รายงานสหกิจศึกษาฉบับสมบูรณ์

การกำหนดระดับความปลอดภัยของอุปกรณ์สำหรับระบบวัดคุมนิรภัยในอุตสาหกรรมกลั่นน้ำมัน

Safety Integrity Level Determination of Devices for Safety Instrument System in Refinery Industry

พงศพล จิตตโสภาวดี

ภาควิชาวิศวกรรมการวัดและควบคุม
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2560

รายงานสหกิจศึกษาฉบับสมบูรณ์

การกำหนดระดับความปลอดภัยของอุปกรณ์
สำหรับระบบวัดคุมนิรภัยในอุตสาหกรรมกลั่นน้ำมัน

Safety Integrity Level Determination of Devices
for Safety Instrument System in Refinery Industry

พงศพล จิตตโสภาวดี

ภาควิชาวิศวกรรมการวัดและควบคุม
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2560

Safety Integrity Level Determination of Devices For Safety Instrument System in Refinery Industry

Phongsapon Jittasopawadee

DEPARTMENT OF INSTRUMENTATION AND CONTROL ENGINEERRING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUE OF TECHNOLOGY LARDKRABANG

ACADEMIC YEAR 2017

โครงงานสหกิจศึกษา การกำหนดระดับความปลอดภัยของอุปกรณ์สำหรับระบบวัดคุมนิรภัยในอุตสาหกรรมกลั่นน้ำมัน

ชื่อ–สกุล นักศึกษา นายพงศพล จิตตโสภาวดี รหัสนักศึกษา 57010812

คณะ วิศวกรรมศาสตร์ **ภาควิชา** วิศวกรรมการวัดและควบคุม

ชื่อ–สกุล อาจารย์นิเทศ ผศ.สุธรรม สัทธรรมสกุล

ชื่อ–สกุล ผู้นิเทศงาน นายปรีดี ศิริแสงเลิศ

ชื่อสถานประกอบการ บริษัท ไทยออยล์ จำกัด (มหาชน)

บทคัดย่อ

โครงงานสหกิจศึกษาฉบับสมบูรณ์นี้เป็นส่วนหนึ่งของวิชาสหกิจศึกษา ที่กำหนดให้นักศึกษาทำโครงงานร่วมกับทางสถานประกอบการเป็นระยะเวลาหนึ่งภาคการศึกษา ซึ่งโครงงานฉบับนี้เป็นการศึกษาเกี่ยวกับระบบวัดคุมนิรภัยภายในโรงกลั่นน้ำมัน เพื่อเป็นแนวทางนำไปใช้พิจารณาระดับความปลอดภัยของอุปกรณ์วัดและอุปกรณ์ควบคุมสุดท้ายในฟังก์ชันนิรภัย เนื่องจากอุปกรณ์ควบคุมสุดท้ายที่ถูกใช้งานอยู่ในปัจจุบันไม่มีการกำหนดระยะเวลาการทดสอบ และซ่อมบำรุงรักษาที่แน่นอนส่งผลให้อุปกรณ์บางส่วนถูกละเลยและไม่ได้รับการดูแลรักษา จึงทำให้ต้องมีการวิเคราะห์ระดับความปลอดภัยและสร้างระยะเวลาในการบำรุงรักษาให้แก่อุปกรณ์ อีกทั้งทำการศึกษาพัฒนาระยะเวลาการทดสอบฟังก์ชันนิรภัยโดยใช้หน่วยกลั่นน้ำมันดิบที่ 3 (CDU-3) มาเป็นกรณีศึกษาเพื่อใช้เป็นแนวทางในการพิจารณาและเป็นข้อมูลเบื้องต้น ในการดำเนินงานพัฒนาระยะการบำรุงรักษาอุปกรณ์ในโรงกลั่นในอนาคตต่อไป

คำสำคัญ : ระดับความปลอดภัย, ระบบวัดคุมนิรภัย และระยะเวลาการทดสอบ

Co-operative Title: Safety Integrity Level Determination of Devices for Safety Instrument System in Refinery Industry

Student Intern Name: Mr. Phongsapon Jittasopawadee

Faculty: Engineering **Department:** Instrumentation and Control Engineering

Advisor Name: Asst.Prof. Sutham Satthamsakul

Mentor Name: Mr. Predee Sirisaenglert

Company: Thai Oil Public Company Limited

ABSTRACT

This cooperative educational report is part of cooperative education. Students are required to complete a project with the institution for a period of one semester. This report is a study of the safety system in refineries as a guideline for determining the safety integrity level of the measuring devices and the final control elements in the safety function. Since the final control elements that are currently in use have no definite test and maintenance schedule, as a result, some devices are forgotten from maintenance. Therefore, safety integrity level analysis and maintenance time are required. Moreover, the study on the development of the safety function test using the third crude oil refining unit (CDU-3) as a guideline for consideration. This is a preliminary step in the development of the equipment's testing interval for the refining operations in the future.

Keywords : Safety Integrity Level, Safety Instrument System and Test Interval

กิตติกรรมประกาศ

โครงงานสหกิจศึกษาฉบับสมบูรณ์ฉบับนี้บรรลุล่วงได้ดีเนื่องด้วยความอนุเคราะห์จาก บริษัท ไทยออยล์ จำกัด (มหาชน) ที่เปิดโอกาสให้ข้าพเจ้าได้เข้าร่วมปฏิบัติโครงการสหกิจศึกษาตลอดระยะเวลาหนึ่งภาคเรียนการศึกษา ข้าพเจ้าต้องขอขอบพระคุณพี่ปรีดี ศิริแสงเลิศ ผู้นิเทศงานและพนักงานบริษัททุกท่านที่ให้ความช่วยเหลือและให้ประสบการณ์ในการทำงานตลอดระยะเวลาสี่เดือน

ขอขอบพระคุณ ผศ.สุธรรม สัทธรรมสกุล และอาจารย์ในหลักสูตรวิศวกรรมการวัดคุมทุกท่านที่ได้ให้ความเมตตาและคำแนะนำแก่ข้าพเจ้าตลอดมา อันเป็นประโยชน์ต่อการทำโครงงานสหกิจศึกษาฉบับนี้

ขอขอบพระคุณบิดามารดาและครอบครัว ที่ให้โอกาสข้าพเจ้าได้เข้ารับการศึกษาเล่าเรียนตลอดจนคอยช่วยเหลือและดูแลเสมอมา คุณประโยชน์อันพึงมาจากโครงงานสหกิจศึกษาฉบับนี้ขอมอบแด่ผู้มีพระคุณทุกท่านและขอมอบให้แก่ผู้ที่สนใจทำการศึกษาในอนาคต

พงศพล จิตตโสภาวดี

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญตาราง (ต่อ)

ตารางที่ **หน้า**

สารบัญภาพ

สารบัญภาพ (ต่อ)

รูปที่ **หน้า**

บทที่ 1
บทนำ

ในบทนี้จะกล่าวถึงภาพรวมของการปฏิบัติงานในโครงงานสหกิจศึกษา ซึ่งประกอบด้วยความเป็นมาและความสำคัญ วัตถุประสงค์ ขอบเขตของโครงงาน วิธีการดำเนินงาน และประโยชน์ที่จะได้รับจากโครงงานเพื่อนำไปวิเคราะห์และจัดทำเอกสารที่เกี่ยวข้องกับระบบวัดคุมนิรภัย

1.1 ความเป็นมาและความสำคัญ

บริษัท ไทยออยล์ จำกัด (มหาชน) เป็นบริษัทที่ประกอบธุรกิจโรงกลั่นน้ำมันปิโตรเลียมสำเร็จรูปเพื่อการจำหน่ายที่มีขนาดใหญ่ที่สุดในประเทศไทย ที่ตั้งปัจจุบันของโรงกลั่นน้ำมันตั้งอยู่ที่อำเภอศรีราชา จังหวัดชลบุรี ด้วยการพัฒนาอย่างต่อเนื่องมาเกือบครึ่งศตวรรษ บริษัท ไทยออยล์ฯ ก้าวจากโรงกลั่นน้ำมันขนาดเล็กขนาด 35,000 บาร์เรลต่อวัน มาเป็นโรงกลั่นน้ำมันขนาด 275,000 บาร์เรลต่อวัน และมีความสามารถในการผลิตที่หลากหลายทั้งน้ำมันสำเร็จรูป ผลิตภัณฑ์ปิโตรเคมี น้ำมันหล่อลื่นพื้นฐาน จนถึงการผลิตพลังงานไฟฟ้าใช้ภายในโรงกลั่น และขายคืนให้แก่การไฟฟ้าฝ่ายผลิตแห่งประเทศไทยเพื่อเพิ่มรายได้ทางด้านธุรกิจพลังงาน โดยทางบริษัทไทยออยล์ฯ มุ่งเน้นไปที่มาตรฐานความปลอดภัยซึ่งเป็นสิ่งสำคัญที่สุดในอุตสาหกรรมการผลิตทั้งหมด จึงได้มีการพิจารณาศึกษาใช้งานอุปกรณ์และระบบวัดคุมนิรภัย เพื่อที่จะสร้างความมั่นคงภายในกระบวนการผลิตให้มีมาตรฐานเป็นที่ยอมรับในระดับโลก

ในปัจจุบันระบบวัดคุมนิรภัยมีความสำคัญอย่างยิ่งในภาคอุตสาหกรรม เนื่องจากมีหน้าที่ระงับเหตุการณ์อันตรายที่อาจเกิดขึ้นเนื่องจากระบบควบคุมพื้นฐานทำงานผิดพลาด อุปกรณ์หลักภายในระบบวัดคุมนิรภัยจะถูกเรียกว่า ฟังก์ชันนิรภัย ที่ประกอบด้วย เครื่องมือวัด หน่วยประมวลผล และอุปกรณ์ควบคุมสุดท้าย โดยพื้นฐานของการพิจารณาและออกแบบฟังก์ชันนิรภัยเหล่านี้จะต้องใช้เครื่องมือที่มีระดับความปลอดภัยหรือระดับ SIL (Safety Integrity Level) ไม่น้อยกว่าระดับความปลอดภัยที่กระบวนการผลิตนั้นต้องการ และเป็นอุปกรณ์ที่ได้รับการรับรองมาตรฐานจากองค์กรที่เกี่ยวข้องแต่เนื่องจากโรงกลั่นน้ำมันไทยออยล์ฯ ถูกสร้างขึ้นมากว่า 50 ปี ซึ่งถูกสร้างขึ้นก่อนที่มาตรฐานความปลอดภัยจะถูกพิจารณาจัดตั้งขึ้น จึงทำให้อุปกรณ์ในระบบวัดคุมนิรภัยที่ถูกติดตั้งไม่มีการประเมินระดับความปลอดภัยและตารางระยะเวลาในการทดสอบ โดยเฉพาะอุปกรณ์ควบคุมสุดท้ายที่มีระยะเวลาการซ่อมบำรุงประมาณ 10 ปี การที่ไม่มีตารางเวลาในการทดสอบทำให้อุปกรณ์บางส่วนถูกละเลยและปล่อยให้ทำงานโดยไม่ได้รับการตรวจสอบ จากปัญหาดังกล่าวโครงงานนี้จึงได้ทำการพิจารณาและคัดกรองระดับความปลอดภัย พร้อมทั้งกำหนดระยะเวลาการทดสอบให้กับอุปกรณ์สุดท้ายของฟังก์ชันวัดคุมนิรภัยโดยใช้มาตรฐานของไทยออยล์ฯ ในการคัดกรอง พร้อมทำการศึกษาระยะเวลาการทดสอบของฟังก์ชันนิรภัยด้วยการคำนวณโดยใช้หน่วยกลั่นน้ำมันดิบที่ 3 (CDU-3) เป็นกรณีศึกษาในการพิจารณาสร้างความถูกต้องของระยะเวลาการบำรุงรักษา

1.2 วัตถุประสงค์ของโครงงาน

1. เพื่อศึกษาการพิจารณาและประเมินระดับความปลอดภัยของฟังก์ชันวัดคุมนิรภัย
2. เพื่อเรียนรู้วิธีการออกแบบฟังก์ชันวัดคุมนิรภัยให้เหมาะสมแก่กระบวนการ

3. สามารถสร้างแนวทางในการวิเคราะห์ความเสี่ยงของเหตุการณ์อันตรายได้ถูกต้อง
4. เพื่อเป็นแนวทางในการพัฒนาระยะเวลาในการบำรุงรักษาฟังก์ชันนิรภัยให้ถูกต้อง
5. เพื่อเรียนรู้กระบวนการ วิธีการในการสร้างระบบนิรภัยของ บริษัท ไทยออยล์ จำกัด (มหาชน)

1.3 ขอบเขตของโครงงาน

โครงงานนี้จะศึกษาเกี่ยวกับการคัดเลือกระดับความปลอดภัย ให้กับอุปกรณ์ในฟังก์ชันวัดคุมนิรภัยในระบบวัดคุมนิรภัย ซึ่งอุปกรณ์นั้นคืออุปกรณ์สุดท้ายที่มีการติดตั้งและใช้งานจริงโดยมีหน้าที่แตกต่างกันอยู่ในหน่วยกลั่นต่าง ๆ เพื่อทำการสร้างตารางเวลาในการบำรุงรักษาด้วยการวิเคราะห์ข้อมูลจากแผนภาพ P&ID (Piping and Instrument Diagram) ตารางสาเหตุและผลกระทบ (Cause and Effect Table) และแผนภาพลอจิก (Logic Diagram) พร้อมทั้งศึกษาการเลือกระยะเวลาการทดสอบอุปกรณ์ในฟังก์ชันนิรภัยให้เหมาะสมโดยใช้หน่วยกลั่นน้ำมันดิบ CDU-3 ด้วยการคำนวณจากสมการ

1.4 วิธีดำเนินงาน

1. ศึกษาข้อมูลและทฤษฎีที่เกี่ยวข้องกับการออกแบบและพัฒนาระบบวัดคุมนิรภัย
2. ลงพื้นที่เพื่อสำรวจการติดตั้งและระบบที่ใช้ในฟังก์ชันวัดคุมนิรภัย
3. ศึกษาความเสี่ยงของผลกระทบจากเหตุการณ์อันตรายของฟังก์ชันนิรภัยแต่ละตัว
4. ศึกษาการเชื่อมต่อของอุปกรณ์ทางแผนภาพลอจิกและแผนภาพ P&ID
5. ศึกษาข้อมูลอุปกรณ์การวัดและควบคุมในฟังก์ชันนิรภัยแต่ละฟังก์ชัน
6. ทำการคัดเลือกระดับความปลอดภัยให้แก่อุปกรณ์สุดท้ายเพื่อสร้างตารางซ่อมบำรุง
7. คัดกรองความเสียหายของอุปกรณ์จากการบันทึกประวัติ
8. คำนวณระยะเวลาในการทดสอบตามค่าระดับความปลอดภัยของฟังก์ชันนิรภัยที่มีอยู่ในหน่วยกลั่น CDU-3
9. ปรับปรุงข้อมูลที่ถูกต้องในการพิจารณาระดับความปลอดภัยของฟังก์ชันนิรภัย
10. จัดทำเอกสารแสดงแนวทางในการเลือกระดับความปลอดภัยของฟังก์ชันนิรภัย และพัฒนาระยะเวลาในการทดสอบ

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้รับความรู้จากการศึกษาหลักการพิจารณาระดับความปลอดภัย และความเสี่ยงของกระบวนการ
2. ได้รับความรู้จากการศึกษาหลักการออกแบบฟังก์ชันวัดคุมนิรภัย
3. ได้เรียนรู้กระบวนการทำงานของกระบวนการต่าง ๆ ภายในบริษัท ไทยออยล์ จำกัด (มหาชน)
4. มีทักษะในการต่อยอดวิเคราะห์สาเหตุและพิจารณาระบบการป้องกันของกระบวนการต่าง ๆ ได้
5. ได้เรียนรู้ระบบการทำงานในกระบวนการผลิตทั้งฝ่ายปฏิบัติการและฝ่ายซ่อมบำรุง
6. ได้ทักษะในการติดต่อประสานงานและทำงานร่วมกับผู้อื่น

บทที่ 2
ทฤษฎีและหลักการที่เกี่ยวข้อง

ในบทนี้จะอธิบายถึงทฤษฎีและหลักการที่เกี่ยวข้องกับโครงงานสหกิจศึกษา ประกอบด้วย ระบบวัดคุมนิรภัย การวิเคราะห์ผลกระทบของกระบวนการ การคัดเลือกระดับความปลอดภัย และการออกแบบฟังก์ชันวัดคุมนิรภัยภายในโรงกลั่นน้ำมัน

2.1 ระบบวัดคุมนิรภัย

ระบบวัดคุมนิรภัยนั้นถูกนำมาใช้งานภายในกระบวนการผลิตต่าง ๆ มากมายไม่ว่าจะเป็นกระบวนการขุดเจาะน้ำมัน กระบวนการกลั่นน้ำมัน และแม้กระทั่งโรงงานนิวเคลียร์ ระบบวัดคุมนิรภัยถูกนำมาใช้ในการตรวจสอบค่าและตัวแปรของกระบวนการในโรงงานต่าง ๆ ให้ถูกควบคุมอยู่ภายในขอบเขตของการปฏิบัติงานที่กำหนด หากกระบวนการทำการวัดและมีค่าตัวแปรที่เกินกว่าค่าที่ถูกกำหนดเอาไว้ในระบบวัดคุมนิรภัย ระบบจะทำงานเพื่อป้องกันไม่ให้เกิดเหตุการณ์อันตรายที่อาจเกิดขึ้นโดยการปิดหรือเปิดวาล์วนิรภัยที่ถูกติดตั้งไว้โดยขึ้นอยู่กับหน้าที่ที่กำหนดไว้ เพื่อป้องกันการรั่วไหลของผลิตภัณฑ์ภายในกระบวนการไม่ทำให้อุปกรณ์เกิดความเสียหาย ป้องกันการเกิดอัคคีภัยและการระเบิด เป็นต้น โดยระบบวัดคุมนิรภัยจะถูกออกแบบและติดตั้งเพื่อให้แน่ใจว่า ผู้ปฏิบัติงาน สิ่งแวดล้อม และทรัพย์สินภายในอุตสาหกรรมจะไม่ได้รับความเสียหายและผลกระทบจากสิ่งที่เกิดขึ้น ระบบวัดคุมนิรภัยจึงถูกพัฒนาขึ้นเพื่อให้ทันกับการเปลี่ยนแปลง และความหลากหลายของอุตสาหกรรม ด้วยเหตุนี้จึงมีการกำหนดมาตรฐานความปลอดภัยขึ้น โดยคณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอเทคนิกส์ หรือ IEC (International Electrotechnical Commission) ในปี ค.ศ. 1998 มีการลงมติรับรองจากคณะกรรมการ ตั้งเป็นมาตรฐาน IEC 61508 “Function Safety of Electrical/Electronic/Programmable Electronics Safety-Related System” ว่าด้วยเรื่องการสร้างและพัฒนาระบบความปลอดภัยของผู้ผลิต โดยมาตรฐาน IEC 61508 นี้จะเป็นมาตรฐานทางอุตสาหกรรมฉบับแรกที่ถูกสร้างขึ้นสำหรับระบบวัดคุมนิรภัยของ IEC ต่อมาเมื่อวิวัฒนาการทางด้านเทคโนโลยีมีความเจริญก้าวหน้าขึ้นอย่างมาก ประกอบกับแต่ละแขนงก็มีความแตกต่างกันจึงได้มีการกำหนดมาตรฐานในการใช้งานเฉพาะกลุ่ม เช่น อุตสาหกรรมการผลิต อุตสาหกรรมการแพทย์ อุตสาหกรรมนิวเคลียร์ และอุตสาหกรรมการขนส่งทางราง เป็นต้น โดยโรงกลั่นน้ำมันไทยออยล์ฯ นั้นถือว่าเป็นอุตสาหกรรมการผลิต ซึ่งในการดำเนินการสร้างระบบวัดคุมนิรภัยจะต้องดำเนินตามมาตรฐาน IEC 61511 “Function Safety: Safety Instrumented System for the process industry sector” ว่าด้วยเรื่องฟังก์ชันนิรภัยสำหรับระบบวัดคุมนิรภัยในอุตสาหกรรมกระบวนการผลิตที่มีการลงมติในปี ค.ศ. 2003 นอกจากนี้ยังมีมาตรฐานการผลิตของ ISA (Instrument Society of America) ได้จัดตั้งมาตรฐานเกี่ยวกับระบบนิรภัยสำหรับอุตสาหกรรมกระบวนการผลิตขึ้น โดยคณะกรรมการบริหารงานความปลอดภัยและสุขภาพอนามัยการประกอบอาชีพ (OSHA : Occupational Safety and Health Administration) คือ มาตรฐาน ANSI/ISA-SP-84.01 “Application of Safety Instrumented Systems for the Process Industries” ว่าด้วยเรื่องการออกแบบฟังก์ชันนิรภัยและการใช้งานระบบวัดคุมนิรภัยเช่นเดียวกันกับ IEC 61511

สำหรับในประเทศไทยนั้นนอกจากจะมีการใช้งานมาตรฐานสากล IEC 61508 แล้ว ได้มีการใช้งานมาตรฐานอื่นควบคู่ไปด้วยคือ พระราชบัญญัติโรงงาน พ.ศ. 2535 และประกาศจากกระทรวงอุตสาหกรรมฉบับที่ 3 (พ.ศ. 2543) ที่ได้อธิบายถึงมาตรการคุ้มครองความปลอดภัยในการดำเนินงานประกอบกิจการโรงงานและขยายโรงงาน ซึ่งกำหนดให้ผู้ผลิตจะต้องจัดทำรายงานการวิเคราะห์ความเสี่ยง (Risk Assessment) จากอันตรายที่อาจเกิดขึ้นในการผลิตและแผนการบริหารความเสี่ยงที่เกิดขึ้น ซึ่งข้อกำหนดเหล่านี้ก็เป็นส่วนหนึ่งของขั้นตอนการออกแบบระบบวัดคุมนิรภัยตามมาตรฐานสากลด้วยเช่นกัน

2.1.1 โครงสร้างของระบบวัดคุมนิรภัย

ระบบวัดคุมนิรภัย (SIS : Safety Instrument System) หรือระบบป้องกันภัยฉุกเฉิน (ESD : Emergency Shut Down System) เป็นระบบที่ถูกติดตั้งเพื่อลดความเสี่ยงและหยุดความไม่ปลอดภัยที่อาจเกิดขึ้นจากกระบวนการผลิตในแต่ละฟังก์ชันการควบคุม ปกติแล้วในการทำงานพื้นฐานนั้นจะมีระบบที่ควบคุมอยู่คือ ระบบควบคุมพื้นฐาน (BPCS : Basic Process Control System) ซึ่งเป็นระบบพื้นฐานในกระบวนการทำงานควบคุมระดับของเหลว ความดัน หรือความร้อนให้อยู่ในย่านระดับที่ต้องการหรือที่กำหนด (Set point) ที่ถูกตั้งไว้เพื่อให้มีประสิทธิภาพตามที่ต้องการมากที่สุด หากกระบวนการเกิดการเปลี่ยนแปลงที่ผิดปกติก็จะส่งสัญญาณเตือนภัยและทำการควบคุม เช่น การขยับวาล์วควบคุมให้กระบวนการกลับคืนมาสู่การทำงาน ซึ่งถ้าหากกระบวนการควบคุมพื้นฐานนี้ไม่สามารถที่จะควบคุมระบบให้กลับมาสู่สภาวะปกติได้ ระบบวัดคุมนิรภัยก็จะต้องเข้ามามีบทบาทในการทำงานต่อไป เพื่อป้องกันไม่ให้กระบวนการเข้าสู่สภาวะอันตราย และป้องกันอันตรายจากความผิดพลาดที่จะเกิดขึ้นจากกระบวนการผลิต ซึ่งประกอบด้วยอุปกรณ์ทางไฟฟ้า อุปกรณ์ทางอิเล็กทรอนิกส์ และระบบอิเล็กทรอนิกส์แบบโปรแกรมได้ หรือ E/E/PES (Electronical/Electronic/Programmable Electronic System) มีองค์ประกอบสำคัญ 3 ส่วนดังนี้

2.1.1.1 อุปกรณ์วัด

อุปกรณ์วัด (Sensing Element) คือ อุปกรณ์ที่ใช้สำหรับวัดสภาวะของกระบวนการผลิตและการเปลี่ยนแปลงค่าตัวแปรต่าง ๆ ของอุปกรณ์การวัดในกระบวนการผลิต (Process Variables) ให้เป็นสัญญาณกระแสไฟฟ้ามาตรฐานขนาด 4 ถึง 20 มิลลิแอมป์ ที่แรงดันกระแสตรง 24 โวลต์ เพื่อส่งไปยังส่วนประมวลผล (Logic Solver) ในการทำงานนั้นจะเหมือนกับอุปกรณ์วัดในระบบควบคุมพื้นฐาน เช่น อุปกรณ์ส่งสัญญาณความดันแตกต่าง (Differential Pressure Transmitter) อุปกรณ์ส่งสัญญาณแรงดัน (Pressure transmitter) เป็นต้น แต่ในกรณีของอุปกรณ์ที่พิจารณาในระบบวัดคุมนิรภัยจะมีการออกแบบที่แตกต่างออกไป ขึ้นอยู่กับค่าความน่าจะเป็นของความล้มเหลวบนความต้องการ (PFD : Probability of Failure on Demand) ของอุปกรณ์ หรืออีกความหมายหนึ่งคือ ค่าความเป็นไปได้ที่อุปกรณ์นั้นจะไม่ทำงานหากเกิดเหตุการณ์อันตราย

2.1.1.2 หน่วยประมวลผล

หน่วยประมวลผล (Logic Solver) คือ อุปกรณ์ที่ใช้สำหรับประมวลผลทางตรรกศาสตร์ของระบบวัดคุมนิรภัย เพื่อใช้ในการควบคุมกระบวนการผลิตให้อยู่ในสภาวะที่ปลอดภัยเมื่อเกิดความผิดปกติขึ้น โดยจะใช้งานอยู่บนระบบพีแอลซี (PLC : Programmable Logic Controller) หรือระบบพีแอลซีนิรภัย (Safety PLC) โดยการทำงานของส่วนประมวลผลจะรับ

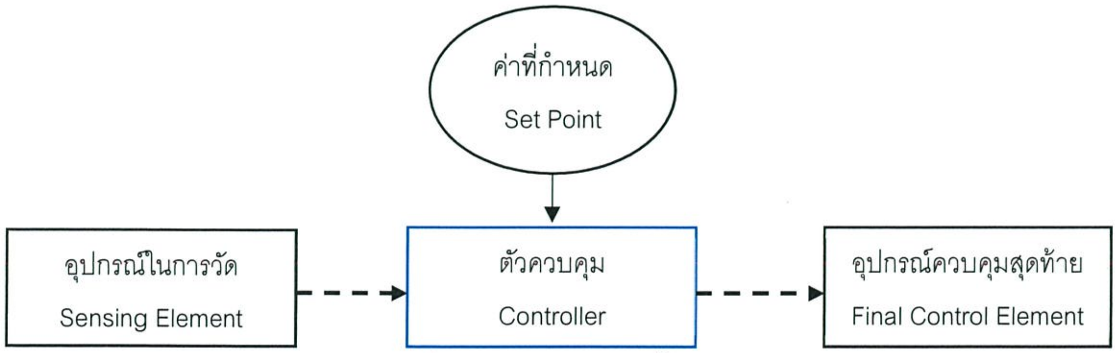
สัญญาณจากอุปกรณ์การวัดเพื่อนำมาทำการเปรียบเทียบทางตรรกศาสตร์กับสัญญาณที่ถูกตั้งไว้ และส่งสัญญาณไปยังอุปกรณ์สุดท้าย โดยผลลัพธ์ของการเปรียบเทียบจะได้เป็นสัญญาณดิจิตอล (0 หรือ 1 ในทางลอจิก) ส่วนประมวลผลจะประกอบไปด้วยอุปกรณ์หลัก ๆ ดังนี้ แหล่งจ่ายพลังงาน (PSU : Power Supply Unit) ตัวประมวลผลกลาง (CPU : Central Processing Unit) ส่วนรับและส่งสัญญาณ (Input and Output Cards) ส่วนติดต่อสื่อสาร (Communication Port) และโปรแกรมในการทำงาน (Safety Management System) เช่น ระบบ FSC (Fail Safe Controller) ของบริษัทฮันนี่เวลล์ ซิสเต็มส์ (ไทยแลนด์) จำกัด เป็นต้น

2.1.1.3 อุปกรณ์สุดท้าย

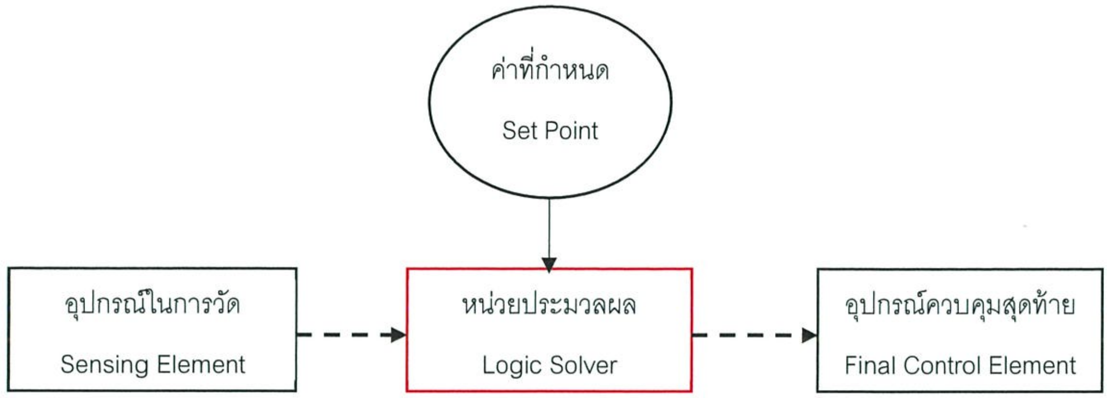
อุปกรณ์สุดท้าย (Final Element) คือ อุปกรณ์ที่ทำหน้าที่ควบคุมกระบวนการ ไม่ว่าจะเป็นการปรับอุณหภูมิ ความดัน ระดับ หรืออัตราการไหล เมื่อเกิดความเสี่ยงอันตรายอุปกรณ์จะรับสัญญาณมาจากหน่วยประมวลผลเป็นสัญญาณไฟฟ้ามาตรฐาน 4 ถึง 20 มิลลิแอมป์ ที่แรงดันกระแสตรง 24 โวลต์ เพื่อควบคุมตัวแปรต่าง ๆ เช่น วาล์วนิรภัย (Shut Down Valve) เป็นต้น

2.1.2 ฟังก์ชันวัดคุมนิรภัย

ฟังก์ชันวัดคุมนิรภัย (SIF : Safety Instrumented Functions) นั้นเป็นฟังก์ชันที่ถูกจัดเตรียมไว้บนระบบนิรภัย (Safety System) ในกระบวนการชนิดต่าง ๆ ซึ่งมีจุดประสงค์ทำให้กระบวนการผลิตอยู่ในสภาวะปลอดภัยจากเหตุการณ์อันตรายที่กำหนด ภายในฟังก์ชันวัดคุมนิรภัยที่จะประกอบไปด้วยทั้ง 3 องค์ประกอบ ประกอบไปด้วยอุปกรณ์ในการวัด หน่วยประมวลผล และอุปกรณ์ควบคุมสุดท้าย จะเห็นได้ว่าระบบควบคุมพื้นฐานในรูปที่ 2.1 นั้นมีองค์ประกอบที่คล้ายคลึงกับฟังก์ชันนิรภัยในรูปที่ 2.2 แต่สิ่งที่แตกต่างกันอย่างชัดเจน คือ หน่วยประมวลผลในฟังก์ชันวัดคุมนิรภัยซึ่งมีการทำงานเป็นแบบดิจิตอลหรือเปิดและปิดเท่านั้น ซึ่งระบบควบคุมพื้นฐานจะสามารถควบคุมได้ทั้งย่านการทำงานตั้งแต่ 0 ถึง 100 เปอร์เซ็น ด้วยตัวควบคุม (Controller) ดังนั้นจะเห็นได้ว่าฟังก์ชันนิรภัยมีความสามารถในการควบคุมกระบวนการที่น้อยกว่าระบบควบคุมพื้นฐาน การใช้งานฟังก์ชันนิรภัยจะถูกติดตั้งเมื่อต้องการความปลอดภัยในกระบวนการเพิ่มขึ้น ระบบวัดคุมนิรภัยนั้นมีความแน่นอนในการทำงานนั่นคือทำและไม่ทำเท่านั้น จึงมีการใช้งานอุปกรณ์ควบคุมสุดท้ายที่มีระดับความปลอดภัยที่ต่างไป เช่น วาล์วนิรภัย การสั่งงานการจ่ายไฟให้แก่ปั๊มและคอมเพลสเซอร์ เป็นต้น

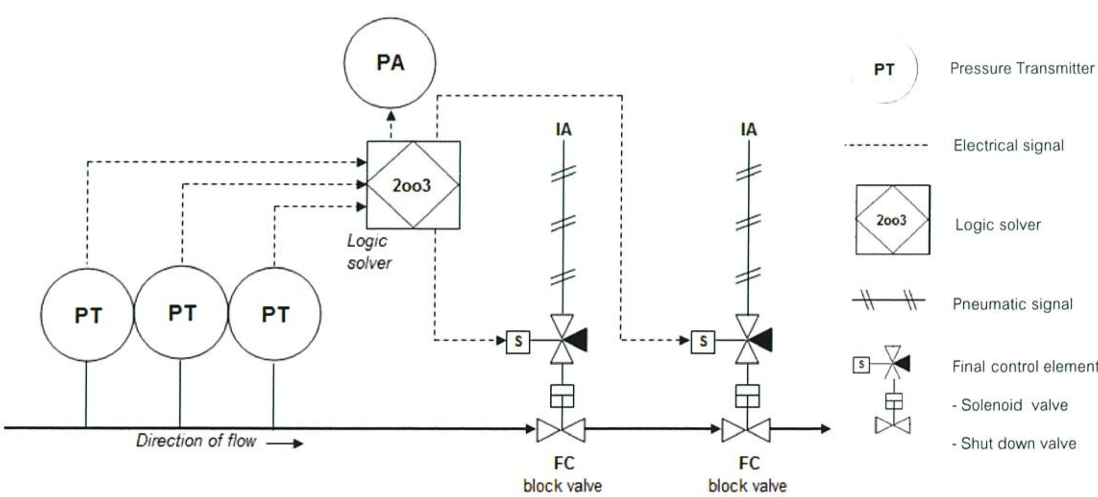


รูปที่ 2.1 ระบบควบคุมพื้นฐาน



รูปที่ 2.2 ฟังก์ชันวัดคุมนิรภัย

ในการทำงานของฟังก์ชันนิรภัยนั้น โปรแกรมการทำงานของฟังก์ชันนิรภัยจะเริ่มด้วยการตรวจสอบค่าที่อ่านได้จากอุปกรณ์วัด โดยข้อมูลจะถูกส่งมาด้วยสัญญาณไฟฟ้ามาตรฐาน 4 ถึง 20 มิลลิแอมป์ เพื่อนำไปเปรียบเทียบกับค่าที่กำหนดไว้ในหน่วยประมวลผล หากมีค่าไม่เกินค่าที่ตั้งไว้ก็จะไม่มีการสั่งการใด ๆ ออกจากส่วนประมวลผลโปรแกรมการทำงานจะกลับไปเริ่มต้นใหม่ แต่ถ้าเมื่อใดที่ค่าที่อ่านได้เกินกว่าค่าที่กำหนด ส่วนประมวลผลจะสั่งให้ทำการให้พลังงาน (Energized) หรือหยุดให้พลังงาน (De-energized) แรงดันกระแสตรง 24 โวลต์ ไปที่โซลินอยล์วาล์วของวาล์วนิรภัยโดยขึ้นอยู่กับการออกแบบ และระบบจะส่งสัญญาณเตือนภัยไปตามส่วนที่เกี่ยวข้อง เพื่อให้ผู้ปฏิบัติงานทำการแก้ไขระบบให้กลับเข้าสู่สภาวะปกติ พร้อมทำการรีเซ็ทโปรแกรมการทำงานเพื่อเริ่มเดินกระบวนการใหม่อีกครั้ง จากรูปที่ 2.3 เป็นการเชื่อมต่อฟังก์ชันนิรภัยเพื่อป้องกันความดันเกินภายในท่อโดยมีอุปกรณ์วัดความดันเกิน 3 ตัวเป็นแบบ 2oo3 (2 out of 3 voting) และอุปกรณ์ควบคุมสุดท้าย คือ โซลินอยล์วาล์วและวาล์วนิรภัย 2 ตัวแบบ 1oo2 (1 out of 2 voting)



รูปที่ 2.3 การเชื่อมต่อฟังก์ชันนิรภัยเพื่อป้องกันความดันเกิน

2.1.3 ระบบนิรภัยอื่น ๆ

ในการติดตั้งระบบนิรภัยในกระบวนการ จะต้องคำนึงถึงผลกระทบที่อาจจะเกิดขึ้นหากการควบคุมภายในกระบวนการเกิดความผิดพลาดเนื่องจากสาเหตุต่าง ๆ นอกจากระบบวัดคุมนิรภัยที่ถูกรองรับด้วยมาตรฐาน IEC 61508 และ 61511 ที่ประกอบไปด้วยอุปกรณ์ไฟฟ้าและอุปกรณ์

อิเลคทรอนิกส์หรือ E/E/PES แล้วนั้น ยังมีระบบนิรภัยอื่น ๆ (Other Safety Related System) ในการพิจารณาโดยแบ่งเป็น 2 ช่วง ได้แก่ ก่อนเหตุการณ์อันตราย (Before Dangerous Event) และหลังเกิดเหตุการณ์อันตราย (After Dangerous Event)

2.1.3.1 ก่อนเกิดเหตุการณ์อันตราย

เมื่อระบบมีแนวโน้มที่กำลังจะเข้าสู่สภาวะอันตราย กระบวนการจะมีความสามารถในการระงับเหตุการณ์ด้วยชั้นป้องกันต่าง ๆ ซึ่งพิจารณาออกมาได้ดังนี้

1) การตอบสนองของผู้ปฏิบัติงาน (Operator Response) ที่จะสำรวจค่าตัวแปรในระบบอยู่เป็นระยะ และจะมีผลต่อเหตุการณ์อันตรายหากผู้ปฏิบัติงานสามารถรู้ได้ว่าระบบกำลังเข้าสู่อันตราย และนำระบบเข้าสู่สภาวะปลอดภัยได้ทันท่วงที
2) วาล์วนิรภัยทางกล (Mechanical Relief Valve) ที่ถูกพิจารณาติดตั้งตามมาตรฐาน ASME/ANSI PTC 25.3 : Safety and Relief valve เพื่อใช้ในการระบายความดัน (Pressure Relief Valve) และความร้อน (Thermal Relief Valve) ในกรณีที่ระบบมีค่าเกินที่กำหนดในอุปกรณ์ทางกล อุปกรณ์ทางกลจะต้องมีค่าต่ำกว่าค่าออกแบบของอุปกรณ์การทำงาน เช่น กระบวนของถังเวสเซล (Vessel) ถูกออกแบบมาให้ทนความดันได้ที่ 150 psig ดังนั้นอุปกรณ์นิรภัยทางกลจะต้องถูกออกแบบให้อยู่ที่ประมาณ 120 psig เพื่อป้องกันการระเบิดเนื่องจากความดันเกิน (Overpressure) ของเวสเซล

