต**. กรุงเทพฯ : ซีเอ็ดยูเคชั่น

IEC 61508, Function Safety of Electrical/Electronic/Programmable Electronic Safety-Related System.

IEC 61511, Function safety-Safety instrumented system for the process industry sector.

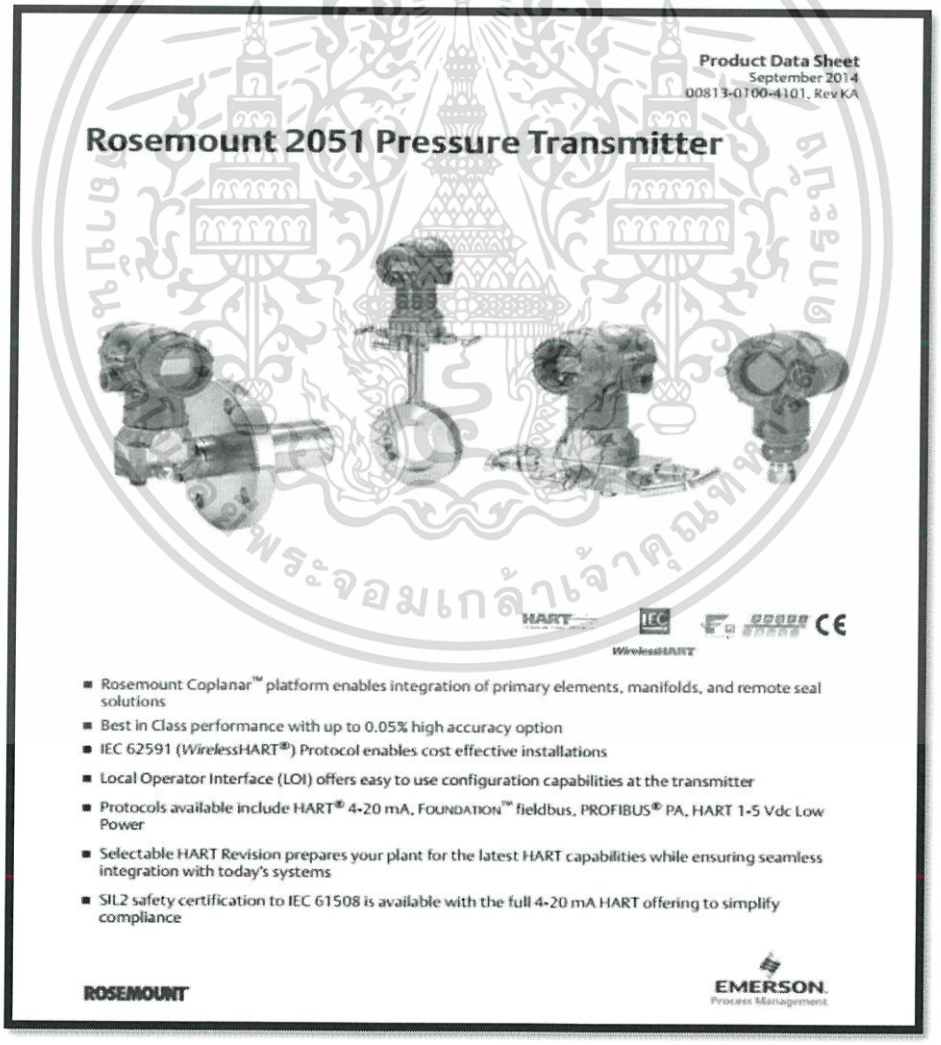
ภาคผนวก ก

ค่าพารามิเตอร์ของอุปกรณ์ในฟังก์ชันวัดคุมนิรภัย (Safety Instrumented Function)

ก.1. อุปกรณ์ที่เลือกใช้และค่าพารามิเตอร์ในการหาค่า PFD_{AVG} และ SFF

ในการออกแบบระบบวัดคุมนิรภัยนั้นการจะได้มาซึ่งค่าระดับความปลอดภัย(SIL) ต้องพิจารณาตัวแปร 2 ตัวที่มีความสำคัญมากคือ SFF และ PFD_{AVG} ซึ่งในภาคผนวก ก.1 จะแสดงรายละเอียดของค่าพารามิเตอร์ในแต่ละส่วนของระบบวัดคุมนิรภัยทั้งหมดที่ใช้ในการคำนวณค่าระดับความปลอดภัย

ก.1.1 Sensor Part



Product Data Sheet
September 2014
00813-0100-4101, Rev KA

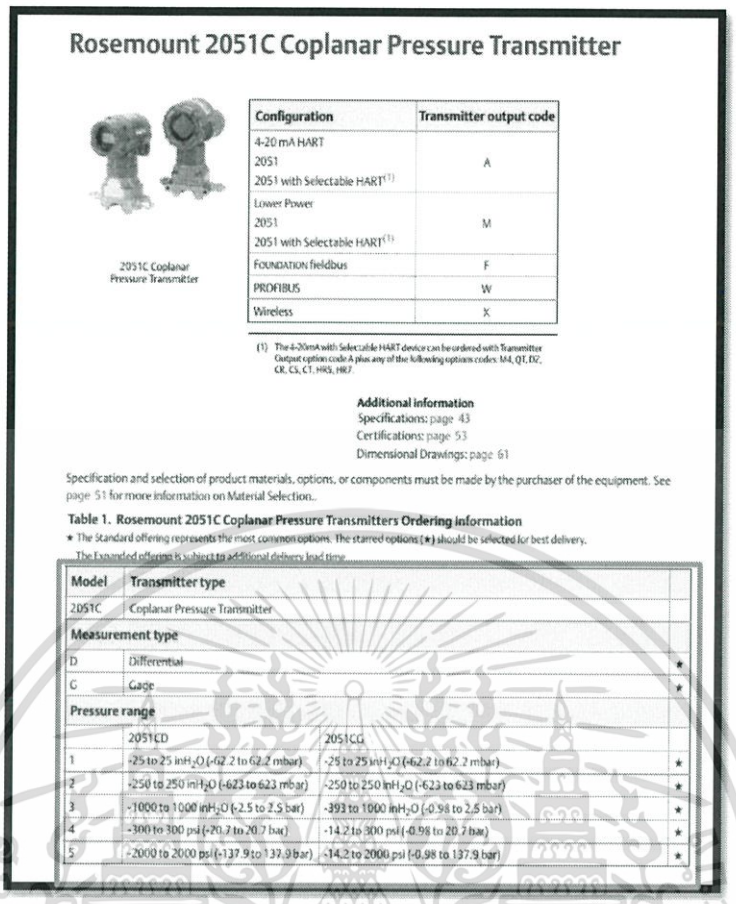
Rosemount 2051 Pressure Transmitter

- Rosemount Coplanar™ platform enables integration of primary elements, manifolds, and remote seal solutions
- Best in Class performance with up to 0.05% high accuracy option
- IEC 62591 (*Wireless*HART®) Protocol enables cost effective installations
- Local Operator Interface (LOI) offers easy to use configuration capabilities at the transmitter
- Protocols available include HART® 4-20 mA, FOUNDATION™ fieldbus, PROFIBUS® PA, HART 1-5 Vdc Low Power
- Selectable HART Revision prepares your plant for the latest HART capabilities while ensuring seamless integration with today's systems
- SIL2 safety certification to IEC 61508 is available with the full 4-20 mA HART offering to simplify compliance

ROSEMOUNT

EMERSON. Process Management

รูปที่ 1 ก แสดงรุ่นของอุปกรณ์วัด (Pressure Transmitter) ที่เลือกใช้งาน



Rosemount 2051C Coplanar Pressure Transmitter

2051C Coplanar Pressure Transmitter

Configuration	Transmitter output code
4-20 mA HART 2051 2051 with Selectable HART(1)	A
Lower Power 2051 2051 with Selectable HART(1)	M
FOUNDATION fieldbus	F
PROFIBUS	W
Wireless	X

(1) The 4-20mA with Selectable HART device can be ordered with Transmitter Output option code A plus any of the following options codes: M4, QT, D2, CR, CS, CT, HR5, HR7.

Additional information
Specifications: page 43
Certifications: page 53
Dimensional Drawings: page 61

Specification and selection of product materials, options, or components must be made by the purchaser of the equipment. See page 51 for more information on Material Selection..

Table 1. Rosemount 2051C Coplanar Pressure Transmitters Ordering Information

★ The Standard offering represents the most common options. The starred options (★) should be selected for best delivery.
The Expanded offering is subject to additional delivery lead time.