2.1.3.2 หลังเกิดเหตุการณ์อันตราย

เมื่อระบบนิรภัยในกระบวนการ ไม่สามารถหยุดเหตุการณ์อันตรายที่เกิดขึ้นมาได้ ระบบนิรภัยภายนอกจะทำหน้าที่ในการลดผลเสียหายให้น้อยที่สุด ได้แก่

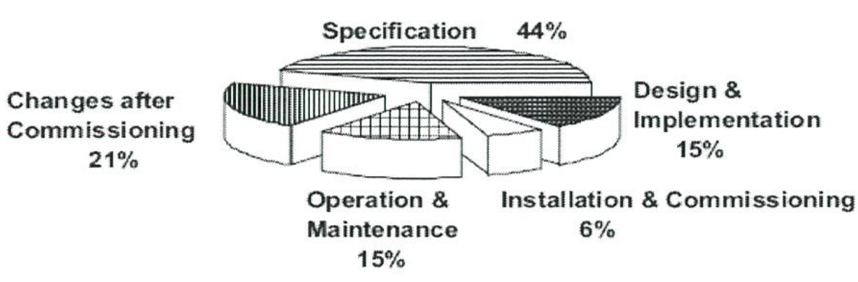
1) ระบบเตือนภัยและอพยพในโรงงาน (Plant Emergency Response) จะส่งเสียงอพยพและทำงาน เมื่อตรวจจับหรือถูกสั่งการว่ามีเหตุการณ์อันตรายเกิดขึ้น ผลของเหตุการณ์มีขอบเขตอยู่ในอาณาเขตของโรงงาน
2) ระบบเตือนภัยและอพยพชุมชน (Community Emergency Response) จะส่งเสียงอพยพและทำงาน เมื่อตรวจจับหรือถูกสั่งการว่ามีเหตุการณ์อันตรายเกิดขึ้น ผลของเหตุการณ์มีขอบเขตที่เหนือกว่าอาณาเขตของโรงงาน

2.1.4 กระบวนการตามมาตรฐานของระบบวัดคุมนิรภัย

เป้าหมายของระบบวัดคุมนิรภัยก็คือ การลดความเสี่ยงของกระบวนการที่มีความอันตรายให้ลงสู่ระดับที่ยอมรับได้ ถึงแม้ว่าการคัดเลือกระดับความปลอดภัยจะค่อนข้างยุ่งยากและซับซ้อนในบางกระบวนการและการทำงานบางชนิด แต่เป้าหมายสูงสุดขององค์กรทุกองค์กรก็คือการทำให้กระบวนการทำงานอยู่ในระดับที่มีความปลอดภัยมากที่สุด ฟังก์ชันนิรภัยจึงถูกออกแบบให้มีระดับความปลอดภัยที่เหมาะสมกับกระบวนการ จากรูปที่ 2.4 ผลจากการศึกษาของหน่วยงานที่ว่าด้วยเรื่องสุขภาพ ความปลอดภัย และสิ่งแวดล้อมภายในโรงงาน (HSE : Health and Safety Executive) ในประเทศอังกฤษแสดงให้เห็นถึงความผิดพลาดในการทำงานของระบบนิรภัย ผลจาก

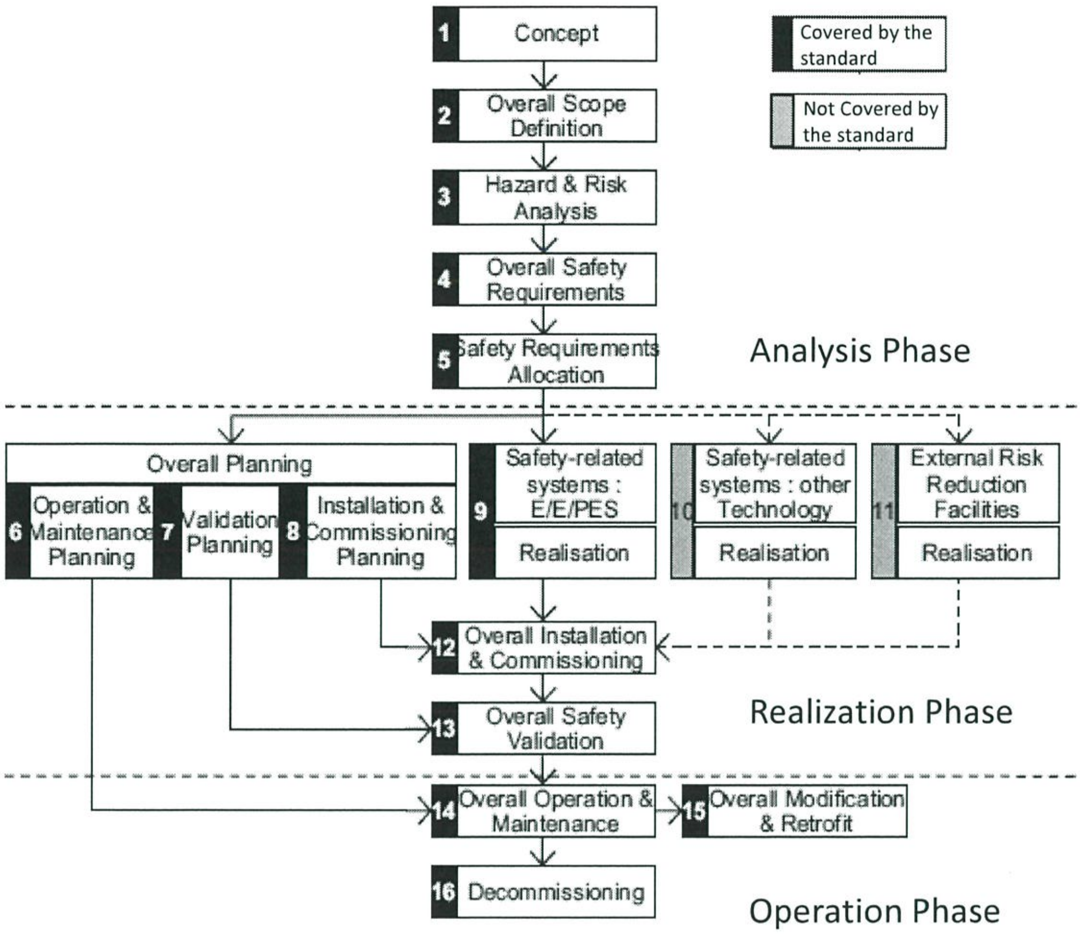
การสำรวจพบว่า 44% จากความเสียหายทั้งหมด เกิดจากปัญหาทางด้านรายละเอียดของข้อมูลที่ไม่เพียงพอต่อการออกแบบแนวทางการป้องกัน จากปัญหาดังกล่าวองค์กรจากชาติต่าง ๆ ที่เกี่ยวข้องกับความปลอดภัยในการทำงาน จึงได้มีการตั้งมาตรฐานกระบวนการทำงานเพื่อเป็นแนวทางให้กับอุตสาหกรรมต่าง ๆ เพื่อนำไปสู่เป้าหมายเดียวกันนั่นคือความปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อม โดยมาตรฐานที่เกี่ยวข้องกับความปลอดภัยที่ได้กล่าวถึงไปแล้ว คือ มาตรฐาน IEC 61508, IEC 61511 และ ANSI/ISA-84.01-1996

สิ่งที่มีอยู่ภายใต้มาตรฐาน IEC 61508, IEC 61511 และ ANSI/ISA-84.01-1996 เป็นพื้นฐานในการอธิบายถึงวิธีการที่ใช้ในการคัดเลือกแนวทางการออกแบบ แนวทางการพัฒนา และแนวทางการบำรุงรักษาระบบวัดคุมนิรภัย พร้อมกับการจดบันทึกเป็นเอกสารที่ใช้ในการตรวจสอบ วิธีที่ใช้ในการยืนยันความถูกต้องของระบบนิรภัย คือ วงจรความปลอดภัย (SLC : SLC Safety Life Cycle) โดยมาตรฐาน IEC 61511 อธิบายความหมายของวงจรความปลอดภัยไว้ว่า “กิจกรรมที่มีส่วนร่วมและจำเป็นในการพัฒนาฟังก์ชันวัดคุมนิรภัย โดยจะเริ่มขึ้นตั้งแต่ช่วงเวลาเริ่มต้นร่างโครงสร้างของโครงการและจนเสร็จสิ้นเมื่อฟังก์ชันนิรภัยไม่สามารถใช้งานได้แล้ว” ความหมายคือครอบคลุมการทำงานของระบบนิรภัยในทุก ๆ ด้านจนกว่าจะหยุดการทำงาน ความต้องการของมาตรฐานวงจรนิรภัยในอุตสาหกรรมเริ่มมีการพัฒนามากว่า 20 ปี เนื่องจากระบบอิเล็กทรอนิกส์และโปรแกรมของระบบนิรภัยมีอัตราการใช้งานที่สูงในภาคอุตสาหกรรม จุดเริ่มต้นในการเริ่มสร้างโครงสร้างและมาตรฐานของวงจรนิรภัย คือ หน่วยงาน U.K. Health and Safety Executive ได้จัดทำเอกสาร Programmable Electronic Systems in Safety Related Application, parts 1 and 2 ในปี ค.ศ. 1987 ที่มุ่งเน้นการใช้งานเกี่ยวกับโปรแกรมของระบบนิรภัย ต่อมา IEC ได้มีการพัฒนาเอกสารมาตรฐาน IEC 61508 ขึ้นมาเพื่อใช้ในอุปกรณ์ไฟฟ้า/อิเล็กทรอนิกส์/ระบบอิเล็กทรอนิกส์แบบโปรแกรมได้และ IEC 61511 เพื่อใช้ในอุตสาหกรรมการผลิตควบคู่กับมาตรฐาน ANSI/ISA-84.01-1996 ของอเมริกาที่เกี่ยวกับการใช้งานระบบนิรภัยในกระบวนการผลิต มาตรฐาน IEC 61508/61511 และ ANSI/ISA-84.01-1996 มีแนวทางของวงจรนิรภัยที่แตกต่างกันเพียงเล็กน้อย แต่ในปัจจุบันจะมีการใช้มาตรฐาน IEC 61511 ในอุตสาหกรรมการผลิตมากกว่าเนื่องจากมีความทันสมัยและมีการยืนยันในขั้นตอนต่าง ๆ ละเอียดกว่ามาตรฐาน ANSI/ISA-84.01-1996 หากพิจารณาถึงแนวทางการปฏิบัติของวงจรนิรภัยของมาตรฐานทั้ง 3 มาตรฐานจะพบว่ามีรูปแบบที่คล้ายคลึงกัน ในการอธิบายนี้จึงขอยกตัวอย่างวงจรความปลอดภัยจากมาตรฐาน IEC 61508 ซึ่งแบ่งขั้นตอนหรือระยะในการทำงานออกเป็น 3 ระยะหลัก คือ ระยะการวิเคราะห์ (Analysis Phase) ระยะการออกแบบและพัฒนา (Realization Phase) และระยะการทำงาน (Operation Phase) ดังแสดงในรูปที่ 2.5



รูปที่ 2.4 ผลสำรวจต้นเหตุปัญหาความผิดพลาดของระบบป้องกัน

ที่มา : William M. Goble, 2005 : หน้าที่ 4



รูปที่ 2.5 วงจรนิรภัย (Safety Life Cycle) จากมาตรฐาน IEC 61508

ที่มา : William M. Goble, 2005 : หน้าที่ 7

2.1.4.1 ระยะการวิเคราะห์

ในระยะการวิเคราะห์ (Analysis Phase) ของวงจรนิรภัยประกอบไปด้วยการเริ่มต้นวางแผนผัง และกำหนดฟังก์ชันนิรภัยในการทำงานที่จำเป็นในกระบวนการที่มีความเสี่ยง ฟังก์ชันการทำงานในแต่ละฟังก์ชันจะต้องได้รับการพิจารณาอย่างละเอียดถี่ถ้วน โดยข้อมูลที่จะได้จากระยะการวิเคราะห์จะเรียกว่า ข้อกำหนดด้านความปลอดภัย (SRS : Safety Requirements Specification) ที่ทำการรวบรวมข้อมูลต่าง ๆ ไว้เพื่อใช้ในกระบวนการของระบบนิรภัยทั้งหมด จากรูปที่ 2.6 แสดงให้เห็นขั้นตอนการทำงานของระบบวัดคุมนิรภัยซึ่งประกอบไปด้วยข้อมูลหลัก คือ ระดับความปลอดภัยของฟังก์ชันนิรภัยที่กระบวนการต้องการ ความถี่และผลกระทบของเหตุการณ์อันตราย ค่าตัวแปรต่าง ๆ ของกระบวนการ แผนภาพลอจิกและการเชื่อมต่อ รวมถึงเทคนิคในการติดตั้งและซ่อมบำรุงในการใช้งาน แบ่งขั้นตอนได้ดังนี้

ขั้นตอนที่ 1 ตั้งโครงร่างของโครงการในการเพิ่มระบบนิรภัย โดยการพิจารณาจากข้อมูลของกระบวนการผลิต เช่น แผนภาพ P&ID แผนภาพลอจิก

ขั้นตอนที่ 2 พิจารณาความอันตรายที่มีโอกาสเกิดขึ้น โดยการนำข้อมูลสถิติของการทำงาน หรือ ข้อมูลจากแหล่งอื่นที่เชื่อถือได้มาทำการพิจารณา

ขั้นตอนที่ 3 วิเคราะห์ผลกระทบของเหตุการณ์ โดยนำเหตุการณ์ที่มีโอกาสที่จะเกิดขึ้นในขั้นตอนที่ 2 มาพิจารณาผลกระทบและความรุนแรงหากเกิดเหตุการณ์อันตรายขึ้น ขั้นตอนนี้อาจใช้เทคนิคในการพิจารณา เช่น การวิเคราะห์ด้วยแผนภาพต้นไม้ (Event Tree Analysis) เป็นต้น

ขั้นตอนที่ 4 วิเคราะห์อัตราการเกิดของเหตุการณ์ โดยนำข้อมูลจากสถิติหรือจากแหล่งอื่นที่เชื่อถือได้ มาทำการคำนวณความน่าจะเป็นของเหตุการณ์อันตรายที่เกิดขึ้น โดยใช้เทคนิค LOPA (Layers of Protection Analysis) พร้อมกับข้อมูลอัตราความเสี่ยง (Failure Rate)

ขั้นตอนที่ 5 การคัดเลือกระดับความปลอดภัย (SIL) ให้แก่กระบวนการ โดยจะต้องพิจารณาก่อนว่า ผลและความน่าจะเป็นของเหตุการณ์อันตรายนั้นมีความร้ายแรงมากเพียงใด และอยู่ในขอบเขตที่รับได้หรือไม่ หากเหตุการณ์มีความรุนแรงหรือเกิดขึ้นถี่เกินไป ก็จะต้องมีการติดตั้งระบบนิรภัยเพิ่มเติมเพื่อให้อยู่ในย่านความเสี่ยงที่ยอมรับได้

ขั้นตอนที่ 6 การจัดทำเอกสารประกอบการพิจารณา โดยจะรวบรวมข้อมูลผลที่ได้จากขั้นตอนทั้งหมด รวมถึงข้อมูลเฉพาะของกระบวนการ เช่น ข้อมูลการทำงานพื้นฐานของอุปกรณ์ ระยะเวลาที่ระบบนิรภัยจะต้องปฏิบัติการ ให้ระบบเข้าสู่ความปลอดภัย ตามระยะเวลาการทดสอบฟังก์ชันนิรภัยที่ต้องการ

2.1.4.2 ระยะการออกแบบและพัฒนา

ระยะการออกแบบและพัฒนา (Realization Phase) ในวงจรนิรภัย คือ ช่วงเวลาการติดตั้งพัฒนาและทดสอบระบบนิรภัยที่ถูกพิจารณาใช้งานในระยะการวิเคราะห์ ระยะการออกแบบและพัฒนาจะไม่สามารถทำได้หากเอกสารข้อกำหนดต่าง ๆ ที่ได้จากระยะการวิเคราะห์ไม่สมบูรณ์และถูกต้อง โดยขั้นตอนการทำงานของระยะการออกแบบและพัฒนาตามรูปที่ 2.7 แบ่งออกได้เป็นดังนี้

ขั้นตอนที่ 7 การเลือกเทคโนโลยีที่ใช้งาน เป็นขั้นตอนการเลือกอุปกรณ์ที่ใช้ในการวัด หน่วยประมวลผล และอุปกรณ์สุดท้ายในฟังก์ชันนิรภัย การเลือกรูปแบบการเชื่อมต่อของฟังก์ชันนิรภัย โดยจะเพิ่มความสามารถของฟังก์ชันนิรภัยมากยิ่งขึ้น จะเรียกว่าอุปกรณ์สำรอง (Redundancy) โดยมีอยู่หลายแบบการใช้งาน เช่น 1oo2 (1 out of 2), 2oo3 (2 out of 3) เป็นต้น พร้อมกับการเลือกรูปแบบการทดสอบ

(Test Philosophy) ของฟังก์ชันวัดคุมนิรภัย ทำการคำนวณค่าความปลอดภัยของฟังก์นิรภัยที่ออกแบบ โดยใช้ค่าอัตราการล้มเหลวของอุปกรณ์ในฟังก์ชันนิรภัย ที่ได้มาจากข้อมูลสถิติ คู่มือความปลอดภัยของหน่วยงานอื่น ๆ ที่ใกล้เคียง หรือจากใบรับรองของอุปกรณ์จากองค์กรที่ได้รับมาตรฐานความปลอดภัย หากพบว่าฟังก์ชันนิรภัยที่ออกแบบ ไม่สามารถใช้งานได้ในระดับความปลอดภัยที่ต้องการ จะต้องพิจารณารูปแบบและข้อมูลที่เกี่ยวข้องใหม่ เพื่อให้ได้ระดับความปลอดภัยที่กระบวนการต้องการ และลดระดับความเสี่ยงของเหตุการณ์อันตรายลง

ขั้นตอนที่ 8 ออกแบบรายละเอียดของระบบนิรภัย ตั้งแต่การเชื่อมต่อของอุปกรณ์ไปสู่หน่วยประมวลผล จนถึงลอจิกในการทำงานของฟังก์ชันนิรภัย และแผนภาพรายละเอียดการเชื่อมต่อ ระบบนิรภัยจะต้องถูกรับรองจากผู้ผลิตเพื่อให้แน่ใจว่าสามารถใช้งานได้อย่างถูกต้อง

ขั้นตอนที่ 9 วางแผนการติดตั้งและตรวจสอบการใช้งาน ในส่วนนี้จะใช้ข้อมูลจากผู้ผลิตอุปกรณ์ ประกอบกับแผนการติดตั้งของผู้ใช้งานในอุตสาหกรรม เพื่อเป็นแนวทางในการตรวจสอบอุปกรณ์ในฟังก์ชันนิรภัย ก่อนที่จะทำการทดสอบการใช้งานจริง (Validation)

ขั้นตอนที่ 10 ตรวจสอบการติดตั้งและตรวจสอบการใช้งานจริง คือขั้นตอนการทดสอบฟังก์ชันนิรภัยอย่างละเอียด ว่าสามารถใช้งานได้ถูกต้องตามที่ออกแบบมา ก่อนทำการติดตั้งลงในกระบวนการผลิตเพื่อใช้ในการลดความเสี่ยง

2.1.4.3 ระยะการทำงาน

ในระยะการทำงาน (Operation Phase) ของวงจรนิรภัยในรูปที่ 2.8 จะเป็นช่วงที่ใช้ระยะเวลานานที่สุดเนื่องจากฟังก์ชันนิรภัยที่ถูกทดสอบและติดตั้งแล้ว จะถูกใช้งานจนกว่าจะมีการเปลี่ยนแปลงอุปกรณ์ในระบบนิรภัยหรือมีการถอดถอนการใช้งานของฟังก์ชันนิรภัยนั้น หากมีการพิจารณาความเสี่ยงใหม่ภายใต้การทำงานของฟังก์ชันนิรภัย จะต้องทำการทดสอบและซ่อมแซมเป็นระยะตามข้อกำหนดด้านความปลอดภัย (SRS : Safety Requirements Specification) เพื่อให้ระบบนิรภัยมีความพร้อมในการทำงานรับมือเหตุการณ์อันตรายอยู่ตลอดเวลา โดยจะแบ่งขั้นตอนได้ดังนี้

ขั้นตอนที่ 11 นำข้อมูลจากการวางแผนความถูกต้องมาตรวจสอบก่อนใช้งานจริง

ขั้นตอนที่ 12 การตรวจสอบข้อมูลก่อนทำการติดตั้งใช้งาน กระบวนการระบบนิรภัยนั้นต้องแน่ใจว่า มีข้อมูลการทำงานด้านต่าง ๆ ของฟังก์ชันนิรภัยและทำการทดสอบที่ถูกต้องตามขั้นตอนกำหนดไว้

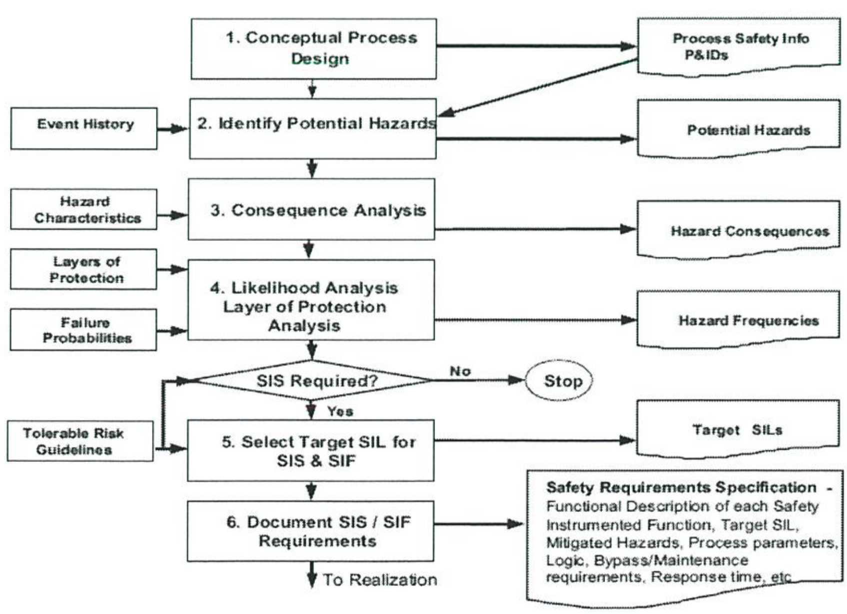
ขั้นตอนที่ 13 นำข้อมูลจากการวางแผนการทำงาน และซ่อมบำรุงมาใช้งานในการทำงาน

ขั้นตอนที่ 14 ติดตั้งและเริ่มดำเนินงานในกระบวนการ โดยขั้นตอนนี้จะเป็นขั้นตอนที่มีระยะเวลานานที่สุดในวงจรนิรภัยซึ่งจะต้องใช้ข้อมูลในการทดสอบฟังก์ชันนิรภัย และการซ่อมบำรุงตามระยะเวลากับวิธีการทดสอบที่แตกต่างกัน

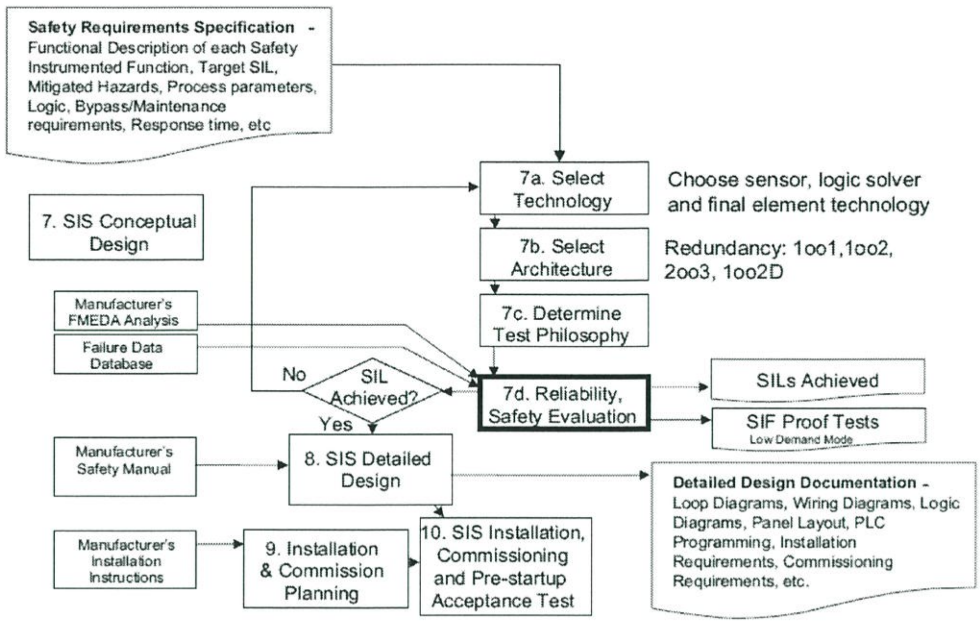
ขั้นตอนที่ 15 การเปลี่ยนแปลงของระบบนิรภัย หากระบบนิรภัยนั้นมีปัญหาให้การจัดการความเสี่ยง หรือจุดการทำงานนั้นเกิดผิดพลาดจะต้องพิจารณาว่า ต้องแก้ไขระบบนิรภัยในช่วงไหน จึงจะสามารถสร้างความถูกต้องปลอดภัยและมั่นคงที่ดีขึ้น แต่หากกระบวนการในระบบนั้นถูกเลิกใช้หรือถูกพิจารณาใหม่แล้วว่าแม้ไม่มีระบบนิรภัย ผลของความเสี่ยงก็อยู่ในเกณฑ์ที่ไม่ร้ายแรง ระบบนิรภัยก็จะเป็นสิ่งที่เกินความจำเป็นในการออกแบบใช้งาน (Over Design) ทำให้เสียเวลาในการทดสอบและซ่อมแซม

ขั้นตอนที่ 16 การถอดถอนการใช้งาน เมื่อระบบนิรภัยไม่มีความจำเป็นอีกต่อไปในกระบวนการ เช่น ระบบนิรภัยมีการทำงานที่ผิดปกติอยู่บ่อยครั้งโดยการหยุดการทำงาน โดยไม่ได้เกิดเหตุการณ์อันตรายขึ้นจริง (Spurious Trip) จะเป็นผลเสียต่อกระบวนการมากกว่าผลดีที่จะได้รับ ทำให้ต้องยกเลิกการใช้ระบบนิรภัยในกระบวนการนั้น ๆ ไป

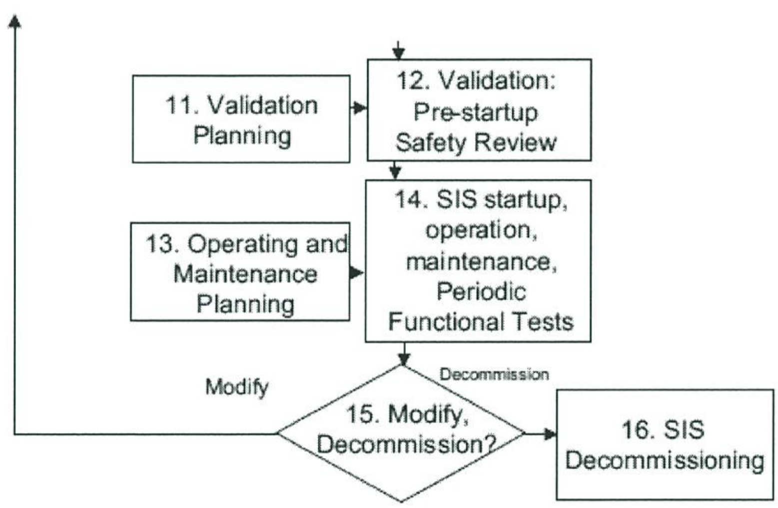
จากขั้นตอนทั้งหมดที่ได้อธิบายไปนั้น แสดงถึงแนวทางในการสร้างวงจรนิรภัยอย่างถูกต้องเพื่อการใช้งานระบบนิรภัยที่มีข้อมูลเป็นสากล และเป็นไปตามมาตรฐานอุตสาหกรรมอื่น ๆ ในเรื่องของความปลอดภัยต่อชีวิต ทรัพย์สิน สิ่งแวดล้อม และผลประกอบการ



รูปที่ 2.6 ขั้นตอนการทำงานของระบบวัดคุมนิรภัยในระยะการวิเคราะห์



รูปที่ 2.7 ขั้นตอนการทำงานของระบบวัดคุมนิรภัยในระยะการออกแบบและพัฒนา



รูปที่ 2.8 ขั้นตอนการทำงานของระบบวัดคุมนิรภัยในระยะการทำงาน

2.2 การวิเคราะห์ผลกระทบของกระบวนการ

การวิเคราะห์ผลกระทบ (Consequence Analysis) ของกระบวนการ คือ ขั้นตอนหนึ่งที่มีความสำคัญในวงจรนิรภัย เพื่อที่จะพิจารณาคัดเลือกระดับความปลอดภัยและแนวทางการรับมือต่อผลกระทบโดยติดตั้งฟังก์ชันนิรภัยในส่วนนั้น ผู้ใช้จะต้องทำการประเมินผลกระทบจากความเสี่ยงในกระบวนการแต่ละส่วนเพื่อเป็นจุดตั้งต้นในการสร้างระบบนิรภัย โดยต้องศึกษากระบวนการด้านในว่ามีผลอันตรายอะไรบ้างโดยทำการวิเคราะห์อันตราย (PHA : Process Hazard Analysis) หรือการทำ HAZOP (Hazard and Operability Study) ซึ่งจะต้องใช้ความรู้จากหลากหลายแขนงการทำงานในการวิเคราะห์ถึงเหตุและผลที่จะเกิดขึ้นหากกระบวนการมีการเปลี่ยนแปลง ภายใต้มาตรฐาน IEC 61508 ได้กำหนดการวิเคราะห์ผลกระทบอันตรายไว้ในขั้นตอนที่ 3 โดยมีวัตถุประสงค์เพื่อ

- ค้นหาแหล่งกำเนิดอันตรายหรือสาเหตุของอุบัติเหตุที่อาจเกิดขึ้นจากกระบวนการผลิต
- ค้นหาอันตรายที่แอบแฝงอยู่ในกระบวนการผลิต

2.2.1 วิธีในการวิเคราะห์ผลกระทบของกระบวนการ

วิธีในการวิเคราะห์ผลกระทบของกระบวนการ เพื่อให้เป็นไปตามวัตถุประสงค์จะมีอยู่หลายวิธีด้วยกันดังนี้

1) Checklist คือ การวิเคราะห์ความเสี่ยงโดยการตั้งคำถาม โดยส่วนใหญ่ Checklist จะใช้ในรูปแบบของกระบวนการที่ค่อนข้างเล็กมีความคล้ายคลึงกันค่อนข้างสูง
2) What – If analysis คือ การวิเคราะห์ความเสี่ยงโดยการตั้งคำถามเช่นเดียวกับ Checklist จึงมีการใช้ร่วมกันอยู่บ่อยครั้ง What – if analysis เป็นการพิจารณาว่าหากเกิดเหตุการณ์ดังต่อไปนี้ขึ้น กระบวนการจะมีผลกระทบอย่างไรบ้าง โดยปกติแล้ววิธีการนี้จะใช้กับกระบวนการที่มีผลกระทบไม่ร้ายแรง
3) Hazard and Operability Studied (HAZOP) คือ วิธีการวิเคราะห์อันตรายที่ใช้กันมากที่สุด การทำ HAZOP นั้นจะทำการพิจารณากระบวนที่ค่อนข้างใหญ่และมีความละเอียดสูง โดยจะนำมาแบ่งเป็นฟังก์ชันการทำงานย่อย ๆ เรียกว่าโหนด (Node) เพื่อทำการวิเคราะห์หาสาเหตุของตัวแปรทุกตัวที่มีผลกระทบในโหนดนั้น ประเมินผลของเหตุการณ์อันตราย พร้อมทั้งพิจารณาชั้นป้องกันเดิมและนำเสนอชั้นป้องกันที่จะต้องเพิ่มเติม
4) Fault Tree Analysis (FTA) คือ การวิเคระห์ความเสี่ยงจากแผนภาพความผิดพลาดที่จะเกิดขึ้นจากกระบวนการในแต่ละส่วน ที่เชื่อมต่อเป็นรูปแบบสัญลักษณ์ลอจิก หรือลอจิกเกต (Logic Gate)
5) Failure Modes and Effect Analysis (FMEA) คือ การวิเคราะห์ความเสี่ยงโดยเน้นไปในเหตุที่ทำให้ระบบอยู่ในสภาวะล้มเหลว และจะส่งผลอย่างไรต่อระบบการทำงาน ผลลัพธ์ในการพิจารณาจะได้ค่าอัตราการเสียหายของกระบวนการ
6) Event Tree Analysis (ETA) คือ การวิเคราะห์ความเสี่ยงโดยพิจารณาจากเหตุที่ทำให้เกิดเหตุการณ์อันตราย โดยผ่านการพิจารณาความเป็นไปได้ในแต่ละขั้นตอน เช่น เกิดการรั่วไหลของท่อส่งน้ำมัน น้ำมันที่รั่วออกมาจะเกิดการลุกไหม้หรือไม่ หากไหม้แล้วจะเกิดอะไรตามมาและหากไม่ไหม้จะส่งผลอย่างไรเป็นต้น

การเลือกใช้งานวิธีการใดนั้น ขึ้นอยู่กับความชำนาญของผู้ดำเนินการ (Chairman) และผู้เข้าร่วมการวิเคราะห์ สำหรับวิธีการที่รู้จักและใช้งานกันอย่างกว้างขวางจะเป็นวิธีที่เรียกว่า HAZOP โดยจะทำการวิเคราะห์ตัวแปรในกระบวนการทุกตัวที่เกิดขึ้น และจะพิจารณาผลกระทบที่ได้จากการเบี่ยงเบนไปของตัวแปรเหล่านั้น ถ้าผลกระทบจากการเบี่ยงเบนของกระบวนการสามารถทำให้เกิดอันตรายได้ ทีมวิเคราะห์ผลกระทบก็จะมีคำแนะนำให้จัดเตรียมฟังก์ชันนิรภัยในการป้องกันอันตรายที่อาจจะเกิดขึ้นดังแสดงในตารางที่ 2.1

ตารางที่ 2.1 ตัวอย่างตารางการทำ HAZOP ของหอกลั่นในส่วน Reboiler

ตาราง HAZOP ของหอกลั่น Node: ส่วน Reboiler			
ค่าตัวแปร : ความดันสูงขึ้น (More Pressure)			
สาเหตุ	ผลกระทบ	ระบบ Safeguards	คำแนะนำจากการพิจารณา
ไม่สามารถควบคุมไอน้ำที่ใช้ในการ Reboiler ทำให้มีความร้อนเกิน	หอกลั่นเกิดความดันเกิน อุปกรณ์ทางกลเสียหาย และรั่วไหล	มีวาล์วนิรภัยทางกลและผู้ปฏิบัติงานแก้ไขหากเกิดอันตราย	ติดตั้งฟังก์ชันนิรภัยเพื่อหยุดความดันเกิน
ท่อ Reboiler ของไอน้ำเกิดการรั่วไหลจากความดันสูง			

2.2.2 รูปแบบผลกระทบของกระบวนการ

การวิเคราะห์ทั้งหมดที่จะถูกนำไปใช้งาน ผู้เข้าร่วมการพิจารณาจะต้องมีความรู้และเชี่ยวชาญในแต่ละเรื่อง ผู้ร่วมวิเคราะห์จะมีตั้งแต่วิศวกรด้านความปลอดภัย วิศวกรซ่อมบำรุงในฝ่ายเครื่องมือวัดและเครื่องกล ผู้ปฏิบัติงานควบคุมกระบวนการ และวิศวกรกระบวนการผลิตในแต่ละกระบวนการต่างที่เกี่ยวข้อง ก็จะมีผลกระทบที่แตกต่างกันไปแต่โดยพื้นฐานในการพิจารณาผลกระทบในกระบวนการ เหตุการณ์อันตรายที่เกิดขึ้นในการผลิตจะสามารถแบ่งออกได้เป็น 3 รูปแบบหลัก คือ ผลจากการติดไฟ (Flammability Effect) ผลจากการระเบิด (Explosion Effect) และผลจากสารพิษรั่วไหล (Toxic Hazard)

(ก) (ข)

รูปที่ 2.9 องค์ประกอบการเกิดของผลกระทบ

(ก) การเกิดไฟจากสามเหลี่ยมไฟ (Fire Triangle)

(ข) การเกิดระเบิดจากห้าเหลี่ยมการระเบิด (Explosion Pentagon)

2.2.2.1 ผลจากการติดไฟ

ผลจากการติดไฟ (Flammability Effect) เป็นผลที่เกิดจากสารผลิตภัณฑ์ที่รั่วไหลออกมาจากกระบวนการที่อยู่ในสภาพที่สามารถติดไฟ โดยการพิจารณาคุณสมบัติการติดไฟจากรูปที่ 2.9 (ก) องค์ประกอบของไฟ (Fire Triangle) จะประกอบไปด้วยการมีความร้อน (Heat) มีเชื้อเพลิง (Fuel) และมีออกซิเจน (Oxygen) ที่เพียงพอและเหมาะสม พลังงานจากความร้อนจากการ

เผาไหม้จะแผ่รังสีกระจายตามสัดส่วนของการเผาไหม้เข้าไปในเครื่องตรวจจับเพลิงไหม้ เนื่องจากการเผาไหม้ทั้งหมดไม่ได้มีควันหรือเขม่าที่สามารถมองเห็นได้เสมอไป การติดไฟของไฮโดรเจน (Hydrogen) ในเวลากลางวันที่จะแผ่รังสีความร้อนเข้มข้นมากเป็นหนึ่งในกรณีนั้น ในการพิจารณาจากการเกิดเพลิงไหม้นั้นจะมีการพิจารณาบริเวณที่เกิด ขนาดพื้นที่ที่จะเกิดเพลิงไหม้จนถึงจุดสิ้นสุด (Endpoint) ความชื้น (Humidity) เขม่าควัน (Smoke) เพื่อกำหนดระดับของรังสีความร้อน (Thermal Radiation Flux) มีหน่วยเป็นกิโลวัตต์ต่อตารางเมตร (kW/m^2) รูปแบบการจุดติดของไฟนั้นมีหลายรูปแบบขึ้นอยู่กับหลายปัจจัย โดยแบ่งประเภทการเกิดเพลิงไหม้ได้เป็น 4 แบบ ประกอบด้วย การเผาไหม้แบบไฟลุกท่วมหรืออ่างไฟ การเผาไหม้จากความดันสูง การเผาไหม้จากการวาบไฟ และการเผาไหม้แบบลูกบอลไฟหรือการระเบิดจากไอของเหลวที่มีความร้อน