Model	Transmitter type		
2051C	Coplanar Pressure Transmitter		
Measurement type			
D	Differential		★
G	Gage		★
Pressure range			
	2051CD	2051CG	
1	-25 to 25 inH$_2$O (-62.2 to 62.2 mbar)	-25 to 25 inH$_2$O (-62.2 to 62.2 mbar)	★
2	-250 to 250 inH$_2$O (-623 to 623 mbar)	-250 to 250 inH$_2$O (-623 to 623 mbar)	★
3	-1000 to 1000 inH$_2$O (-2.5 to 2.5 bar)	-393 to 1000 inH$_2$O (-0.98 to 2.5 bar)	★
4	-300 to 300 psi (-20.7 to 20.7 bar)	-14.2 to 300 psi (-0.98 to 20.7 bar)	★
5	-2000 to 2000 psi (-137.9 to 137.9 bar)	-14.2 to 2000 psi (-0.98 to 137.9 bar)	★

รูปที่ 2 ก แสดง Model ของอุปกรณ์วัดที่เลือกใช้งาน Rosemount 2051 Coplanar Pressure Transmitter

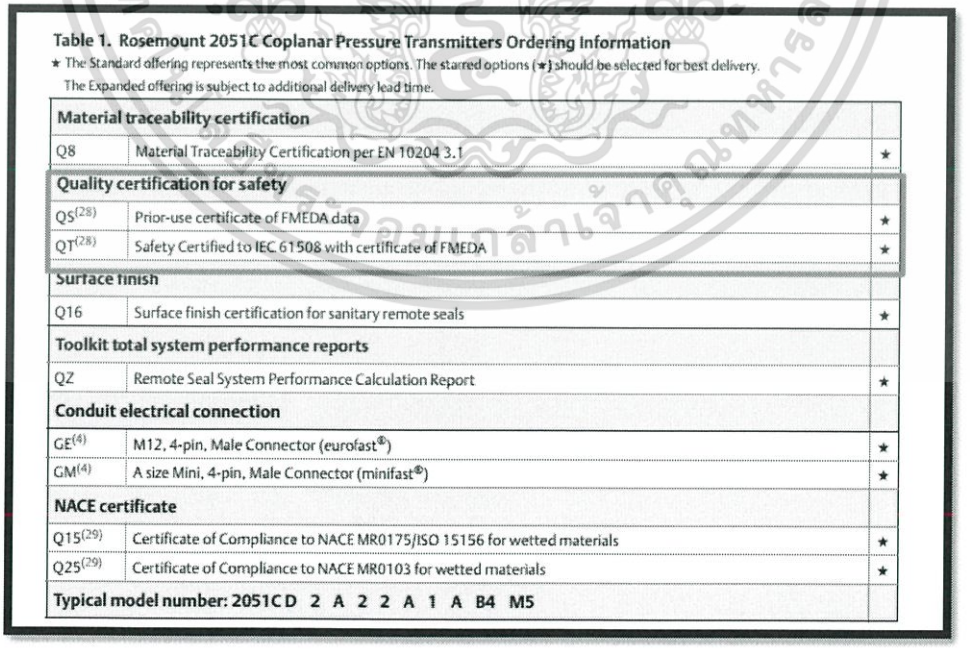
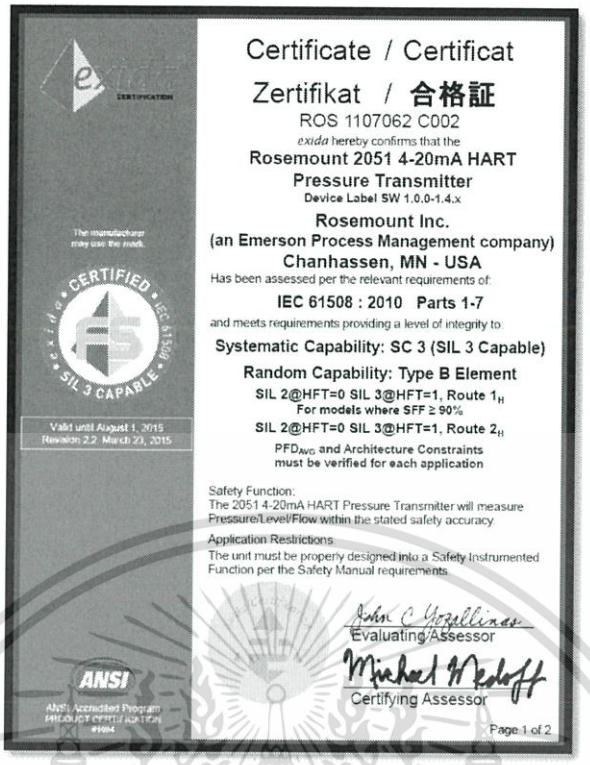


Table 1. Rosemount 2051C Coplanar Pressure Transmitters Ordering Information

★ The Standard offering represents the most common options. The starred options (★) should be selected for best delivery.
The Expanded offering is subject to additional delivery lead time.

Material traceability certification		
Q8	Material Traceability Certification per EN 10204 3.1	★
Quality certification for safety		
QS(28)	Prior-use certificate of FMEDA data	★
QT(28)	Safety Certified to IEC 61508 with certificate of FMEDA	★
Surface finish		
Q16	Surface finish certification for sanitary remote seals	★
Toolkit total system performance reports		
QZ	Remote Seal System Performance Calculation Report	★
Conduit electrical connection		
GE(4)	M12, 4-pin, Male Connector (eurofast®)	★
GM(4)	A size Mini, 4-pin, Male Connector (minifast®)	★
NACE certificate		
Q15(29)	Certificate of Compliance to NACE MR0175/ISO 15156 for wetted materials	★
Q25(29)	Certificate of Compliance to NACE MR0103 for wetted materials	★
Typical model number: 2051C D 2 A 2 2 A 1 A B4 M5		

รูปที่ 3 ก แสดงการผ่านการรับรองการใช้งานในโหมด Safety ของอุปกรณ์วัดที่เลือกใช้งานจาก FMEDA



Certificate / Certificat

Zertifikat / 合格証

ROS 1107062 C002

exida hereby confirms that the

Rosemount 2051 4-20mA HART Pressure Transmitter

Device Label SW 1.0.0-1.4.x

Rosemount Inc.

(an Emerson Process Management company)

Chanhassen, MN - USA

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2@HFT=0 SIL 3@HFT=1, Route 1_H

For models where SFF ≥ 90%

SIL 2@HFT=0 SIL 3@HFT=1, Route 2_H

PFD_{AVG} and Architecture Constraints must be verified for each application

Safety Function:

The 2051 4-20mA HART Pressure Transmitter will measure Pressure/Level/Flow within the stated safety accuracy.

Application Restrictions:

The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

The manufacturer may use the mark.

CERTIFIED IEC 61508 SIL 3 CAPABLE

Valid until August 1, 2015

Revision 2.2 March 23, 2015

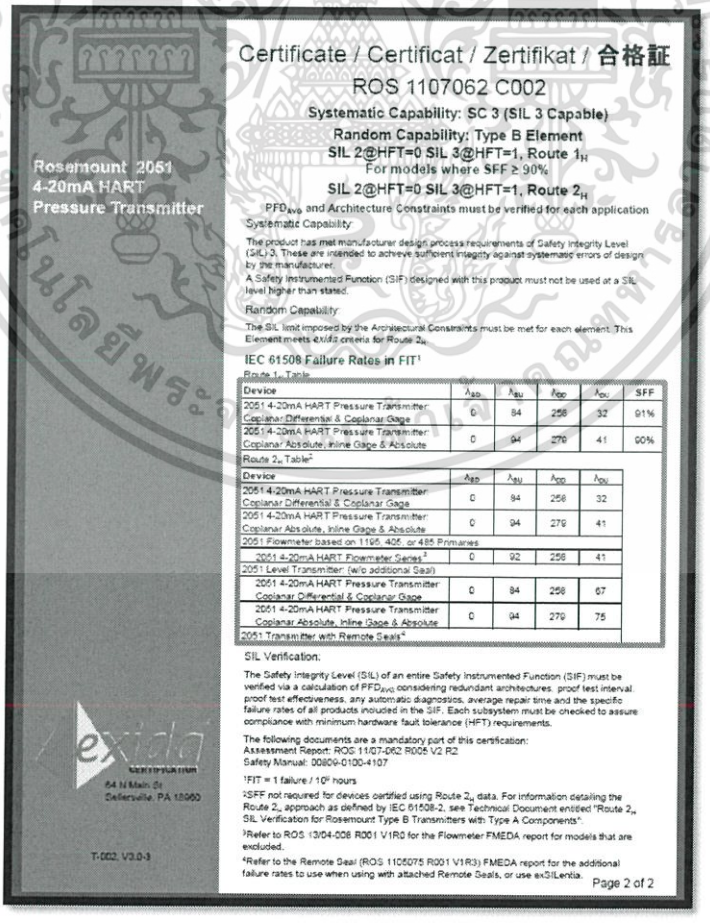
ANSI Accredited Program PRODUCT CERTIFICATION #1004

Evaluating Assessor

Certifying Assessor

Page 1 of 2

รูปที่ 4 ก แสดงใบ Certificate ของอุปกรณ์วัด (Pressure Transmitter) ที่เลือกใช้งาน



Rosemount 2051 4-20mA HART Pressure Transmitter

Certificate / Certificat / Zertifikat / 合格証

ROS 1107062 C002

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2@HFT=0 SIL 3@HFT=1, Route 1_H

For models where SFF ≥ 90%

SIL 2@HFT=0 SIL 3@HFT=1, Route 2_H

PFD_{AVG} and Architecture Constraints must be verified for each application

Systematic Capability:

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This Element meets *exida* criteria for Route 2_H.

IEC 61508 Failure Rates in FIT[1]

Route 1_H Table

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
2051 4-20mA HART Pressure Transmitter: Coplanar Differential & Coplanar Gage	0	84	258	32	91%
2051 4-20mA HART Pressure Transmitter: Coplanar Absolute, Inline Gage & Absolute	0	94	270	41	90%

Route 2_H Table[2]

Device	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
2051 4-20mA HART Pressure Transmitter: Coplanar Differential & Coplanar Gage	0	84	258	32
2051 4-20mA HART Pressure Transmitter: Coplanar Absolute, Inline Gage & Absolute	0	94	270	41
2051 Flowmeter based on 1195, 405, or 485 Primaries				
2051 4-20mA HART Flowmeter Series[3]	0	92	256	41
2051 Level Transmitter: (w/o additional Seal)				
2051 4-20mA HART Pressure Transmitter: Coplanar Differential & Coplanar Gage	0	84	258	67
2051 4-20mA HART Pressure Transmitter: Coplanar Absolute, Inline Gage & Absolute	0	94	270	75
2051 Transmitter with Remote Seals[4]				

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of this certification:
Assessment Report: ROS 11/07-062 R005 V2 R2
Safety Manual: 00809-0100-4107

[1]FIT = 1 failure / 10^9 hours

[2]SFF not required for devices certified using Route 2_H data. For information detailing the Route 2_H approach as defined by IEC 61508-2, see Technical Document entitled "Route 2_H SIL Verification for Rosemount Type B Transmitters with Type A Components".