1) การเผาไหม้แบบไฟลุกท่วมหรืออ่างไฟ (Pool fire) คือ รูปแบบของการติดไฟที่คล้ายอ่างซึ่งจะลุกท่วมทั่วบริเวณ เมื่อการรั่วไหลเป็นของเหลวที่เป็นเชื้อเพลิง (Spilled Flammable Liquids) ขนาดพื้นที่ในการเกิดอ่างไฟจะขึ้นอยู่กับขนาดของเปลวไฟที่เผาไหม้อยู่ และยังขึ้นอยู่กับขนาดพื้นที่ของการรั่วไหลและคุณสมบัติของเชื้อเพลิง หากทำการเปรียบเทียบการรั่วไหลและการติดไฟของน้ำมันดีเซลและก๊าซ LNG (Liquid Natural Gas) ในการเกิดรูปแบบอ่างไฟที่มีขนาดพื้นที่เท่ากันจะสามารถตอบได้อย่างชัดเจนว่าอ่างไฟของก๊าซ LNG จะมีพื้นที่ความเสียหายที่มากกว่าน้ำมันดีเซลมาก เนื่องจากในการเผาไหม้น้ำมันดีเซลนั้นจะเกิดเขม่าควันค่อนข้างสูง เขม่าควันนั้นเป็นตัวขัดขวางพลังงานการแผ่รังสีความร้อน อีกทั้งก๊าซ LNG มีความดันไอที่สูงและใช้ความร้อนต่ำกว่าดีเซลในการละเหยกลายเป็นไอ
2) การเผาไหม้จากความดันสูง (Jet fire) คือ รูปแบบของการติดไฟที่เกิดจากสารที่สามารถติดไฟได้ในกระบวนการที่มีความดันสูง เกิดการรั่วไหลออกมา ผลจากพลังงานจลน์ของสารที่พุ่งออกมาด้วยความดันสูงจะช่วยสนับสนุนให้เกิดการผสมกันระหว่างสารที่รั่วไหล ออกซิเจนในอากาศและเกิดเปลวเพลิงที่พวยพุ่งออกมาจากกระบวนการ ขนาดของเปลวเพลิงถูกพิจารณาจากเงื่อนไขต่าง ๆ ของการรั่วไหล ความดันและขนาดของพื้นที่ในการรั่วไหล เป็นส่วนสำคัญในการเกิดการเผาไหม้จากความดันสูงจากการที่สารนั้นพุ่งออกมาด้วยความเร็ว ทำให้ยิ่งห่างไกลจากจุดรั่วไหลมากเท่าใด ก็จะยิ่งมีออกซิเจนในการผสมทำให้เกิดเปลวเพลิง นอกเหนือจากนั้นองค์ประกอบอื่น ๆ จะถูกพิจารณาคล้ายกับกรณีอ่างไฟ
3) การเผาไหม้จากการวาบไฟ (Flash Fire) คือ ผลจากการจุดติดของกลุ่มก้อนไอที่ติดไฟได้ เมื่อความเร็วของการเปลวเพลิงช้าเกินกว่าจะเกิดคลื่นการระเบิด (Explosive Shock Wave) ซึ่งเปลวไฟจะเคลื่อนที่จากจุดติดไฟไปจนถึงจุดที่มีการผสมของเชื้อเพลิงและอากาศ จุดสิ้นสุดการเกิดเพลิงไหม้จะเป็นพื้นที่ที่เกิดความเสียหายจากการวาบไฟ การเผา

ไหม้จากการวาบไฟจะมีเวลาที่น้อยกว่าแบบอ่างไฟ และจากแบบความดันสูงจึงทำให้มีความเสียหายกับตัวอุปกรณ์น้อยกว่า

4) การเผาไหม้แบบลูกบอลไฟ การระเบิดจากไอของของเหลวที่มีความร้อน (Fireball/BLEVE) คือ ผลจากการรั่วไหลอย่างฉับพลันของก๊าซไวไฟหรือการระเหยของของเหลวที่อยู่ภายใต้ความดัน และเกิดการระเบิดฉับพลัน โดยจะคล้ายคลึงกับการเผาไหม้แบบความดันสูงอยู่ช่วงระยะหนึ่งในการรั่วไหลแต่แตกต่างเพียงรูปร่างของเปลวเพลิง ในเวลาอันสั้นต่อมาก๊าซไวไฟ และของเหลวที่ระเหยจะเกิดการขยายตัวของกลุ่มก้อนก๊าซที่ไวไฟ (Vapor Cloud) และอยู่ในสภาวะช่วงของการติดไฟ (UFL : Upper Flammability Limit) หากมีการจุดติดของการเผาไหม้ จะเกิดการระเบิดด้วยเปลวเพลิงลักษณะเป็นลูกไฟอย่างฉับพลัน และเนื่องจากความหนาแน่นจากการเผาไหม้ ทำให้ลูกไฟมีความหนาแน่นต่ำลงและลอยตัวขึ้นไปบนอากาศ โดยจะถูกเรียกว่า เมฆเห็ด (Mushroom Cloud) ที่มีรูปร่างเหมือนเห็ด นอกจากลูกบอลไฟแล้ว การเกิดเพลิงไหม้แบบ BLEVE (Boiling Liquid Expanding Vapor Explosion) ในถังเวสเซลที่เก็บของเหลวไวไฟก็มีจะลักษณะเหมือนกัน โดยที่การเกิดไฟที่เผาจากด้านนอก จะทำให้ของเหลวด้านในมีอุณหภูมิสูงขึ้นและระเหยตัวทำให้มีความดันสูงขึ้น จนผิวของถังเวสเซลไม่สามารถทนต่อความดันได้จึงเกิดการแตกหักและเกิด BLEVE ซึ่งมีผลเสียหายค่อนข้างกว้างและไม่สามารถควบคุมได้เนื่องจากการระเบิดของถัง ทำให้เหล็กที่แตกพุ่งไปในทุกทิศทาง ก๊าซหรือไอที่ไวไฟมีการฟุ้งกระจายทั่วบริเวณส่งผลให้เกิดความเสียหายที่ค่อนข้างรุนแรงมาก

อย่างไรก็ตามแม้ไม่เกิดเพลิงไหม้ ผลิตภัณฑ์ที่มีความร้อนก็ยังสามารถสร้างความเสียหายให้แก่ชีวิต กระบวนการ และอุปกรณ์รอบข้างได้เช่นกัน

2.2.2.2 ผลจากการระเบิด

ผลจากการระเบิด (Explosion Effect) จากรูปที่ 2.9 (ข) การเกิดระเบิดจากห้าเหลี่ยมการระเบิด ซึ่งประกอบไปด้วย เชื้อเพลิง อ็อกซิเจน ความร้อน เช่นดียวกับการเกิดไฟ แต่การระเบิดจะมีองค์ประกอบเพิ่มเติมขึ้นมานั่นคือ การกระจายตัว (Dispersion) ของกระบวนการและการจำกัด (Confinement) ของอุปกรณ์ ผลจาการระเบิดจะทำให้เกิดคลื่นกระแทก (Blast Wave) จากการเกิดแรงดันเกินสูงกว่าระดับที่อุปกรณ์สามารถทนได้ ซึ่งเกิดค่อนข้างมากในกระบวนการผลิต จากข้อมูลการสำรวจใน 752-Management of Hazards Associated with Location of Process Plant Building, The Effects of Nuclear Weapons พบว่าหากความดันเกินจากการออกแบบเพียง 0.5 psig สามารถทำให้กระจกแตกและความดันเกิน 5 psig ทำให้เกิดความเสียหายของผิวอุปกรณ์และมีสิทธิ์ในการรั่วไหลตามหน้าแปลน (Flange) โดยแบ่งประเภทการระเบิดไหม้ได้เป็น 2 แบบ ได้แก่ การระเบิดของกลุ่มก้อนไอ และการระเบิดทางกายภาพ

1) การระเบิดของกลุ่มก้อนไอ (VCE : Vapor Cloud Explosion) คือ การระเบิดจากสารไวไฟในสภาพก๊าซ โดยที่การระเบิดประเภทนี้มีลักษณะการเกิดโดยก๊าซที่ติดไฟจำนวนมาก เกิดการรั่วไหลออกมาผสมกับ

อากาศโดยรอบ เมื่อมีการเกิดประกายไฟขึ้นมาและมีพลังงานเพียงพอในการระเบิด จะทำให้เกิดการระเบิดของกลุ่มก้อนไอขึ้นพร้อมเกิดคลื่นกระแทก หากพลังงานในการเกิดประกายไฟมีพลังงานไม่ถึงการระเบิด จะทำให้เกิดการเผาไหม้แบบลูกบอลไฟทันที

2) การระเบิดทางกายภาพ (Physical Explosion) คือ เกิดจากการระเบิดของอุปกรณ์ที่มีความดันสูงอยู่ภายใน เกิดการสะสมพลังงานศักย์ (Potential Energy) ซึ่งเปลี่ยนเป็นพลังงานจลน์ (Kinetic Energy) หลังจากที่เกิดการรั่วไหล การระเบิดทางกายภาพอาจเกิดลูกบอลไฟได้เช่นกันหากสารนั้นไวไฟและมีการจุดติดของประกายไฟ

2.2.2.3 ผลจากสารพิษรั่วไหล

ผลจากสารพิษรั่วไหล (Toxic Hazard) ของสารพิษที่เกิดขึ้นตลอดเวลาในกระบวนการผลิตโดยเฉพาะคาร์บอนไดออกไซด์ คาร์บอนมอนน็อกไซด์ คลอรีน เป็นต้น แม้ว่าการรั่วไหลของสารพิษในกระบวนการจะส่งผลเพียงเล็กน้อยให้แก่อุปกรณ์เกิดความเสียหาย แต่อาจจะส่งกระทบเสียหายอย่างใหญ่หลวงแก่คนงาน ชุมชน และสิ่งแวดล้อมรอบข้างได้ สารพิษที่รั่วไหลจะมีความรุนแรงมากเท่าใดจะขึ้นอยู่กับค่าตัวแปรต่าง ๆ ดังต่อไปนี้

1) ปริมาณการรั่วไหลของสารพิษ คือ ตัวแปรสำคัญที่จะบอกถึงความอันตรายของสารพิษที่รั่วไหล โดยทั่วไปปริมาณการรั่วไหลที่มากขึ้นจะทำให้มีการแพร่กระจายมากขึ้น แต่หากเป็นก๊าซระยะในการแพร่กระจายจะไม่เพิ่มขึ้นเป็นเชิงเส้นกับปริมาณการรั่วไหล
2) เวลาของการรั่วไหล คือ ส่วนประกอบในการพิจารณาหากสารพิษมีการรั่วไหลในช่วงเวลาที่แตกต่าง ก็จะเกิดความเสียหายที่แตกต่างกันในการรั่วไหลจะมีปริมาณและความเข้มข้นมากหากเวลานั้นยาวนาน
3) รูปแบบของภูมิศาสตร์ของกระบวนการ คือ พื้นที่ที่กระบวนการถูกติดตั้งก็มีผลต่อความเสียหายจากการรั่วไหล หากพื้นที่ตั้งอยู่เหนือลมระดับความรุนแรงก็จะสูงต่อชุมชนและสิ่งแวดล้อมมากขึ้น
4) ความหนาแน่นของสารที่รั่วไหล คือ ตัวแปรที่บ่งบอกถึงระดับความอันตรายของสารพิษ การรั่วเพียงเล็กน้อยของกระบวนการที่มีความเข้มข้นมาก อาจจะมีผลกระทบมากกว่าการรั่วไหลที่มีความเข้มช้นน้อยแต่ระยะเวลานาน
5) สภาพแวดล้อมในการแพร่กระจาย คือ สภาพโดยรอบกระบวนการมีสิ่งที่ทำให้เกิดความเสียหายได้มากจากสารพิษ ผลกระทบจะมีสูงหากมีเขตชุมชนอยู่โดยรอบหรือสารพิษรั่วไหลลงทะเล เป็นต้น
6) ระยะสิ้นสุดของความเข้มข้นของสารพิษ (Endpoint) คือ คือระยะในการที่สารพิษนั้นไม่มีความรุนแรง ปลอดภัยต่อสิ่งมีชีวิต และสิ่งแวดล้อม ยกตัวอย่างเช่น การระเบิดของโรงงานไฟฟ้านิวเคลียร์ที่เชอร์โนบิลของสหภาพโซเวียดในขณะนั้น เกิดการรั่วไหลของสารพิษทำให้เป็นมะเร็งในต่อมไทรอยด์ จึงต้องทำการอพยพผู้คนออกนอกเขตของการรั่วไหลของสารพิษ

2.2.3 การคำนวณระยะการเสียหายและผลกระทบ

ผลกระทบของเหตุการณ์อันตรายจะขึ้นอยู่กับขนาดของพื้นที่ ที่มีความเสียหายเกิดขึ้นและตัวแปรในการหลีกเลี่ยงจากผลกระทบ เมื่อตัวแปรทั้งสองตัวสามารถหาได้ก็จะสามารถคำนวณหาผลกระทบต่อชีวิต (PLL : Probable Loss of Life) และการประเมินค่าเงินในความเสียหาย (EV : Expected Value of Loss) การคำนวณจำนวนคนที่อยู่ในพื้นที่ความเสี่ยง (Occupancy) จะได้มาจากฟังก์ชันของขนาดของพื้นที่ความเสี่ยงกับความหนาแน่นของคนที่อยู่ในพื้นที่ความเสี่ยง จะได้เป็นสมการที่ (2.1) และการคำนวณหาผลกระทบต่อชีวิตจากเหตุการณ์อันตรายด้วยฟังก์ชันความสัมพันธ์ของตัวแปรจำนวนคนในพื้นที่ความเสี่ยงและค่าโอกาส (Vulnerability) ในการที่จะบาดเจ็บสาหัส จะได้ดังสมการที่ (2.2) ดังนี้

$$O_{person} = A_{effect} \times \rho_{person} \qquad (2.1)$$

เมื่อ O_{person} คือ ตัวแปรของจำนวนคนในพื้นที่ความเสี่ยง (คน)
A_{effect} คือ ขนาดพื้นที่ความเสี่ยง (เมตร^2)
ρ_{person} คือ ความหนาแน่นของประชากรในพื้นที่ความเสี่ยง (คน/เมตร^2)

$$PLL = O_{person}\ V \qquad (2.2)$$

เมื่อ PLL คือ ผลกระทบต่อชีวิต (คน/เหตุการณ์)
V คือ ค่าความเสี่ยงในการที่จะบาดเจ็บสาหัส

เมื่อทำการพิจารณาผลกระทบต่อชีวิต และขนาดพื้นที่ของเหตุการณ์อันตรายแล้วต่อมาจะต้องพิจารณาผลกระทบต่อทรัพย์สิน และธุรกิจที่ออกมาเป็นจำนวนเม็ดเงินที่จะต้องเสียไปหากเกิดเหตุการณ์อันตราย หากกระบวนการเกิดเหตุการณ์อันตรายแล้วจำเป็นต้องหยุดกระบวนการผลิตนั่นคือความเสียหายที่เป็นรูปแบบของธุรกิจ (Loss of Business) เนื่องจากผลิตภัณฑ์ไม่สามารถส่งออกและจำหน่ายออกสู่ตลาดได้ หากกระบวนการเกิดความเสี่ยงแล้วอุปกรณ์ในการผลิตเสียหายไม่สามารถใช้งานต่อได้จึงต้องหยุดการผลิตและซ่อมแซมอุปกรณ์ นั่นคือความเสียหายในรูปแบบของทรัพย์สิน (Loss of Asset) ซึ่งโดยปกติแล้วทั้งสองรูปแบบความเสียหายจะเกิดขึ้นพร้อม ๆ กันหากเกิดเหตุการณ์อันตราย วิธีในการพิจารณาผลกระทบในทรัพย์สินและธุรกิจนั้นสามารถคำนวณออกมาเป็นตัวเลขเชิงปริมาณได้จากสมการที่ (2.1) และ (2.2) โดยการเปลี่ยนความหนาแน่นของประชากรในพื้นที่ความเสี่ยงด้วยความหนาแน่นของจำนวนเงินที่เกิดความเสียหายในพื้นที่ความเสี่ยง (Capital Density) ซึ่งจะเป็นจำนวนเงินของกระบวนการนั้น ๆ ในการคำนวณค่าที่ถูกต้องและสมเหตุสมผลของพื้นที่ความเสี่ยง จะต้องพิจารณาเป็นหน่วยการผลิตและอุปกรณ์โดยรอบ ซึ่งจะไม่ใช่การประเมินความเสียหายทั้งโรงงานอุตสาหกรรมซึ่งเป็นวิธีที่ผิดและไม่สะท้อนความเป็นจริง การประเมินจำนวนเงินจากความเสียหายที่ง่ายที่สุด คือ จำนวนค่าใช้จ่ายในการซ่อมแซม หรือเปลี่ยนแปลงอุปกรณ์ (Replacement Cost) ซึ่งสามารถหาข้อมูลได้จาก ประสบการณ์ของผู้ปฏิบัติการ (Estimates from Site Personal) ข้อมูลจากประวัติการติดตั้ง และข้อมูลทั่วไปจากมาตรฐาน โดยเขียนเป็นสมการ

คำนวณค่าความเสียหายในพื้นที่ความเสี่ยง (Cost) ได้ในสมการที่ (2.3) และคำนวณค่าเงินในความเสียหายได้ในสมการที่ (2.4) โดยข้อมูลที่นำมาคำนวณในสมการนี้จะเป็นแนวทางที่สามารถนำไปสู่การประมาณค่าความเสียหายต่อชีวิตและทรัพย์สินได้ ผลลัพธ์จะมีความแม่นยำมากขึ้นหากข้อมูลที่นำมาพิจารณานั้นมีค่าที่ละเอียดมากขึ้น หรืออาจมีการใช้งานโปรแกรมเครื่องมือในการคำนวณหาความเสียหายต่าง ๆ ได้เช่น โปรแกรม FETCH^{TM} ซึ่งถูกพัฒนาโดย Exida และ ARCHIE^{TM} ที่ถูกพัฒนาโดย EPA, FEMA และ DOT เป็นต้น

$$O_{cost} = A_{effect} \text{ x } \rho_{person} \tag{2.3}$$

เมื่อ O_{cost} คือ ตัวแปรของค่าความเสียหายในพื้นที่ความเสี่ยง (จำนวนเงิน)
A_{effect} คือ ขนาดพื้นที่ความเสี่ยง (เมตร^2)
ρ_{person} คือ ความหนาแน่นของความเสียหายในพื้นที่ความเสี่ยง (จำนวนเงิน/เมตร^2)

$$EV = O_{cost} V \tag{2.4}$$

เมื่อ EV คือ ค่าเงินในความเสียหาย (จำนวนเงิน)
V คือ ค่าความเสี่ยงในการที่อุปกรณ์จะเสียหาย

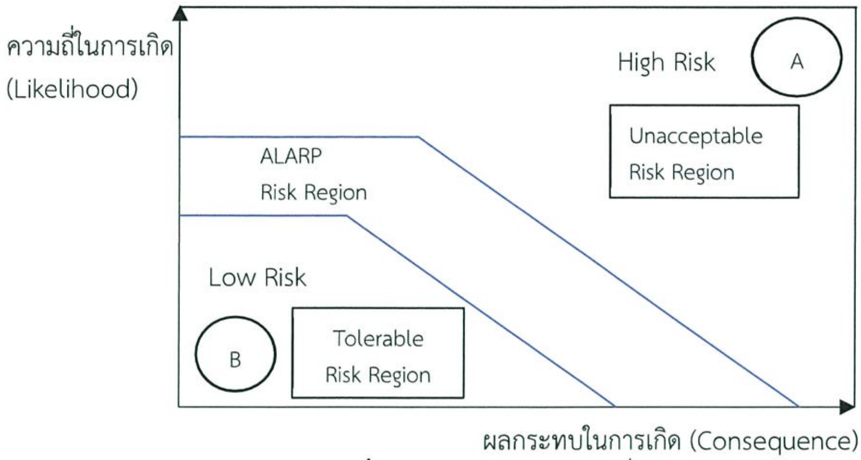
2.3 การคัดเลือกระดับความปลอดภัย

ในการคัดเลือกระดับความปลอดภัยที่เหมาะสมภายในกระบวนการนั้น จะต้องพิจารณาหลายปัจจัยโดยใช้ข้อมูลของเหตุการณ์ในอดีตที่เคยเกิดขึ้นหรือการคาดคะเนต่าง ๆ เพื่อให้ได้ระดับความปลอดภัยนั้นมา

2.3.1 ความเสี่ยง

ก่อนที่จะทำการคัดเลือกระดับความปลอดภัยของกระบวนการ จะต้องทำความเข้าใจความหมายของคำว่าความเสี่ยง ซึ่งได้ระบุความหมายอยู่ในหัวข้อ 3.1.5 ของ IEC 61508-4 ไว้ดังนี้ “ความเสี่ยงจะเป็นการรวมกันของความเป็นไปได้ของเหตุการณ์อันตราย กับความรุนแรงจากเหตุการณ์นั้น” หรือกล่าวคือ ถ้ามีความเป็นไปได้ของเหตุการณ์อันตรายที่เกิดขึ้นได้บ่อยครั้งและมีผลกระทบความรุนแรง (Severity) ก็จะเรียกว่ามีความเสี่ยงสูง แต่ถ้าเหตุการณ์อันตรายไม่มีโอกาสเกิดขึ้นหรือเกิดขึ้นได้น้อยและผลกระทบไม่มีความรุนแรงก็จะเรียกว่ามีความเสี่ยงต่ำ ค่าความเสี่ยงจึงสามารถแสดงในรูปแบบแผนภาพระหว่างความรุนแรงจากเหตุการณ์อันตราย ดังแสดงในรูปที่ 2.10 ซึ่งจากแผนภาพความเสี่ยงจะเห็นได้ว่าที่จุด A จะมีความเสี่ยงที่สูงเนื่องจากมีความรุนแรงของเหตุการณ์อันตรายสูงและมีความเป็นไปได้ของการเกิดเหตุการณ์สูงเช่นเดียวกัน ซึ่งในจุดนี้จะจัดอยู่ในย่านความเสี่ยงที่ยอมรับไม่ได้ (Unacceptable Risk Region) ส่วนที่จุด B จะมีค่าความเสี่ยงที่ต่ำเนื่องจากมีความรุนแรงจากเหตุการณ์อันตรายและมีความเป็นไปได้ที่จะเกิดต่ำ ซึ่งในส่วนนี้จะจัดอยู่ในย่านความเสี่ยงที่ยอมรับได้ (Tolerable Risk Region) และจะเป็นจุดที่กระบวนการผลิตต้องการออกแบบเพื่อให้มีความปลอดภัยที่สูง ดังนั้นหากทำการวิเคราะห์อันตรายของกระบวนการผลิตแล้ว

พบว่ากระบวนการนั้นมีความเสี่ยงที่อยู่ในย่านที่ยอมรับไม่ได้ ก็จะต้องทำการติดตั้งระบบนิรภัยเพื่อให้กระบวนการมีความปลอดภัยมากขึ้น

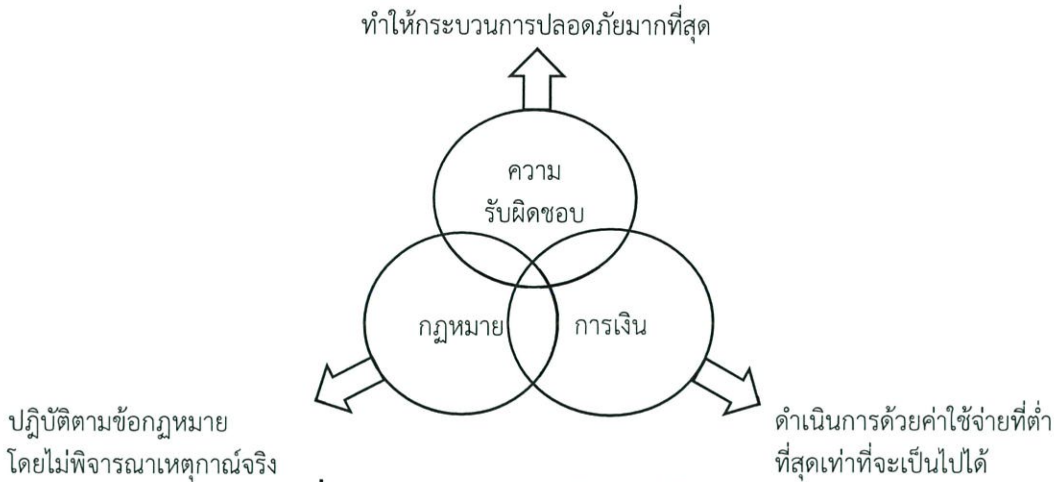


รูปที่ 2.10 แผนภาพความเสี่ยง

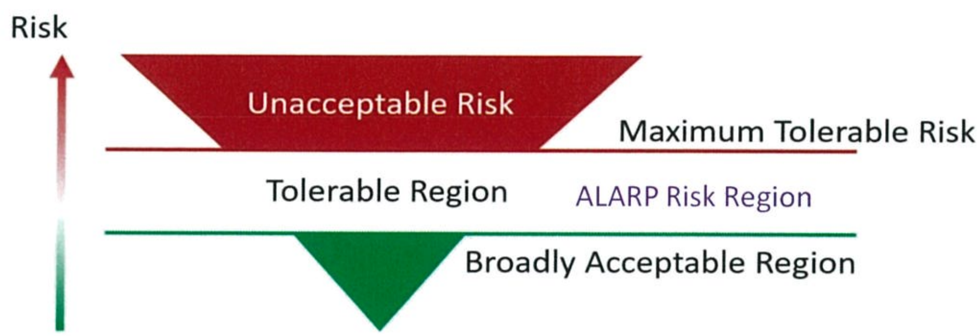
2.3.1.1 แนวทางสู่ค่าความเสี่ยงที่ยอมรับได้

สำหรับแนวทางสู่ค่าความเสี่ยงที่ยอมรับได้ (Tolerable Risk Guidelines) นั้น เมื่อได้ผ่านการวิเคราะห์อันตรายของกระบวนการผลิตแล้วพบว่า กระบวนการผลิตที่จะออกแบบก่อสร้างนั้นมีความเสี่ยงต่ออันตรายมากน้อยเพียงใด บริษัทหรือองค์กรต่าง ๆ ที่ทำงานเกี่ยวกับกระบวนการที่มีความอันตรายมีหน้าที่ในการกำจัดความเสี่ยงนั้นเพื่อให้เป็นไปตามกฎหมาย ศีลธรรม และเหตุผลทางธุรกิจตามรูปที่ 2.11 ซึ่งอาจจะไม่ได้เป็นสัดส่วนกับผลประโยชน์ที่จะได้รับ ดังนั้นการเลือกบรรทัดฐานความเสี่ยงที่ยอมรับได้ต้องถูกเลือกอย่างระมัดระวัง เพื่อให้มีความสมดุลย์ทางด้านธุรกิจ การเลือกใช้แนวทางที่ดีสุดจากรูปที่ 2.11 จะเป็นการพิจารณาเหตุการณ์จริงที่เกิดขึ้นและการออกแบบอย่างเหมาะสมถูกต้องตามแนวทางที่แต่ละกระบวนการต้องการ ด้วยเหตุนี้องค์กร UK's HSE ได้เสนอการดำเนินการตามขั้นตอนที่เรียกว่า ALARP (As Low As Reasonably Practicable) ที่อยู่ระหว่างความเสี่ยงที่ยอมรับได้และไม่ได้ ดังแสดงในรูปที่ 2.12 วิธีนี้จะแสดงได้ว่ามีระดับความเสี่ยงที่อยู่ระหว่างย่านที่ยอมรับไม่ได้ (Intolerable) และย่านที่มีค่าความเสี่ยงที่ยอมรับได้ (Tolerable) ซึ่งภายในย่าน ALARP จะเป็นย่านที่มีความเสี่ยงต่ำที่สุดที่ยอมรับได้และไม่ต้องมีการพิจารณาลดความเสี่ยงเพิ่มเติมเนื่องจากการดำเนินการลดค่าความเสี่ยงทำไม่ได้ในทางปฏิบัติ หรือมีค่าใช้จ่ายที่ไม่เหมาะสมกับประโยชน์ที่จะได้รับ โดยปกติแล้วประเทศต่าง ๆ ทั่วโลกไม่ได้มีบรรทัดฐานในการกำหนดความเสี่ยงที่ยอมรับได้ ทำให้เจ้าของกระบวนการผลิตจะต้องพิจารณาระดับความเสี่ยงที่ยอมรับได้เอง โดยย่านขอบเขตของความเสี่ยงที่ยอมรับได้ (Tolerable Region) นั้นจะสามารถยอมรับได้ในกรณีพิเศษหากว่าการพัฒนาระบบนิรภัยเป็นดังนี้

1) การลดความเสี่ยงไม่สามารถทำได้เพิ่มในทางปฏิบัติ หรือประโยชน์ที่ได้รับจะไม่เป็นสัดส่วนกับการเพิ่มการป้องกัน
2) ผลจากการเพิ่มชั้นป้องกันไม่ช่วยแก้ปัญหาได้เท่าที่ควร



รูปที่ 2.11 รูปแบบแนวทางในการสร้างระบบนิรภัย



รูปที่ 2.12 ขอบเขตของความเสี่ยง (Risk Region)

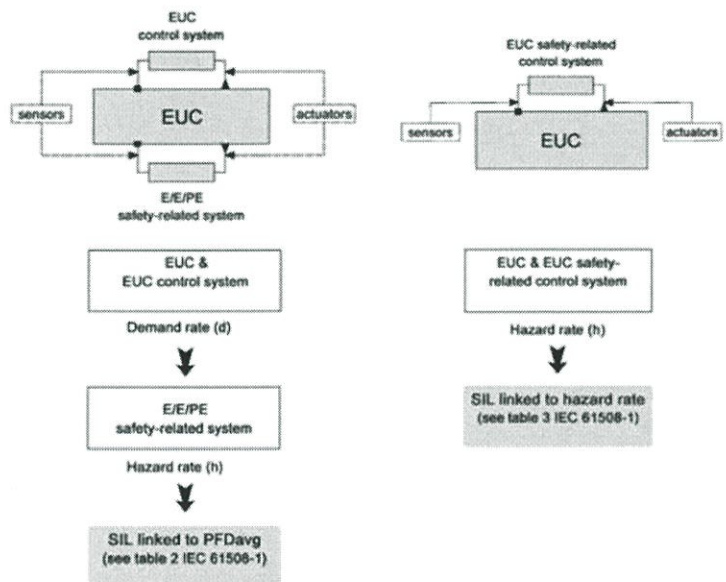
2.3.1.2 ประเภทของความเสี่ยง

ในการประเมินความเสี่ยงนั้น ความถี่และความเสี่ยงของเหตุการณ์จะถูกนำมาใช้ในการพิจารณาผลกระทบซึ่งจะถูกแบ่งออกเป็น 3 ประเภท คือ ความเสี่ยงต่อชีวิต (Personal) ความเสี่ยงต่อธุรกิจ (Asset) และความเสี่ยงต่อสิ่งแวดล้อม (Environment) หากกล่าวถึงตัวเลขที่จะมากำหนดค่าในเชิงปริมาณของความเสี่ยงแล้ว ไม่มีตัวเลขที่แน่ชัดในการกำหนดปริมาณของความเสี่ยงเนื่องจากอุตสาหกรรมในแต่ละแขนงก็มีรูปแบบสภาพแวดล้อมที่แตกต่างกันไป ทำให้ตัวแปรของความเสี่ยงไม่สามารถพิจารณาอย่างตรงไปตรงมาได้ ความเสี่ยงนั้นอาจถูกพิจารณาเป็นรูปแบบเชิงปริมาณ และเชิงคุณภาพใช้ในการประเมินความเสี่ยงคนละรูปแบบซึ่งมีความหมายแตกต่างกันดังนี้

1) การประเมินเชิงปริมาณ (Quantity Method) คือ การประเมินระดับความเสี่ยงให้อยู่ในรูปของตัวเลข 1 ครั้งต่อปีหรือ 0.5 ครั้งต่อปี เช่น ความเสี่ยงสำหรับความเสียหายมีที่มูลค่า 50 ล้านบาท เสียชีวิตประมาณ 5 ราย เป็นต้น
2) การประเมินเชิงคุณภาพ (Quality Method) คือ การประเมินระดับความเสี่ยงให้อยู่ในรูปของคำพูดหรือความรู้สึก มาก น้อย รุนแรง เช่น ความเสี่ยงสำหรับความเสียหายที่มีมูลค่าสูงมาก และมีผู้เสียชีวิตหลายราย เป็นต้น

2.3.2 ระดับความปลอดภัย

รูปแบบของระบบนิรภัยมีหลายรูปแบบให้ผู้ใช้ได้เลือกใช้งาน โดยค่าตัวแปรที่จะนำมากำหนดว่าจะใช้รูปแบบตามมาตรฐาน IEC 61508/61511 นั้น จะขึ้นอยู่กับค่าระดับความปลอดภัยหรือค่า SIL (Safety Integrity Level) ของฟังก์ชันนิรภัยเพื่อมาทำการลดความเสี่ยงที่เกิดขึ้นในกระบวนการ ซึ่งค่าระดับความปลอดภัยจะใช้แสดงค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดบนความต้องการหรือค่า PFD_{avg} (Average Probability of Failure on Demand) หรืออีกในความหมายหนึ่งคือ ค่าของความเป็นไปได้ที่ฟังก์ชันนิรภัยจะไม่สามารถทำงานได้ในเวลาที่ต้องการ โดยค่า PFD_{avg} ตามมาตรฐาน ได้กำหนดค่าระดับความปลอดภัยที่ขึ้นอยู่กับการทำงานของระบบป้องกันหรือระบบนิรภัยเป็น 2 รูปแบบ ได้แก่ โหมดความต้องการต่ำและโหมดความต้องการสูง ผู้ใช้จะต้องพิจารณาก่อนว่ารูปแบบในการทำงานของอุปกรณ์ที่อยู่ภายใต้การควบคุม (EUC : Equipment Under Control) ในกระบวนการนั้นจัดอยู่ในการทำงานแบบใดดังแสดงในรูปที่ 2.13



(ก) (ข)

รูปที่ 2.13 ระบบนิรภัยในแต่ละแบบ

(ก) โหมดความต้องการต่ำ (ข) โหมดความต้องการสูง

2.3.2.1 โหมดความต้องการต่ำ

ความหมายของโหมดความต้องการต่ำ (Low Demand Mode) ซึ่งระบุไว้ในหัวข้อ 3.5.1.2 ของมาตรฐาน IEC 61508-4 ว่า “การทำงานของอุปกรณ์จะมีความถี่ความต้องการบนระบบนิรภัยไม่มากกว่า 1 ครั้งต่อปีหรือไม่มากกว่าสองเท่าของความถี่ในการทดสอบการทำงาน” โดยค่าระดับความปลอดภัยได้ถูกแบ่งออกเป็น 4 ระดับตามมาตรฐาน IEC 61508-1 ตารางที่ 2 ดังแสดงในตารางที่ 2.2 ซึ่งจะเห็นว่าค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดที่มีมากกว่า 10^{-1} หรือไม่มีระดับความปลอดภัยนั้นหมายความว่า จากการประเมินไม่มีความเสี่ยงจึงไม่จำเป็นต้องติดตั้งฟังก์ชันนิรภัย สามารถติดตั้งเพียงแค่ฟังก์ชันควบคุมพื้นฐานและสัญญาณเตือนบนระบบควบคุมก็เพียงพอ ส่วนที่ค่าระดับความปลอดภัย SIL 1 นั้นจะหมายความว่าจากการประเมิน กระบวนการมีความเสี่ยง

และยอมให้ฟังก์ชันนิรภัยทำงานล้มเหลวที่ความน่าจะเป็น 0.01 – 0.1 ครั้ง จึงจำเป็นต้องติดตั้งฟังก์ชันนิรภัยที่มีระดับ SIL 1 หรือสูงกว่าเพื่อลดความเสี่ยง และในส่วนค่าระดับความปลอดภัยที่ SIL 4 จะหมายความว่าจากการประเมิน กระบวนการนั้นมีความเสี่ยงสูงมากและยอมให้ฟังก์ชันนิรภัยทำงานล้มเหลวที่ความน่าจะเป็นเพียง 0.00001 – 0.0001 ครั้ง จึงจำเป็นต้องติดตั้งฟังก์ชันนิรภัยที่มีระดับความปลอดภัย SIL 4 เท่านั้น

ตารางที่ 2.2 ตารางค่าระดับความปลอดภัยที่ความต้องการต่ำ

ระดับ SIL	ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดบนความต้องการ (PFD_{avg})
-	$>10^{-1}$
1	$\geq 10^{-2}$ to $<10^{-1}$
2	$\geq 10^{-3}$ to $<10^{-2}$
3	$\geq 10^{-4}$ to $<10^{-3}$
4	$\geq 10^{-5}$ to $<10^{-4}$

ในโหมดความต้องการต่ำ อัตราความอันตราย (Hazard Rate) ขึ้นอยู่กับอัตราความต้องการ (Rate of Demands) บนระบบนิรภัยและความเป็นไปได้ที่จะมีความผิดพลาดในการทำงานของระบบนิรภัยในฟังก์ชันนิรภัย ดังสมการที่ (2.5) ซึ่งแสดงให้เห็นว่าฟังก์ชันนิรภัยทำงานในโหมดความต้องการต่ำ ที่ค่าระดับความปลอดภัยใด ๆ จะสามารถหาได้จากอัตราความอันตรายและอัตราความต้องการ จากตารางที่ 2.2 ระดับความปลอดภัยที่ความต้องการต่ำสามารถพิจารณาหาค่าตัวแปรการลดความเสี่ยง (RRF : Risk Reduction Factor) ได้จากส่วนกลับของค่า PFD_{avg} ที่ระดับความปลอดภัยของระบบนิรภัยระดับต่าง ๆ แสดงได้ดังตารางที่ 2.3

$$h = d \times PFD_{avg} \tag{2.5}$$

เมื่อ h คือ อัตราความอันตรายที่ถูกกำหนดขึ้นมาตามความต้องการของผู้ใช้

d คือ อัตราการเกิดของเหตุการณ์อันตราย

PFD_{avg} คือ ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดบนความต้องการ

ตารางที่ 2.3 ค่าการลดความเสี่ยงของระบบนิรภัยในแต่ละระดับความปลอดภัย

ระดับ SIL	ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดในบนความต้องการ (PFD_{avg})	ตัวแปรการลดความเสี่ยง ($1/PFD_{avg}$)
-	$>10^{-1}$	<10
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to ≤ 100
2	$\geq 10^{-3}$ to $<10^{-2}$	>100 to ≤ 1000
3	$\geq 10^{-4}$ to $<10^{-3}$	>1000 to ≤ 10000
4	$\geq 10^{-5}$ to $<10^{-4}$	>10000 to ≤ 100000

2.3.2.2 โหมดความต้องการสูง

ความหมายของโหมดความต้องการสูง (High Demand Mode) ในหัวข้อ 3.5.12 ของ IEC 61508-4 ระบุไว้ว่า “ความถี่ของความต้องการบนระบบนิรภัยมากกว่าหนึ่งครั้งต่อปี หรือมากกว่าสองเท่าของความถี่ในการทดสอบการทำงาน” โดยระดับความปลอดภัยจะแบ่งออกเป็น 4 ระดับตามมาตรฐาน IEC 61508-1 ตารางที่ 3 ดังแสดงในตารางที่ 2.4 และฟังก์ชันในการทำงานแบบความต้องการสูง จะใช้ค่าของอัตราความอันตรายมาเป็นตัวกำหนดระดับของความปลอดภัยดังสมการที่ (2.6)

$$h = PDF \tag{2.6}$$

เมื่อ h คือ อัตราความอันตรายที่ถูกกำหนดขึ้นมาตามความต้องการของผู้ใช้

PDF คือ ค่าความน่าจะเป็นของการเกิดอันตรายต่อชั่วโมง

ตารางที่ 2.4 ตารางค่าระดับความปลอดภัยที่ความต้องการสูง

ระดับ SIL	ค่าความน่าจะเป็นของการเกิดอันตรายต่อชั่วโมง (Probability of Dangerous Failure per hour)
-	$>10^{-5}$
1	$\geq 10^{-6}$ to $<10^{-5}$
2	$\geq 10^{-7}$ to $<10^{-6}$
3	$\geq 10^{-8}$ to $<10^{-7}$
4	$\geq 10^{-9}$ to $<10^{-8}$

2.3.3 การคัดเลือกระดับความปลอดภัยของกระบวนการ

ในการพิจารณาระดับความปลอดภัยจากมาตรฐาน IEC 61508 ในขั้นตอนที่ 5 ของวงจรความปลอดภัย จะต้องพิจารณากระบวนการว่ามีความเสี่ยงอยู่ในระดับใดในการวิเคราะห์อันตรายที่กล่าวมา ขั้นตอนต่อมาคือการคัดเลือกระดับความปลอดภัยตามวิธีต่าง ๆ เช่น กราฟความเสี่ยง (Risk Graph) เมตริกความเสี่ยง (Risk Matrix) และ ระดับชั้นการป้องกัน (LOPA : Layers of Protection Analysis) เพื่อนำค่าระดับความปลอดภัยมาทำการพิจารณาสร้างฟังก์ชันนิรภัยที่กระบวนการต้องการ เมื่อฟังก์ชันควบคุมพื้นฐานไม่สามารถหยุดการเบี่ยงเบนของตัวแปรในกระบวนการได้ โดยในมาตรฐานจะอธิบายเพียงแค่ระดับชั้นการป้องกันและเมตริกความเสี่ยงเท่านั้น โดยข้อมูลที่ใช้สำหรับการคัดเลือกระดับความปลอดภัยที่กล่าวไปแล้ว ต้องการข้อมูลจากหลายฝ่าย หากเป็นอุตสาหกรรมกระบวนการผลิตนั้นใน IEC 61511 มีการแนะนำให้มีผู้ดำเนินการที่ประกอบไปด้วย

1) วิศวกรกระบวนการผลิต (Process Specialist/Technologist)
2) วิศวกรการควบคุม (Process Control Engineer)
3) ผู้ปฏิบัติงานควบคุมกระบวนการ (Operation Management)

4) ผู้เชี่ยวชาญหรือวิศวกรทางด้านความปลอดภัย (Safety/ Reliability Engineer)
5) วิศวกรเครื่องมือวัด (Instrument Engineer)
6) ผู้มีประสบการณ์ในการทำงานภายใต้การพิจารณา (Maintenance or etc.)