[3]Refer to ROS 13/04-008 R001 V1R0 for the Flowmeter FMEDA report for models that are excluded.

[4]Refer to the Remote Seal (ROS 1105075 R001 V1R3) FMEDA report for the additional failure rates to use when using with attached Remote Seals, or use exSILentia.

exida CERTIFICATION 64 N Main St Sellersville, PA 18960

T-002, V3.0-3

Page 2 of 2

รูปที่ 5 ก แสดงค่าพารามิเตอร์ที่ใช้ในการคำนวณหาค่า PFD_{AVG} และ SFF ของอุปกรณ์วัด

ก.1.2. Safety PLC

SIEMENS

Data sheet **6ES7317-2FK13-0AB0**

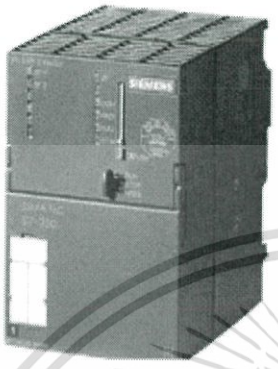


Figure similar

*** SPARE PART*** SIMATIC S7-300 CPU317F-2 PN/DP, CENTRAL PROCESSING UNIT WITH 1024 KBYTE WORKING MEMORY, 1. INTERFACE MPI/DP 12MBIT/S, 2. INTERFACE ETHERNET PROFINET, MICRO MEMORY CARD NECESSARY FOR USE WITH SOFTWARE OPTION S7 DISTRIBUTED SAFETY V5.4 OR HIGHER

Product type designation	
General information	
Hardware product version	01
Firmware version	V2.6
Engineering with	
• Programming package	STEP 7 V5.4 SP2 or higher, S7 Distributed Safety V5.4 or higher
Supply voltage	
Rated value (DC)	
• 24 V DC	Yes
permissible range, lower limit (DC)	20.4 V
permissible range, upper limit (DC)	28.8 V
External protection for supply cables (recommendation)	2 A min.
Input current	
Current consumption (rated value)	650 mA
Current consumption (in no-load operation), typ.	100 mA
Inrush current, typ.	2.5 A
I^2t	1 $A^2 \cdot s$
Power losses	
Power loss, typ.	3.5 W
Memory	
Work memory	
• Integrated	1 Mbyte; For program and data

รูปที่ 6 ก แสดงข้อมูลทั่วไปของตัวควบคุม (CPU) ที่เลือกใช้งาน

SIEMENS

SIMATIC
S7-300
CPU 317F-2 PN/DP, 6ES7317-2FK13-0AB0, Edition 01, as of firmware V2.3.4

Product Information

Introduction

This Product Information contains important information on 6ES7317-2FK13-0AB0. It is a separate component and should be considered more up-to-date than the information in the manuals and catalogs if uncertainties arise.

Validity of this Product Information

This Product Information is valid for CPU 317F-2 PN/DP with order number 6ES7317-2FK13-0AB0, as of hardware release 01 and as of firmware version V2.3.4.

This Product Information describes the specifications of CPU 317F-2 PN/DP compared to CPU 317-2 PN/DP with order number 6ES7317-2EK13-0AB0. Additional information on the CPU 317-2 PN/DP is available in the corresponding manual in the documentation package 6ES7398-8FA10-8BA0, version 12/2006, which you require in addition to this Product Information.

Areas of Application

CPU 317F-2 PN/DP is mainly designed for personal and machine safety and burner controls. In addition to the safety program, you can also program standard applications.

You intend to use CPU 317F-2 PN/DP for	then you require
Safety-related applications	STEP 7 as of version 5.3 + Service Pack 3 + HSP 106 (for firmware V2.3.4) or STEP 7 as of version 5.4 + Service Pack 1 + HSP 120 (for firmware V2.5.1) STEP 7 as of version 5.4 + Service Pack 2 (for firmware as of V2.6.0) Optional package S7 Distributed Safety V5.4
Standard applications	STEP 7 as of version 5.3 + Service Pack 3 + HSP 106 (for firmware V2.3.4) or STEP 7 as of version 5.4 + Service Pack 1 + HSP 120 (for firmware V2.5.1) STEP 7 as of version 5.4 + Service Pack 2 (for firmware as of V2.6.0)

Overview of the altered default values of CPU 317F-2 PN/DP

Function	CPU 317-2 PN/DP (6ES7317-2EK13-0AB0)	CPU 317F-2 PN/DP (6ES7317-2FK13-0AB0)
Default Value Size of process image I/O	256 Bytes/256 Bytes	1024 Bytes/1024 Bytes

Special Handling of the "RAMtoROM" Function:

Data blocks of the safety program are not copied to the load memory by the work memory.

Startup protection for inconsistent safety program

The CPU 317F-2 PN/DP as of firmware version V2.5.1 in connection with safety programs which were created with S7 Distributed Safety as of V5.4 SP1, supports the detection of an inconsistent safety program. This means that the F-CPU detects an inconsistent safety program in the startup. The F-CPU then goes to Stop and the following diagnostic event is then entered in the diagnostic buffer of the F-CPU:

- "Inconsistent safety program"

รูปที่ 7 ก แสดงเวอร์ชันของตัวควบคุม (CPU) ที่เลือกใช้งาน

Restrictions with SFC 22 "CREAT_DB", SFC 23 "DEL_DB" and SFC 82 "CREA_DBL"

F-DBs can neither be created nor deleted.

Restrictions with SFC 83 "READ_DBL" and SFC 84 "WRIT_DBL"

The target address may not point to an F-DB.

Restrictions when configuring the retentive behavior of data blocks

The configuration of retentive data blocks is not supported for F-DBs.

This means that the current values of the F-DBs will not be retentive in the event of Power OFF/ON and Restart (STOP-RUN) of the F-CPU. The F-DBs retain the initial values from the loading memory.

In the block properties of the F-DBs, the "Non-Retain" check box is activated and thus grayed out.

Probabilities of Failure

Below are the values for the CPU 317F-2 PN/DP probabilities of failure:

	Operation in Low Demand Mode low demand mode (average probability of failure on demand)	Operation in High Demand or Continuous Mode high demand/continuous mode (probability of a dangerous failure per hour)	Proof-test interval
F-compatible CPU 317F-2 PN/DP 6ES7317-2FK13-0AB0	4.76E-05	1.09E-09	10 years

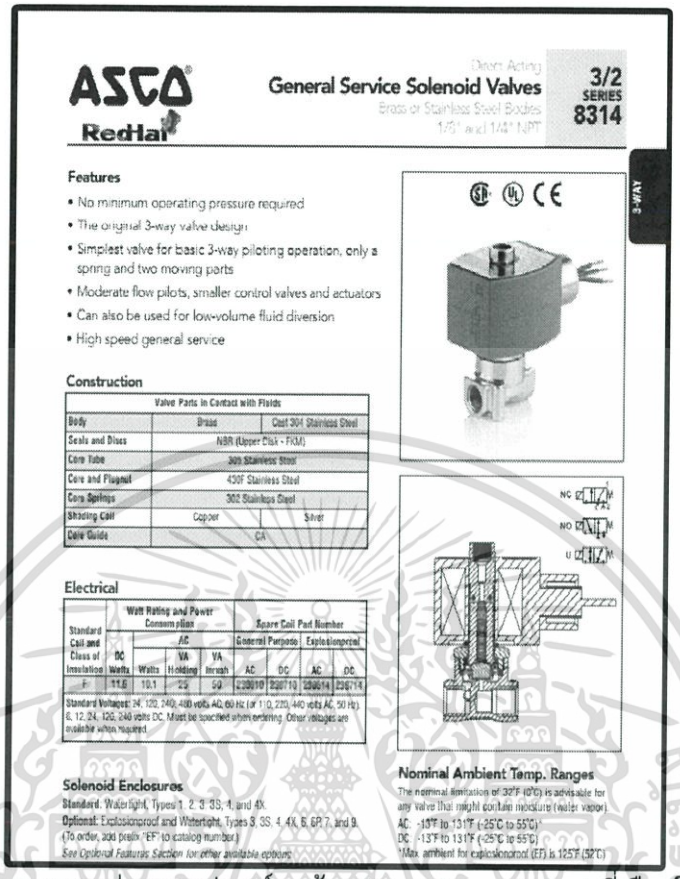
Operation with Safety Protector 6ES7195-7KF00-0XA0

⚠ WARNING

The safety protector (order number 6ES7195-7KF00-0XA0, product version **01** and **02**) unlike other modules, must not be inserted in the same rack as the F-CPU. This restriction does not apply to safety protector product versions **03** and higher.

รูปที่ 8 ก ตารางแสดงค่า PFD_{AVG} ของ ตัวควบคุม (CPU317-F 2 PN/DP)

ก.1.3. Shutdown Valve



ASCO RedHat

Direct Acting
General Service Solenoid Valves
Brass or Stainless Steel Bodies
1/8" and 1/4" NPT

3/2 SERIES 8314

3-WAY

Features

- No minimum operating pressure required
- The original 3-way valve design
- Simplest valve for basic 3-way piloting operation, only a spring and two moving parts
- Moderate flow pilots, smaller control valves and actuators
- Can also be used for low-volume fluid diversion
- High speed general service

Construction

Valve Parts in Contact with Fluids		
Body	Brass	Cast 304 Stainless Steel
Seals and Discs	NBR (Upper Disk - FKM)	
Core Tube	305 Stainless Steel	
Core and Plugnut	430F Stainless Steel	
Core Springs	302 Stainless Steel	
Shading Coil	Copper	Silver
Core Guide	CA	

Electrical

Standard Coil and Class of Insulation	Watt Rating and Power Consumption				Spare Coil Part Number			
		AC			General Purpose		Explosionproof	
	DC Watts	Watts	VA Holding	VA Inrush	AC	DC	AC	DC
F	11.6	10.1	22	50	238010	238713	238014	238714

Standard Voltages: 24, 120, 240, 480 volts AC, 60 Hz (or 110, 220, 440 volts AC, 50 Hz). 6, 12, 24, 120, 240 volts DC. Must be specified when ordering. Other voltages are available when required.

Solenoid Enclosures

Standard: Watertight, Types 1, 2, 3, 3S, 4, and 4X.
Optional: Explosionproof and Watertight, Types 7, 9, 7S, 9S, 4, 4X, 6, 6P, 7, and 9. (To order, add prefix "EF" to catalog number.)
See Optional Features Section for other available options.

Nominal Ambient Temp. Ranges

The nominal limitation of 32°F (0°C) is advisable for any valve that might contain moisture (water vapor).
AC: -13°F to 131°F (-25°C to 55°C)*
DC: -13°F to 131°F (-25°C to 55°C)
*Max. ambient for explosionproof (EF) is 125°F (52°C)

รูปที่ 9 ก แสดงรุ่นของอุปกรณ์สุดท้าย (Shutdown Valve) ที่เลือกใช้งาน

CERTIFICATION

The manufacturer may use the mark.

CERTIFIED • SIL 3 CAPABLE • exida

Report:
ASC 01301001 R001 V1R2
Assessment Report

Valid until February 26, 2016
Revision 1.1 March 21, 2013

ANSI
ANSI Accredited Program
PRODUCT CERTIFICATION

Certificate / Certificat
Zertifikat / 合格証

ASC 1301001 C001

exida hereby confirms that the:

Series 8314 Solenoid Valves

ASCO
Florham Park, NJ - USA

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A Element

SIL 2 @ HFT=0; SIL 3 @ HFT = 1; Route 2_H

PFD_{avg} and Architecture Constraints must be verified for each application

Safety Function:
The Valve will move to the designed safe position when de-energized / energized within the specified safety time.

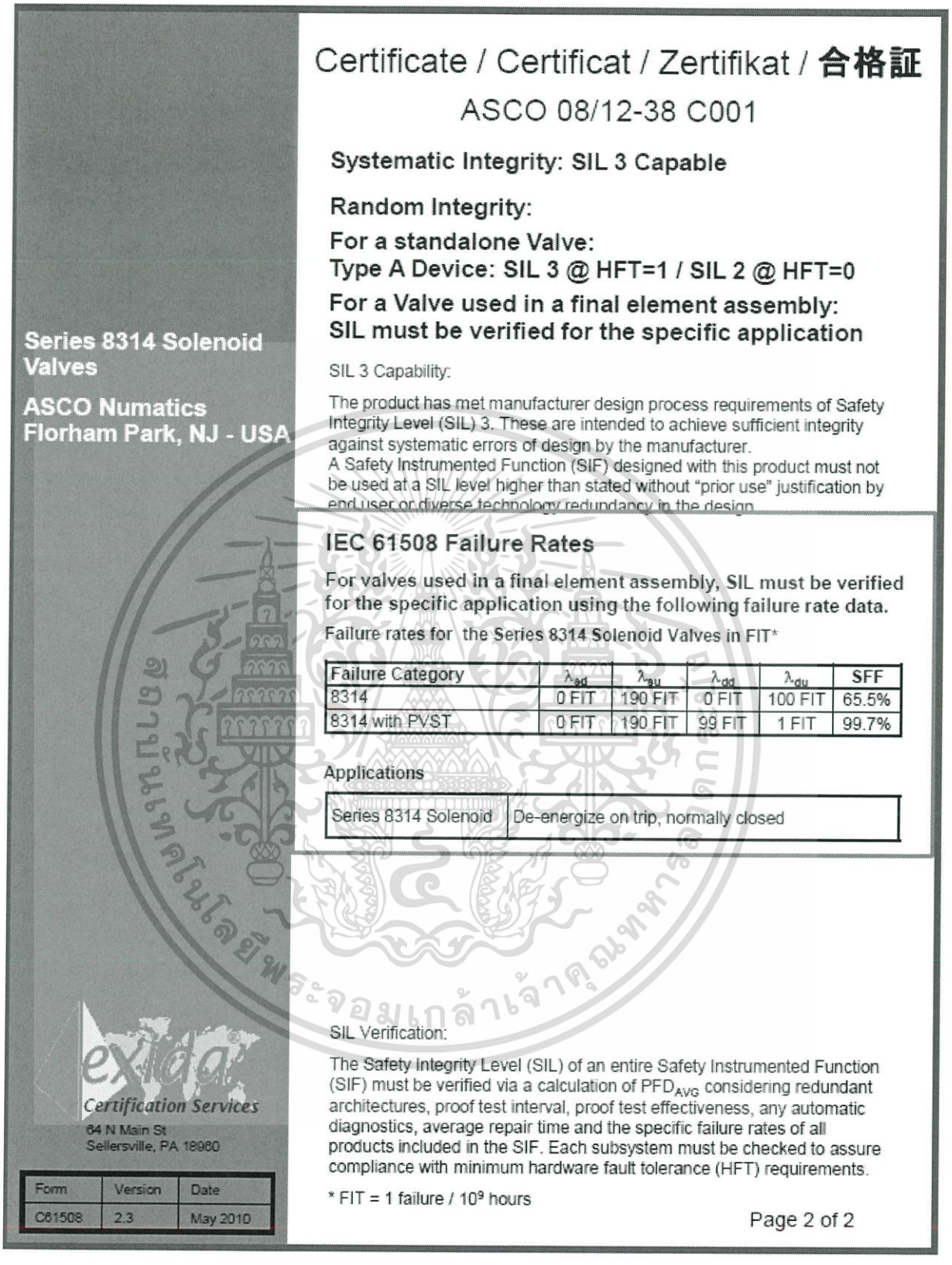
Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Evaluating Assessor

Certifying Assessor

Page 1 of 2

รูปที่ 10 ก แสดงใบ Certificate ของ Solenoid valve ที่เลือกใช้งาน



Certificate / Certificat / Zertifikat / 合格証

ASCO 08/12-38 C001

Systematic Integrity: SIL 3 Capable

Random Integrity:

For a standalone Valve:
Type A Device: SIL 3 @ HFT=1 / SIL 2 @ HFT=0

For a Valve used in a final element assembly:
SIL must be verified for the specific application

Series 8314 Solenoid Valves

ASCO Numatics
Florham Park, NJ - USA

SIL 3 Capability:

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated without "prior use" justification by end user or diverse technology redundancy in the design.

IEC 61508 Failure Rates

For valves used in a final element assembly, SIL must be verified for the specific application using the following failure rate data.

Failure rates for the Series 8314 Solenoid Valves in FIT*

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
8314	0 FIT	190 FIT	0 FIT	100 FIT	65.5%
8314 with PVST	0 FIT	190 FIT	99 FIT	1 FIT	99.7%

Applications

Series 8314 Solenoid	De-energize on trip, normally closed

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

* FIT = 1 failure / 10^9 hours

exida Certification Services
64 N Main St
Sellersville, PA 18960

Form	Version	Date
C61508	2.3	May 2010

Page 2 of 2

รูปที่ 11 ก แสดงค่าพารามิเตอร์ที่ใช้ในการคำนวณหาค่า PFD_{AVG} และ SFF ของอุปกรณ์สุดท้ายที่เลือกใช้งาน

ก.2. ค่าพารามิเตอร์ที่ใช้ในการหาค่าความผิดพลาดร่วม (β)

มาตรฐาน IEC 61508-6 Annex D ได้แสดงแนวทางในการคำนวณหาค่า β สำหรับอุปกรณ์ส่งสัญญาณ (Sensing Element), อุปกรณ์สุดท้าย (Final Element) และส่วนประมวลผล (Safety PLC) ที่แยกออกจากกัน

ในการทำให้มีค่าความเป็นไปได้ของการเกิดความผิดพลาดร่วมกัน (β) ต่ำสุดแล้ว การจัดทำแบบแผนที่เหมะสมในระบบสามารถช่วยลดค่า β ให้น้อยลงได้

รูปที่ 12(ก) แสดงรายการและค่าจำนวนที่เกี่ยวข้องที่อยู่บนพื้นฐานการวินิจฉัยทางวิศวกรรม (Engineering Judgment) ซึ่งเป็นตัวแทนสำหรับแต่ละรายการที่ช่วยลดความผิดพลาดร่วม เนื่องจากอุปกรณ์ส่งสัญญาณ และอุปกรณ์สุดท้ายจะมีการปฏิบัติที่แตกต่างจากส่วนประมวลผลที่เป็นระบบอิเลคทรอนิคส์ที่โปรแกรมทำงานได้ จึงต้องมีการแสดงตารางทั้งสองระบบออกจากกัน

ตารางที่ 1 ก แสดง Scoring programmable electronics or sensors/actuators

Item	X_{LS}	Y_{LS}	X_{SA}	Y_{SA}
Separation/segregation				
Are all signal cables for the channels routed separately at all positions?	1.5	1.5	1.0	2.0
Are the logic system channels on separate printed-circuit boards?	3.0	1.0		
Are the logic system channels in separate cabinets?	2.5	0.5		
If the sensors/actuators have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?			2.5	1.5
If the sensors/actuators have dedicated control electronics, is the electronics for each channel indoors and in separate 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			
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 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	
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
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 analysed 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 which will ensure that all component failures (or degradations) are detected, the root causes established and other similar items are inspected for similar potential causes of failure?		1.5	0.5	1.5

ตารางที่ 2 ก แสดง Scoring programmable electronics or sensors/actuators (ต่อ)

Item	X_{LS}	Y_{LS}	X_{SA}	Y_{SA}
Procedures/human interface (continued)				
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, must not be relocated?	0.5	0.5	0.5	0.50
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
Do the system have low diagnostic coverage (60% to 90%) and report failures to the level of a field-replaceable module?	0.5			
Do the system have medium diagnostics coverage (90% to 99%) and report failures to the level of a field-replaceable module?	1.5	1.0		
Do the system have high diagnostics coverage (>99%) and report failures to the level of a field-replaceable module?	2.5	1.5		
Do 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
Will the system be operating 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
Environmental testing				
Has a 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 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 that must 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.				