2.3.3.1 การคัดเลือกระดับความปลอดภัยด้วยวิธีการแบ่งระดับชั้นป้องกัน

การคัดเลือกระดับความปลอดภัยของกระบวนการ ด้วยวิธีการแบ่งระดับชั้นป้องกันหรือ LOPA คือ แนวทางในการคัดเลือกระดับความปลอดภัยตามมาตรฐาน IEC 61511-3 ที่เป็นการพิจารณาเชิงปริมาณ ซึ่งการใช้งานวิธีการแบ่งระดับชั้นป้องกันนี้ เป็นการพิจารณาที่ค่อนข้างยากและใช้เวลานาน เนื่องจากต้องใช้ข้อมูลการวิเคราะห์อัตราการเกิดอันตรายในแต่ละชั้นการป้องกันอิสระ (IPL : Independent Protection Layers) ที่มีค่อนข้างมาก ถึงอย่างนั้นวิธีระดับชั้นป้องกัน ก็เป็นวิธีที่ละเอียดที่สุดในการพิจารณาคัดเลือกระดับความปลอดภัยให้แก่ระบบนิรภัย การพิจารณาอัตราความเสี่ยงของเหตุการณ์อันตรายในกระบวนการโดยใช้วิธีการแบ่งระดับชั้นป้องกันตามรูปที่ 2.14 เป็นการแยกระดับชั้นเพื่อแบ่งการพิจารณาโดยละเอียดในแต่ละชั้นการป้องกันโดยแบ่งออกเป็น 7 ชั้นการป้องกัน ได้แก่

1) Process Design คือ การป้องกันอันตรายจากอุปกรณ์เอง เช่น ถังแยกน้ำมันและก๊าซสามารถทนความร้อนได้สูงกว่าระดับที่ออกแบบไว้
2) BPCS คือ ระบบควบคุมกระบวนการ (Basic Process Control System) เช่น การเปิดปิดวาล์วจากตัวแปรที่กำหนด
3) Alarm, Operator Action คือ การป้องกันอันตรายโดยเกิดสัญญาณเตือนมาจากระบบควบคุม และผู้ปฏิบัติการสั่งการได้ทันท่วงที
4) Automation Action SIS หรือ ESD คือ การป้องกันอันตรายโดยใช้ระบบวัดคุมนิรภัยที่สั่งการโดยพีแอลซี โดยระบบจะถูกแยกออกจากระบบควบคุมพื้นฐานเพื่อลดโอกาสเสียหายจากระบบ
5) Active/Passive Protection คือ การป้องกันอันตรายโดยใช้อุปกรณ์ที่ติดตั้งเสริมเข้าไปในกระบวนการ เป็นการป้องกันโดยอุปกรณ์ทางกล เช่น วาล์วนิรภัย ฝาครอบปะทุ (Rupture disk) เป็นต้น
5) Plant Emergency Response คือ การป้องกันอันตรายหลังจากที่มีการรั่วไหลของกระบวนการออกมาแล้ว เช่น การควบคุมพื้นที่การแพร่กระจายของสารเคมี สัญญาณอพยพ เป็นต้น
6) Community Emergency Response คือ การป้องกันอันตรายหลังจากที่มีการรั่วไหลซึ่งไม่สามารถควบคุมเอาไว้ภายในโรงงานได้ จึงต้องประกาศสัญญาณอพยพให้แก่ผู้คนบริเวณโดยรอบ

โดยการคำนวณนั้น จะต้องทราบความถี่ของเหตุการณ์อันตรายสำหรับไดอะแกรมการแบ่งระดับชั้นป้องกันในรูปที่ 2.15 ซึ่งสามารถหาได้จากสมการที่ (2.7) เมื่อได้ความถี่ของเหตุการณ์หลังการป้องกันแล้ว นำมาคำนวณหาค่า PFD_{avg} ของระบบนิรภัยในตารางระดับความปลอดภัยของ IEC 61508 จากสมการที่ (2.5) ซึ่งจะได้ระดับความปลอดภัยที่ต้องการและค่าการลดความเสี่ยงของฟังก์ชันนิรภัยด้วยสมการที่ (2.8)

$$F = F_A \times P_1 \times P_2 \times \ldots \times P_N \quad (2.7)$$

เมื่อ F คือ ความถี่ของเหตุการณ์อันตรายหลังการป้องกัน (ต่อปี)

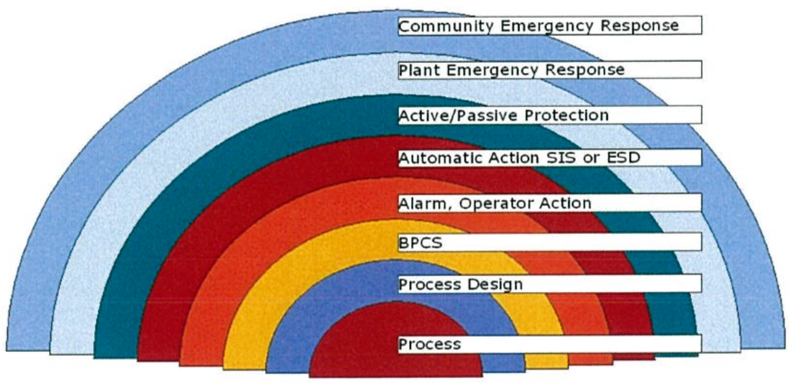
F_A คือ ความถี่ของเหตุการณ์อันตรายก่อนการป้องกัน (ต่อปี)

P_1 คือ ความน่าจะเป็นของการเกิดเหตุการณ์อันตรายชั้นป้องกันที่ 1

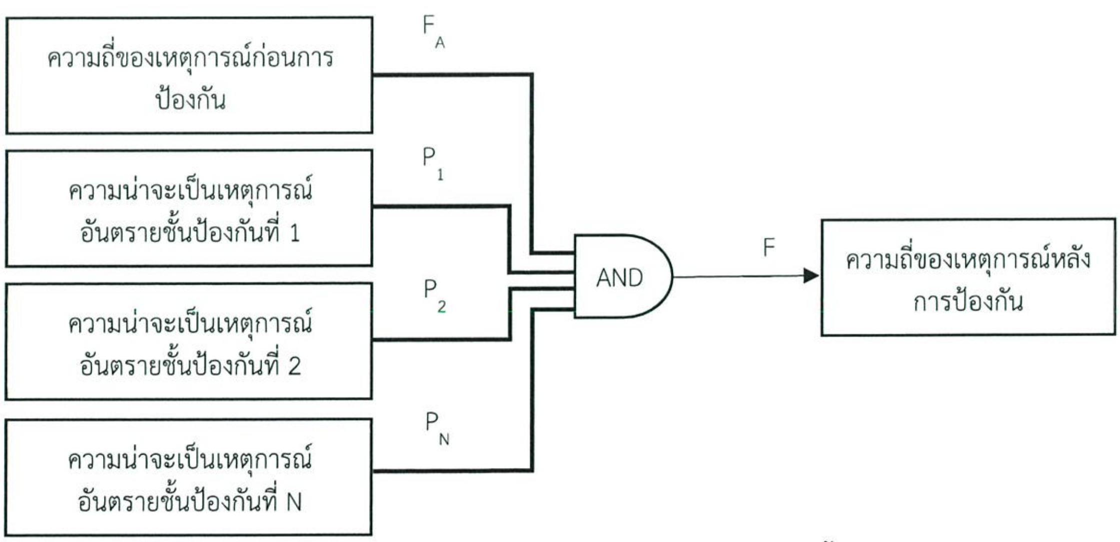
P_2 คือ ความน่าจะเป็นของการเกิดเหตุการณ์อันตรายชั้นป้องกันที่ 2

P_N คือ ความน่าจะเป็นของการเกิดเหตุการณ์อันตรายชั้นป้องกันที่ N

$$PFD_{avg} = h / F \tag{2.8}$$



รูปที่ 2.14 โครงสร้างพื้นฐานของการพิจารณาความเสี่ยงโดยใช้เทคนิคการแบ่งชั้นป้องกัน



รูปที่ 2.15 การคำนวณความถี่ของเหตุการณ์โดยการแบ่งชั้นป้องกัน

2.3.3.2 การคัดเลือกระดับความปลอดภัยด้วยวิธีการเมตริกความเสี่ยง

การประเมินความเสี่ยงด้วยตารางเมตริกความเสี่ยง (Risk Matrix) นั้นเป็นที่แพร่หลายในอุตสาหกรรมหลาย ๆ แห่ง ในการกำหนดระดับความปลอดภัยของกระบวนการ เนื่องจากเมตริกความเสี่ยงนั้นมีการใช้งานที่ไม่ซับซ้อน ระบบเมตริกความเสี่ยงจะต้องพิจารณาความถี่ของเหตุการณ์อันตราย (Frequency of Occurrence) และผลกระทบที่มีต่อชีวิต (Health Loss)

ทรัพย์สิน (Asset Loss) และสิ่งแวดล้อม (Environmental Loss) โดยความถี่ของเหตุการณ์จะถูกนำมาพิจารณาอยู่ในช่วงของเมตริกความเสี่ยง ดังต่อไปนี้

1) ความถี่ของการเกิดเหตุการณ์ (Frequency of Occurrence) จะต้องถูกประเมินจากผู้เข้าร่วมการประเมิน โดยพิจารณาอัตราการเกิดของสาเหตุจากประสบการณ์หรือฐานข้อมูลที่เชื่อถือได้ ความถี่ของการเกิดเหตุการณ์นั้นจะถูกแบ่งเป็นช่วงของปริมาณความถี่ แบ่งออกเป็น 5 ระดับดังตารางที่ 2.5
2) ผลกระทบต่อชีวิตและความปลอดภัย (Health and Safety Loss) เป็นตัวแปรที่พิจารณาจากความรุนแรงของเหตุการณ์ ต่อการบาดเจ็บ จำนวนความเสียชีวิตของผู้ปฏิบัติงาน และผู้คนที่อยู่บริเวณโดยรอบ โดยแบ่งระดับของผลกระทบออกเป็น 6 ระดับดังตารางที่ 2.6
3) ผลกระทบต่อทรัพย์สิน (Asset and Product Loss) เป็นตัวแปรที่แสดงถึงค่าความเสียหายเป็นเม็ดเงินในกระบวนการ ที่ต้องหยุดการผลิตและความเสียหายของเครื่องจักรจากเหตุการณ์อันตราย สามารถแบ่งออกได้เป็น 6 ระดับดังตารางที่ 2.7
4) ผลกระทบต่อสิ่งแวดล้อม (Environment Loss) เป็นค่าที่แสดงถึงการเสียหายต่อสิ่งแวดล้อม ซึ่งใช้ช่วงตัวแปรในการประเมินหากเกิดเหตุการณ์อันตราย โดยจะแบ่งเป็นปริมาณขอบเขตของพื้นที่แบ่งออกได้เป็น 6 ระดับ ดังตารางที่ 2.8

ตารางที่ 2.5 แสดงระดับความถี่ของเหตุการณ์

ระดับความถี่	คำอธิบาย
A	สาเหตุอาจเกิดขึ้นในเวลาภายใน 1 ปี (High)
B	สาเหตุอาจเกิดขึ้นในเวลาเกิน 1 ปี แต่ไม่เกิน 10 ปี (Medium)
C	สาเหตุอาจเกิดขึ้นในเวลาเกิน 10 ปี แต่ไม่เกิน 100 ปี (Minor)
D	สาเหตุอาจเกิดขึ้นในเวลาเกิน 100 ปี แต่ไม่เกิน 1000 ปี (Low)
E	สาเหตุอาจเกิดขึ้นในเวลาเกิน 1000 ปี (Very Low)

ตารางที่ 2.6 แสดงระดับผลกระทบต่อชีวิตและความปลอดภัย

ระดับผลกระทบ	คำอธิบาย
H0	ไม่มีการบาดเจ็บ (No Injury)
H1	บาดเจ็บเล็กน้อย (Slight Injury)
H2	บาดเจ็บเล็กน้อยและต้องหยุดรักษา (Minor Injury and Loss Time)
H3	บาดเจ็บมากต้องหยุดงานรักษาในโรงพยาบาล (Major Injury and Loss Time)
H4	บาดเจ็บรุนแรงเกิดการเสียชีวิต 1 ถึง 3 คน (Permanent Injury or 1-3 Casualties)
H5	เสียชีวิตมากกว่า 3 คน (More than 3 Casualties)

ตารางที่ 2.7 แสดงระดับผลกระทบต่อทรัพย์สิน

ระดับผลกระทบ	คำอธิบาย
L0	รวมมูลค่าการเสียหายน้อยกว่า 1 K$ (Less than 1 K$)
L1	รวมมูลค่าการเสียหายประมาณ 1-10 K$ (Between 1-10 K$)
L2	รวมมูลค่าการเสียหายประมาณ 10-100 K$ (Between 10-100 K$)
L3	รวมมูลค่าการเสียหายประมาณ 100 K-1 M$ (Between 100 K-1 M$)
L4	รวมมูลค่าการเสียหายประมาณ 1 -10 M$ (Between 1-10 M$)
L5	รวมมูลค่าการเสียหายมากกว่า 10 M$ (More than 10 M$)

ตารางที่ 2.8 แสดงระดับผลกระทบต่อสิ่งแวดล้อม

ระดับผลกระทบ	คำอธิบาย
E0	ไม่มีผลกระทบต่อสิ่งแวดล้อม (No Effect)
E1	กระทบต่อสิ่งแวดล้อมเพียงเล็กน้อย (Slight effect)
E2	กระทบต่อสิ่งแวดล้อมชั่วคราว อยู่ในขอบเขต (Minor Effect)
E3	กระทบต่อสิ่งแวดล้อมชั่วคราว ออกไปภายนอกขอบเขต (Moderate Effect)
E4	กระทบต่อสิ่งแวดล้อมถาวรและอยู่ภายนอกขอบเขต (Major Effect)
E5	กระทบต่อสิ่งแวดล้อมถาวรและออกไปภายนอกขอบเขตในระดับชาติ (Massive Effect)

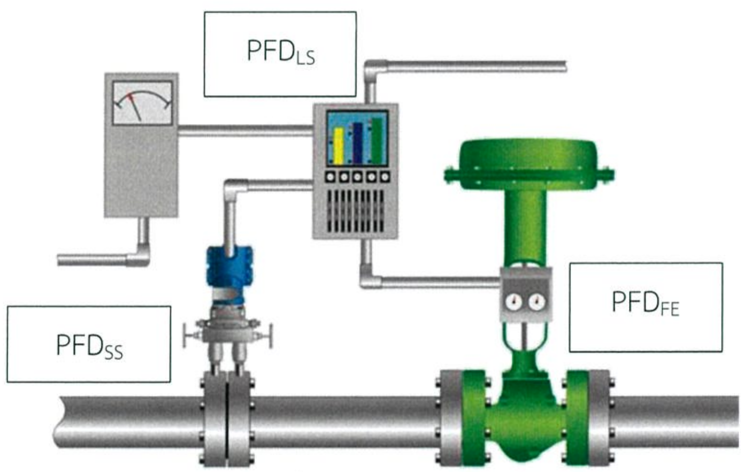
โดยหากนำข้อมูลต่าง ๆ มาเขียนในตารางเมตริกความเสี่ยงโดยใช้เมตริกอ้างอิงจากมาตรฐานของเชลล์ (Shell's Risk Matrix Assessment) ในตารางที่ 2.9 ซึ่งจากตารางที่ 2.9 การเลือกระดับความเสี่ยงในแต่ละผลกระทบนั้นจะนำมาพิจารณาร่วมกัน และทำการเลือกระดับความปลอดภัยที่สูงที่สุดที่เกิดจากผลกระทบใด ๆ เช่น หากการประเมินถูกพิจารณาออกมาว่ามีความถี่ของเหตุการณ์ที่ระดับ A ผลกระทบต่อชีวิตระดับ H0 ผลกระทบต่อทรัพย์สินระดับ L1 และผลกระทบต่อสิ่งแวดล้อมระดับ E2 ซึ่งจะได้ระดับความปลอดภัยที่ต้องการที่ระดับ SIL 0, SIL 1 และ SIL 2 ตามลำดับ ผู้ทำการประเมินจะต้องเลือกระดับความปลอดภัยที่ติดตั้งให้มีระดับสูงสุดที่ SIL 2 เป็นต้น

ตารางที่ 2.9 เมตริกความเสี่ยงในการคัดเลือกระดับความปลอดภัย

ความถี่ของเหตุการณ์	ระดับความปลอดภัยที่ต้องการ (Requisite SILs)					
A	-	SIL 1	SIL 2	SIL 3	SIL 4	X
B	-	SIL 1	SIL 2	SIL 3	SIL 4	SIL 4
C	-	-	SIL 1	SIL 2	SIL 3	SIL 3
D	-	-	-	SIL 1	SIL2	SIL 2
E	-	-	-	-	SIL1	SIL 1
Health/Safety Loss	H0	H1	H2	H3	H4	H5
Asset/Product loss	L0	L1	L2	L3	L4	L5
Environmental Loss	E0	E1	E2	E3	E4	E5

2.3.4 การคัดเลือกระดับความปลอดภัยในฟังก์ชันนิรภัย

เมื่อทำการคัดเลือกระดับความปลอดภัย ของกระบวนการโดยการวิเคราะห์ความเสี่ยงของเหตุการณ์อันตรายเป็นที่เรียบร้อย หากพบว่ากระบวนการต้องการระดับความปลอดภัยตั้งแต่ SIL 1 ขึ้นไป ฟังก์ชันวัดคุมนิรภัยจึงจะถูกพิจารณาติดตั้งให้สามารถใช้งานในระดับความปลอดภัยที่กำหนดได้ โดยจะประกอบด้วยส่วนสำคัญ 3 ส่วนนั่นคือ หน่วยย่อยของอุปกรณ์วัด (Sensing Element Sub System) หน่วยย่อยของหน่วยประมวลผล (Logic Solver Sub System) และหน่วยย่อยของอุปกรณ์สุดท้าย (Final Element Sub System) โดยแต่ละองค์ประกอบจะมีค่าความผิดพลาดของตนเอง โดยค่าความผิดพลาดในการทำงานนี้จะนำไปสู่การพิจารณารูปแบบของระบบนิรภัยต่อไป ในรูปที่ 2.16 จะแสดงถึงค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดในฟังก์ชันนิรภัยโดยการหาผลรวมระหว่างแต่ละองค์ประกอบในฟังก์ชันนิรภัยได้ดังสมการที่ (2.9) นำไปหาค่าระดับความปลอดภัยในตารางของ IEC 61508 ที่ฟังก์ชันนิรภัยสามารถทำได้ ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดในฟังก์ชันนิรภัย (PFD_{SIF}) และระดับความปลอดภัยจะมีความสัมพันธ์กันแบบลอการิทึมฐานสิบซึ่งสามารถสร้างความสัมพันธ์ได้ดังสมการ (2.10) ซึ่งจะถูกคำนวณโดยการออกแบบอุปกรณ์ในระบบวัดคุมนิรภัยในหัวข้อถัดไป



รูปที่ 2.16 ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดในฟังก์ชันนิรภัยแต่ละส่วน

$$PFD_{SIF} = PFD_{SS} + PFD_{LS} + PFD_{FE} \tag{2.9}$$

เมื่อ PFD_{SIF} คือ ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดในฟังก์ชันนิรภัย

PFD_{SS} คือ ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดของเครื่องมือวัด

PFD_{LS} คือ ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดของหน่วยประมวลผล

PFD_{FE} คือ ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดของอุปกรณ์สุดท้าย

$$SIL = -\log_{10}(PFD_{SIF}) \tag{2.10}$$

เมื่อ SIL คือ ระดับความปลอดภัยที่ฟังก์ชันนิรภัยนั้นใช้งานได้

PFD_{SIF} คือ ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดในฟังก์ชันนิรภัย

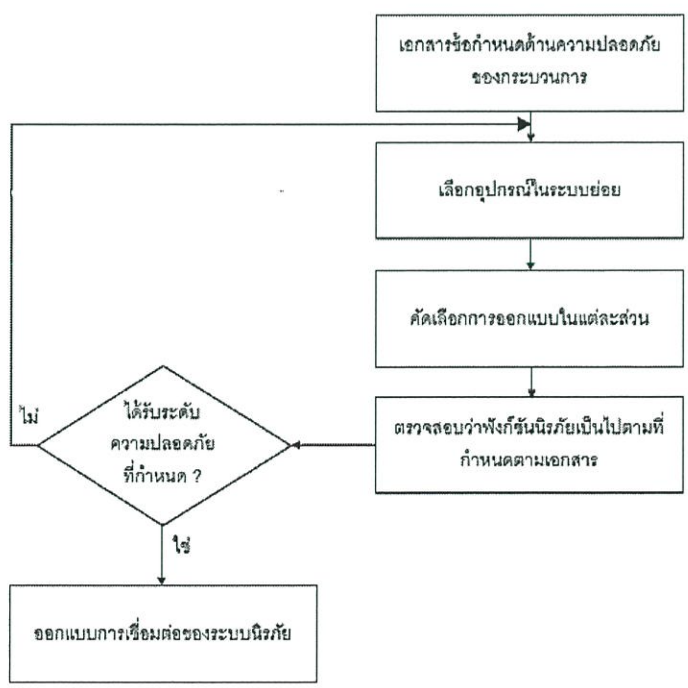
2.4 การออกแบบฟังก์ชันวัดคุมนิรภัย

ในระบบวัดคุมนิรภัยนั้นหลังจากที่ได้รับค่าระดับความปลอดภัย จากการประเมินความเสี่ยงเรียบร้อยแล้ว ผู้ปฏิบัติงานต้องทำการออกแบบฟังก์ชันในการทำงานที่ถูกต้องตาม ข้อกำหนดของกระบวนการซึ่งเป็นสิ่งที่สำคัญและต้องใช้ความละเอียดรอบคอบอย่างยิ่ง

2.4.1 ขั้นตอนการออกแบบฟังก์ชันวัดคุมนิรภัย

จากขั้นตอนการกำหนดความปลอดภัยในกระบวนการขั้นตอนที่ 5 และการจัดเตรียมเอกสารตามข้อกำหนดด้านความปลอดภัยของกระบวนการ (SRS) ในขั้นตอนที่ 6 ของมาตรฐาน IEC 61508 ก่อนที่จะทำการพิจารณาในขั้นตอนที่ 7 โดยเอกสารข้อกำหนดด้านความปลอดภัยของกระบวนการทั้งหมดที่ต้องการในกระบวนการจากการรวบรวมข้อมูลเหล่านี้ มีจุดประสงค์เพื่อให้ผู้ออกแบบเข้าใจถึงกระบวนการของฟังก์ชันนิรภัยที่จะทำการออกแบบอุปกรณ์และรูปแบบการติดตั้งที่เหมาะสมจากข้อมูลที่กำหนด ได้แก่

1) ความเป็นอันตรายของผลกระทบ (Consequences)
2) ความถี่ของการเกิดเหตุการณ์อันตราย (Likelihood)
3) แผนภาพกระบวนการผลิตที่เกี่ยวข้อง (P&ID)
4) ข้อกำหนดของกระบวนการผลิตในสภาวะปลอดภัย (Safe State)
5) รายละเอียดของฟังก์ชันนิรภัย (SIF Description)
6) รายละเอียดของตัวแปรกระบวนการที่ต้องการ (Process Parameters)
7) ค่าระดับความปลอดภัยของฟังก์ชันนิรภัย (SIL Level)
8) รายละเอียดการทดสอบการทำงาน (Proof Test Description)



รูปที่ 2.17 ขั้นตอนการออกแบบอุปกรณ์

รูปที่ 2.17 แสดงถึงขั้นตอนการออกแบบอุปกรณ์ ซึ่งหลังจากนำข้อมูลจากข้อกำหนดมาแล้ว ผู้ออกแบบจะต้องพิจารณาเลือกอุปกรณ์ในแต่ละหน่วยย่อยของฟังก์ชันนิรภัยและ

ทำการออกแบบรูปแบบการติดตั้งพร้อมทั้งนำมาคำนวณค่าระดับความปลอดภัยในฟังก์ชัน ว่าสามารถใช้งานได้ในกระบวนการที่ทำการออกแบบหรือไม่

2.4.2 ตัวแปรพื้นฐานในการออกแบบระบบนิรภัย

2.4.2.1 ความผิดพลาดหรืออัตราความผิดพลาด

ความผิดพลาดหรืออัตราความผิดพลาด (λ : Failure Rate) คือ จำนวนของอุปกรณ์อย่างหนึ่งที่คาดว่าจะเสียในช่วงเวลาที่กำหนด โดยการประเมินจากข้อมูลทางสถิติของความเสียหายในอุปกรณ์แบบเดียวกัน ข้อมูลอัตราความเสียหายที่มีความแม่นยำจะสามารถวิเคราะห์และประเมินความสามารถในการทำงานของอุปกรณ์ได้ โดยเขียนความสัมพันธ์ของความผิดพลาดกับระยะเวลาได้ดังสมการที่ (2.11) และค่าอัตราความผิดพลาดนี้จะสามารถนำไปคำนวณค่าความผิดพลาดของอุปกรณ์ในเวลาที่ต้องการ ได้จากการประมาณทางคณิตศาสตร์ในอนุกรมเทย์เลอร์ (Taylor Series) ของ e^x ดังแสดงในสมการที่ (2.12) และเมื่อแทนค่า $f(0), f'(0), f''(0), f'''(0), \ldots, f^{\infty}(0) = e^0 = 1$ ลงในสมการที่ (2.12) จะได้สมการของ e^x ตามสมการที่ (2.13) เพื่อความสะดวกในการพิจารณาทำการลดค่าโดยการประมาณใช้เพียงแค่สองเทอมแรกจะได้ $e^x = 1+x$ และเปลี่ยนจากตัวแปร x เป็น $-\lambda T_i$ จะได้สมการ e^x ใหม่ดังสมการที่ (2.14) จากสมการการคำนวณค่า PFD จากความสัมพันธ์ของช่วงเวลาและค่าอัตราความผิดพลาดจะแสดงได้ดังสมการที่ (2.15) นำค่า $e^{-\lambda T_i}$ ในสมการที่ (2.14) แทนลงในสมการที่ (2.15) จะได้สมการการคำนวณค่า PFD ดังแสดงในสมการที่ (2.16) และทำการหาค่าเฉลี่ยโดยใช้การอินทิเกรตกับระยะเวลาในการทดสอบฟังก์ชัน จะได้สมการการคำนวณค่า PFD_{avg} ดังสมการที่ (2.17)

$$\lambda = \frac{F}{T \times N} \tag{2.11}$$

โดยที่ λ คือ อัตราความผิดพลาด (ครั้งต่อหน่วยเวลา)

F คือ จำนวนครั้งของความผิดพลาด (ครั้ง)

T คือ ระยะเวลาในการทำงาน (หน่วยเวลา)

N คือ จำนวนของอุปกรณ์ที่ยังทำงานได้อยู่หลังระยะเวลาในการทำงาน

$$e^x = f(0)\frac{x^0}{0!} + f'(0)\frac{x^1}{1!} + f''(0)\frac{x^2}{2!} + f'''(0)\frac{x^3}{3!} + \ldots \tag{2.12}$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \approx 1+x \tag{2.13}$$

$$e^{-\lambda T_i} = 1 - \lambda T_i \tag{2.14}$$

จากสมการของค่า PFD จะได้

$$PFD = 1 - e^x = 1 - e^{-(\lambda T_i)} \tag{2.15}$$

แทนสมการที่ (2.14) ลงในสมการที่ (2.15)

$$PFD = \lambda T_i \tag{2.16}$$

$$PFD_{avg} = \frac{1}{T_i}\int_0^{T_i} PFD(t)\,dt \tag{2.17}$$

เมื่อ PFD_{avg} คือ ค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดบนความต้องการ

PFD คือ ค่าความน่าจะเป็นของความผิดพลาดบนความต้องการ

λ คือ อัตราความผิดพลาด (ครั้งต่อหน่วยเวลา)

T_i คือ ระยะเวลาในการทดสอบฟังก์ชัน (หน่วยเวลา)

โดยปกติแล้วอัตราความผิดพลาดของอุปกรณ์จะนิยมใช้หน่วยเป็น FITS หรือ Failure In Time ซึ่งเป็นเวลา 10^{-9} ชั่วโมง เช่น 50 FITS จะได้เท่ากับ $50x10^{-9}$ ชั่วโมง ประเภทของความผิดพลาดสามารถแบ่งได้เป็น 2 ประเภท คือ ความปลอดภัยจากความผิดพลาด (Fail Safe) และความอันตรายจากความผิดพลาด (Fail Dangerous) ซึ่งอธิบายได้ดังนี้

1) ความปลอดภัยจากความผิดพลาด (λ^S : Fail Safe) ในเครื่องมือจะหมายถึง การทำงานของฟังก์ชันวัดคุมนิรภัยที่ไม่ได้มีอันตรายเกิดขึ้นจริงหรือเรียกว่า “False Trip” หรือ “Spurious Trip” ในความผิดพลาดรูปแบบนี้ การทำงานของฟังก์ชันวัดคุมนิรภัยเกิดจากอุปกรณ์ในฟังก์ชันอ่านค่าผิดพลาดหรือเสียหาย ยกตัวอย่างด้วยการใช้งานเครื่องมือวัดความแตกต่างของท่อส่งน้ำมันที่มีความร้อน เพื่อป้องกันไม่ให้มีอัตราการไหลที่ต่ำ กระบวนการในขณะนั้นทำงานปกติและไม่มีเหตุการณ์อันตราย แต่วงจรในทรานสมิตเตอร์เกิดเสียหายทำให้อุปกรณ์การวัดอ่านค่าความดันได้สูงเกินค่าที่ตั้งไว้ ทำให้ฟังก์ชันทำงานวาล์วนิรภัยทำการปิดท่อของกระบวนการและหยุดปั๊ม จากตัวอย่างข้างต้นจะเห็นว่าเป็นความผิดพลาดที่เกิดจากอุปกรณ์ส่งสัญญาณ ไม่ใช่ความผิดปกติของกระบวนการแต่อย่างใด และกระบวนการถูกสั่งให้หยุดแต่ไม่มีอันตรายเกิดขึ้น
2) ความอันตรายจากความผิดพลาด (λ^D : Fail Dangerous) ในความหมายของ IEC 61508 นั้นเป็นความผิดพลาดของฟังก์ชันวัดคุมนิรภัย ที่ไม่สามารถป้องกันการเกิดขึ้นของเหตุการณ์อันตรายในกระบวนการได้ ยกตัวอย่างเช่น กระบวนการมีการใช้งานของวาล์วนิรภัยชนิดปิดแน่นสนิทซึ่งมีหน้าที่ในการปิดเพื่อหยุดกระบวนการ หากความดันในกระบวนการสูงเกินค่าที่กำหนดเอาไว้ ฟังก์ชันนิรภัยจะสั่งการให้วาล์วปิดทันที แต่ผลจากการอุดตันและความหนืดของก้านวาล์วจากสิ่งสกปรกทำให้วาล์วนั้นไม่สามารถปิดลงได้ เป็นต้น เหตุการณ์ในลักษณะนี้แสดงถึงความอันตรายจากความผิดพลาด เนื่องจากถึงแม้ฟังก์ชันจะรับรู้ความอันตรายจากกระบวนการ แต่ก็ไม่สามารถปฏิบัติหน้าที่นิรภัยได้

2.4.2.2 ตัวแปรระยะเวลา

ระยะเวลาในฟังก์ชันนิรภัยเป็นสิ่งที่สำคัญมากในการพิจารณา โดยเฉพาะระยะเวลาในการทดสอบอุปกรณ์ว่าการใช้งานป้องกันอันตรายนั้นสามารถใช้งานได้จริง ซึ่งตัวแปรในเรื่องของระยะเวลาสามารถแบ่งออกได้เป็น ช่วงเวลาของการทำงาน (Operating Interval) และช่วงเวลาในการทดสอบและซ่อมบำรุง (Testing and Maintenance Interval)

1) ช่วงเวลาของการทำงาน (Operating Interval)
   - 1.1) ระยะเวลาเฉลี่ยก่อนการเกิดความผิดพลาด (MTTF : Mean Time To Failure) คือ ช่วงของเวลาที่ใช้งานอุปกรณ์จนเกิดความผิดพลาดซึ่งเป็นส่วนกลับของอัตราความผิดพลาด
   - 1.2) ระยะเวลาเฉลี่ยในการซ่อมแซมอุปกรณ์ (MTTR : Mean Time To Restore) คือ ช่วงเวลาที่อุปกรณ์เกิดการผิดพลาดและซ่อมบำรุงจนสามารถใช้งานได้ใหม่ โดยปกติแล้วระยะในการซ่อมจะอยู่ที่ประมาณ 8-24 ชั่วโมง ขึ้นอยู่กับชนิดของอุปกรณ์และความสำคัญในการใช้งาน
   - 1.3) ระยะเวลาเฉลี่ยระหว่างการเสียหาย (MTBF : Mean Time Between Failure) คือ ช่วงเวลาที่เริ่มตั้งแต่อุปกรณ์เกิดความล้มเหลวครั้งแรกและครั้งที่สอง

2) ช่วงเวลาในการทดสอบและซ่อมบำรุง (Testing and Maintenance Interval)
   - 2.1) ระยะเวลาในการทดสอบ (T_i : Proof Test Interval) หมายถึง ระยะเวลาก่อนที่ฟังก์ชันนิรภัย จะถูกตรวจสอบความถูกต้องโดยผู้ปฏิบัติงาน เพื่อเป็นการกำหนดระยะเวลาการทำงานของอุปกรณ์ เช่น หากระยะการเสียหายของอุปกรณ์อยู่ที่ 5 ปี การกำหนดระยะการทดสอบฟังก์ชันจะอยู่ที่น้อยกว่า 5 ปี การทดสอบจะช่วยค้นหาความผิดพลาด ที่การทำงานปกติหาไม่เจอ ซึ่งสามารถแสดงได้ดังรูปที่ 2.19
   - 2.2) ระยะเวลาการซ่อมบำรุงครั้งใหญ่ (Major Turnaround) หมายถึง ระยะเวลาของการหยุดกระบวนการประจำปี ซึ่งจะเกิดขึ้นทุก 4 ถึง 6 ปีต่อครั้ง โดยในช่วงการซ่อมแซมจะเป็นการซ่อมบำรุงอุปกรณ์ในฟังก์ชันนิรภัย คือ อุปกรณ์วัด อุปกรณ์สุดท้าย ซึ่งจะถอดจากกระบวนการ และนำมาเช็คการรั่วไหลพร้อมเปลี่ยนอุปกรณ์ภายใน (Overhaul) เช่น ประเก็น (Gasket) และโอริง (O-ring) โดยจะสามารถค้นหาอัตราความผิดพลาดที่ไม่สามารถหาเจอในการทดสอบฟังก์ชันได้

สามารถเขียนความสัมพันธ์เป็นสมการที่ (2.18) และ (2.19) ซึ่งจากความสัมพันธ์ในสมการที่ (2.19) สามารถแสดงได้โดยรูปที่ 2.18 จากรูปจะแสดงให้เห็นถึงความสัมพันธ์ของเวลาในแต่ละรูปแบบต่อกันโดยตัวแปรเวลาที่ถูกพิจารณาใช้งานอยู่เสมอ คือ ระยะเวลาเฉลี่ยก่อนเกิดความผิดพลาด แสดงให้เห็นถึงระยะเวลาก่อนที่กระบวนการจะหยุดทำงาน

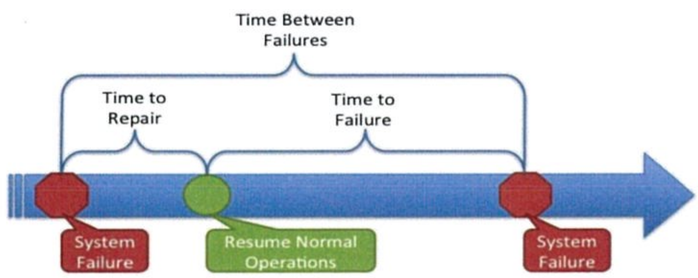
โดยความผิดพลาดของอุปกรณ์ และเป็นการหยุดทำงานที่ทำให้ระบบเกิดความเสียหายเพราะเหตุการณ์อันตราย

$$MTTF = \frac{1}{\lambda} \tag{2.18}$$

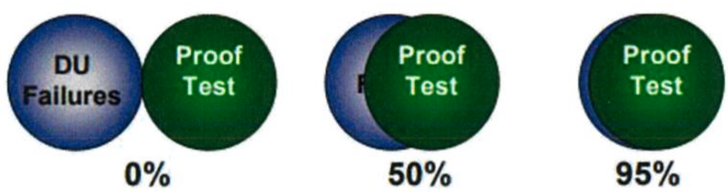
เมื่อ MTTF คือ ระยะเวลาเฉลี่ยก่อนจะเกิดความผิดพลาด (หน่วยเวลา)
λ คือ อัตราความผิดพลาด (ครั้งต่อหน่วยเวลา)

$$MTBF = MTTF + MTTR \tag{2.19}$$

เมื่อ MTTR คือ ระยะเวลาเฉลี่ยในการซ่อมแซมของอุปกรณ์หากเกิดความผิดพลาด (หน่วยเวลา)
MTBF คือ ระยะเวลาเฉลี่ยระหว่างการเสียหายแต่ละครั้ง (หน่วยเวลา)