ตารางที่ 3 ก Calculation of β or β_D

Score (S or S_D)	Corresponding value of β or β_D for the:	
	Logic system	Sensors or actuators
120 or above	0.5%	1%
70 to 120	1%	2%
45 to 70	2%	5%
Less than 45	5%	10%
NOTE 1 The maximum levels of β_D 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 β_D lower than 0.5% for the logic system and 1% for the sensors would be difficult to justify.		

จากการวินิจฉัยทางวิศวกรรมจะได้รายการต่างๆของเครื่องมือวัดความดันเป็นดังนี้

ตารางที่ 4 ก การวินิจฉัยทางวิศวกรรม

Item	Logic subsystem		Sensor and final element	
	X_{LS}	Y_{LS}	X_{SA}	Y_{SA}
Diversity				
Are separate test methods and people used for each channel during commissioning?	1	0.5	1	1
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	1	1
Are inputs and outputs protected from potential levels of over-voltage and over-current?	1.5	0.5	1.5	0.5
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	-	3
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	-	3
Are all field failures fully analysed with feedback into the design? (Documentary evidence of the procedure is required.)	0.5	3.5	0.5	3.5

ตารางที่ 5 ก การวินิจฉัยทางวิศวกรรม(ต่อ)

Procedures/human interface				
Is there a written system of work which will ensure that all component failures (or degradations) are detected, the root causes established and other similar items are inspected for similar potential causes of failure?	-	1.5	0.5	0.5

การคำนวณหาค่าความผิดพลาดร่วม

จากสูตร $S = X_{SA} + Y_{SA}$

โดยที่ S = ผลรวมของค่า X_{SA} และ Y_{SA}

X_{SA} = การปรับปรุงระบบอัตโนมัติ

Y_{SA} = การตรวจสอบภาพรวมสาเหตุที่พบบ่อยที่สุด

จากตารางที่ 4 ก และ 5 ก จะได้ค่า $X_{SA} = 5$ และ $Y_{SA} = 13$ ดังนั้นจะได้ค่า $S = 18$

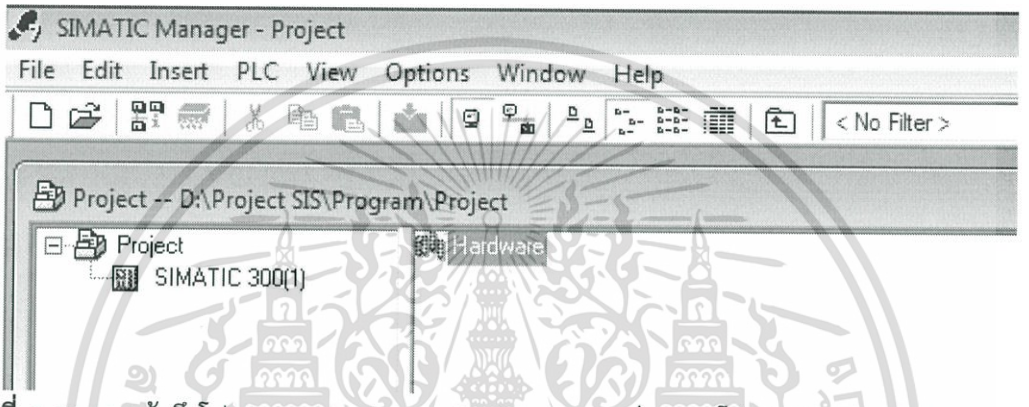
ดังนั้นจากตารางที่ 3 ก จะได้ค่าความผิดพลาดร่วมของอุปกรณ์วัด (Sensor) ที่ใช้ในกระบวนการ (β) = 10 %

ภาคผนวก ข
การตั้งค่าคอนฟิกของระบบอัตโนมัติ
(Automation System: AS)

ข.1. Hardware Configuration

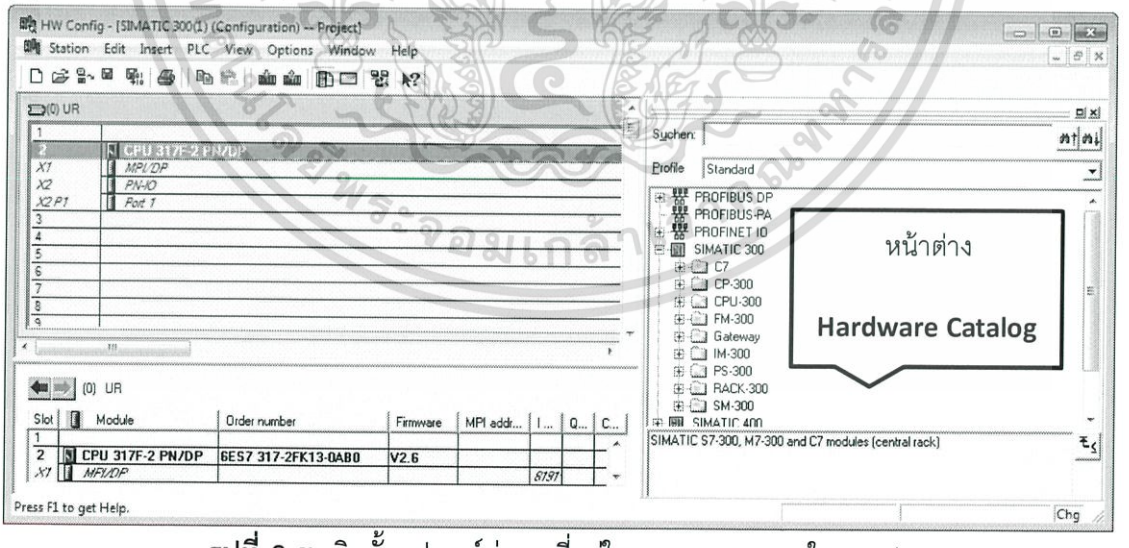
มีขั้นตอนดังต่อไปนี้

1. คลิกที่ SIMATIC 300(1) ใน Project window > ดับเบิ้ลคลิกที่ ข้อความ Hardware เพื่อเข้าสู่โปรแกรม Hardware Configuration ดังรูปที่ 1(ข)



รูปที่ 1 ข การเข้าถึงโปรแกรม Hardware Configuration ผ่านทางโปรแกรม SIMATIC Manager

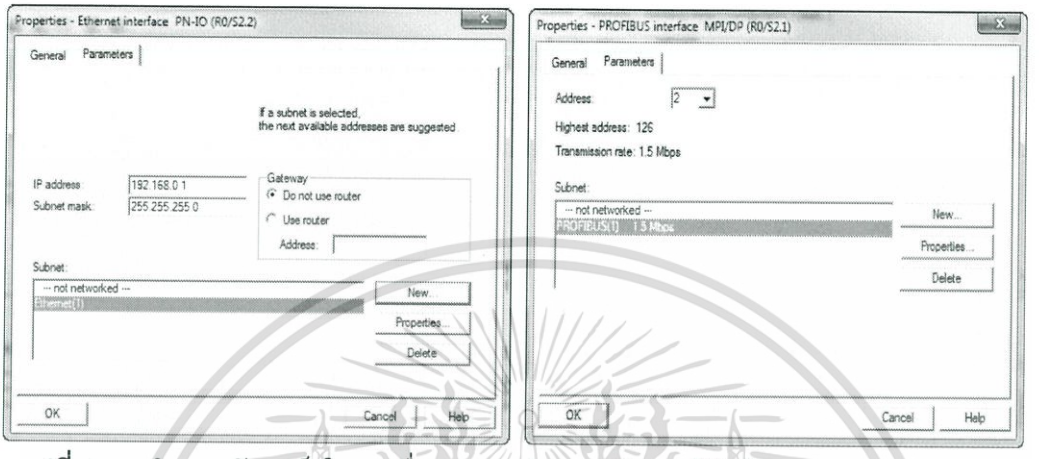
2. ติดตั้ง Rack: Rail, CPU 317F-2PN/DP โดยเลือกจาก Hardware Catalog ดังรูปที่ 2 (ข)



รูปที่ 2 ข ติดตั้งอุปกรณ์ต่างๆ ที่อยู่ในระบบควบคุมลงใน Rack

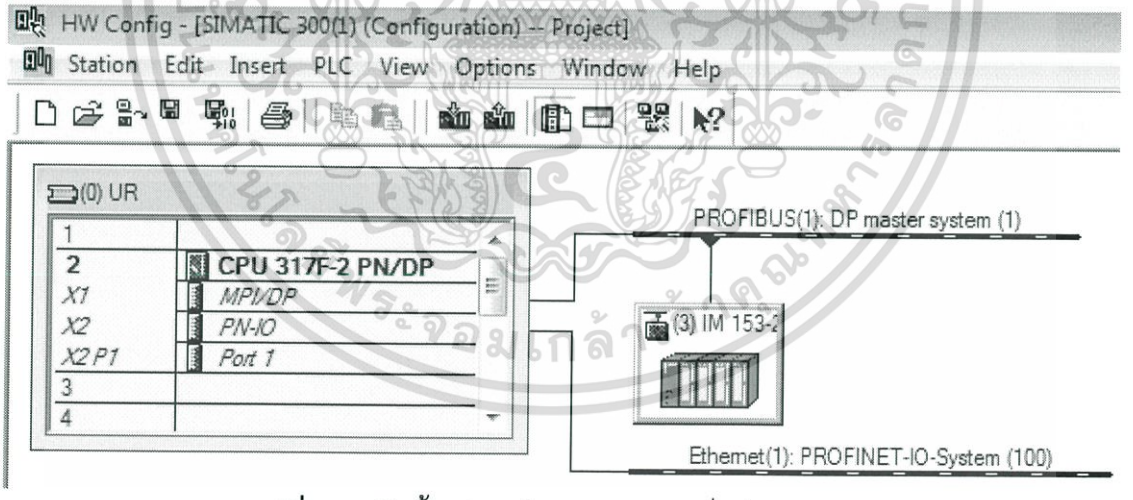
3. กำหนด Address และอัตราความเร็วในการรับ-ส่งข้อมูลของบัสแบบต่างๆ (MPI, PROFIBUS-DP)