รูปที่ 2.18 ความสัมพันธ์ระหว่างตัวแปรเวลาในช่วงเวลาของการทำงาน



รูปที่ 2.19 แสดงความสัมพันธ์ของระยะเวลาการทดสอบกับอัตราความผิดพลาด

2.4.2.3 ค่าความครอบคลุม

ค่าความครอบคลุม (Coverage Factor) ในเรื่องของฟังก์ชันนิรภัยนี้แสดงถึงความสามารถในการค้นพบอันตรายที่มีอยู่ในอุปกรณ์ต่าง ๆ ในฟังก์ชันนิรภัย ซึ่งอาจหมายถึงการทำการทดสอบฟังก์ชันวัดคุมนิรภัย (Proof Testing of Safety Instrument System) หรือการค้นพบความเสี่ยงอันตรายของอุปกรณ์โดยเครื่องมือที่ทันสมัย เช่น ทรานสมิตเตอร์อัจฉริยะ (Smart Transmitter) ซึ่งมีฟังก์ชันแจ้งเตือนโดยอัตโนมัติ (Automatic Diagnostic) เป็นต้น ซึ่งการค้นพบความอันตรายเหล่านี้ทำให้อัตราความอันตรายที่เกิดขึ้นจากอุปกรณ์มีอัตราที่น้อยลงอย่างมาก ดังนั้นอัตราความผิดพลาดจะเหลือความอันตรายจากความผิดพลาดที่ไม่สามารถตรวจพบ (Undetected Failure) ซึ่งจะเป็นส่วนสำคัญในการคำนวณค่าระดับความปลอดภัยของฟังก์ชันวัดคุมนิรภัย และเขียนเป็นสมการค่าความครอบคลุมได้ดังสมการที่ (2.20) ตัวแปรค่าความครอบคลุมนี้มีผลต่อความอันตรายจากความผิดพลาดและความปลอดภัยจากความผิดพลาด เช่นเดียวกัน โดยส่วนที่ตรวจพบจะเป็นความปลอดภัยจากความผิดพลาดที่ตรวจพบ (Fail Safe Detected) และความอันตรายจากความผิดพลาดที่ตรวจพบ (Fail Dangerous Detected) ส่วนที่ตรวจไม่พบจะเป็นความปลอดภัยจากความ

ผิดพลาดที่ตรวจไม่พบ (Fail Safe Undetected) และความอันตรายจากความผิดพลาดที่ตรวจไม่พบ (Fail Dangerous Undetected) โดยความสัมพันธ์ของอัตราความผิดพลาดแต่ละชนิดนั้นแสดงได้ดังสมการที่ (2.21)

$$C^D = \frac{\lambda^{DD}}{\lambda} = \frac{\lambda^{DD}}{\lambda^{DD}+\lambda^{DU}} \tag{2.20}$$

$$\lambda = \lambda^S+\lambda^D = \left(\lambda^{SD}+\lambda^{SU}\right)+\left(\lambda^{DD}+\lambda^{DU}\right) \tag{2.21}$$

เมื่อ C^D คือ ค่าความครอบคลุม

λ^S คือ อัตราความปลอดภัยจากความผิดพลาด

λ^D คือ อัตราความอันตรายจากความผิดพลาด

λ^{SD} คือ อัตราความปลอดภัยจากความผิดพลาดที่ตรวจพบ

λ^{SU} คือ อัตราความปลอดภัยจากความผิดพลาดที่ตรวจไม่พบ

λ^{DD} คือ อัตราความอันตรายจากความผิดพลาดที่ตรวจพบ

λ^{DU} คือ อัตราความอันตรายจากความผิดพลาดที่ตรวจไม่พบ

2.4.2.4 อัตราส่วนความผิดพลาดนิรภัย

อัตราส่วนความผิดพลาดนิรภัย (SFF : Safety Failure Fraction) ในแต่ละอุปกรณ์เป็นค่าตัวแปรที่สำคัญในการออกแบบฟังก์ชั้นวัดคุมนิรภัย ซึ่งเป็นสัดส่วนระหว่างอัตราความผิดพลาดทั้งหมด กับอัตราความปลอดภัยจากความผิดพลาดรวมเข้ากับอัตราความอันตรายจากความผิดพลาดที่ตรวจพบ ภายในมาตรฐาน IEC 61508 และ IEC 61511 มีรูปแบบของความสัมพันธ์เป็นดังสมการที่ (2.22) หากอุปกรณ์ในฟังก์ชันนิรภัยภัยนั้นมีค่าอัตรส่วนความผิดพลาดนิรภัยที่สูง ก็จะแสดงว่าอุปกรณ์นั้นมีความสามารถในระบบนิรภัย และสามารถใช้ในกระบวนการที่มีระดับความปลอดภัยสูงเช่นกัน

$$SFF = \frac{\lambda^{SD}+\lambda^{SU}+\lambda^{DD}}{\lambda^{SD}+\lambda^{SU}+\lambda^{DD}+\lambda^{DU}} \tag{2.22}$$

2.4.2.5 ค่าปัจจัยจากสาเหตุร่วม

ค่าปัจจัยจากสาเหตุร่วม (β : Common Cause Factor) คือ ค่าที่แสดงถึงความผิดพลาดที่เกิดจากสาเหตุเดียวกันในการทำงาน จะมีอยู่ในการคำนวณของอุปกรณ์ในระบบนิรภัยที่เป็นรูปแบบการสำรองที่มากกว่าหนึ่งตัวขึ้นไป ตัวแปรนี้จะขึ้นอยู่กับการติดตั้งและการวิเคราะห์จากผู้เชี่ยวชาญ เช่น การเดินสายของอุปกรณ์วัดในรูปแบบ 1oo2 voting เดินสายไปสู่ตู้ควบคุมด้วยกล่องแยกจุดเดียวกันหรือไม่ ถ้าอยู่จุดเดียวกันแล้วค่าปัจจัยจากสาเหตุร่วมจะมีเปอร์เซ็นต์ที่สูงขึ้นและแสดงถึงค่าความผิดพลาดที่มากขึ้น เป็นต้น โดยค่าตัวแปรนี้ในมาตรฐาน IEC 61508 part 6, Annex D ได้มีการกำหนดตารางคะแนนสำหรับค่าปัจจัยจากสาเหตุร่วม เพื่อใช้เป็นแนวทางสำหรับการประเมินระดับความปลอดภัยของฟังก์ชันนิรภัยดังตารางที่ 2.10 ซึ่งค่าคะแนน (Score) ในตารางนั้นจะถูกนำไปใช้โดยการประเมินจากทีมวิศวกร โดยปกติระบบนิรภัยทั่วไปจะอยู่ที่ 75 คะแนนถึง 125 คะแนน ค่าที่สูงที่สุดของค่าปัจจัยจากสาเหตุร่วมที่ถูกแสดงขึ้นในตารางจะมีค่า

น้อยกว่าค่าที่ใช้งานปกติ สะท้อนให้เห็นถึงเทคนิคและข้อกำหนดที่ถูกพิจารณานอกเหนือจากมาตรฐาน เพื่อใช้ในการลดความเสี่ยงของความผิดพลาดในระบบและจะมีผลเป็นค่าปัจจัยจากสาเหตุร่วมออกมา สำหรับหน่วยประมวลผลที่มีค่าต่ำกว่า 0.5 % และอุปกรณ์วัดหรืออุปกรณ์ควบคุมสุดท้ายที่มีค่าต่ำกว่า 1 % มีผลกระทบกระทบต่ำ

ตารางที่ 2.10 ตารางค่าปัจจัยจากสาเหตุร่วมจากการประเมินคะแนนจากตารางของ IEC 61508

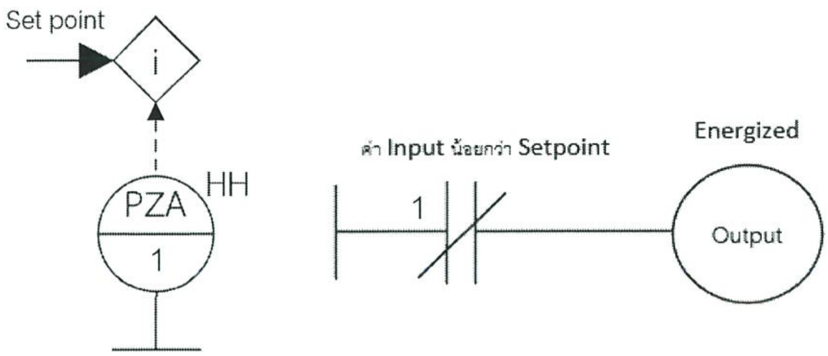
คะแนน (S or S_D)	ค่าปัจจัยจากสาเหตุร่วม	
	หน่วยประมวลผล	อุปกรณ์วัดหรืออุปกรณ์ควบคุมสุดท้าย
120 หรือสูงกว่า	0.5 %	1 %
70 ถึง 120	1 %	2 %
45 ถึง 70	2 %	5 %
น้อยกว่า 45	5 %	10 %

2.4.3 รูปแบบการเชื่อมต่อของอุปกรณ์นิรภัย

การเลือกรูปแบบการใช้งานของอุปกรณ์บนระบบนิรภัยนั้นเป็นสิ่งสำคัญ เนื่องจากบางระบบมีความต้องการใช้งานสูง หากการออกแบบระบบไม่ดีอาจทำให้เกิดผลกระทบที่อันตรายตามมา โดยปกติแล้วหากกระบวนการใดมีความสำคัญมาก การออกแบบจะต้องพิจารณาติดตั้งอุปกรณ์ที่มีรูปแบบที่เรียกว่า อุปกรณ์สำรอง ของอุปกรณ์วัด หน่วยประมวลผล และอุปกรณ์ควบคุมสุดท้าย ในการใช้อุปกรณ์สำรองที่ติดตั้งในกระบวนการมีหลากหลายรูปแบบการเชื่อมต่อ ขึ้นอยู่กับตัวอุปกรณ์และความอันตรายของกระบวนการ โดยรูปแบบของการเชื่อมต่ออุปกรณ์สำรองที่ใช้งานในอุตสาหกรรมจะมีดังนี้

2.4.3.1 อุปกรณ์แบบ 1oo1

อุปกรณ์แบบ 1oo1 (One out of One voting) จะมีอุปกรณ์เพียงตัวเดียว หรือเรียกว่า การออกแบบที่ไม่มีอุปกรณ์สำรอง (No Redundancy) ซึ่งมีการใช้งานมากที่สุดในบรรดารูปแบบต่าง ๆ เนื่องจากการติดตั้งอุปกรณ์ที่น้อยทำให้ค่าใช้จ่ายน้อยตามไปด้วย ซึ่งหากพิจารณาแล้วจะคล้ายกับระบบควบคุมปกติของการบวนการ แต่ในระบบ 1oo1 จะเป็นฟังก์ชันนิรภัยที่เข้ามาป้องกันเหตุการณ์อันตราย โดยระบบนิรภัยแบบ 1oo1 แสดงการทำงานได้ดังรูปที่ 2.20 โดยภายในรูปเป็นการแสดงการเชื่อมต่อแบบ 1oo1 ของอุปกรณ์วัดซึ่งจะเป็นการวัดความดันเกินในกระบวนการ ค่าที่วัดได้จากทรานสมิตเตอร์จะถูกส่งไปเปรียบเทียบกับสัญญาณที่ตั้งไว้ ในการทำงานปกติของฟังก์ชัน ลอจิกจะมีลักษณะที่เรียกว่าปกติปิด หรือ Normally Close ที่ลอจิก 0 ซึ่งทำให้มีเอาท์พุตเท่ากับ 1 และให้พลังงาน (Energized) แก่อุปกรณ์สุดท้าย หากค่าความดันในกระบวนการมีค่าเกินระดับที่ตั้งไว้ ผลลัพธ์ของการเปรียบเทียบจะได้ 1 จากโครงสร้างลอจิกที่เป็นแบบปกติปิดทำให้ลอจิกของเอาท์พุตเป็น 0 และหยุดการให้พลังงาน (De-Energized) เพื่อทำการปิดหรือเปิดอุปกรณ์สุดท้ายเพื่อป้องกันเหตุการณ์อันตราย การเชื่อมต่ออุปกรณ์แบบ 1oo1 ตามมาตรฐาน ISA-TR84.00.02-2002 part 2 ว่าด้วยการออกแบบฟังก์ชันวัดคุมนิรภัยมีการคำนวณหาค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดบนความต้องการ (PFD_{avg}) แสดงได้ในสมการที่ (2.23)



(ก) (ข)

รูปที่ 2.20 การเชื่อมต่ออุปกรณ์วัดแบบ 1oo1

(ก) ภาพจาก P&ID (ข) Ladder Diagram

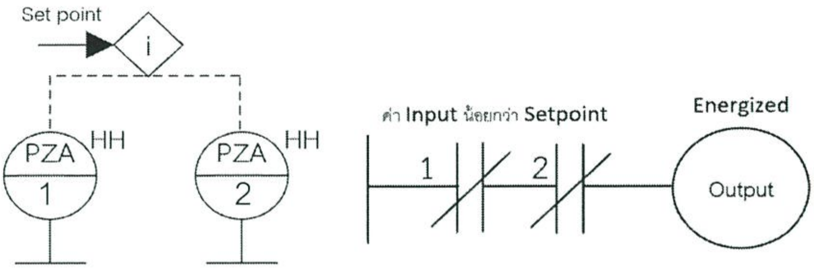
$$PFD_{avg} = (\lambda^{DU} x \frac{Ti}{2}) \tag{2.23}$$

เมื่อ λ^{DU} คือ อัตราความอันตรายจากความผิดพลาดอันตรายที่ตรวจพบ

Ti คือ ระยะเวลาระหว่างการทำการทดสอบฟังก์ชันวัดคุมนิรภัยในแต่ละครั้ง

2.4.3.2 อุปกรณ์แบบ 1oo2

อุปกรณ์รูปแบบ 1oo2 (One out of Two voting) นั้นมีการใช้งานอย่างแพร่หลายในระบบวัดคุมนิรภัยที่ต้องการความปลอดภัยในระดับสูงขึ้น โดยรูปแบบนี้จะแสดงถึงการสำรองอุปกรณ์ในกระบวนการ หากอุปกรณ์ตัวใดมีล้มเหลวต่อการทำหน้าที่อุปกรณ์นิรภัยอีกตัวจะยังสามารถทำหน้าที่ของฟังก์ชันได้ การใช้งานรูปแบบ 1oo2 สามารถออกแบบได้ทั้ง อุปกรณ์วัด หน่วยประมวลผล และอุปกรณ์สุดท้ายขึ้นอยู่กับความต้องการ แสดงการเชื่อมต่อได้ดังรูปที่ 2.21 ภายในรูปเป็นการแสดงการเชื่อมต่อแบบ 1oo2 ของอุปกรณ์วัดความดันเกินในกระบวนการ ค่าที่วัดได้จากทรานสมิตเตอร์ทั้งสองตัวจะถูกส่งไปเปรียบเทียบกับสัญญาณที่ตั้งไว้ ในการทำงานปกติของฟังก์ชันลอจิกมีลักษณะที่เรียกว่าปกติปิดที่ลอจิก 0 ซึ่งทำให้เอาท์พุตเท่ากับ 1 และจะให้พลังงานแก่อุปกรณ์ควบคุมสุดท้าย โดยมีลักษณะการเชื่อมต่อลอจิกทั้งสองเป็นแบบ AND หมายความว่า หากอุปกรณ์วัดตัวใดตัวหนึ่งเกิดการเสียหายไม่สามารถอ่านค่าความดันเกินได้ขณะเกิดอันตราย ระบบจะยังสามารถเข้าสู่ภาวะปลอดภัยได้โดยอีกตัวหนึ่งที่ยังทำงานอยู่ หากค่าความดันในกระบวนการมีค่าเกินระดับที่ตั้งไว้ ผลลัพธ์ของการเปรียบเทียบของอุปกรณ์ทั้งสองตัวจะได้ 1 จากโครงสร้าง Ladder Diagram ที่เป็นแบบปกติปิดทำให้เอาท์พุตเป็น 0 และหยุดทำงาน ทำการปิดหรือเปิดอุปกรณ์ควบคุมสุดท้ายเพื่อป้องกันเหตุการณ์อันตราย การเชื่อมต่ออุปกรณ์แบบ 1oo2 ตามมาตรฐาน ISA-TR84.00.02-2002 part 2 ว่าด้วยการออกแบบฟังก์ชันวัดคุมนิรภัยมีการคำนวณหาค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดบนความต้องการ (PFD_{avg}) แสดงได้ในสมการที่ (2.24)



(ก) (ข)

รูปที่ 2.21 การเชื่อมต่ออุปกรณ์วัดแบบ 1oo2

(ก) ภาพจาก P&ID (ข) Ladder Diagram

$$PFD_{avg}=\left[(\lambda^{DU})^2 x \frac{Ti^2}{2}\right]+\left[\lambda^{DU} x\, \lambda^{DD} x \text{ MTTR } xTi\right]+\left[\beta x\, \lambda^{DU} x \frac{Ti}{2}\right] \quad (2.24)$$

เมื่อ λ^{DU} คือ อัตราความอันตายจากความผิดพลาดที่ตรวจไม่พบ

λ^{DD} คือ อัตราความอันตายจากความผิดพลาดที่ตรวจพบ

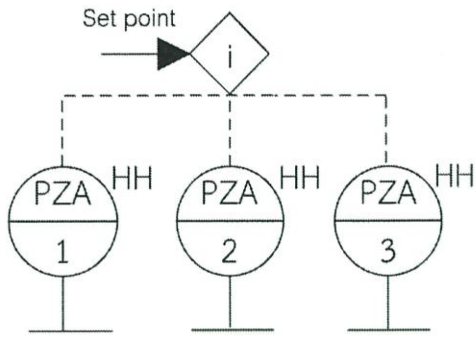
Ti คือ ระยะเวลาระหว่างการทำการทดสอบฟังก์ชันวัดคุมนิรภัยในแต่ละครั้ง

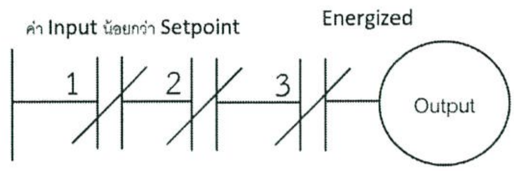
β คือ ค่าปัจจัยจากสาเหตุร่วม

MTTR คือ ระยะเวลาที่ใช้ในการซ่อมบำรุงแต่ละครั้ง (Mean Time To Repair)

2.4.3.3 อุปกรณ์แบบ 1oo3

อุปกรณ์ที่ใช้งานในรูปแบบ 1oo3 (One out of Three voting) ในระบบนิรภัยที่ต้องการความปลอดภัยในระดับสูงขึ้น ซึ่งสามารถป้องกันเหตุการณ์อันตรายได้ดีกว่ารูปแบบของ 1oo2 โดยรูปแบบของ 1oo3 แสดงถึงการสำรองอุปกรณ์หากอุปกรณ์หนึ่งหรือสองตัวมีความผิดปกติต่อการทำหน้าที่ อุปกรณ์นิรภัยอีกตัวหนึ่งจะยังสามารถทำหน้าที่ของระบบได้ การใช้งานของรูปแบบ 1oo3 สามารถเป็นได้ทั้ง อุปกรณ์วัด หน่วยประมวลผล และอุปกรณ์ควบคุมสุดท้าย แสดงการทำงานได้ดังรูปที่ 2.22 โดยภายในรูปที่เป็นการแสดงการเชื่อมต่อแบบ 1oo3 ของอุปกรณ์วัดความดันเกินในกระบวนการ โดยค่าที่วัดได้จากทรานสมิตเตอร์ทั้งสามตัวจะถูกส่งไปเปรียบเทียบกับสัญญาณที่ตั้งไว้ ในการทำงานปกติของฟังก์ชันลอจิกมีลักษณะที่เรียกว่าปกติปิดที่ลอจิก 0 ซึ่งทำให้เอาท์พุตเท่ากับ 1 ซึ่งจะให้พลังงานแก่อุปกรณ์ควบคุมสุดท้ายโดยมีลักษณะการเชื่อมต่อลอจิกทั้งสามเป็นแบบ AND หมายความว่า หากอุปกรณ์วัดหนึ่งถึงสองตัวเกิดการเสียหายไม่สามารถอ่านค่าความดันเกินได้ขณะเกิดอันตรายระบบจะยังสามารถเข้าสู่สภาวะปลอดภัยได้โดยอีกตัวหนึ่งที่ยังทำงานอยู่ หากค่าความดันในกระบวนการมีค่าเกินระดับที่ตั้งไว้ ผลลัพธ์ของการเปรียบเทียบของอุปกรณ์ทั้งสองตัวจะได้ 1 ซึ่งจากโครงสร้าง Ladder Diagram ที่เป็นแบบปกติปิดทำให้อาท์พุทเป็น 0 และหยุดทำงาน ทำการปิดหรือเปิดอุปกรณ์สุดท้ายเพื่อป้องกันเหตุการณ์อันตราย การเชื่อมต่ออุปกรณ์แบบ 1oo3 ตามมาตรฐาน ISA-TR84.00.02-2002 part 2 ว่าด้วยการออกแบบฟังก์ชันวัดคุมนิรภัยมีการคำนวณหาค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดบนความต้องการ (PFD_{avg}) แสดงได้ในสมการที่ (2.25)





(ก) (ข)

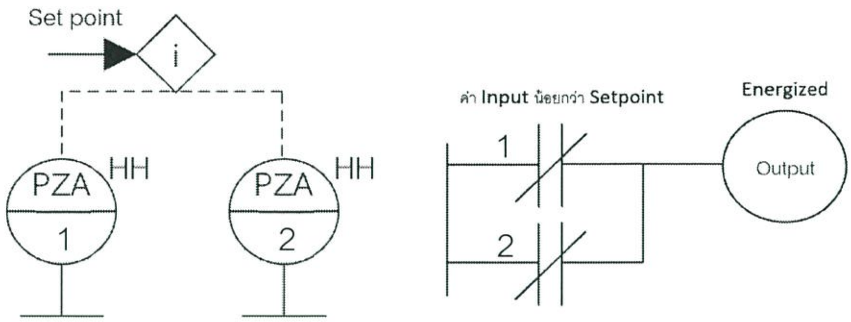
รูปที่ 2.22 การเชื่อมต่ออุปกรณ์วัดแบบ 1oo3

(ก) ภาพจาก P&ID (ข) Ladder Diagram

$$PFD_{avg} = \left[(\lambda^{DU})^3 x \frac{Ti^3}{4}\right] + \left[(\lambda^{DU})^2 x\, \lambda^{DD} x \text{ MTTR } xTi^2\right] + \left[\beta x\, \lambda^{DU} x \frac{Ti}{2}\right] \quad (2.25)$$

2.4.3.4 อุปกรณ์แบบ 2oo2

อุปกรณ์รูปแบบ 2oo2 (Two out of Two voting) นั้นมีรูปแบบการใช้งานที่คล้ายกันกับแบบ 1oo1 โดยรูปแบบของ 2oo2 จะไม่ได้เพิ่มระดับความปลอดภัยในแก่ระบบเท่ากับแบบ 1oo1 รูปแบบของ 2oo2 ไม่มีการสำรองอุปกรณ์ไว้ในกระบวนการ การทำงานของฟังก์ชันนิรภัยนั้นจะต้องให้อุปกรณ์ทั้งสองตัวนั้นมีความพร้อมในการใช้งานป้องกันอันตราย หากอุปกรณ์ตัวใดตัวหนึ่งไม่สามารถทำงานหน้าที่ของระบบนิรภัยได้ กระบวนการการก็จะเกิดอันตรายโดยทันที การใช้งานของรูปแบบ 2oo2 สามารถเป็นได้ทั้ง อุปกรณ์วัด หน่วยประมวลผล และอุปกรณ์ควบคุมสุดท้าย แต่โดยปกตินั้นจะไม่นิยมใช้งานในกระบวนการแสดงการทำงานได้ดังรูปที่ 2.23 โดยภายในรูปเป็นการแสดงการเชื่อมต่อแบบ 2oo2 ของอุปกรณ์วัดความดันเกินในกระบวนการ โดยค่าที่วัดได้จากทรานสมิตเตอร์ทั้งสองตัวจะถูกส่งไปเปรียบเทียบกับสัญญาณที่ตั้งไว้ ในการทำงานปกติลอจิกมีลักษณะที่เรียกว่าปกติปิด ที่ลอจิก 0 จะทำให้ลอจิกของเอาท์พุตเท่ากับ 1 ซึ่งจะให้พลังงานแก่อุปกรณ์ควบคุมสุดท้าย โดยมีลักษณะการเชื่อมต่อกันเป็นแบบ OR หมายความว่าหากอุปกรณ์วัดหนึ่งหรือสองตัวเกิดการเสียหายไม่สามารถอ่านค่าความดันเกินได้ขณะเกิดอันตรายระบบจะไม่สามารถเข้าสู่ภาวะปลอดภัยได้ หากค่าความดันในกระบวนการมีค่าเกินระดับที่ตั้งไว้ ผลลัพธ์ของการเปรียบเทียบของอุปกรณ์ทั้งสองตัวจะได้ 1 จากโครงสร้าง Ladder Diagram ที่เป็นแบบปกติปิด ทำให้เอาท์พุตเป็น 0 และถูกหยุดทำงาน ทำการปิดหรือเปิดอุปกรณ์สุดท้ายเพื่อป้องกันเหตุการณ์อันตราย การเชื่อมต่ออุปกรณ์แบบ 2oo2 ตามมาตรฐาน ISA-TR84.00.02-2002 part 2 ว่าด้วยการออกแบบฟังก์ชันวัดคุมนิรภัย มีการคำนวณหาค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดบนความต้องการ (PFD_{avg}) แสดงได้ในสมการที่ (2.26)



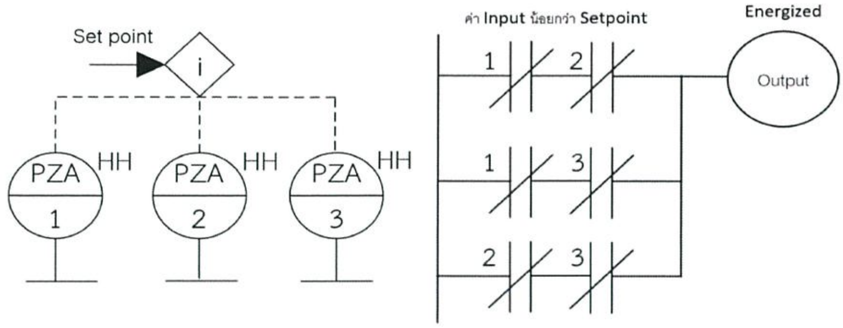
(ก) (ข)

รูปที่ 2.23 การเชื่อมต่ออุปกรณ์วัดแบบ 2oo2
(ก) ภาพจาก P&ID (ข) Ladder Diagram

$$PFD_{avg} = (\lambda^{DU} xTi) + (\beta \text{ x } \lambda^{DU} xTi) \tag{2.26}$$

2.4.3.5 อุปกรณ์แบบ 2oo3

อุปกรณ์ที่ใช้งานในรูปแบบ 2oo3 (Two out of Three voting) ในระบบนิรภัยที่ต้องการความปลอดภัยในระดับสูงขึ้น แต่จะป้องกันเหตุการณ์อันตรายได้ในระดับที่ต่ำกว่ารูปแบบ 1oo2 โดยรูปแบบของ 2oo3 แสดงถึงการสำรองอุปกรณ์หากอุปกรณ์หนึ่งตัวมีความผิดปกติต่อการทำหน้าที่ อุปกรณ์อีกสองตัวจะยังสามารถทำหน้าที่ของระบบได้ การใช้งานของรูปแบบ 2oo3 สามารถเป็นได้ทั้ง อุปกรณ์วัด หน่วยประมวลผล และอุปกรณ์สุดท้าย แต่ส่วนใหญ่จะถูกใช้งานในรูปแบบอุปกรณ์วัดเท่านั้น แสดงการทำงานได้ดังรูปที่ 2.24 ภายในรูปเป็นการแสดงการเชื่อมต่อแบบ 2oo3 ของอุปกรณ์วัดความดันเกินในกระบวนการ โดยค่าที่วัดได้จากทรานสมิตเตอร์ทั้งสามตัวจะถูกส่งไปเปรียบเทียบกับสัญญาณที่ตั้งไว้ ในการทำงานปกติของลอจิกมีลักษณะเป็นปกติปิดที่ลอจิก 0 ทำให้เอาท์พุตเท่ากับ 1 ซึ่งจะให้พลังงานแก่อุปกรณ์ควบคุมสุดท้าย โดยมีลักษณะการเชื่อมต่อลอจิกภายในรูปที่ 2.24 (ข) เป็นการ AND ระหว่างคู่ลอจิกทั้งสามคู่ คือ 1,2 1,3 และ 2,3 จากนั้นนำสัญญาณทั้งสามมาทำการ AND กันก่อนไปที่เอาท์พุต หมายความว่า หากอุปกรณ์วัดหนึ่งตัวเกิดการเสียหายไม่สามารถอ่านค่าความดันเกินได้ขณะเกิดอันตราย ระบบจะยังสามารถเข้าสู่ภาวะปลอดภัยได้โดยอีกสองตัวที่ยังทำงาน หากค่าความดันในกระบวนการเกินระดับที่ตั้งไว้ผลลัพธ์ของการเปรียบเทียบอุปกรณ์ทั้งสองตัวจะได้ 1 จากโครงสร้าง Ladder Diagram ที่เป็นแบบปกติปิดทำให้เอาท์พุตเป็น 0 และถูกหยุดทำงาน ทำการปิดหรือเปิดอุปกรณ์สุดท้ายเพื่อป้องกันเหตุการณ์อันตราย การเชื่อมต่ออุปกรณ์แบบ 2oo3 ตามมาตรฐาน ISA-TR84.00.02-2002 part 2 ว่าด้วยการออกแบบฟังก์ชันวัดคุมนิรภัยมีการคำนวณหาค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดบนความต้องการ (PFD_{avg}) แสดงได้ในสมการที่ (2.27)



(ก) (ข)

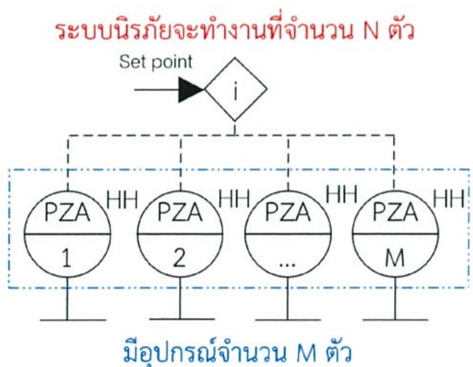
รูปที่ 2.24 การเชื่อมต่ออุปกรณ์วัดแบบ 2oo3

(ก) ภาพจาก P&ID (ข) Ladder Diagram

$$PFD_{avg} = \left[(\lambda^{DU})^2 x Ti^2\right] + \left[\ 3\lambda^{DU} x\ \lambda^{DD} x\ MTTR\ x\ Ti\right] + \left[\beta x\ \lambda^{DU} x \frac{Ti}{2}\right] \quad (2.27)$$

2.4.3.6 อุปกรณ์รูปแบบอื่น

รูปแบบการทำงานของ MooN (M out of N voting) โดย M คือ จำนวนอุปกรณ์ที่ฟังก์ชันนิรภัยต้องการเพื่อทำงานและ N คือ จำนวนอุปกรณ์ทั้งหมดที่ติดตั้งในฟังก์ชันเพื่อป้องกันอันตราย ซึ่งรูปแบบ MooN ก็จะเป็นรูปแบบเบื้องต้นของรูปแบบอื่น ๆ ได้แก่ 3oo4 4oo5 และ 6oo10 เป็นต้น การใช้งานในแต่ละรูปแบบของ MooN จะขึ้นอยู่กับกระบวนการที่แตกต่างกันและผู้ใช้งาน แสดงการเชื่อมต่อได้ในรูปที่ 2.25 จากรูปสามารถเขียนการคำนวณหาค่าความน่าจะเป็นเฉลี่ยของความผิดพลาดบนความต้องการ (PFD_{avg}) ได้ดังสมการที่ (2.28) โดยค่าอัตราความผิดพลาดอันตรายที่เกิดจากค่าปัจจัยจากสาเหตุร่วม (λ^C) สามารถคำนวณหาได้ดังสมการที่ (2.29)



รูปที่ 2.25 การเชื่อมต่ออุปกรณ์วัดแบบ MooN

$$PFD_{avg} = \left[\frac{N!}{(M-1)!(N-M+1)!}\right] x \left[\frac{(\lambda^{DU} x Ti)^{(N-M+1)}}{N-M+2}\right] + (\lambda^C Ti) \quad (2.28)$$

$$\lambda^C = \beta\, \lambda^{DU} \quad (2.29)$$

เมื่อ λ^C คือ อัตราความอันตรายจากความผิดพลาดที่เกิดจากค่าปัจจัยจากสาเหตุร่วม

M คือ จำนวนอุปกรณ์ที่ฟังก์ชันวัดคุมนิรภัยต้องการเพื่อทำงาน

N คือ จำนวนอุปกรณ์ทั้งหมดที่ติดตั้งในฟังก์ชันวัดคุมนิรภัยเพื่อป้องกันอันตราย

2.4.4 ข้อกำหนดสำหรับการออกแบบระบบนิรภัย

2.4.4.1 ข้อจำกัดของการออกแบบ

ข้อจำกัดของการออกแบบ (Architecture Constraint) เป็นข้อกำหนดที่ใช้กับรูปแบบหน่วยย่อยเครื่องมือวัด หน่วยย่อยของหน่วยประมวลผล และหน่วยย่อยของอุปกรณ์ควบคุมสุดท้าย การใช้งานขึ้นอยู่กับระดับความปลอดภัยของฟังก์ชันนิรภัยและคุณภาพความมั่นคงของอุปกรณ์ที่เลือกใช้ มาตรฐาน IEC 61508 ได้มีการกำหนดจำนวนอุปกรณ์ต่ำที่สุดที่ยอมให้เกิดความผิดพลาดได้ (HFT : Minimum Hardware Fault Tolerance) ตามค่าระดับความปลอดภัยและอัตราส่วนความผิดพลาดนิรภัย ซึ่งจะถูกแยกเป็นอุปกรณ์ชนิด A (Type A Device) และอุปกรณ์ชนิด B (Type B Device) โดยอุปกรณ์ชนิด A เป็นอุปกรณ์จำพวกอุปกรณ์พื้นฐานในวงจรไฟฟ้า เช่น ตัวเก็บประจุคาปาซิเตอร์ ตัวต้านทาน เป็นต้น หากเป็นอุปกรณ์ทางเครื่องมือวัดและควบคุมจะเป็นจำพวก สวิทช์แรงดัน สวิทช์ระดับ รีเลย์ โซลินอยล์วาล์ว และวาล์ว อุปกรณ์แบบที่กล่าวจะมีการใช้งานที่ไม่ซับซ้อนและสามารถตรวจสอบการทำงานได้ครบถ้วน ส่วนอุปกรณ์ชนิด B เป็นอุปกรณ์จำพวกที่มีความซับซ้อนอยู่ในตัวอุปกรณ์ เช่น ไมโครโปรเซสเซอร์ วงจรรวม อุปกรณ์อิเล็กทรอนิกส์จำพวกนี้จะถูกใช้งานในอุปกรณ์และใช้เป็นโปรแกรมในการควบคุม เช่น ทรานสมิตเตอร์อัจฉริยะ หน่วยประมวลผล เป็นต้น โดยอุปกรณ์ทั้งสองชนิดจะใช้ค่าที่กำหนดจากตารางในการออกแบบจำนวนของอุปกรณ์ต่ำที่สุดที่ยอมให้เกิดความผิดพลาดโดยจะมีทั้งหมด 3 แบบ ตามเกณฑ์ของ IEC 61508 คือ 0 1 และ 2 ตัว ซึ่งตัวเลขนี้จะเป็นตัวบ่งบอกว่าที่ระดับความปลอดภัยนั้น ๆ จะต้องมีการติดตั้งจำนวนอุปกรณ์กี่ตัวเพื่อให้ฟังก์ชันวัดคุมนิรภัยตอบรับความต้องการของกระบวนการได้ โดยอุปกรณ์ชนิด A จะแสดงค่าจำนวนอุปกรณ์ต่ำสุดอยู่ในตารางที่ 2.11 และอุปกรณ์ชนิด B จะแสดงค่าจำนวนอุปกรณ์ต่ำสุดอยู่ในตารางที่ 2.12 จากทั้งสองตารางจะเห็นว่าการจำนวนการเชื่อมต่อของอุปกรณ์จะขึ้นอยู่กับระดับความปลอดภัยและอัตราส่วนความผิดพลาดนิรภัยของอุปกรณ์แต่ละชนิดแต่ละรุ่น โดยในปัจจุบันจะมีเอกสารรับรอง (Certified Data) จากองค์กรต่าง ๆ เช่น Exida, TUV หรือ FM เป็นต้น

เมื่อพิจารณาถึงอุปกรณ์ที่ถูกใช้งานมานาน ที่มีการติดตั้งก่อนที่จะมีการออกมาตรฐานนิรภัย IEC 61511 จะมีการออกข้อกำหนดให้ผู้ใช้งานอุปกรณ์สามารถลดจำนวนของตัวอุปกรณ์ลงได้หนึ่งตัว โดยจะสามารถทำได้ถ้าผลิตภัณฑ์นั้นอยู่บนพื้นฐานของ “Prior-Use หรือ Proven-in-Use” ซึ่งเป็นไปตามข้อกำหนดดังนี้

1) อุปกรณ์ยินยอมให้มีการปรับแต่งเฉพาะตัวแปรในกระบวนการเท่านั้น เช่น ย่านการวัด การปรับเทียบศูนย์ เป็นต้น
2) การปรับแต่งต้องมีการป้องกัน เช่น จุดต่อป้องกัน รหัสผ่าน เป็นต้น
3) จะต้องใช้ในฟังก์ชันที่มีระดับความปลอดภัยน้อยกว่าระดับ SIL 4

ความหมายของ Prior-Use หรือ Proven-in-Use ได้อธิบายไว้ว่าผู้ใช้จะต้องมีการพัฒนาแนวทางในการยืนยันการใช้งานตามมาตรฐานแต่ละหน่วยย่อยของอุปกรณ์ในฟังก์ชันวัดคุมนิรภัย ตามมาตรฐาน IEC 61508 ตอนที่ 2 และ 3 ซึ่งแต่ละฟังก์ชันจะต้องมีรายละเอียดดังนี้

1) มีรายละเอียดของอุปกรณ์อย่างชัดเจนรวมไปถึงข้อมูลในการออกแบบ
2) มีข้อมูลความผิดพลาดในการใช้งานที่คล้ายคลึงกันรวมไปถึงสภาวะการใช้งานสำหรับอุปกรณ์
3) มีข้อมูลของค่าความครอบคลุมและอัตราส่วนความผิดพลาดนิรภัย

ซึ่งข้อมูลเพิ่มเติมจะถูกแสดงอยู่ในมาตรฐาน IEC 61511-1 clause 11.5.3

ตารางที่ 2.11 ตารางจำนวนอุปกรณ์ต่ำที่สุดที่สามารถผิดพลาดได้ของอุปกรณ์ชนิด A

SFF	Hardware Fault Tolerance		
TYPE A	0	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

ตารางที่ 2.12 ตารางจำนวนอุปกรณ์ต่ำที่สุดที่สามารถผิดพลาดได้ของอุปกรณ์ชนิด B

SFF	Hardware Fault Tolerance		
TYPE B	0	1	2
< 60 %	Not Allowed	SIL 1	SIL 3
60 % < 90 %	SIL 1	SIL 2	SIL 3
90 % < 99 %	SIL2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

2.4.5 ออกแบบหน่วยย่อยอุปกรณ์วัดในฟังก์ชันวัดคุมนิรภัย

อุปกรณ์ในฟังก์ชันวัดคุมนิรภัยในโครงงานนี้จะมีการวัดทั้งหมด 3 ประเภท คือ ความดัน อัตราการไหล และระดับ โดยจะอธิบายรายละเอียดได้ดังนี้

2.4.5.1 การวัดความดันในระบบวัดคุมนิรภัยด้วยทรานสมิตเตอร์ความดัน

การวัดความดันด้วยทรานสมิตเตอร์ความดันนั้น มีเซนเซอร์ที่ใช้กันอยู่หลายรูปแบบ ได้แก่ เซนเซอร์แบบเกจความเครียด (Strain Gauge) เซนเซอร์ชนิดเปียโซรีซิสทีฟ (Piezoresistive) และเซนเซอร์ชนิดค่าความจุไฟฟ้า (Capacitance Sensor) เป็นต้น แต่ในปัจจุบันเซนเซอร์ที่ถูกใช้งานอยู่ในทรานสมิตเตอร์ความดันมากที่สุดคือชนิดค่าความจุไฟฟ้า เนื่องจากมีค่าความถูกต้องที่ดี เป็นเชิงเส้น และมีเสถียรภาพที่ดีในระยะยาว โดยจะใช้หลักการของการเปลี่ยนแปลงความจุทางไฟฟ้า ซึ่งเกิดจากความดันที่แตกต่างของกระบวนการที่วัดและความดันบรรยากาศทำให้เกิดความเปลี่ยนแปลงของค่าความจุภายในทรานสดิวเซอร์ ค่าความจุที่แตกต่างนั้นจะถูกเปลี่ยนเป็นแรงดันไฟฟ้าและกระแสไฟ 4 ถึง 20 มิลลิแอมป์ จากวงจรในทรานสมิตเตอร์ ความสัมพันธ์ของทรานสมิตเตอร์ความดันชนิดความจุแสดงได้โดยสมการที่ (2.30) ซึ่งหากนำค่าความดันไฟฟ้าเข้ามาพิจารณาจะมีความสัมพันธ์ได้ดังสมการที่ (2.31) การทำงานแสดงได้ในรูปที่ 2.26 จะเห็นว่าความดันที่เข้ามาทั้งสองข้างของทรานดิวเซอร์มีการเปลี่ยนแปลงของแผ่นเพลท ซึ่งเป็นแผ่นเซรามิก และทำให้เกิดการเปลี่ยนแปลงของระยะห่างของแผ่นเพลททั้งสอง เกิดเป็นค่าที่แตกต่างของความจุไฟฟ้า โดยการเชื่อมต่อของทรานสมิตเตอร์ความดันชนิดความจุไฟฟ้านั้นสามารถใช้ได้ทั้งการวัดความดันเกจและ

ความดันแตกต่าง ในการวัดความดันเกจด้านความดันสูงจะต่อท่อความดันมาจากกระบวนการส่วนในด้านความดันต่ำจะถูกเชื่อมต่อกับความดันบรรยากาศ การใช้งานทรานสมิตเตอร์ความดันแสดงได้ดังรูปที่ 2.27 จากรูประบบวัดคุมนิรภัยจะเป็นการใช้งานที่คล้ายกับทรานสมิตเตอร์ความดันในระบบควบคุมปกติ แต่จะพิจารณาเพียงจุดเดียวในย่านการวัดเพื่อเป็นการป้องกันกระบวนการที่มีค่าสูงหรือต่ำกว่าย่านการควบคุม การวัดความดันในกระบวนการจะใช้ท่อส่งแรงดันต่อกับจุดที่ต้องการวัดผ่านบล็อกวาล์วและวาล์วมานิโฟลด์

$$C = \frac{\varepsilon A}{d} \tag{2.30}$$

เมื่อ C คือ ค่าความจุไฟฟ้า (ฟารัด)

ε คือ ค่าไดอิเล็กตริกของตัวกลาง (ฟารัด)

A คือ พื้นที่ของแผ่นเพลททั้งสอง (เมตร)

d คือ ระยะห่างของแผ่นเพลททั้งสอง (เมตร)

$$\Delta e = \frac{e_S K_1}{d}(P_H - P_L) = K(P_H - P_L) \tag{2.31}$$

เมื่อ Δe คือ ผลต่างของแรงดันไฟฟ้า (โวลต์)

K_1 คือ ค่าคงที่ความสัมพันธ์ของแผ่นความจุไฟฟ้าและแรงดัน

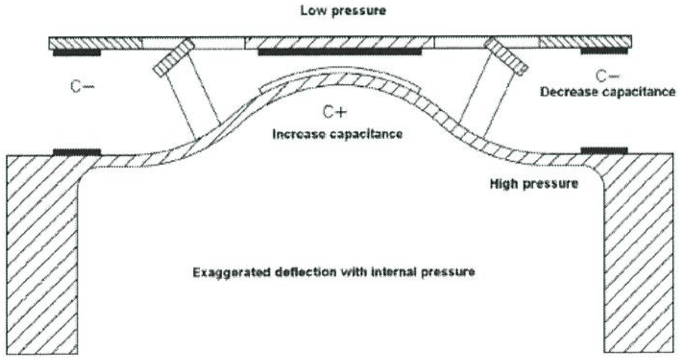
K คือ ค่าคงที่ของทรานดิวเซอร์ความจุไฟฟ้า

d คือ ระยะห่างของแผ่นเพลททั้งสอง (เมตร)

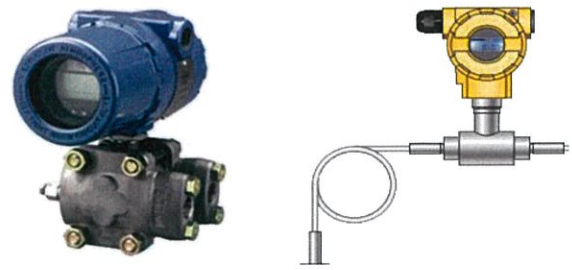
P_H คือ ความดันด้านสูงหรือความดันจากกระบวนการ

P_L คือ ความดันด้านต่ำหรือความดันจากบรรยากาศ (14.7 psia)

e_S คือ แรงดันไฟฟ้าจากแหล่งจ่าย (โวลต์)



รูปที่ 2.26 ทรานสดิวเซอร์ความดันโดยหลักการเปลี่ยนแปลงความจุไฟฟ้า



รูปที่ 2.27 ทรานสมิตเตอร์ความดันแบบค่าความจุและรูปแบบการเชื่อมต่อ

2.4.5.2 การวัดอัตราไหลในระบบนิรภัยด้วยทรานสมิตเตอร์ความดันแตกต่าง

การวัดอัตราการไหลโดยใช้ทรานสมิตเตอร์ความดันแตกต่าง ในโครงงานนี้จะใช้อุปกรณ์เดียวกับทรานสมิตเตอร์วัดความดัน ซึ่งเป็นเซนเซอร์แบบค่าความจุไฟฟ้าโดยการวัดจะแตกต่างจากการวัดความดันเกจโดยมีการต่อวัดความดันสูงและความดันต่ำทั้งสองฝั่ง การวัดอัตราการไหลแบบความดันแตกต่างนั้นจะใช้อุปกรณ์ในการสร้างความดันแตกต่าง คือ แผ่นออริฟิส (Orifice Plate) ที่ถูกติดตั้งอยู่ในท่อของกระบวนการ โดยแผ่นออริฟิสมีหลักการการวัดแบบมิเตอร์ความสูงเปลี่ยนแปลง (Variable Head Meters) แสดงได้ดังรูปที่ 2.28 โดยที่รูของแผ่นออริฟิสจะมีขนาดที่เล็กกว่าท่อ เมื่อของไหลไหลผ่านจะทำให้เกิดความแตกต่างของความดันขาเข้า (Upstream) และขาออก (Downstream) จากแผ่น ออริฟิสโดยความดันแตกต่างที่เกิดขึ้นจะมีความสัมพันธ์กับอัตราการไหล จากรูปแสดงความสัมพันธ์ด้วยสมการของแบร์นูลลี (Bernoulli Equation) จะได้ดังสมการที่ (2.32) เนื่องจากเป็นการไหลแบบ อุดมคติมีท่อในระนาบเดียวกันจะได้ค่าความสูงขาเข้าและขาออกเท่ากันแสดงได้ดังสมการที่ (2.33) จากสมการการไหลอย่างต่อเนื่อง (Continuity Equation) จะได้อัตราการไหลที่พื้นที่หน้าตัดใด ๆ แสดงดังสมการที่ (2.34) นำสมการที่ (2.34) แทนลงในสมการที่ (2.33) เพื่อหาความสัมพันธ์ของความเร็วขาออกของการไหล (v_2) แสดงดังสมการที่ (2.35) การคำนวณอัตราการไหลในอุดมคติแสดงได้ดังสมการที่ (2.36)

ในทางปฏิบัติอัตราการไหลนั้นจะน้อยกว่าในสมการ เนื่องจากการสูญเสียในการไหลจากความเสียดทาน ชนิดของการไหล รูปแบบของอุปกรณ์ และการเคลื่อนที่ไหลวน ซึ่งจะเรียกค่าตัวแปรนี้ว่า สัมประสิทธิ์การปล่อย (C_d : Coefficient of Discharge) แสดงได้ดังสมการ (2.34) และอัตราการไหลในทางปฏิบัติจากค่าคงที่และความดันแตกต่างจะแสดงได้ดังสมการที่ (2.35) การติดตั้งเครื่องมือวัดความดันแตกต่างแสดงได้ดังรูปที่ 2.29 จากรูปความดันแตกต่างของแผ่นออริฟิสจะถูกนำออกจากกระบวนการไปโดยท่อส่งความดัน ไปที่ทรานสดิวเซอร์ค่าความจุไฟฟ้าเพื่อพิจารณาเป็นสัญญาณกระแสไฟฟ้า 4 ถึง 20 มิลลิแอมป์ ในทรานสมิตเตอร์

$$\rho g h_1 + \frac{1}{2}\rho v_1^2 + P_1 = \rho g h_2 + \frac{1}{2}\rho v_2^2 + P_2 \qquad (2.32)$$

$$P_1 - P_2 = \frac{1}{2}\rho(v_2^2 - v_1^2) \qquad (2.33)$$

เมื่อ P_1 คือ ความดันขาเข้าของการไหล (ปาสคาล)

P_2 คือ ความดันขาออกของการไหล (ปาสคาล)

ρ คือ ค่าความหนาแน่นของของไหล (กรัมต่อลูกบาศก์เมตร)
v_1 คือ ค่าความเร็วในการไหลขาเข้า (เมตรต่อวินาที)
v_2 คือ ค่าความเร็วในการไหลขาออก (เมตรต่อวินาที)

$$Q = A_1 v_1 = A_2 v_2 \tag{2.34}$$

เมื่อ Q คือ อัตราการไหล
A_1 คือ พื้นที่หน้าตัดของท่อ (ตารางเมตร)
A_2 คือ พื้นที่หน้าตัดของแผ่นออริฟิส (ตารางเมตร)

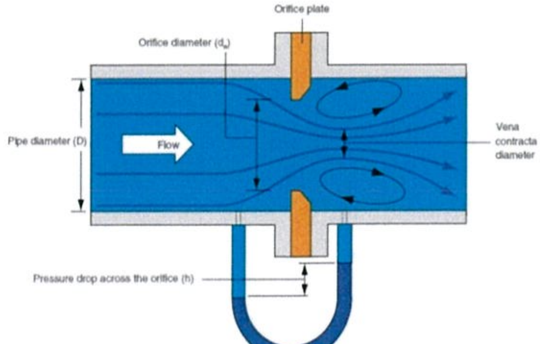
$$v_2 = \sqrt{\frac{2(P_1-P_2)}{\rho\left(1-\frac{d}{D}\right)^4}} \tag{2.35}$$

$$Q_{theory} = A_2 v_2 = \frac{\pi d^2}{4}\sqrt{2}\frac{1}{\sqrt{1-\left(\frac{d}{D}\right)^4}}\sqrt{\frac{\Delta P}{\rho}} \tag{2.36}$$

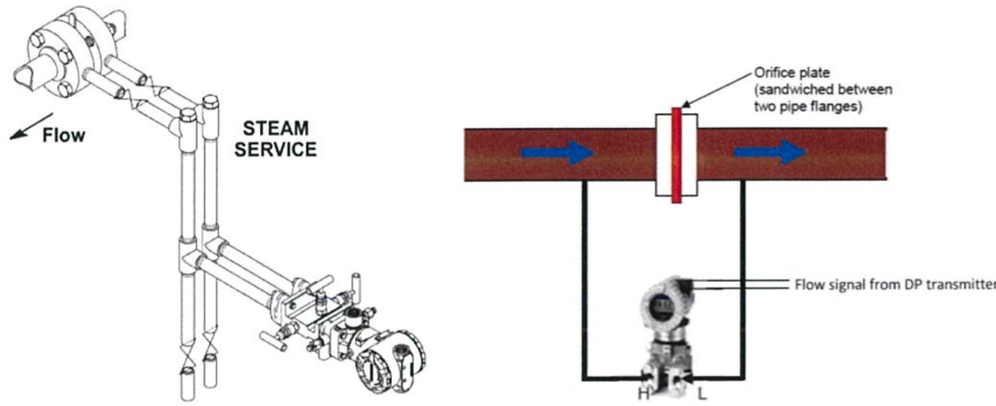
$$C_d = \frac{Q_{actual}}{Q_{theory}} \tag{2.37}$$

$$Q_{actual} = C_d\ \frac{\pi d^2}{4}\sqrt{2}\frac{1}{\sqrt{1-\left(\frac{d}{D}\right)^4}}\sqrt{\frac{\Delta P}{\rho}} = K\sqrt{\Delta P} \tag{2.38}$$

เมื่อ Q_{actual} คือ อัตราการไหลในทางปฏิบัติ
Q_{theory} คือ อัตราการไหลในทางทฤษฎี
C_d คือ สัมประสิทธิ์การปล่อย
d คือ เส้นผ่านศูนย์กลางของแผ่นออริฟิส (เมตร)
D คือ เส้นผ่านศูนย์กลางของท่อ (เมตร)
K คือ ค่าคงที่ของสมการ
ΔP คือ ความดันแตกต่าง (ปาสคาล)



รูปที่ 2.28 รูปบบของมิเตอร์ความสูงเปลี่ยนแปลง



รูปที่ 2.29 การเชื่อมต่อการวัดของทรานสมิตเตอร์ความดันแตกต่าง

2.4.5.3 การวัดระดับในระบบนิรภัยด้วยดิสเพลสเซอร์

การวัดระดับโดยใช้ดิสเพลสเซอร์ (Displacer) นั้นใช้ทฤษฎีการแทนที่ของวัตถุด้วยของเหลวโดยอาศัยหลักการของอาร์คิมิดิสที่กล่าวไว้ว่า หากวัตถุหนึ่งถูกจมลงไปในของเหลวทั้งหมดหรือบางส่วนจะทำให้เกิดแรงพยุงแรงหนึ่งกระทำบนวัตถุจากของเหลวที่ถูกแทนที่ แรงพยุงหรือแรงลอยตัว (Buoyancy) จะมีการเปลี่ยนแปลงตามวัตถุซึ่งเป็นทรงกระบอกจุ่มลงในของเหลวทำให้สามารถทราบค่าของระดับของของเหลวนั้นได้ วัสดุทรงกระบอกนี้มีชื่อทางเทคนิคเรียกว่า “ดิสเพลสเซอร์” ภายในอุปกรณ์วัดจะมีการแขวนดิสเพลสเซอร์ไว้ที่ตาชั่งน้ำหนัก เมื่อดิสเพลสเซอร์จมลงอยู่ในของเหลว น้ำหนักที่ถูกชั่งก็จะมีค่าลดลงจากแรงพยุงขึ้นของของเหลวซึ่งเขียนเป็นสมการหลักการของดิสเพลสเซอร์ได้ดังสมการที่ (2.39) จากรูปที่ 2.30 เมื่อมีการเปลี่ยนแปลงระดับของเหลวแรงพยุงจะมีผลต่อสปริงที่ทำหน้าที่เป็นแรงดึง โดยสปริงนั้นติดอยู่กับแท่งเหล็กซึ่งจะขยับขึ้นลงในแนวดิ่งและเหนี่ยวนำให้ค่าความดันของ LVDT (Linear Variable Differential Transformer) เปลี่ยนแปลง ผลคือความดันนั้นจะส่งไปเปลี่ยนเป็นกระแส 4 ถึง 20 มิลลิแอมป์ ผ่านทางวงจรอิเล็กทรอนิกส์เพื่อส่งค่าของระดับในแก่ระบบควบคุม

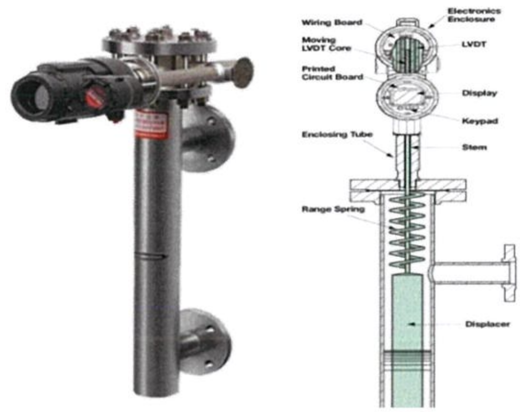
การวัดระดับของดิสเพลสเซอร์ในฟังก์ชันวัดคุมนิรภัยนั้น ถูกใช้งานอย่างแพร่หลายโดยจะติดตั้งควบคู่กับการวัดระดับของระบบควบคุมพื้นฐานมีอยู่ 2 รูปแบบ ได้แก่ การติดตั้งกับการวัดระดับควบคุมที่มีย่านการวัดเท่ากัน และการติดตั้งกับการวัดระดับควบคุมที่มีย่านการวัดไม่เท่ากัน การใช้งานทั้งสองแบบแสดงได้ดังรูปที่ 2.31 โดยทั้งสองแบบมีความแตกต่างกันในเรื่องของความต้องการของระบบนิรภัย หากต้องการความละเอียดของการวัดระดับและต้องการเปรียบเทียบกันระหว่างฟังก์ชันวัดคุมนิรภัยและระบบควบคุมจะต้องใช้ในรูปแบบดังรูปที่ 2.31 (ก) แต่หากต้องการใช้งานไม่ต้องการการเปรียบเทียบ และใช้งานเพื่อยับยั้งเหตุการณ์อันตรายที่อาจจะเกิดขึ้นเท่านั้น ควรจะใช้งานการติดตั้งดังรูปที่ 2.31 (ข)

$$F = W - w \tag{2.39}$$

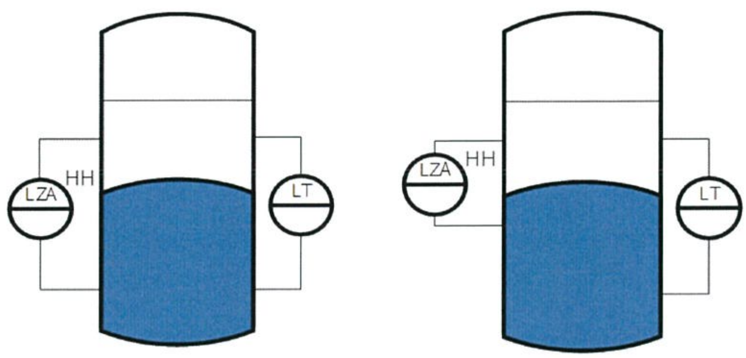
เมื่อ F คือ แรงพยุง (นิวตัน)

W คือ น้ำหนักของดิสเพลสเซอร์ที่ชั่งในอากาศ (กิโลกรัม)

w คือ น้ำหนักของดิสเพลสเซอร์ที่ชั่งในของเหลว (กิโลกรัม)



รูปที่ 2.30 เครื่องมือวัดระดับชนิดดิสเพลสเซอร์



(ก) (ข)

รูปที่ 2.31 การต่ออุปกรณ์วัดระดับในกระบวนการ
(ก) แบบย่านเท่ากัน (ข) และการต่อแบบย่านไม่เท่ากัน

2.4.5.4 ความผิดพลาดในทรานสมิตเตอร์

ค่าความผิดพลาดในทรานสมิตเตอร์นั้นมีทั้งอัตราความปลอดภัยจากความผิดพลาดและอัตราความอันตรายจากความผิดพลาด ตามมาตรฐาน NAMUR NE 43 กล่าวถึงการใช้งานอุปกรณ์ทรานสมิตเตอร์นอกย่านการใช้งานโดยที่ปกติแล้วทรานสมิตเตอร์จะส่งสัญญาณอยู่ที่ 4 ถึง 20 มิลลิแอมป์ แต่ในความเป็นจริงแล้วภายในทรานสมิตเตอร์มีการออกแบบให้อยู่ที่ 3.6 มิลลิแอมป์ และ 21.6 มิลลิแอมป์ เมื่อ ทรานสมิตเตอร์มีปัญหาจะถูกส่งไปนอกย่านด้านใดด้านหนึ่งซึ่งเรียกว่า ย่านเสียหาย (Scale Burnout) ซึ่งสามารถแบ่งสาเหตุการเสียหายได้เป็นดังนี้

1) ทรานสมิตเตอร์อ่านค่าเกินย่านการวัด (Over Range) ความผิดพลาดในการออกนอกย่านการวัดจะถูกแบ่งตามการผ่านจุดที่กระบวนการจะต้องการหยุด ได้แก่
   1.1) ค่าที่ออกนอกย่านของทรานสมิตเตอร์ "ผ่าน" จุดหยุดกระบวนการก่อนจะออกนอกย่านการวัด จะเป็นอัตราความปลอดภัยจากความผิดพลาดเพราะกระบวนการสามารถหยุดได้
   1.2) ค่าที่ออกนอกย่านของทรานสมิตเตอร์ "ไม่ผ่าน" จุดหยุดกระบวนการก่อนจะออกนอกย่านการวัด จะเป็นอัตราความ

อันตรายจากความผิดพลาด เพราะกระบวนการไม่สามารถหยุดได้แต่จะรู้เพียงว่าอุปกรณ์นั้นเสียหาย

2) ทรานสมิตเตอร์อ่านค่าในย่านการวัด (Under Range)

2.1) หากทรานสมิตเตอร์มีค่าเปลี่ยนแปลงไป แต่ยังอยู่ในย่านการวัด จะไม่ถือว่าเป็นความผิดพลาดใด ๆ เนื่องจากเกิดจากสัญญาณรบกวน (Noise)

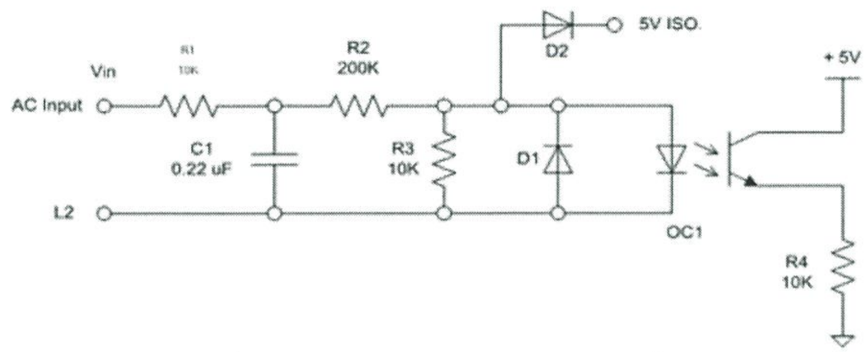
2.2) หากทรานสมิตเตอร์มีค่าที่ไม่เปลี่ยนแปลง (Freeze) หรือเกิดการเลื่อนของสัญญาณ (Signal Drift) จะถือว่าเป็นอัตราความอันตรายจากความผิดพลาดที่ไม่สามารถตรวจพบ เนื่องจากกระบวนการไม่สามารถรับรู้ถึงสัญญาณที่อันตรายได้ และไม่สามารถรู้ถึงการเสียหายของอุปกรณ์ได้

2.4.6 ออกแบบหน่วยประมวลผลในฟังก์ชันนิรภัย

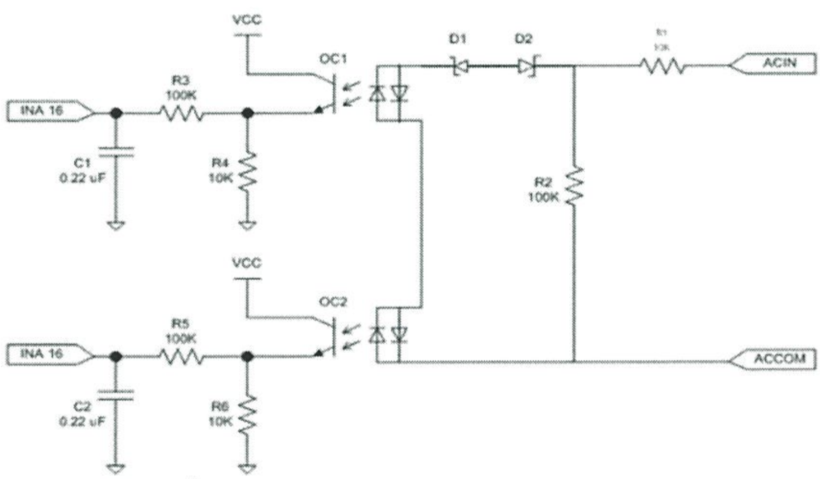
หน่วยประมวลผลในฟังก์ชันวัดคุมนิรภัยใช้ระบบพีแอลซี (PLC : Programmable Logic Controller) ซึ่งเป็นระบบในการอ่านค่า คำนวณตัวแปรทางตรรกศาสตร์ และทำการออกคำสั่งเป็นดิจิตอล (0 และ 1) โดยการใช้งานปกตินั้นจะใช้เป็นพีแอลซีทั่วไปและในงานนิรภัยจะใช้ระบบพีแอลซีนิรภัย โดยพีแอลซีนิรภัยนั้นให้ความสำคัญกับระบบวินิจฉัยภายใน (Internal Diagnostic) และอุปกรณ์ฮาร์ดแวร์ที่มีการสำรองอยู่ภายในการทำงาน เมื่อเกิดความผิดพลาดจะสามารถเปลี่ยนไปใช้งานอุปกรณ์อีกตัวได้ทันที เช่น การสำรองของแหล่งจ่ายไฟ (Power Supply Redundancy) การสำรองของอุปกรณ์ควบคุม (Controller Redundancy) เป็นต้น พีแอลซีทั่วไปและพีแอลซีนิรภัยมีความแตกต่างกันของวงจรภายใน วงจรอิเล็กทรอนิกส์ของพีแอลซีทั่วไปแสดงได้ดังรูปที่ 2.32 จะแสดงถึงวงจรของพีแอลซีทั่วไปที่โมดูลอินพุท การกรองและแบ่งแรงดันที่ไดโอด D1 และ D2 จะจำกัดแรงดันที่ไปยังวงจรเชื่อมต่อทางแสง (Opto-isolate) ก่อนที่ไมโครคอมพิวเตอร์จะอ่านสัญญาณแรงดันตกคร่อมตัวต้านทาน R4 มีค่า 5 โวลต์ หากแรงดันอินพุทต่ำกว่า 0 โวลต์จะทำให้วงจรเชื่อมต่อทางแสงไม่นำกระแส ทำให้แรงดันที่ R4 มีค่าเป็น 0 โวลต์

ในส่วนของพีแอลซีนิรภัย จะมีวงจรที่ออกแบบมาสำหรับระบบวินิจฉัยความผิดพลาด (Diagnostic System) ซึ่งจะให้ความเชื่อมั่นในการทำงานสูง วงจรจะถูกใช้การเชื่อมต่อทางแสงจำนวน 2 ชุด ระบบจะทำการอ่านค่าผ่านอุปกรณ์ทั้งสองในสภาวะปกติค่าที่อ่านได้จะเหมือนกันทั้งสองชุด เพื่อเป็นการป้องกันหากอุปกรณ์ตัวใดตัวหนึ่งเสียหาย แสดงการเชื่อมต่อได้ดังรูปที่ 2.33 ในการเชื่อมต่อของพีแอลซีนิรภัยกับอุปกรณ์อินพุตและเอาท์พุต สัญญาณจะถูกส่งข้อมูลมาจากอินพุตคือทรานสมิตเตอร์ส่งสัญญาณ 4 ถึง 20 มิลลิแอมป์ มาที่อนาล็อกอินพุตโมดูลหรือพร็อกซิมิตี้สวิตช์ที่จะส่งสัญญาณแบบ 24 โวลต์ มาที่ดิจิตอลอินพุตโมดูลและจะถูกประมวลผลในโปรเซสเซอร์หลักเพื่อทำการสั่งการ (Execute) ไปที่ดิจิตอลเอาท์พุตโมดูลให้แก่อุปกรณ์ควบคุมสุดท้ายเพื่อป้องกันอันตรายในระบบพีแอลซีนิรภัยแสดงดังรูปที่ 2.34 จากรูปการออกแบบพีแอลซีนิรภัยในระบบนิรภัยจะต้องพิจารณาความผิดพลาดในอุปกรณ์ต่าง ๆ ของหน่วยประมวลผลตั้งแต่อินพุตเทอร์มินอลถึงเอาท์พุตเทอร์มินอลพอร์ท (ETP : External Terminal Port) โดยปกติแล้วพีแอลซีนิรภัยนั้นจะมีค่าอัตราส่วนความผิดพลาดนิรภัยอยู่ในอัตราที่ค่อนข้างสูงและมากกว่า 95 เปอร์เซ็นต์ เสมอ แม้ความผิดพลาดของระบบพีแอลซีนิรภัยจะมีค่าน้อยมาก แต่ก็จะต้องถูกนำมาพิจารณาในการคำนวณด้วยเช่นกัน แสดงการคำนวณอัตราความผิดพลาดได้ดังสมการที่ (2.40) ในการเลือกใช้งานพีแอลซีนิรภัยผู้ใช้จะต้อง

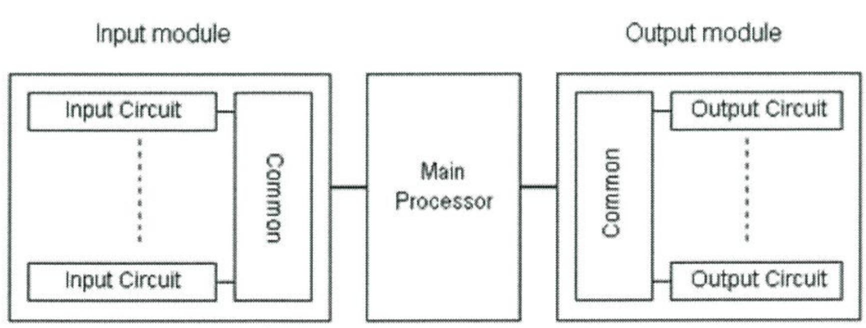
คำนึงถึงความปลอดภัยที่ต้องการและหน่วยประมวลผลที่มีใบรับรองด้านมาตรฐานนิรภัยเป็นหลัก เช่น มาตรฐาน TUV Rheinhart มาตรฐาน Exida เป็นต้น โดยระบบต้องมีระยะเวลาในการประมวลผล (Scan Time) ที่อยู่ในระยะเวลาที่เรียกว่า “ระยะเวลาความปลอดภัยของกระบวนการ” หรือ Process Safety Time ที่ผู้ใช้งานกำหนด



รูปที่ 2.32 วงจรอิเล็กทรอนิกส์ของ PLC ทั่วไป



รูปที่ 2.33 วงจรอิเล็กทรอนิกส์ของ Safety PLC



รูปที่ 2.34 การทำงานของ Safety PLC

$$\lambda_{\text{Safety PLC}} = n_{ic}\lambda_{ic} + n\lambda_{ip} + \lambda_{mp} + m_{oc}\lambda_{oc} + m\lambda_{op} \qquad (2.40)$$

เมื่อ $\lambda_{Safety\ PLC}$ คือ อัตราความผิดพลาดของพีแอลซีนิรภัยในแต่ละฟังก์ชัน

n_{ic} คือ จำนวนวงจรอินพุต (Input Channels) ในแต่ละฟังก์ชัน

λ_{ic} คือ อัตราความผิดพลาดของวงจรอินพุต

n คือ จำนวนของอินพุตโมดูล

λ_{ip} คือ อัตราความผิดพลาดของอินพุตโมดูล

λ_{mp} คือ อัตราความผิดพลาดของหน่วยประมวลผลกลาง

m_{oc} คือ จำนวนของวงจรเอาต์พุต (Output channels) ในแต่ละฟังก์ชัน

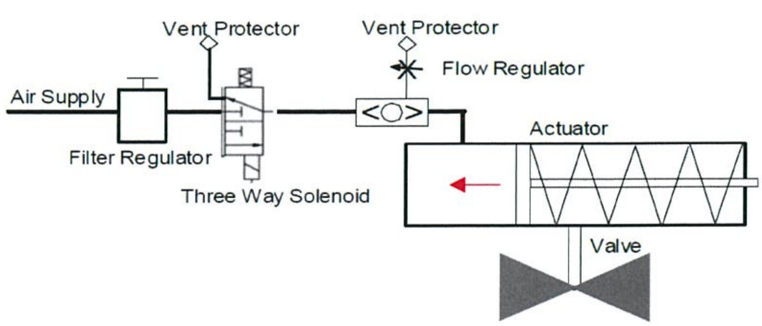
λ_{oc} คือ อัตราความผิดพลาดของวงจรเอาต์พุต

m คือ จำนวนของเอาต์พุตโมดูล

λ_{op} คือ อัตราความผิดพลาดของเอาต์พุตโมดูล

2.4.7 ออกแบบอุปกรณ์ควบคุมสุดท้ายในฟังก์ชันนิรภัย

รูปแบบของอุปกรณ์สุดท้ายในฟังก์ชันวัดคุมนิรภัยนั้นจะเป็นวาล์วเปิดปิด (On/off Valve) โดยส่งสัญญาณแรงดันไปที่โซลินอยล์วาล์วทำให้เกิดการส่งจ่ายลมไปที่หัวขับเพื่อเพิ่มแรงดันต้านกับสปริงด้านในเพื่อที่จะปิดหรือเปิดก้านวาล์ว แสดงรายละเอียดการเชื่อมต่อตามรูปที่ 2.35 ซึ่งในรูปแสดงถึงขั้นตอนในการส่งแหล่งจ่ายลมไปที่หัวขับ โดยลมจะผ่านการกรองจากชุดกรองลม (Filter Regulator) เพื่อดักจับฝุ่น ไม่ให้สิ่งสกปรกเข้าไปอุดตันตามจุดต่าง ๆ ของหัวขับวาล์ว ก่อนที่จะผ่านโซลินอยล์วาล์วแบบ 3/2 ปกติปิด (3/2 way Normally Closed) ซึ่ง จะต้องให้พลังงาน 24 โวลต์ จากหน่วยประมวลผลเพื่อเปลี่ยนการทำงานของโซลินอยล์วาล์ว เมื่อแหล่งจ่ายลมผ่านโซลินอยล์วาล์วมาแล้ว ก็จะมาพบกับชุดปรับแรงดัน (Pressure Regulator) เพื่อลดแรงดันจากแหล่งจ่ายลมไม่ให้สูงเกินไปกับอุปกรณ์ (โดยปกติแหล่งจ่ายจะมีแรงดัน 5 บาร์เกจ และหลังจากผ่านตัวปรับแรงดันจะอยู่ที่ประมาณ 3.5 บาร์เกจ) ก่อนที่จะเข้าสู่หัวขับวาล์วเพื่อที่จะขยับก้านวาล์วเพื่อเปิดวาล์ว และหากต้องการปิดวาล์วจะต้องทำการหยุดให้พลังงานแก่โซลินอยล์วาล์ว เพื่อส่งลมในหัวขับวาล์วออกไปส่วนประกอบต่าง ๆ ในการอธิบายนี้เป็นเพียงข้อมูลเบื้องต้นเท่านั้นการออกแบบกระบวนการผลิตจริงขึ้นอยู่กับแนวคิดและความปลอดภัยที่ผู้ใช้ต้องการ การเลือกใช้รูปแบบของวาล์วในระบบวัดคุมนิรภัยจะต้องเป็นวาล์วแบบเปิดปิดหรือที่เรียกกันว่า Shut Off Valve เป็นส่วนใหญ่ การเลือกใช้นั้นมีอยู่หลายชนิดขึ้นอยู่กับค่าสัมประสิทธิ์ของการไหล (C_V : Flow Coefficient) ที่ต้องการ ความดันตกคร่อมในระบบ รูปแบบวาล์วที่เหมาะสมกับกระบวนการและราคาที่พึงพอใจต่อผู้ใช้งาน การเลือกใช้งานของวาล์วจะแสดงองค์ประกอบได้ดังต่อไปนี้

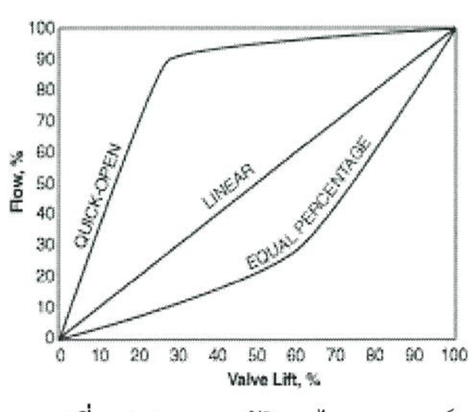


รูปที่ 2.35 องค์ประกอบของอุปกรณ์สุดท้ายในฟังก์ชันนิรภัย

2.4.7.1 คุณสมบัติการไหลของวาล์ว

คุณสมบัติการไหลของวาล์ว (Flow Characteristic) จะมีความสัมพันธ์กับกระบวนการที่ควบคุม ซึ่งจะเกิดจากการหน่วง การสูญเสียความดันในกระบวนการหรือองค์ประกอบที่วาล์วนั้นต้องการ คุณสมบัติเหล่านี้เป็นสิ่งจำเป็นที่ต้องมีความเข้าใจหากทำการเลือกติดตั้งวาล์วในกระบวนการทำงานแต่ละชนิด แสดงคุณสมบัติการเคลื่อนที่ของวาล์วต่ออัตราไหลได้ดังรูปที่ 2.36 จากรูปคุณสมบัติถูกแบ่งเป็น 3 รูปแบบ คุณสมบัติการไหล ได้แก่ คุณสมบัติเชิงเส้น คุณสมบัติเปอร์เซ็นต์เท่ากัน และคุณสมบัติเปิดอย่างรวดเร็ว