โดยกำหนดให้บัส MPI มีการเชื่อมต่อเป็นแบบ Ethernet(1) และมี Address เท่ากับ 1 สำหรับการเชื่อมต่อตัวควบคุมเข้ากับคอมพิวเตอร์สำหรับเขียนโปรแกรม หรือคอมพิวเตอร์สำหรับการปฏิบัติงานก็ได้ และกำหนดให้ Address ของบัสโปรฟิบัสดีพี [PROFIBUS(2)] เท่ากับ 2 และมีอัตราเร็วรับ-ส่งข้อมูลเท่ากับ 1.5 Mbps สำหรับเชื่อมต่อตัวควบคุมเข้ากับ Remote I/O ดังรูปที่ 3(ข)



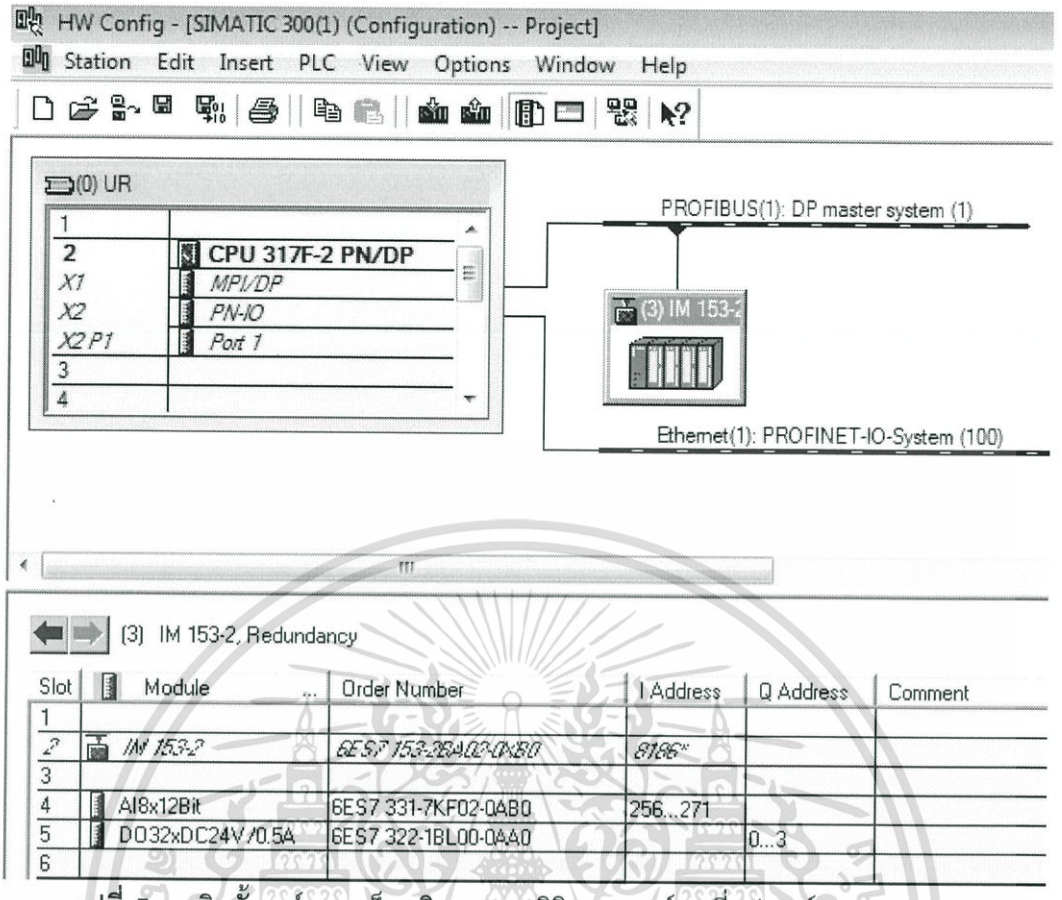
รูปที่ 3 ข กำหนดอัตราเร็วในการสื่อสารระหว่างคอมพิวเตอร์กับตัวควบคุม และ Remote I/O

4. ติดตั้งอุปกรณ์ Remote I/O ET200M IM 153-2 ลงบนบัสของโปรฟิบัสดีพี ดังรูปที่ 4(ข) และเลือกบัส Address ของ Remote I/O เท่ากับ 3 ดังรูปที่ 4(ข)



รูปที่ 4 ข ติดตั้งอุปกรณ์ Remote I/O ที่อยู่นอก Rack

5. ติดตั้งการ์ดอนาล็อกอินพุต (SM331 AI 8*12 BIT) และการ์ดดิจิตอลเอาท์พุต (SM322 DO 32*DC24V/0.5A) ลงที่อุปกรณ์ Remote I/O ดังรูปที่ 5(ข)



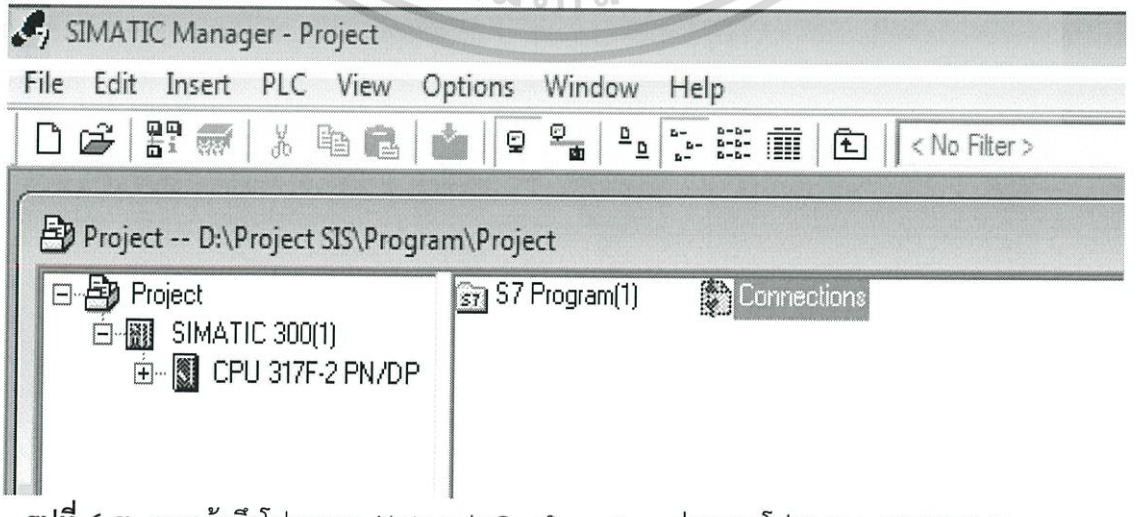
รูปที่ 5 ข ติดตั้งการ์ดอนาล็อกอินพุตและดิจิตอลเอาท์พุตที่อุปกรณ์ Remote I/O

6. ทำการบันทึก และตรวจสอบความถูกต้อง ด้วยการเรียกใช้ฟังก์ชัน Save and Compile

ข.2 NETWORK CONFIGURATION

มีขั้นตอนดังต่อไปนี้

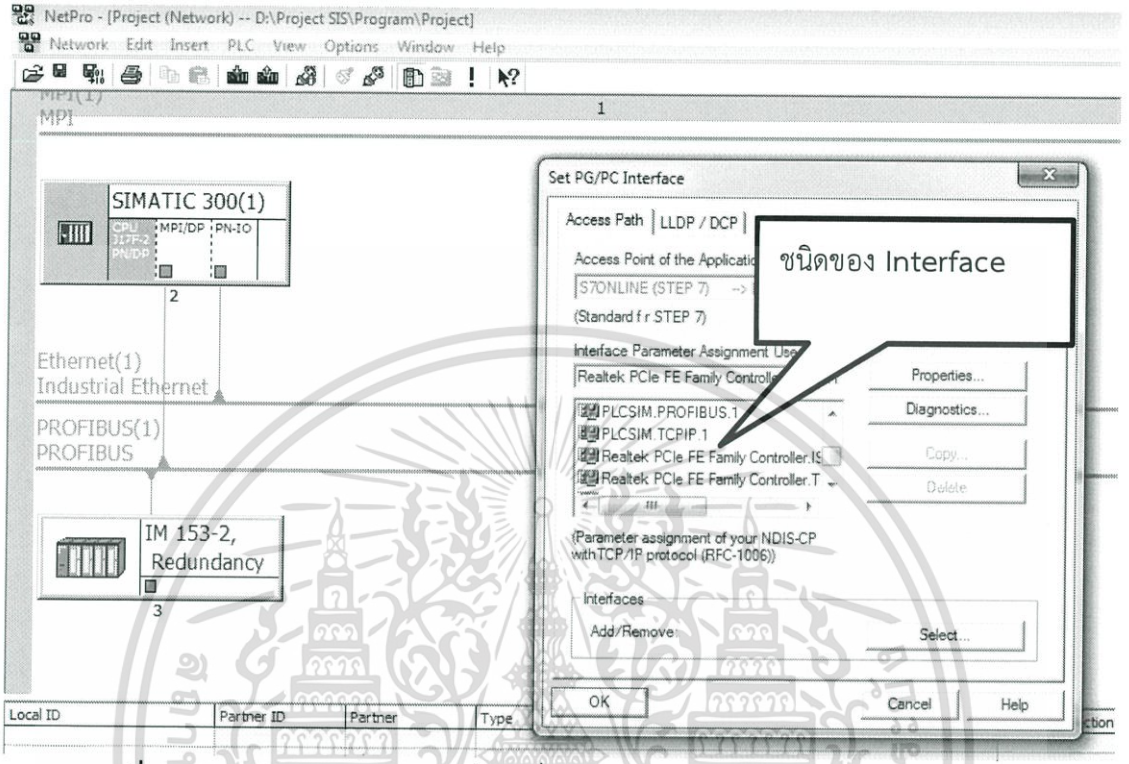
1. คลิกที่ SIMATIC 300(1) ใน Project window > CPU 317F-2PN/DP > ดับเบิลคลิกที่ Connection เพื่อเข้าสู่โปรแกรม Network Configuration ดังรูปที่ 6(ข)



รูปที่ 6 ข การเข้าถึงโปรแกรม Network Configuration ผ่านทางโปรแกรม SIMATIC Manager

2. ทำการกำหนดพารามิเตอร์การเชื่อมต่อระหว่างคอมพิวเตอร์เข้ากับตัวควบคุม

คลิก Option ที่แถบเมนู > Set PG/GC Interface เลือก > Interface parameter Realtex PCIe FE Family Controller.TCPIP.1 > OK ดังรูปที่ 7(ข)



รูปที่ 7 ข การกำหนดพารามิเตอร์การเชื่อมต่อระหว่างคอมพิวเตอร์เข้ากับตัวควบคุม

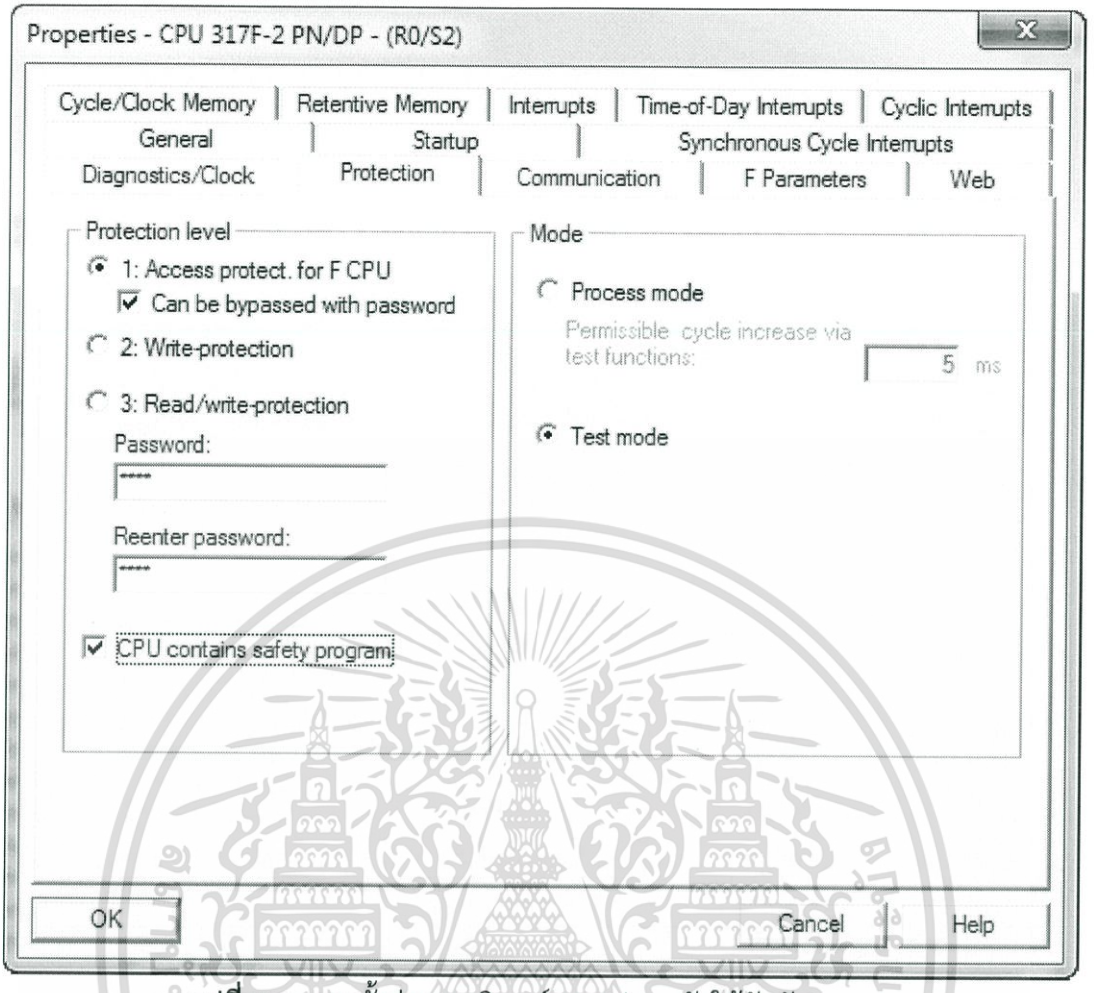
3. ทำการบันทึก และตรวจสอบความถูกต้อง ด้วยการเรียกใช้ฟังก์ชัน Save and Compile

4. ส่งถ่ายข้อมูลการกำหนดค่า Configure Network ไปยังตัวควบคุม โดยการเรียกใช้ฟังก์ชัน Download PLC

ข.3 วิธีการตั้งค่าพารามิเตอร์ตัวควบคุมให้สามารถทำงานได้ในการใช้งาน Safety Program

มีขั้นตอนดังต่อไปนี้

1. ทำการดับเบิลคลิกที่ CPU ในหน้าต่าง Hardware Configuration > คลิกเลือกที่ Protection > ทำการตั้งค่าตัวควบคุมดังรูปที่ 8(ข)



รูปที่ 8 ข การตั้งค่าพารามิเตอร์ความปลอดภัยให้กับตัวควบคุม

หมายเหตุ Password ที่เราใส่เข้าไปนั้น เป็นรหัสที่ป้องกันในการเข้าถึงการทำ Hardware Configuration ในครั้งถัดไป เพื่อทำการแก้ไขหรือโปรแกรมการทำงานต่างๆ

ภาคผนวก ค
วิธีการสร้าง Safety Program โดยการตั้ง F-Runtime Group

ค.1 ส่วนประกอบและการเรียกใช้งาน Safety Program

ส่วนประกอบสำคัญในการเขียนและเรียกใช้งาน Safety Program นั้นสามารถอธิบายได้ดังรูปที่ 1(ค) และ 2(ค) ดังนี้

- Data Block1: (DB1) คือ ส่วนของการเขียนโปรแกรมทั่วไป
- Function1: (FC1) คือ ฟังก์ชันที่เรียกใช้งานใน F-Runtime Group
- Function Block1: (FB1) คือส่วนของการเขียน Safety Program หลักที่ถูกตั้งเป็น F- Runtime Group ในการใช้งานฟังก์ชัน Safety Program
- Datablock1: (DB1) คือ ที่เก็บข้อมูลของ Function Block1: (FB1)
- FB2 – FB... คือ Function Block อื่นๆ ที่เราต้องการจะใช้งานเป็นฟังก์ชัน Safety

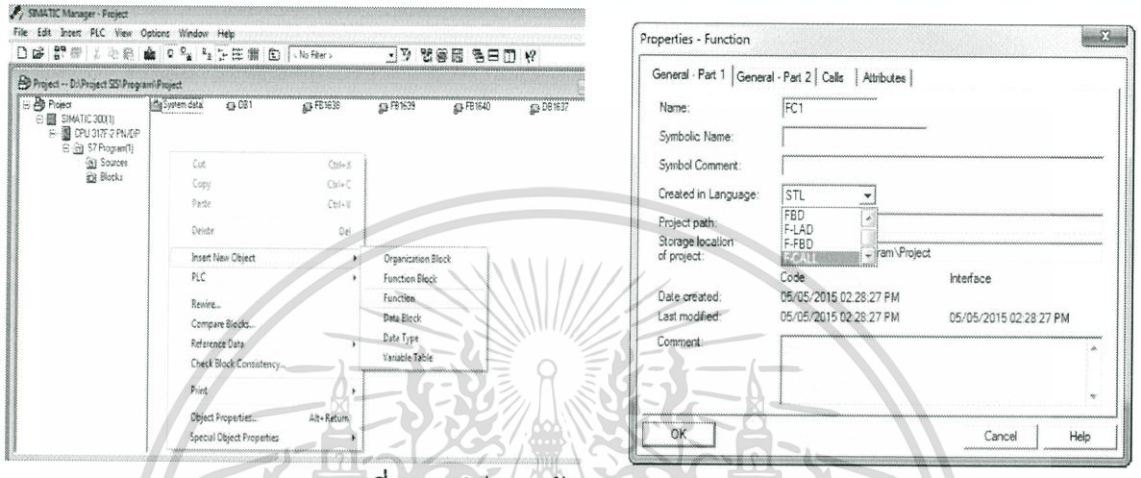
รูปที่ 1 ค การเรียกใช้งานใน Safety Program