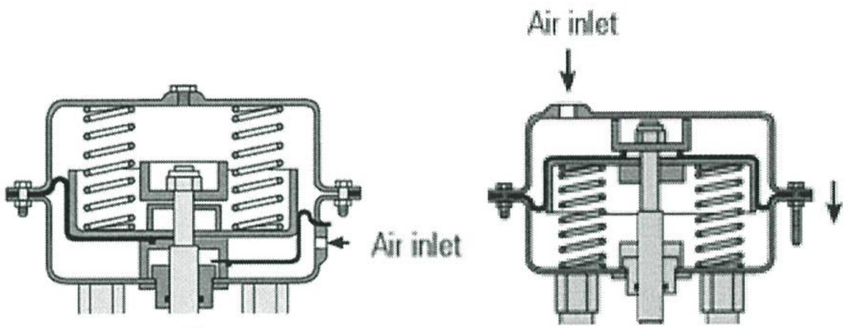
1) คุณสมบัติเชิงเส้น (Linear Characteristics) หมายถึง ความสัมพันธ์การเคลื่อนที่ของวาล์วกับอัตราการไหลที่เปลี่ยนแปลงแบบเชิงเส้น ค่าเอาท์พุตที่ส่งไปมีความเป็นเชิงเส้นกับอัตราการไหล หากต้องการให้อัตราการไหลอยู่ที่ 50 % ก็จะให้วาล์วมาเปิดอยู่ที่ 50 % เป็นต้น โดยจะเหมาะสำหรับกระบวนการที่ไม่มีความหน่วง แรงดันตกคร่อมวาล์วค่อนข้างคงที่ และการควบคุมไม่ซับซ้อน
2) คุณสมบัติเปอร์เซ็นต์เท่ากัน (Equal Percentage Characteristics) หมายถึง ความสัมพันธ์ของการเคลื่อนที่ของวาล์วกับอัตราการไหลที่เปลี่ยนแปลงแบบไม่เป็นเชิงเส้นหรือเอกซ์โพเนนเชียล เนื่องจากเกิดการหน่วงในกระบวนการ แรงดันตกคร่อมส่วนใหญ่จึงไปอยู่ที่อุปกรณ์การเปิดปิดของวาล์วในย่านต่ำนั้น จะมีความหน่วงกับอัตราการไหลสูงและในย่านสูงจะมีอัตราการไหลที่เพิ่มขึ้นอย่างรวดเร็ว เพื่อลดความหน่วงในกระบวนการโดยส่วนใหญ่ กระบวนจะใช้วาล์วแบบเอกซ์โพเนนเชียลในการควบคุม เช่น โกลบวาล์ว (Globe Valve)
3) คุณสมบัติเปิดอย่างรวดเร็ว (Quick Opening) เป็นรูปแบบวาล์วที่เมื่อเปิดขึ้นเพียงเล็กน้อย ก็จะทำให้อัตราการไหลผ่านอย่างรวดเร็วจนเกือบจะถึงอัตรการไหลสูงสุด คุณสมบัติแบบนี้จะถูกใช้ในวาล์วเปิดปิดที่ติดตั้งในระบบวัดคุมนิรภัย เพื่อความรวดเร็วในการหยุดอันตราย เช่น บอลวาล์ว (Ball Valve) บัตเตอร์ฟลายวาล์ว (Butterfly Valve)



รูปที่ 2.36 คุณสมบัติการไหลของวาล์ว

2.4.7.2 หัวขับวาล์ว

หัวขับวาล์ว (Actuator) นั้นมีการใช้งานหลายรูปแบบ เช่น จากแรงดันลม (Pneumatic) หรือไฮดรอลิก (Hydraulic) ในที่นี้จะกล่าวถึงแต่เพียงหัวขับวาล์วแบบแรงดันลมเท่านั้น หัวขับวาล์วแบบแรงดันลมเป็นอุปกรณ์ในการกำหนดการเคลื่อนที่ของวาล์วโดยใช้แหล่งจ่ายลมเพื่อมาดันกับสปริงด้านใน สามารถทำงานโดยแบ่งเป็นสองรูปแบบ ได้แก่ ปกติปิดและปกติเปิด แสดงได้ดังรูปที่ 2.37 จากรูปหัวขับวาล์วจะได้รับลมเพื่อเข้ามาขับการเคลื่อนที่ของก้านวาล์วตามลักษณะของหัววาล์ว โดยการขับหัววาล์วนั้นจะใช้แรงต้านจากแรงสปริงกับแรงดันลมผ่านไดอะแฟรมในการดึงหรือดันก้านวาล์วเพื่อเปลี่ยนแปลงการทำงานของวาล์วในกระบวนการ สิ่งสำคัญในหัวขับวาล์วที่ใช้กับฟังก์ชันวัดคุมนิรภัยคือระยะเวลาในการทำงานของหัวขับวาล์ว ซึ่งหมายถึงระยะเวลาที่วาล์วจะต้องปิดหรือเปิดให้ทันเวลาที่กำหนดก่อนที่กระบวนการจะเกิดความเสียหายจากเหตุการณ์อันตราย โดยจะมีค่าแตกต่างกันขึ้นอยู่กับการขนาดของหัวขับวาล์ว ขนาดของวาล์ว ในแต่ละกระบวนการ



รูปที่ 2.37 หัวขับวาล์วแบบปกติปิดและปกติเปิด

2.4.7.3 องค์ประกอบของวาล์วในระบบนิรภัย

คุณสมบัติของวาล์วในระบบวัดคุมนิรภัยนั้นจะเป็นวาล์วเปิดปิด แบบเปิดอย่างรวดเร็ว วาล์วเปิดปิดที่ใช้งานกันมากในระบบวัดคุมนิรภัยจะเป็นบอลวาล์วซึ่งจะมีความรวดเร็วในการเปิดและปิดเนื่องจากการหมุนของบอลในการขวางการไหลจะหมุนเพียง 90 องศา (Quarter Turn) เพื่อให้ถึง 100 เปอร์เซ็น เท่านั้น และจำเป็นต้องมีคุณสมบัติในการปิดแน่นสนิท (Tight Shut Off) ซึ่งเป็นสิ่งที่สำคัญมากในระบบวัดคุมนิรภัย วาล์วแบบอื่น เช่น โกลบวาล์ว บัตเตอร์ฟลายวาล์ว หรือวาล์วชนิดอื่นก็สามารถใช้งานกับระบบวัดคุมนิรภัยได้เช่นกัน องค์ประกอบหลักภายในของวาล์วจะแสดงได้ดังนี้

1) ตัววาล์ว (Valve Body) จะทำหน้าที่รับแรงอัดจากความดันซึ่งจะยึดติดกับท่อด้วยหน้าแปลนแบบต่าง ๆ พร้อมกับติดประเก็นในการยึดกับท่อ การเลือกชนิดของตัววาล์วเป็นส่วนสำคัญของความทนทานต่อสภาพแวดล้อมและกระบวนการ
2) ฝาครอบวาล์ว (Valve bonnet) เป็นส่วนสำคัญในการเชื่อมต่อระหว่างด้านนอกและด้านในของวาล์วที่สัมผัสกับกระบวนการ (Trim Part) บ่าวาล์วต้องมีการป้องกันการรั่วไหลของกระบวนการจากด้านใน โดยการติดตั้งประเก็นระหว่างตัววาล์วและบ่าวาล์ว

3) ทริมวาล์ว (Trim Part) เป็นชื่อที่ใช้เรียกส่วนที่สัมผัสโดยตรงกับกระบวนการของวาล์วและสามารถถอดมาซ่อมและเปลี่ยนแปลงได้

3.1) หน้าวาล์ว (Valve) เป็นส่วนที่สำคัญอีกอย่างของวาล์วโดยหน้าวาล์วจะเป็นส่วนที่บอกถึงประสิทธิภาพ และความสามารถในการปิดแน่นสนิท (Tight Shut Off) เช่น บอล เกต ดิส เป็นต้น ซึ่งขึ้นอยู่กับชนิดของวาล์ว หากเป็นแบบโกลบวาล์วจะสามารถเปลี่ยนหน้าวาล์ว (Plug) ให้เป็นแบบเชิงเส้น เอกซ์โพเนนเชียล หรือแบบเปิดอย่างรวดเร็วได้

3.2) บ่า (Seat) จุดบ่ารับหน้าวาล์วภายในวาล์ว มีหน้าที่รับหน้าวาล์วเมื่อถูกปิดลงมาเพื่อให้ไม่มีการไหลเกิดขึ้น บ่าวาล์วจะมีจำนวนมากกว่าหนึ่งก็ได้ ขึ้นอยู่กับการออกแบบและใช้งาน

3.3) ก้านวาล์ว (Stem) เป็นก้านในการขยับวาล์วตามการทำงานของหัวขับวาล์ว ซึ่งสามารถแบ่งการใช้งานได้เป็นก้านวาล์วแบบหมุน (Rotary Stem) ที่ใช้จำพวกวาล์วแบบหมุน 90 องศา แบบบอลวาล์ว และก้านวาล์วแบบสไลด์ (Sliding Stem) เป็นการขยับวาล์วแบบเกตวาล์ว

3.4) แพ็คกิ้งวาล์ว (Valve Packing) ทำหน้าที่ป้องกันการรั่วไหลจากบ่าวาล์ว มีส่วนสัมผัสโดยตรงกับกระบวนการกับก้านวาล์ว

2.4.7.4 ข้อกำหนดของวาล์วในระบบนิรภัย

วาล์วที่ถูกใช้งานในระบบวัดคุมนิรภัยจะต้องมีข้อกำหนดในการใช้งานบางประการที่จำเป็นจะต้องมี คือ การใช้วาล์วแบบเปิดอย่างรวดเร็ว การเลือกวัสดุของวาล์ว วาล์วนิรภัยจะต้องมีคุณสมบัติที่ปิดแน่นสนิท (Tight Shut Off) เพื่อป้องกันการรั่ว (Leakage) จากการปิดไม่สนิทของวาล์ว โดยคุณสมบัตินี้จะมีผลในการเลือกใช้งานวาล์วนิรภัยที่มีระดับการรั่วไหล หรือ (Leakage Class) ตามมาตรฐานสากล ANSI/FCI 70-2 : 1976 (R1982) อยู่ที่ระดับ Class V และ VI หรือภายใต้มาตรฐาน IEC 60534-4 ได้อธิบายขั้นตอนการทดสอบและผลลัพธ์ที่จะต้องได้สำหรับวาล์วที่เป็นแบบปิดแน่นสนิทไว้ดังนี้

1) สำหรับวาล์วที่มีระดับการรั่วไหล Class V จะเป็นวาล์วแบบพอร์ตเดี่ยว (Single Port) หรือพอร์ตเดียวแบบสมดุล (Balanced Single Port) จะต้องมีซีลลูกสูบ (Tight Piston Seal) และบ่าวาล์วแบบโลหะ (Metal to Metal Seat) พร้อมทั้งมีคุณสมบัติดังต่อไปนี้

1.1) ทดสอบการรั่วไหลโดยใช้น้ำขณะทดสอบที่ 100 psig หรือ ที่ความดันที่ตัววาล์วสามารถทนได้สูงสุด

1.2) อุณหภูมิของน้ำอยู่ที่ 50 – 125 องศาฟาเรนไฮน์ (10 – 52 องศาเซลเซียส)

1.3) ผลลัพธ์จะต้องมีอัตราการรั่วไหลต่ำกว่า 0.0005 มิลลิลิตรต่อนาทีของน้ำต่อระยะของเส้นผ่าศูนย์กลางต่อความดันแตกต่าง (มิลลิลิตร/นาที/นิ้ว/psi)

1.4) คุณลักษณะของวาล์ว Class V

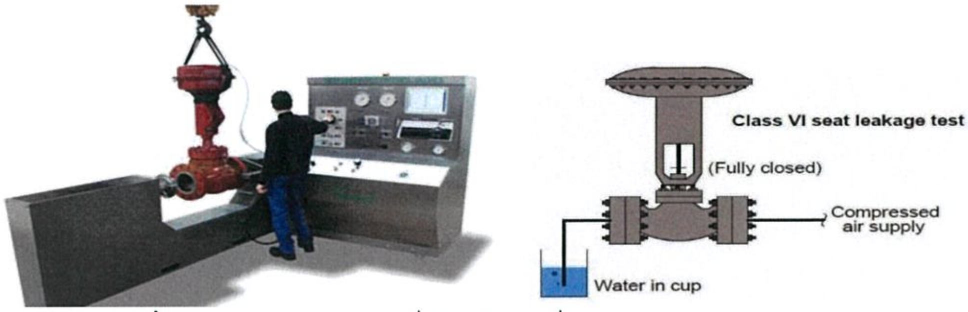
- ไม่สมดุล (Unbalanced), พอร์ตเดี่ยว, บ่าวาล์วแบบโลหะ (Lapped Metal Seat), โหลดที่บ่าวาล์วสูง (High Seat Load)
- สมดุล, พอร์ตเดี่ยว, ลูกสูบเทฟลอน (Teflon Piston Rings), บ่าวาล์วแบบอ่อน (Soft Seat) ซึ่งมีความยืดหยุ่นกว่าแบบโลหะ, โหลดที่บ่าวาล์วต่ำ (Low Seat Load)
- ไม่สมดุล, พอร์ตเดี่ยว, บ่าวาล์วแบบโลหะอ่อน (Soft Metal Seats), โหลดที่บ่าวาล์วสูง

2) สำหรับวาล์วที่มีระดับการรั่วไหล Class VI จะเป็นวาล์วแบบ บ่าวาล์วแบบอ่อน ซึ่งจะถูกสร้างโดยวัสดุประเภทเทฟลอนที่มีความยืดหยุ่นเพื่อความสนิทของการปิด พร้อมมีคุณสมบัติดังนี้
    2.1) ทดสอบการรั่วไหลโดยใช้ลมหรือไนโตรเจนที่ 50 psig หรือที่ความดันที่ตัววาล์วสามารถทนได้สูงสุด
    2.2) อุณหภูมิของน้ำอยู่ที่ 50 – 125 องศาฟาเรนไฮน์ (10 – 52 องศาเซลเซียส)
    2.3) ผลลัพธ์อัตราการรั่วไหลระดับ Leakage Class V คือต่ำกว่า 0.0005 มิลลิลิตรต่อนาทีของน้ำต่อระยะของเส้นผ่าศูนย์กลางต่อความดันแตกต่าง (มิลลิลิตร/นาที/นิ้ว/psi)
    2.4) การติดตั้งจะเป็นแบบไม่สมดุล, พอร์ตเดี่ยว, บ่าวาล์วแบบอ่อน, โหลดที่บ่าวาล์วต่ำ

2.4.7.5 การทดสอบวาล์วในรอบเวลาที่กำหนด

การทดสอบวาล์วนั้นประกอบไปด้วยการทดสอบ 2 รูปแบบ

1) การทดสอบฟังก์ชัน (Function Test) คือ การทดสอบการเปิดและปิดของวาล์วนิรภัยว่ายังสามารถทำงานได้ตามระยะเวลาที่กำหนด แต่จะไม่มีการถอดอุปกรณ์ใด ๆ ดังนั้นจึงจำเป็นต้องมีการเปิดท่อทางผ่าน (Bypass) ของกระบวนการเพื่อใช้ในการซ่อมบำรุงไว้ หากไม่มีจะใช้วิธีการยึด (Clamp) ก้านวาล์วไม่ให้ปิดลง
2) การทดสอบช่วงซ่อมบำรุง (Overhaul Test) คือ การทดสอบในช่วงที่วาล์วถูกนำออกจากกระบวนการช่วงหยุดการทำงาน เพื่อทำการเปลี่ยนอุปกรณ์ภายใน เช่น โอริง (O-ring) แพ็คกิ้ง หรือทำความสะอาดหน้าวาล์ว เป็นต้น พร้อมทั้งจะต้องทำการทดสอบการรั่วไหลตามมาตรฐาน เพื่อทดสอบการใช้งานของวาล์วว่ายังเป็นไปตามระดับการรั่วไหลเดิมของวาล์วหรือไม่ แสดงการทดสอบการรั่วไหลในรูปที่ 2.38 จากรูปจะให้ของไหลไหลผ่านจากฝั่งหนึ่งของวาล์ว มายังอีกฝั่งที่ถูกปิดอยู่ซึ่งหากมีการรั่วไหล น้ำหรืออากาศจะเข้าไปในเครื่องวัดเพื่อหาปริมาตรที่รั่วออกมาจากหน้าวาล์วที่ปิดไม่สนิท ซึ่งประเภทและค่าสัมประสิทธิ์ของวาล์วนั้น ก็จะมีผลต่ออัตราการรั่วไหลด้วยเช่นกัน



รูปที่ 2.38 การทดสอบการรั่วไหลโดยเครื่อง Valve pressure test

บทที่ 3
การดำเนินงาน

ในการคัดเลือกระดับความปลอดภัยและการพัฒนาระบบวัดคุมนิรภัย จะแบ่งการดำเนินงานเป็น 3 ส่วน ได้แก่ การศึกษาและรวบรวมข้อมูลของโครงงาน การคัดเลือกระดับความปลอดภัยให้แก่ฟังก์ชันวัดคุมนิรภัย และส่วนศึกษาการปรับปรุงระยะเวลาในการทดสอบตามสถิติความเสียหายโดยใช้หน่วยกลั่นน้ำมันดิบ CDU-3 เป็นแนวทางในการพิจารณา

3.1 การศึกษาและรวบรวมข้อมูลของโครงงาน

ศึกษาและรวบรวมข้อมูลพื้นฐานในการปฏิบัติงานก่อนที่จะเริ่มทำการวิเคราะห์ผล และทำการคัดเลือกในขั้นตอนต่าง ๆ เพื่อที่จะพิจารณาข้อมูลในวงกว้างและครอบคลุมข้อมูลที่จำเป็น

3.1.1 ศึกษาการทำงานของกระบวนการ

ในโครงงานนี้จะทำการศึกษาการทำงานและการออกแบบของระบบวัดคุมนิรภัยในหน่วยกลั่นน้ำมันดิบที่ 3 (CDU : Crude Distillation Unit) ซึ่งมีกำลังในการกลั่นประมาณ 24,200 ถึง 25,280 ตันต่อวัน หน้าที่ของหน่วยนี้คือการกลั่นน้ำมันดิบโดยใช้หอกลั่นในการแยกสารผสมของน้ำมันที่ผ่านการแยกเกลือและเพิ่มความร้อนด้วยจุดเดือดที่แตกต่างกัน โดยจะต้องทำการควบคุมอุณหภูมิและความดันให้ได้ตามที่ต้องการ ซึ่งจะได้ผลผลิตเป็น แนฟทาเบา (Light Naphtha) เคโรซีนน้ำมันแก๊สเบา (Light gas oil) น้ำมันแก๊สหนัก (Heavy gas oil) และส่วนเหลือจากภายใต้หอกลั่นหรือกากบรรยากาศ (Atmospheric Residue) เพื่อส่งต่อให้แก่กระบวนการอื่น ๆ ต่อไป

3.1.2 ศึกษาการทำงานของอุปกรณ์

เนื่องจากโครงงานนี้เป็นการตรวจสอบระดับความปลอดภัยของฟังก์ชันนิรภัย ของหน่วยกลั่นน้ำมันดิบ CDU-3 จึงต้องทำการศึกษาข้อมูลการทำงานของอุปกรณ์หลักของกระบวนการ ที่ใกล้กับจุดที่มีการติดตั้งฟังก์ชันวัดคุมนิรภัยซึ่งประกอบไปด้วย

1) หอกลั่นน้ำมันดิบ (Crude Distillation Column) คือ หอที่ใช้ในการกลั่นและแยกสารผสมในน้ำมันดิบออกจากกัน โดยการใช้จุดเดือดในการคัดแยกสารต่าง ๆ การควบคุมความดัน อุณหภูมิ และระดับน้ำในหอกลั่นจะช่วยในการทำให้การแยกสารเป็นไปตามที่ต้องการ
2) เตาเผา (Furnace) คือ เตาที่ใช้ในการให้ความร้อนแก่กระบวนการโดยจะใช้การเผาไหม้ของน้ำมันหรือก๊าซร่วมกันกับอากาศ เพื่อสร้างเปลวไฟเพิ่มอุณหภูมิให้แก่น้ำมันดิบเพื่อเข้าสู่หอกลั่น
3) เวสเซล (Vessel) คือ เป็นถังพักที่ใช้ในกระบวนการต่าง ๆ เช่น แยกของไหลชนิดที่มีการปนเฟส (Phase Separator) หรือใช้ในกระบวนการรีฟลักซ์ ของหอกลั่น เป็นต้น
4) คอมเพลสเซอร์ (Compressor) คือ อุปกรณ์ที่ทำหน้าที่ดูดก๊าซหรืออากาศโดยใช้หลักการการอัดอากาศด้วยการหมุนของใบพัดจากมอเตอร์ ทำให้มีอุณหภูมิและความดันสูงขึ้นพร้อมกับการแลกเปลี่ยนความร้อนกับไอน้ำ

5) ปั๊ม (Pump) คือ อุปกรณ์ที่ใช้ในการดูดของเหลวโดยใช้มอเตอร์ในการขับใบพัดเพื่อสร้างแรงดูด ปั๊มสามารถใช้งานได้ทั้งแก๊สและของเหลว
6) ถังเก็บผลิตภัณฑ์ (Tank) คือ ถังที่ใช้ในการเก็บน้ำมันหรือผลิตภัณฑ์ที่ผ่านกระบวนการกลั่นมาแล้วก่อนจะส่งเข้ากระบวนการอื่นหรือรอการจ่ายน้ำมัน

3.1.3 ศึกษาการใช้งานมาตรฐานวัดคุมนิรภัย

เนื่องจากโครงงานนี้เกี่ยวข้องโดยตรงกับความปลอดภัย จึงจำเป็นที่จะต้องนำมาตรฐานในระดับสากลที่ได้รับการยอมรับและใช้กันอย่างแพร่หลาย มาใช้ในการพิจารณาเพื่อให้มีความถูกต้องและใกล้เคียงมากที่สุด โดยมาตรฐานของระบบวัดคุมนิรภัยที่เลือกนำมาใช้งานจะเป็นมาตรฐาน IEC 61508 IEC 61511 และ ANSI/ISA-TR-84.00 เช่น เรื่องของระดับความปลอดภัย ข้อกำหนดในการออกแบบ วิธีการคำนวณตามรูปแบบของอุปกรณ์ เป็นต้น

3.1.4 ศึกษาสาเหตุการติดตั้งของฟังก์ชันนิรภัย

เพื่อให้ทราบถึงวัตถุประสงค์ในการติดตั้ง และศึกษาต้นเหตุของผลกระทบของการติดตั้งฟังก์ชันวัดคุมนิรภัยเพื่อป้องกันอันตราย เช่น ความดันของเชื้อเพลิงแก๊สสูงเกินระดับที่ปลอดภัยทำให้เกิดอะไรกับระบบ มีความอันตรายอย่างไร มีผลกระทบเบื้องต้นมากเพียงใด เป็นต้น โดยใช้ข้อมูลจากการวิเคราะห์อันตราย HAZOP และตารางสาเหตุและผลกระทบ (Cause & Effect Table) แสดงตัวอย่างรายละเอียดดังกล่าวได้ดังตารางที่ 3.1 และ 3.2

ตารางที่ 3.1 ตัวอย่างตารางจากการวิเคราะห์อันตราย HAZOP ความดันสูงของหอกลั่น

สาเหตุ	เหตุการณ์	ผลที่เกิดขึ้น	ความเสียหายที่อาจเกิดขึ้น
หอกลั่นมีความดันสูง	วาล์วขาออกของหอกลั่นไม่ทำงาน	เกิดความดันเกินในหอกลั่น	ผลิตภัณฑ์ไม่เป็นไปตามข้อกำหนด เนื่องจากมีน้ำมันหนักปะปนไปในน้ำมันเบาด้านบน

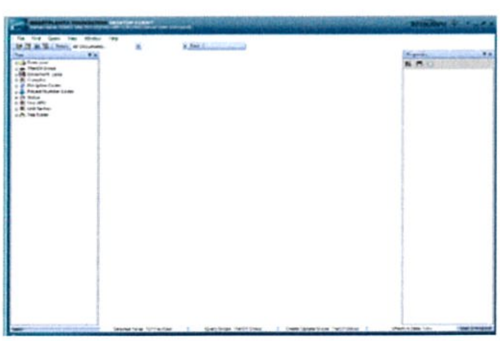
ตารางที่ 3.2 ตัวอย่างตาราง Cause & Effect ของฟังก์ชันนิรภัยป้องกันความดันสูงจากหอกลั่น

Effect / Cause		วาล์ว Off gas UZ-001		วาล์ว Fuel gas UZ-011/012	วาล์ว UZ-021/022/023/024
อุปกรณ์วัด	ค่าที่ฟังก์ชันนิรภัยทำงาน	ATM open	Heater close	Close	Close
PZA-001HH Overhead C-101 high high	2.5 barg	X	X	X	X

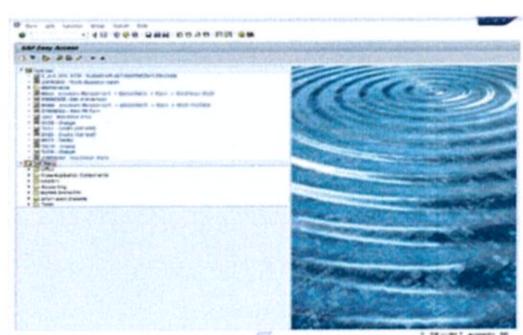
3.1.5 รวบรวมข้อมูลของฟังก์ชันวัดคุมนิรภัย

เนื่องจากต้องทำการพิจารณาระดับความปลอดภัยของฟังก์ชันวัดคุมนิรภัย ที่ถูกติดตั้งอยู่ ดังนั้นจะต้องศึกษาข้อมูลที่จำเป็นในการคำนวณและเพื่อให้ใกล้เคียงกับปัจจุบันเพื่อปรับปรุงให้เป็นข้อมูลที่ถูกต้อง เช่น รูปแบบการเชื่อมต่อของอุปกรณ์ (Configuration) ประวัติความผิดพลาด (Failure History) และระยะเวลาการทดสอบ (Test Interval) เป็นต้น โดยใช้ข้อมูลจากแผนภาพและโปรแกรมต่าง ๆ ภายในบริษัท ไทยออยล์ฯ ได้แก่

1) แผนภาพ P&ID (Piping and Instrumentation Diagram) เป็นแผนภาพที่แสดงเกี่ยวกับรายละเอียดของระบบท่อ และอุปกรณ์วัดคุมต่าง ๆ ของกระบวนการ เพื่อบอกรูปแบบการเชื่อมต่อและชื่อของอุปกรณ์ภายในระบบควบคุม
2) แผนภาพลอจิก (Logic Diagram) เป็นแผนภาพแสดงการเชื่อมต่อทางตรรกศาสตร์ของระบบ ซึ่งจะใช้ในระบบนิรภัยเพื่อเป็นการสั่งงานเปิด/ปิดการทำงานของระบบ แสดงการทำงานของฟังก์ชันวัดคุมนิรภัยในแต่ละฟังก์ชัน โดยโรงกลั่นไทยออยล์ฯ จะใช้ระบบนิรภัยแบ่งออกเป็น 2 ระบบใหญ่ ๆ คือ ระบบ Triconex และระบบ Failed Safe Controller (FSC)
3) โปรแกรม INTools ใช้ในการรวบรวมข้อมูลเกี่ยวกับอุปกรณ์ต่าง ๆ ที่มีการติดตั้งในกระบวนการ เช่น รายชื่อของอุปกรณ์ ข้อมูลการทำงานของอุปกรณ์ การเชื่อมต่อของอุปกรณ์ และการติดตั้งอุปกรณ์ เป็นต้น
4) โปรแกรม SAP (Smart Asset Plant management) เป็นโปรแกรมการบริหารงานและการสั่งซื้ออุปกรณ์ที่ใช้ในบริษัท ไทยออยล์ฯ โดยรวบรวมข้อมูลในการเข้าปฏิบัติการในโรงกลั่นของหน่วยซ่อมบำรุงตามใบสั่งงาน ที่จะแบ่งเป็นงานซ่อมบำรุงเพื่อป้องกัน (Preventive Maintenance) และซ่อมบำรุงเพื่อแก้ไข (Corrective Maintenance) ซึ่งจะนำข้อมูลมาแยกประเภทของการซ่อมบำรุงอุปกรณ์เพื่อสร้างเป็นอัตราความผิดพลาด (Failure Rate)



(ก)



(ข)

รูปที่ 3.1 หน้าต่างโปรแกรมที่ใช้งานในการพิจารณาฟังก์ชันนิรภัย

ก) โปรแกรม INTools ข) โปรแกรม SAP

3.2 การคัดเลือกระดับความปลอดภัยให้แก่ฟังก์ชันนิรภัย

3.2.1 เกณฑ์การคัดเลือกระดับความปลอดภัยให้แก่อุปกรณ์สุดท้าย

เนื่องจากปัจจุบันมีเพียงตารางการทดสอบของอุปกรณ์วัด แต่ไม่มีตารางเวลาในการซ่อมแซมอุปกรณ์สุดท้ายนั่นคือวาล์วของฟังก์ชันนิรภัยในกระบวนการผลิต การดำเนินงานเริ่มจากการคัดเลือกระดับความปลอดภัย ให้แก่วาล์วเปิดปิดในฟังก์ชันนิรภัย (UZ Valve) เพื่อสร้างตารางการซ่อมบำรุงและทดสอบของวาล์ว โดยใช้ตารางการประเมินโดยวิธีลัด (Short Cut Method) ของบริษัทไทยออยล์ฯ ที่แสดงอยู่ในตารางที่ 3.3

ตารางที่ 3.3 แสดงข้อมูลการคัดเลือกระดับความปลอดภัยโดยวิธีลัด

อุปกรณ์	คำบรรยาย	ระดับความปลอดภัย	ระยะเวลาในการดูแลรักษา
เตาเผา (Furnace)	ความร้อนขาออกของฟีตสูง เชื้อเพลิงน้ำมัน/แก๊สมีความดันต่ำ อากาศที่ใช้ในการเผาไหม้อัตราการไหลต่ำ ตรวจสอบการจุดติดของไฟเตาเผา	SIL 2	5 ปี
รีแอคเตอร์ (Reactor)	ความร้อนในรีแอคเตอร์สูง	SIL 2	5 ปี
ถัง (Tank)	ถังน้ำมันดิบ แนฟทา และเบนซินมีระดับสูง	SIL 1	2 ปี
ปั๊ม (Pump)	ป้องกันความดันต้านกลับ	SIL 2	5 ปี
ปั๊ม (Pump)/ คอมเพรสเซอร์ (Compressor)	ฟีตขาออกมีความร้อนสูง น้ำมันหล่อลื่นมีความดันต่ำ วัดการสั่นสะเทือน	SIL 1	5 ปี
ท่อส่งฟีตสู่เตาเผา (Feed coil)	ฟีตของเตาเผามีอัตราการไหลต่ำ	SIL 1	5 ปี
วาล์วไฮดรอลิก (ROV)	วาล์วทำงานโดยระบบไฮดรอลิก	SIL 1	2 ปี
สเปรย์น้ำ (Spray water)	สเปรย์น้ำเนื่องจากการตรวจจับไฟ	SIL 1	2 ปี
เวสเซล (Vessel)	ลดความดันในเวสเซลเนื่องจากความดันสูง	SIL 1	5 ปี
เตาต้มน้ำ (Boiler)	ระดับน้ำในหม้อพักไอน้ำต่ำ ไอน้ำขาออกมีอุณหภูมิสูง	SIL 2	2 ปี
เครื่องกำเนิดไฟฟ้า (Generator)	ระบบป้องกันเครื่องจักรกล	SIL 1	5 ปี

ตารางที่ 3.3 แสดงข้อมูลการคัดเลือกระดับความปลอดภัยโดยวิธีลัด (ต่อ)

อุปกรณ์	คำบรรยาย	ระดับความปลอดภัย	ระยะเวลาในการดูแลรักษา
อื่น ๆ (Other)	หอกลั่นมีระดับของเหลวสูง และอื่น ๆ	SIL 1	5 ปี
ไม่ใช่วาล์วแบบปิดแน่นสนิท (NTSOV)	ไม่ใช่ระบบป้องกันโดยใช้ Tight Shut Off Valve	-	-

3.2.2 การดึงข้อมูลจากโปรแกรม INTools

โดยจากการดึงข้อมูล ชื่ออุปกรณ์ คำบรรยาย รุ่นของอุปกรณ์ หมายเลขแผนภาพ P&ID และชื่อของแผนภาพลอจิก ในโปรแกรม INTools ลงสู่ตาราง Excel ซึ่งจะมีข้อมูลรายชื่อของอุปกรณ์ที่อาจเป็นวาล์วเปิดปิดในระบบนิรภัยอยู่จำนวน 1,631 tags แบ่งออกเป็น ระบบนิรภัยบนระบบ FSC จำนวน 1,003 tags และบนระบบ Triconex จำนวน 628 tags ซึ่งจะได้ข้อมูลแสดงได้ดังรูปที่ 3.2 จากรูปบอกถึงข้อมูลที่สำคัญต่อการคัดเลือกระดับความปลอดภัยดังต่อไปนี้

1) ชื่อของ Instrument tags: UZ valve ซึ่งจะเป็นวาล์วเปิด/ปิดในระบบนิรภัย
2) คำอธิบาย: F-2101 Fuel gas แสดงถึงการเป็นฟังก์ชันนิรภัยบนท่อส่งเชื้อเพลิงแก๊ส (Fuel gas) ไปที่เตาเผา F-2101
3) ประเภทของอุปกรณ์: On/Off valve คือ วาล์วเปิด/ปิด
4) รุ่นหรือโมเดลของอุปกรณ์: NELES 7300-71-2236XTZ1
5) ชื่อของแผนภาพ P&ID: 0000-0-00-00001
6) ตำแหน่งการติดตั้ง: FIELD แสดงถึงอุปกรณ์จะถูกติดตั้งอยู่ในกระบวนการ
7) ชื่อของแผนภาพลอจิก: TOP_CDU3_1

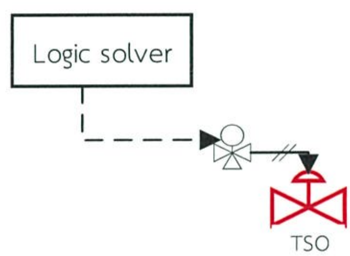
Categorize: UZ Valve
Description: F-101 FUEL GAS
Instrument type: ON/OFF VALVE
MFR/Model name: NELES 7300-71-2236XTZ1
Drawing number: 0000-0-00-00001
Located: FIELD
Logic diagram: TOP_CDU3_1

รูปที่ 3.2 ตัวอย่างข้อมูลของ Instrument tag จากในโปรแกรม INTools

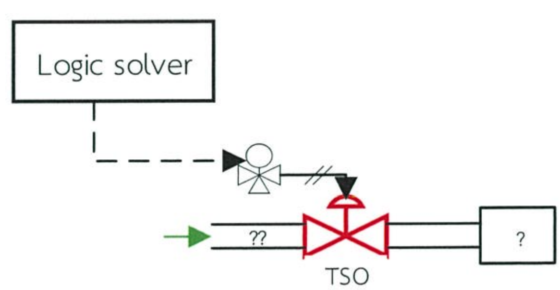
3.2.3 พิจารณาข้อมูลในแผนภาพ P&ID

หลังจากได้รับเลขแผนภาพ P&ID มาแล้ว ทำการพิจารณาการเชื่อมต่อของอุปกรณ์ในรายชื่ออุปกรณ์นั้น ๆ ว่ามีคุณสมบัติใดบ้าง ดังนี้

1) มีรูปแบบเป็นอุปกรณ์สุดท้ายของฟังก์ชันนิรภัยหรือไม่
   โดยรูปแบบการเชื่อมต่อหากเป็นฟังก์ชันนิรภัย จะเป็นการเชื่อมต่อด้วยการให้สัญญาณดิจิตอล 24 โวลต์ (เส้นประ) ไปที่โซลินอยล์วาล์วเพื่อทำงานและนำลมออกจากส่วนหัวขับวาล์วทำการปิดวาล์วแสดงได้ดังรูปที่ 3.3
2) อยู่ใกล้เคียงกับอุปกรณ์ใด
   อุปกรณ์สุดท้ายทำหน้าที่อะไร เช่น วาล์วเปิด/ปิดถูกติดตั้งอยู่บนท่อน้ำมันก่อนส่งเข้าถังเก็บเพื่อที่จะป้องกันการเกิดน้ำมันล้นถัง อุปกรณ์ที่ใช้ในระบบนิรภัยก็จะมีระดับความปลอดภัยอยู่ในประเภทถังเก็บ (Tank) เป็นต้น โดยแสดงได้ดังรูปที่ 3.4



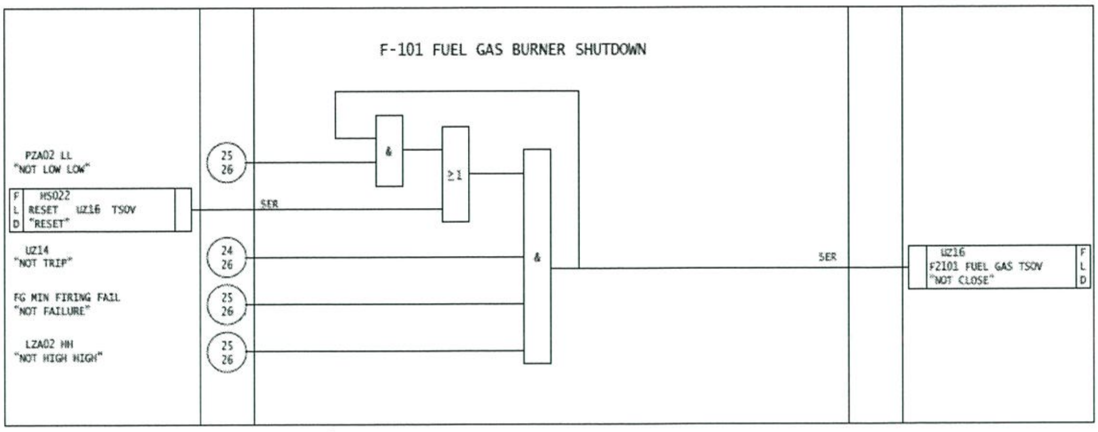
รูปที่ 3.3 การเชื่อมต่อของโซลินอยล์วาล์วและวาล์วในระบบนิรภัย



รูปที่ 3.4 การเชื่อมต่อของวาล์วในระบบนิรภัยกับกระบวนการและอุปกรณ์

3.2.4 พิจารณาข้อมูลในแผนภาพลอจิก

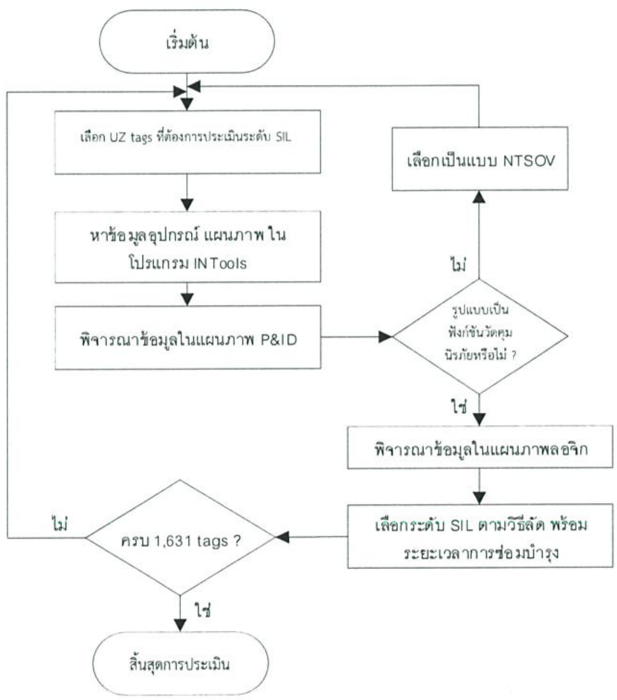
ข้อมูลภายในแผนภาพลอจิกจะอธิบายถึงการพิจารณาทางตรรกศาสตร์ ของค่าตัวแปรในกระบวนการกับค่าที่ตั้งไว้ไม่ให้เกิดอันตรายขึ้น โดยในที่นี้จะแสดงถึงสาเหตุการเกิดอันตรายที่ฟังก์ชันนิรภัยนั้นป้องกัน เช่น ความดันในท่อต่ำ ระดับของเหลวสูง เป็นต้น แสดงได้ดังรูปที่ 3.5 จากรูปจะเห็นว่าฟังก์ชันจะสั่งปิดวาล์ว UZ016 ซึ่งจะทำงานเมื่ออุปกรณ์วัดความดัน PZA02LL วัดความดันได้ต่ำกว่าค่าที่กำหนดหรือที่อุปกรณ์วัดระดับ LZA02HH วัดระดับได้สูงกว่าค่าที่กำหนด