รูปที่ 2 ค การตั้งค่าเป็น F-Runtime Group

ค.2 วิธีการสร้าง F-Runtime Group

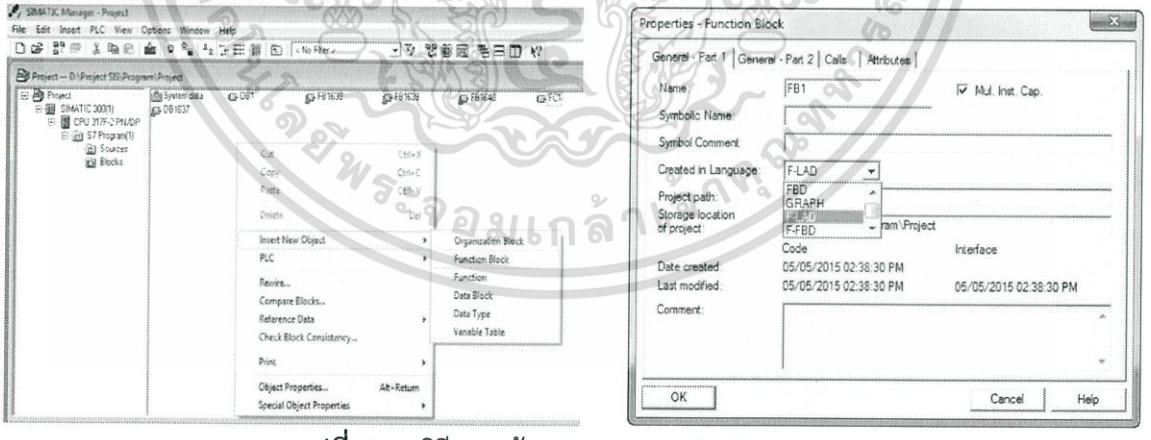
นั้นมีขั้นตอนดังต่อไปนี้

1. สร้าง FC1 โดยคลิกที่ SIMATIC 300(1) ใน Project window > CPU 317F-2PN/DP > S7 Program(1) > Blocks > คลิกขวาพื้นที่ว่าง > Insert New Object > Function (โดยเราเลือกให้ FC1 นั้นเป็น F-CALL) ดังรูปที่ 3(ค)



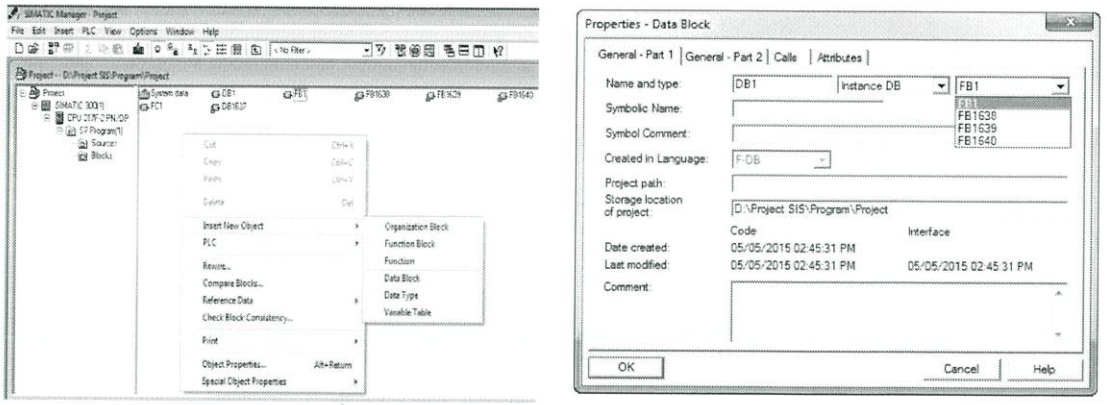
รูปที่ 3 ค วิธีการสร้าง Function1: FC1

2. สร้าง FB1 โดยคลิกที่ SIMATIC 300(1) ใน Project window > CPU 317F-2PN/DP > S7 Program(1) > Blocks > คลิกขวาพื้นที่ว่าง > Insert New Object > Function Block (โดยเราเลือกให้ FB1 นั้นเป็น F-LAD) ดังรูปที่ 4(ค)



รูปที่ 4 ค วิธีการสร้าง Function Block1: FB1

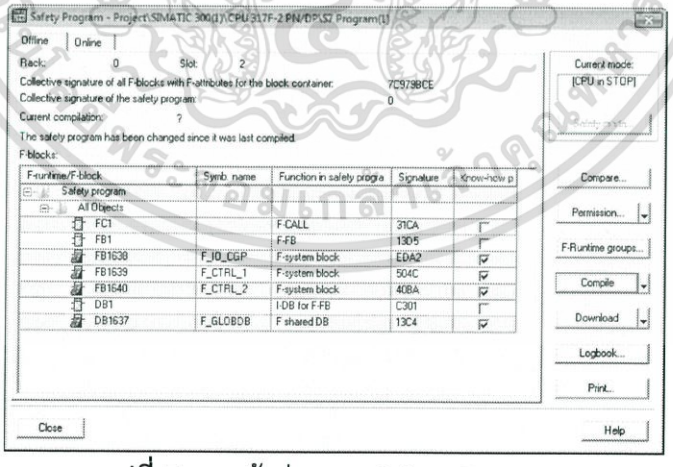
3. สร้าง DB1 โดยคลิกที่ SIMATIC 300(1) ใน Project window > CPU 317F-2PN/DP > S7 Program(1) > Blocks > คลิกขวาพื้นที่ว่าง > Insert New Object > Data Block (โดยเราเลือกให้ DB1 นั้นเป็น Instance DB และให้เลือกชี้ไปเก็บข้อมูลของ FB1) ดังรูปที่ 5(ค)



รูปที่ 5 ค วิธีการสร้าง Data Block1: DB1

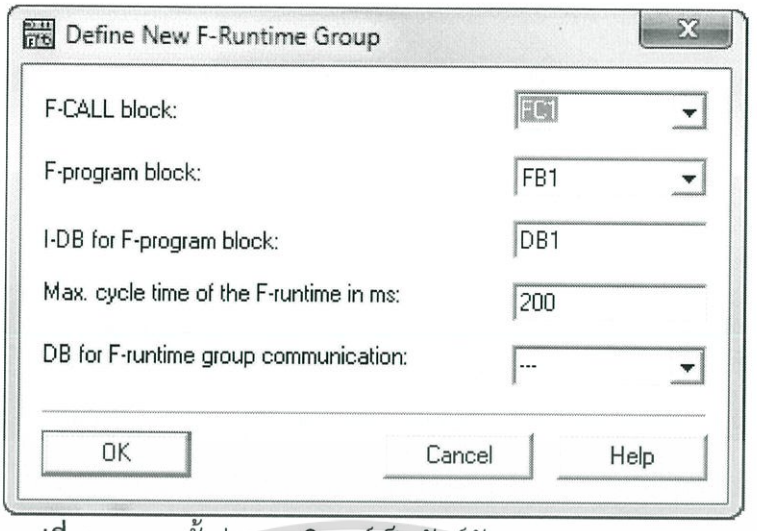
4. หลังจากทำการสร้าง FC1, FB1 และ DB1 เรียบร้อยแล้ว ในขั้นตอนนี้เป็นขั้นตอนของการตั้งค่า F-Runtime Group โดยคลิกเลือกที่สัญลักษณ์ Safety Program ดังรูปที่ 6(ค)

รูปที่ 6 ค สัญลักษณ์ของ Safety Program

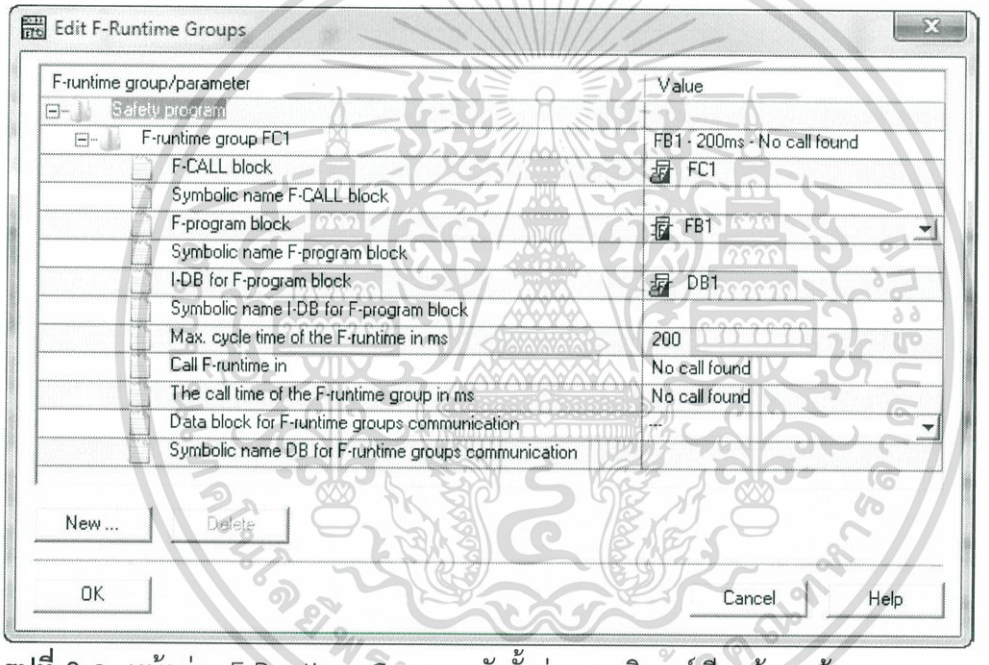


รูปที่ 7 ค หน้าต่างของ Safety Program

5. ทำการสร้าง F-Runtime Group โดยคลิกเลือกที่ F-Runtime Group > New จากนั้นตั้งค่า F-Runtime Group โดยมี FC1 เป็น F-Call block, FB1 เป็น F-program block และมี DB1 เป็นที่เก็บข้อมูลของ F-Program block ดังรูปที่ 8(ค) จากนั้นคลิก OK



รูปที่ 8 ค การตั้งค่าพารามิเตอร์เป็นฟังก์ชัน F-Runtime Group



รูปที่ 9 ค หน้าต่าง F-Runtime Group หลังตั้งค่าพารามิเตอร์เรียบร้อยแล้ว

6. ทำการตรวจสอบความถูกต้องของฟังก์ชัน F-Runtime Group ที่สร้างขึ้นมาด้วยการเรียกใช้ฟังก์ชัน Compile ในหน้าต่าง Safety Program

7. ทำการส่งถ่ายข้อมูลการกำหนดค่า F-Runtime Group ไปยังตัวควบคุม