รูปที่ 3.5 แผนภาพลอจิกแสดงถึงสาเหตุอันตราย

3.2.5 แผนภาพการไหลของการคัดเลือกระดับความปลอดภัยของวาล์วเปิด/ปิด

จากการพิจารณาการทำงานของฟังก์ชันวัดคุมนิรภัย สามารถเขียนเป็นแผนภาพการไหล (Flow Diagram) ของการคัดเลือกระดับความปลอดภัย ได้ดังรูปที่ 3.6



รูปที่ 3.6 แผนภาพการไหลของการคัดเลือกระดับ SIL

3.3 ศึกษาการปรับปรุงระยะเวลาในการทดสอบโดยใช้หน่วยกลั่น CDU-3

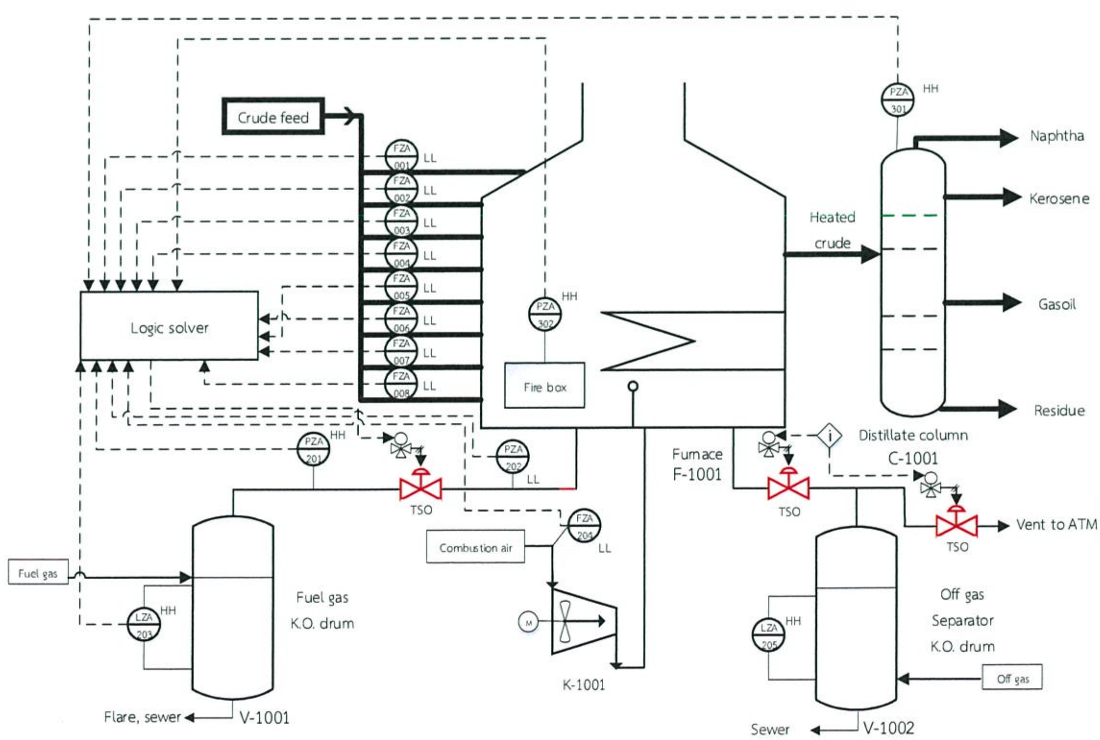
หลังจากได้ทำการคัดเลือกระดับความปลอดภัยด้วยวิธีการลัดแล้ว จะทำการศึกษาระยะเวลาในการซ่อมบำรุงและทดสอบใหม่ โดยใช้การคำนวณด้วยค่าอัตราความผิดพลาดและระดับความปลอดภัยที่ได้จากการคัดกรอง

3.3.1 การทำงานของฟังก์ชันวัดคุมนิรภัยในหน่วย CDU-3

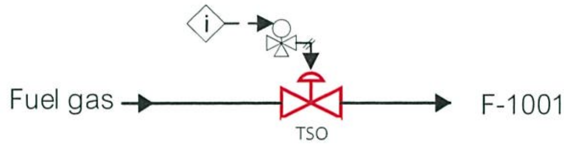
โดยการพิจารณาการทำงานจากตารางสาเหตุและผลกระทบ และการวิเคราะห์อันตราย HAZOP ในหน่วยกลั่น CDU-3 ซึ่งจะได้ตารางการทำงานแบ่งออกเป็น 3 ฟังก์ชันนิรภัยในอุปกรณ์หลัก ได้แก่ ฟังก์ชันนิรภัยในส่วนเตาเผา F-1001 หอกลั่น C-1001 และหม้อพักน้ำ V-1007 โดยจะสามารถทำการแยกพิจารณาได้ดังนี้

3.3.1.1 ฟังก์ชันนิรภัยในส่วนเตาเผา F-1001

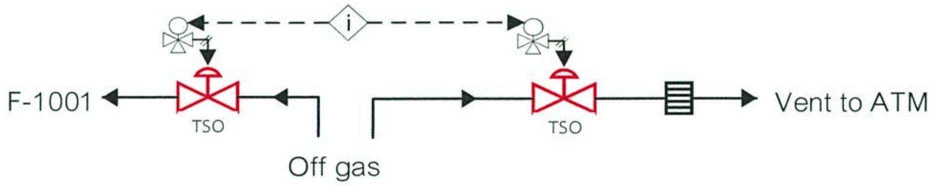
ในส่วนของเตาเผาหมายเลข F-1001 มีการพิจารณาใช้อุปกรณ์วัดอัตราการไหลของน้ำมันขาเข้าทั้ง 8 ท่อ (FZA001LL-FZA008LL) วัดระดับของเชื้อเพลิงน้ำมัน (LZA203HH) วัดความดันในท่อของเชื้อเพลิงแก๊ส (PZA201HH, PZA202LL) วัดอัตราการไหลของอากาศในการเผาไหม้ (FZA204LL) วัดระดับของแก๊สทิ้ง (LZA205HH) วัดความดันของหอกลั่น (PZA301HH) และวัดความดันของห้องเผาไหม้ (PZA302HH) ดังแสดงในรูปที่ 3.7 เพื่อป้องกันอันตรายโดยใช้อุปกรณ์ควบคุมสุดท้ายเพื่อหยุดกระบวนการในจุดต่าง ๆ เช่น การปิดท่อส่งเชื้อเพลิงแก๊ส ปิดท่อส่งแก๊สทิ้งเข้าสู่เตาเผาและเปิดท่อส่งแก๊สทิ้งเพื่อระบายออก เป็นต้น เพื่อระงับเหตุการณ์อันตรายจึงทำการพิจารณาอุปกรณ์แต่ละตัวได้ดังตารางที่ 3.4 จากข้อมูลในตารางสามารถนำไปพิจารณาข้อมูลในแต่ละอุปกรณ์โดยการสำรวจข้อมูลต่าง ๆ ได้แก่ ข้อมูลผลกระทบจากวิศวกรความมั่นคง ข้อมูลรูปแบบการเชื่อมต่อจากแผนภาพลอจิกและข้อมูลอุปกรณ์จากโปรแกรม INTools พิจารณาแยกการวิเคราะห์ออกได้เป็น 2 ส่วน ได้แก่ อุปกรณ์วัด และอุปกรณ์ควบคุมสุดท้าย แสดงการเชื่อมต่ออุปกรณ์ควบคุมสุดท้ายที่ท่อเชื้อเพลิงแก๊สและท่อส่งแก๊สทิ้งได้ดังรูปที่ 3.8 และ 3.9 ตามลำดับ และแสดงข้อมูลการทำงานของอุปกรณ์วัดและอุปกรณ์ควบคุมสุดท้ายได้ดังตารางที่ 3.5 และ 3.6 ตามลำดับ



รูปที่ 3.7 แสดงแผนภาพการเชื่อมต่อของฟังก์ชันนิรภัยในเตาเผา F-1001



รูปที่ 3.8 แสดงการเชื่อมต่อของวาล์วนิรภัยเชื้อเพลิงแก๊ส



รูปที่ 3.9 แสดงการเชื่อมต่อของวาล์วนิรภัยแก๊สทิ้ง

ตารางที่ 3.4 ข้อมูลการทำงานของอุปกรณ์วัดในฟังก์ชันนิรภัยในเตาเผา F-1001

อุปกรณ์	ลำดับ	Sensor	คำอธิบาย	ตัวแปร	ค่าของตัวแปร		หน่วย
					LL	HH	
เตาเผา F-1001	1-8	FZA-001 LL ถึง FZA-008	Crude feed coil 1-8	อัตราการไหล	887	-	ตันต่อวัน
เตาเผา F-1001	9	PZA-302 HH	Fire box	ความดัน	-	4	มิลลิบาร์เกจ
ถัง V-1002	10	LZA-205 HH	Off gas separator	ระดับ	-	50	%
ถัง V-1001	11	LZA-203 HH	Fuel gas knockout drum	ระดับ	-	50	%
	12	PZA-201 HH	Fuel gas ไป F-1001	ความดัน	-	1.8	บาร์เกจ
	13	PZA-202 LL	Fuel gas ไป F-1001	ความดัน	0.04	-	บาร์เกจ
หอกลั่น C-1001	14	PZA-301 HH	Distillate column	ความดัน	-	2.5	บาร์เกจ
คอมเพลสเซอร์ K-1001	15	FZA-204 LL	อากาศในการเผาไหม้	อัตราการไหล	940	-	ตันต่อวัน

ตารางที่ 3.5 รายระเอียดของอุปกรณ์วัดในฟังก์ชันเตาเผา F-1001

รายชื่ออุปกรณ์	คำอธิบาย	อุปกรณ์วัด	รูปแบบการเชื่อมต่อ	สาเหตุการติดตั้ง
FZA-001 ถึง 008 LL	อัตราการไหลของฟีทต่ำมากกว่า 2 ท่อ	แผ่นออริฟิส/ทรานสมิตเตอร์ความดันแตกต่าง 8 เครื่อง	2oo8	ป้องกันมิให้ท่อที่ติดตั้งอยู่ในเตาเผา เกิดการเสียหาย เนื่องจากการไม่มีของไหลวิ่งอยู่ในท่อ ทำให้เกิดความร้อนตามจุด (Hotspot) และอาจทำให้น้ำมันเกิดการรั่วไหลซึ่งเป็นสาเหตุของเพลิงไหม้ และฟังก์ชันต้องการอย่างน้อย 2 ท่อที่มีอัตราการไหลต่ำในการหยุดทำงาน
PZA-302 HH Fire Box	ห้องเผาไหม้มีความดันสูง	ท่อส่งความดัน/ทรานสมิตเตอร์วัดความดัน 1 เครื่อง	1oo1	จากการที่ห้องเผาไหม้ ไม่มีการจุดติดของไฟแต่เชื้อเพลิงยังคงถูกส่งเข้าไป ทำให้ไม่มีการเผาไหม้ หากสะสมไว้นานอาจส่งผลต่อการวาบไฟ ทำให้เตาเผาเกิดเพลิงไหม้ และอาจระเบิดได้
LZA-205 HH	ระดับน้ำในถังดักของเหลวในเชื้อเพลิงแก๊สทิ้ง V-1002 สูง	ดิสเพลสเซอร์/ทรานสมิตเตอร์วันระดับ 1 เครื่อง	1oo1	ทำให้มีของเหลวปะปนเข้าไปในห้องเผาไหม้ การที่มีของเหลวปนเข้าไปกับแก๊สทิ้งในห้องเผาไหม้ เมื่อเกิดความร้อนจะทำให้ของเหลวขยายตัว และกลายเป็นไออย่างรวดเร็ว เกิดความดันที่สูงในห้องเผาไหม้ และอาจทำให้ระเบิดพร้อมเกิดเพลิงไหม้ได้
LZA-203 HH	ระดับน้ำในถังดักของเหลวในเชื้อเพลิงแก๊ส V-1001 สูง	ดิสเพลสเซอร์/ทรานสมิตเตอร์วันระดับ 1 เครื่อง	1oo1	ทำให้มีของเหลวปะปนเข้าไปในห้องเผาไหม้ การที่มีของเหลวปนเข้าไปกับแก๊สในห้องเผาไหม้เมื่อเกิดความร้อน จะทำให้ของเหลวขยายตัว และกลายเป็นไออย่างรวดเร็ว เกิดความดันที่สูงในห้องเผาไหม้ และอาจทำให้ระเบิดพร้อมเกิดเพลิงไหม้ได้
PZA-201 HH	เชื้อเพลิงแก๊สมีความดันสูง	ท่อส่งความดัน/ทรานสมิตเตอร์วัดความดัน 1 เครื่อง	1oo1	หากความดันของแก๊สสูงเกินไป จะทำให้ไฟในห้องเผาไหม้ดับ เนื่องจากอัตราส่วนของเชื้อเพลิงในห้องเผาไหม้มีสูงเกินไป หากเชื้อเพลิงแก๊สมีสูงและอัดแน่นอยู่ในห้องเผาไหม้ ทำให้มีความเสี่ยงหากเกิดการจุดติดของประกายไฟ และทำให้เตาเผาเกิดการระเบิดหรือไฟไหม้ได้

ตารางที่ 3.5 รายระเอียดของอุปกรณ์วัดในฟังก์ชันเตาเผา F-1001 (ต่อ)

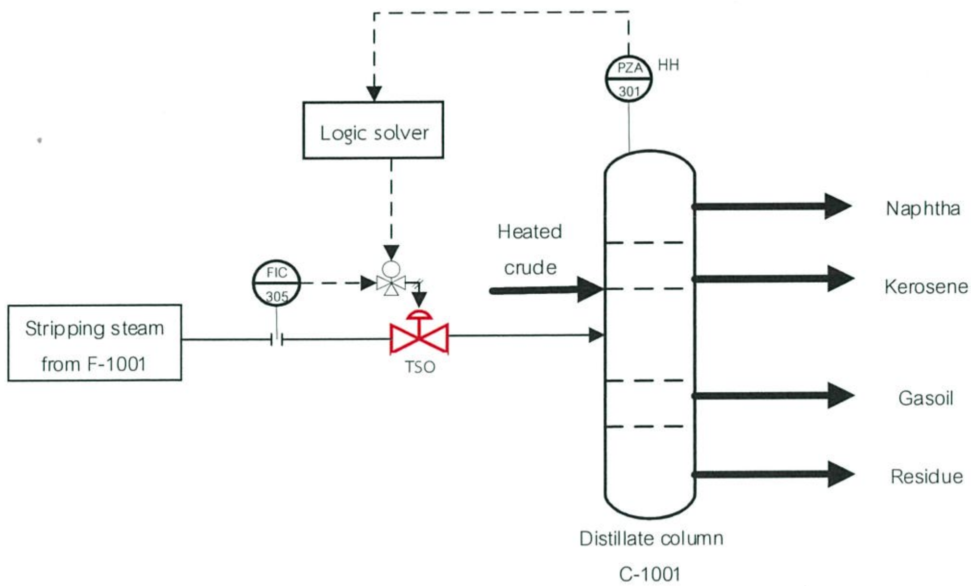
รายชื่ออุปกรณ์	คำอธิบาย	อุปกรณ์วัด	รูปแบบการเชื่อมต่อ	สาเหตุการติดตั้ง
PZA-202 LL	เชื้อเพลิงแก๊สมีความดันต่ำ	ท่อส่งความดัน/ทรานสมิตเตอร์วัดความดัน 1 เครื่อง	1oo1	หากความดันของแก๊สมีต่ำเกินไป จะทำให้ไฟในห้องเผาไหม้ค่อย ๆ ดับ และทำให้ห้องเผาไหม้เกิดความดันเกิน ทำให้มีความเสี่ยง หากเกิดจุดติดของประกายไฟ และทำให้เตาเผาเกิดการระเบิดหรือไฟไหม้ได้
PZA-301 HH	หอกลั่น C-1001 มีความดันสูง	ท่อส่งความดัน/ทรานสมิตเตอร์วัดความดัน 1 เครื่อง	1oo1	เป็นการป้องกันความดันสูง ของหอกลั่นน้ำมันดิบ C-1001 หากความดันในหอกลั่นสูงเกิน จะทำให้ผลิตภัณฑ์ที่ได้จะไม่ตรงกับความต้องการ (Off spec) และมีความเสี่ยงการเกิดความดันเกิน เกิดการรั่วไหลตามหน้าแปลน
FZA-204 LL	อากาศที่ใช้ในการเผาไหม้มีอัตราการไหลต่ำ	แผ่นออริฟิส/ทรานสมิตเตอร์ความดันแตกต่าง 8 เครื่อง	1oo1	เป็นการป้องกัน หากอัตราการไหลของอากาศในการเผาไหม้ต่ำ เนื่องจากถ้าการเผาไหม้ในห้องเผาไหม้มีอากาศน้อย จะทำให้อัตราส่วนของเชื้อเพลิง และอากาศนั้นไม่ทำให้เกิดการเผาไหม้ เกิดการเผาไหม้ที่ไม่สมบูรณ์ และไฟในเตาเผาดับเกิดความดันเกิน ในห้องเผาไหม้มีความเสี่ยง ต่อการระเบิดพร้อมกับไฟไหม้

ตารางที่ 3.6 รายระเอียดของอุปกรณ์สุดท้ายในฟังก์ชันเตาเผา F-1001

รายชื่ออุปกรณ์	คำอธิบาย	อุปกรณ์สุดท้าย	รูปแบบการเชื่อมต่อ	Class Leak
UZ-001	วาล์วนิรภัยในท่อส่งเชื้อเพลิงแก๊ส (Fuel gas)	Solenoid valve: Maxseal IC04 On/Off valve: Ball valve	1oo1	Class V (Tight Shut Off)
UZ-002, UZ-003	วาล์วนิรภัยในท่อส่งแก๊สทิ้ง (Off gas)	Solenoid valve: Maxseal IC04 On/off valve: Globe valve พอร์ตเดี่ยว	1oo1	Class V (Tight Shut Off)

3.3.1.2 ฟังก์ชันนิรภัยวาล์วในส่วนหอกลั่น C-1001

การวัดความดันใน C-1001 จะเป็นฟังก์ชันวัดคุมนิรภัยในการหยุดการส่งของไอน้ำแยกส่วน (Stripping Steam) หากมีความดันในหอกลั่นน้ำมันดิบสูงเกิน สามารถแสดงการเชื่อมต่อได้ดังรูปที่ 3.10 และการทำงานของฟังก์ชันวัดคุมนิรภัยจากตารางที่ 3.7 สามารถพิจารณาแยกการวิเคราะห์ออกเป็นได้ 2 ส่วนได้แก่ อุปกรณ์วัด และอุปกรณ์สุดท้าย ตามตารางที่ 3.8 และ 3.9 ตามลำดับและการเชื่อมต่ออุปกรณ์ควบคุมสุดท้ายแสดงได้ดังรูปที่ 3.11 ซึ่งจะเห็นว่ารูปแบบการเชื่อมต่อของวาล์วไม่ได้เป็นวาล์วเปิดปิด แต่เป็นวาล์วควบคุมโดย FIC-305 ซึ่งรูปแบบนี้เป็นฟังก์ชันนิรภัยที่มีการติดตั้งแบบเก่าซึ่งจะเพิ่มเติมเพียงแค่โซลินอยล์วาล์วเข้ามา จะติดตั้งให้กับกระบวนการที่ต้องการปลอดภัยไม่สูงมีระดับความปลอดภัย SIL เท่ากับ 1



รูปที่ 3.10 แสดงแผนภาพการเชื่อมต่อของฟังก์ชันนิรภัยในหอกลั่น C-1001

ตารางที่ 3.7 ข้อมูลการทำงานของอุปกรณ์วัดในฟังก์ชันนิรภัยในหอกลั่น C-1001

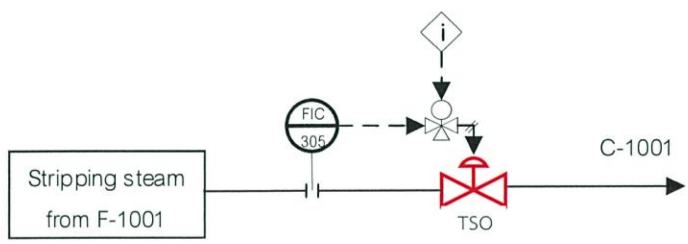
อุปกรณ์	ลำดับ	Sensor	คำอธิบาย	ตัวแปร	ค่าของตัวแปร		หน่วย
					LL	HH	
หอกลั่น C-1001	13	PZA-301 HH	Distillate Column	ความดัน	-	2.5	บาร์เกจ

ตารางที่ 3.8 รายระเอียดของอุปกรณ์วัดในฟังก์ชันหอกลั่น C-1001

รายชื่ออุปกรณ์	คำอธิบาย	อุปกรณ์วัด/ทรานสมิตเตอร์	รูปแบบการเชื่อมต่อ	สาเหตุการติดตั้ง
PZA-301 HH	หอกลั่น C-1001 มีความดันสูง	ท่อส่งความดัน/ทรานสมิตเตอร์ความดัน 1 เครื่อง	1oo1	เป็นการป้องกันความดันสูง ของหอกลั่นน้ำมันดิบ C-1001 หากความดันในหอกลั่นนั้นสูงเกิน จะทำให้ผลิตภัณฑ์ที่ได้ไม่ตรงกับความต้องการ

ตารางที่ 3.9 รายระเอียดของอุปกรณ์สุดท้ายในฟังก์ชันหอกลั่น C-1001

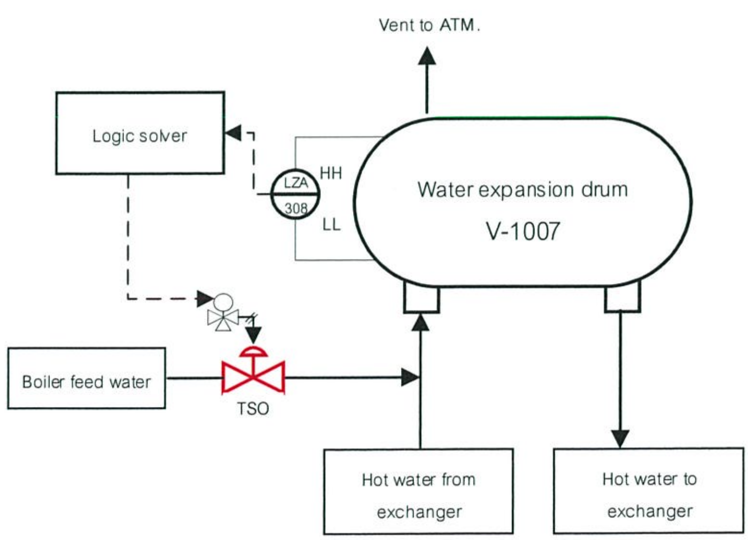
รายชื่ออุปกรณ์	คำอธิบาย	อุปกรณ์สุดท้าย	รูปแบบการเชื่อมต่อ	Class Leak
UZ-004	วาล์วนิรภัยท่อส่งไอน้ำแยกส่วน	Solenoid valve: Maxseal IC04 Control Valve: Globe valve พอร์ตเดี่ยว	1oo1	Class V (Tight shut off)



รูปที่ 3.11 แสดงการเชื่อมต่อของวาล์วนิรภัยท่อส่งไอน้ำแยกส่วน

3.3.1.3 ฟังก์ชันนิรภัยในส่วนหม้อพักน้ำ V-1007

การวัดระดับน้ำใน V-1007 ที่แสดงการเชื่อมต่อดังรูปที่ 3.12 จะเป็นฟังก์ชันวัดคุมนิรภัยในการหยุดการส่งของน้ำที่ใช้ในการต้มเป็นไอ (Boiler Feed Water) เข้าสู่ถังเวสเซลและนำไปหมุนเวียนในหน่วยกลั่น CDU-3 หากมีระดับน้ำเกินจากย่านที่กำหนดไว้ตามข้อมูลในตารางที่ 3.10 โดยสามารถแยกการวิเคราะห์ออกได้เป็น 2 ส่วน ได้แก่ อุปกรณ์วัดและอุปกรณ์สุดท้ายดังตารางที่ 3.11 และ 3.12 ตามลำดับและแสดงการเชื่อมต่ออุปกรณ์ควบคุมสุดท้ายได้ดังรูปที่ 3.13



รูปที่ 3.12 แสดงแผนภาพการเชื่อมต่อของฟังก์ชันนิรภัยในถังเวสเซล V-1007

ตารางที่ 3.10 ข้อมูลการทำงานของอุปกรณ์วัดในฟังก์ชันนิรภัยในถังเวสเซล V-1007

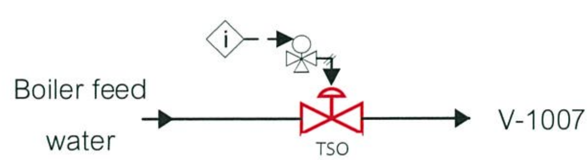
อุปกรณ์	ลำดับ	อุปกรณ์วัด	คำอธิบาย	ตัวแปร	ค่าของตัวแปร		หน่วย
					LL	HH	
ถังเวสเซล V-1007	14	LZA-308 LL และ HH	ระดับน้ำร้อน ใน V-1007	ระดับ	23%	66%	ตันต่อวัน

ตารางที่ 3.11 รายระเอียดของอุปกรณ์วัดในฟังก์ชันถังเวสเซล V-1007

รายชื่ออุปกรณ์	คำอธิบาย	อุปกรณ์วัด/ทรานสมิตเตอร์	รูปแบบการเชื่อมต่อ	สาเหตุการติดตั้ง
LZA-308 HH และ LL	ถังเวสเซล V-1007 มีระดับสูง	ดิสเพลสเซอร์/ทรานสมิตเตอร์วัดระดับ 1 เครื่อง	1oo1	เป็นการป้องกันไม่ให้ระดับน้ำร้อนในหม้อพักน้ำ V-1007 มีระดับสูงและต่ำเกินไป ซึ่งหากน้ำร้อนมีระดับต่ำเกินไปจะไม่มีน้ำในการหมุนเวียน ไปแลกเปลี่ยนความร้อนในอุปกรณ์แลกเปลี่ยนความร้อนและหากน้ำมีระดับสูงเกินไปจะทำให้ถังเกิดการอัดแน่นของมวลน้ำและทำให้รั่วไหลตามหน้าแปลนได้

ตารางที่ 3.12 รายระเอียดของอุปกรณ์สุดท้ายในฟังก์ชันถังเวสเซล V-1007

รายชื่ออุปกรณ์	คำอธิบาย	อุปกรณ์สุดท้าย	รูปแบบการเชื่อมต่อ	Class Leak
UZ-005	วาล์วนิรภัยท่อส่งน้ำร้อน	Solenoid valve: Maxseal IC04 Control Valve: Globe valve พอร์ทเดี่ยว	1oo1	Class V (Tight shut off)



รูปที่ 3.13 แสดงการเชื่อมต่อของวาล์วนิรภัยท่อส่งน้ำร้อน

3.3.2 คำนวณระยะเวลาในการทดสอบตามระดับความปลอดภัย

3.3.2.1 พิจารณาระดับความปลอดภัยใน CDU-3

จากการประเมินระดับความปลอดภัยด้วยวิธีลัดโดยการแยกประเภทของอุปกรณ์ดังแสดงในตารางที่ 3.4 ได้ระดับความปลอดภัยในฟังก์ชันวัดคุมนิรภัยในหน่วยกลั่น CDU-3 ดังตารางที่ 3.13 จากตารางพิจารณาฟังก์ชันวัดคุมนิรภัยให้ได้ระดับความปลอดภัยที่ประเมิน

ตารางที่ 3.13 ระดับความปลอดภัยจากการประเมินด้วยวิธีลัด

ฟังก์ชันวัดคุมนิรภัย	ระดับความปลอดภัยที่ต้องการ
เตาเผา F-1001	1 และ 2
หอกลั่น C-1001	1
หม้อพักน้ำ V-1007	1

3.3.2.2 ตารางระดับความปลอดภัยจากมาตรฐาน IEC 61508

เนื่องจากการทำงานของฟังก์ชันวัดคุมนิรภัยของไทยออยล์ฯ เป็นแบบความต้องการต่ำ ดังนั้นจะใช้ตารางการแบ่งระดับความปลอดภัยด้วยตารางที่ 2.2 การคำนวณระยะเวลาการทำการทดสอบจะนำค่า PFD_{avg} ที่ต่ำที่สุดในย่านระดับความปลอดภัยมาใช้ เช่น ในระดับ SIL 2 จะนำค่า 10^{-3} มาคำนวณ เป็นต้น โดยแสดง PFD_{avg} ที่ต่ำที่สุดในแต่ละย่านได้ดังตารางที่ 3.14

ตารางที่ 3.14 ค่า PFD_{avg} ที่ต่ำที่สุดในแต่ละระดับความปลอดภัย

ระดับความปลอดภัย	ค่าเฉลี่ยความเป็นไปได้ของความผิดพลาดที่ต่ำที่สุดในแต่ละย่าน (PFD_{avg})
1	10^{-2}
2	10^{-3}
3	10^{-4}
4	10^{-5}

3.3.2.3 ความเสียหายของอุปกรณ์วัดและควบคุมสุดท้ายจากข้อมูลประวัติ

จากโปรแกรม SAP จะสามารถดูข้อมูลรายละเอียดประวัติการทำงานได้ โดยจะมีการอธิบายถึงสาเหตุการเสียหายและผลกระทบของอุปกรณ์ในฟังก์ชันวัดคุมนิรภัย แบ่งเป็นงานซ่อมแซมและงานดูแลป้องกัน ซึ่งจะมีข้อความในการปิดงานเมื่อสำเร็จลุล่วง ได้แก่

1) Safeguard I/O Normal คือ ข้อความเมื่อระบบเกิดความผิดพลาด และไปตรวจสอบตามเวลาแล้วไม่เจอความผิดพลาดที่อุปกรณ์
2) Safeguard I/O Revealed Failure คือ ข้อความเมื่อระบบเกิดความผิดพลาด และไปตรวจสอบตามเวลาแล้วพบความผิดพลาดที่อุปกรณ์
3) Safeguard I/O Un-Revealed Failure คือ ข้อความเมื่อระบบไม่เกิดความผิดพลาด และไปตรวจสอบตามเวลาแล้วเจอความผิดพลาดที่อุปกรณ์

และจะทำคัดกรองเพียงแต่ข้อความ Safeguard I/O Revealed Failure และ Safeguard I/O Un-Revealed Failure เพื่อทำการพิจารณารูปแบบการเสียหายที่เป็นความผิดพลาดอันตรายที่ไม่สามารถตรวจสอบได้ เช่น สัญญาณของทรานสมิตเตอร์ค้าง วาล์วเปิดค้าง เป็นต้น โดยภายในฟังก์ชันวัดคุมนิรภัยของหน่วย CDU-3 จะมีอุปกรณ์วัดที่ติดตั้งอยู่ 3 ชนิด คือ ทรานสมิตเตอร์วัดความดัน ทรานสมิตเตอร์วัดอัตราการไหล และทรานสมิตเตอร์วัดระดับ สามารถหาอัตราความเสียหายของ

อุปกรณ์เหล่านี้ออกมาจากโปรแกรม SAP และคำนวณอัตราความอันตรายจากความผิดพลาดที่ตรวจไม่พบ (λ^{DU}) ได้โดยสมการที่ (3.1) ผลลัพธ์จากการคำนวณจะแสดงได้ดังตารางที่ 3.15

$$\lambda^{DU} = \frac{N}{T \times n} \tag{3.1}$$

เมื่อ λ^{DU} คือ อัตราความอันตรายจากความผิดพลาดที่ตรวจไม่พบ (ต่อปี)

N คือ จำนวนความผิดพลาดอันตรายที่ตรวจไม่พบของอุปกรณ์

T คือ ระยะเวลาในการพิจารณานับความเสียหาย (ปี)

n คือ จำนวนของอุปกรณ์ที่พิจารณา

ตารางที่ 3.15 อัตราความผิดพลาดจากโปรแกรม SAP ของฟังก์ชันนิรภัยทั้งหมดในโรงกลั่น

อุปกรณ์ในฟังก์ชันนิรภัย	จำนวนอุปกรณ์	จำนวนความผิดพลาดอันตรายที่ตรวจไม่พบ					λ^{DU} (ต่อปี)
		2014	2015	2016	2017	ผลรวม	
ทรานสมิตเตอร์วัดความดันชนิดความดันแตกต่าง	826	-	1	-	-	1	0.0003
ทรานสมิตเตอร์วัดอัตราการไหลชนิดความดันแตกต่าง	297	-	-	1	-	1	0.0008
ทรานสมิตเตอร์วัดระดับชนิดดิสเพลสเซอร์	213	-	-	1	-	1	0.0012
โซลินอยล์วาล์ว	2258	1	-	-	1	2	0.0002
วาล์วเปิด/ปิด	1466	-	5	1	2	8	0.0014

3.3.2.4 อัตราความเสียหายของหน่วยประมวลผล

หน่วยกลั่น CDU-3 มีการใช้งานหน่วยประมวลผลเป็นระบบ FSC และเนื่องจากเอกสารค่าความผิดพลาดนั้นไม่ได้ถูกเก็บบันทึกไว้ จึงจะใช้ข้อมูลความผิดพลาดจากโปรแกรม SIFPro โดยจะได้ค่าความผิดพลาดของ Generic SIL 3 certified Safety PLC แสดงได้ดังตารางที่ 3.16 สามารถคำนวณหาค่าอัตราส่วนความผิดพลาดนิรภัย (SFF) ได้โดยสมการที่ (2.22) จะได้ค่าอัตราส่วนความผิดพลาดนิรภัยเท่ากับ 99.61% ดังนั้นความสามารถในระบบวัดคุมนิรภัยของหน่วยประมวลผลนี้จะมีค่อนข้างสูง

ตารางที่ 3.16 ค่าความผิดพลาดของ Generic safety PLC ในโปรแกรม SIFPro

ความผิดพลาด	ค่าความผิดพลาด (ต่อปี)
ความผิดพลาดอันตราย (λ_D)	1.518×10^{-4}
ความผิดพลาดนิรภัย (λ_S)	3.873×10^{-2}

3.3.2.5 คำนวณระยะเวลาการทดสอบของอุปกรณ์ในแต่ละฟังก์ชัน

คำนวณระยะเวลาการทดสอบจากสมการค่า PFD_{avg} กับรูปแบบการเชื่อมต่อของอุปกรณ์ด้วยค่าอัตราความผิดพลาดอันตรายที่ไม่สามารถตรวจสอบได้ (λ_{DU}) แสดงตัวอย่างผลการคำนวณระยะเวลาการทดสอบฟังก์ชันวัดคุมนิรภัยของเตาเผา F-1001 ได้ดังตารางที่ 3.17

ตารางที่ 3.17 แสดงตัวแปรของอุปกรณ์ฟังก์ชันลำดับที่ 1-8 Crude feed coil อัตราการไหลต่ำ

อุปกรณ์	การเชื่อมต่อ	PFD_{avg}	λ^{DU} (ต่อปี)	λ^{C} (ต่อปี)	ระยะเวลาในการทดสอบ (ปีต่อครั้ง)
ทรานสมิตเตอร์ความดันแตกต่าง	สมการที่ (2.24) MooN (2oo8)	0.01 (SIL 1)	8.0×10^{-4}	1.6×10^{-5} (β มีค่าเท่ากับ 2%)	508.992
หน่วยประมวลผล	สมการที่ (2.21) 1oo1 voting	0.001 (SIL 2)	1.518×10^{-4}	-	13.175
อุปกรณ์สุดท้าย (โซลินอยล์วาล์วและวาล์ว)	สมการที่ (2.21) 1oo1 voting	0.001 (SIL 2)	1.6×10^{-3}	-	1.25

3.3.3 คัดเลือกระยะเวลาการทดสอบฟังก์ชันใหม่

จากตัวอย่างการคำนวณระยะเวลาการทดสอบของฟังก์ชันลำดับที่ 1-8 Crude Feed Coil มีอัตราการไหลต่ำในตารางที่ 3.17 สามารถสรุปผลออกมาเป็นระยะเวลาการทดสอบเก่าและใหม่ได้ดังตารางที่ 3.18 จากตารางแสดงระยะเวลาการทดสอบแบบเก่า ระยะเวลาจากการคำนวณ และระยะเวลาใหม่ที่ควรเปลี่ยน ในระยะเวลาการทดสอบแบบเก่าอุปกรณ์วัด หน่วยประมวลผล และอุปกรณ์ควบคุมสุดท้ายจะมีระยะเวลา 3 ปี ทุกครั้งที่มีการเปลี่ยนแปลง และ 1.5 ปี ตามลำดับ ผลจากการคำนวณแสดงให้เห็นว่าบางค่านั้นควรลดระยะในการทดสอบเพื่อให้ได้ระดับความปลอดภัยที่ต้องการ เช่น อุปกรณ์ควบคุมสุดท้ายจาก 1.5 ปี เหลือ 1 ปี เป็นต้น ซึ่งการเลือก

ระยะเวลาใหม่ตามมาตรฐานการออกแบบ (DEP : Design and Engineering Practice) ของโรงกลั่นไทยออยล์ จะกำหนดให้มีระยะเวลาทดสอบฟังก์ชันที่เกี่ยวข้องกับระบบนิรภัยได้ไม่เกิน 3 ปี ถึงแม้ว่าการคำนวณจะออกมาเกินระยะเวลานั้นก็ตาม ตารางที่ 3.19 แสดงการเลื่อนระยะเวลาการทดสอบฟังก์ชันวัดคุมนิรภัยในแต่ละระดับความปลอดภัย ที่ SIL 1 จะให้มีการเพิ่มลดระยะเวลาทีละขั้นขั้นละ 12 เดือน ส่วนที่ SIL 2 ขั้นละ 6 เดือน และจะถูกปัดขึ้นลงตามผลการคำนวณ เช่น ฟังก์ชันระดับ SIL 2 ที่มีการทดสอบ 1.5 ปี มีการคำนวณใหม่ได้ 1.30 ปี ดังนั้นระยะเวลาที่เลือกใหม่จะเป็น 1 ปี เป็นต้น

ตารางที่ 3.18 เปรียบเทียบการทดสอบฟังก์ชันเก่าและใหม่

อุปกรณ์ในฟังก์ชันนิรภัย	ระยะเวลาทดสอบแบบเก่า	ระยะเวลาทดสอบจากการคำนวณใหม่	ระยะเวลาการทดสอบที่ควรเลือกใหม่
อุปกรณ์วัด FZA-001 – 008 (SIL 1)	3 ปี	508.992 ปี	3 ปี
หน่วยประมวลผล (SIL 2)	ทุก ๆ ครั้งที่มีการเปลี่ยนแปลงระบบนิรภัย	13.175 ปี	13 ปี หรือ ทุก ๆ ครั้งที่มีการเปลี่ยนแปลงระบบนิรภัย
อุปกรณ์ควบคุมสุดท้าย (SIL 2)	1.5 ปี	1.25 ปี	1 ปี

ตารางที่ 3.19 ระยะเวลาในการทดสอบแบบเก่าและการเลื่อนระยะ

ระดับ SIL	ระยะเวลาการทดสอบแบบเก่า	การเลื่อนระยะการทดสอบ
1	3 ปี	12 เดือน
2	1.5 ปี	6 เดือน

บทที่ 4
ผลจากการคัดเลือกและการปรับปรุงระยะเวลาการทดสอบ

ในบทนี้จะแสดงผลการคัดเลือกระดับความปลอดภัย ให้แก่วาล์วในฟังก์ชันวัดคุมนิรภัย และผลของการปรับปรุงระยะเวลาการทดสอบฟังก์ชันในหน่วยกลั่น CDU-3 ตามมาตรฐานของบริษัท ไทยออยล์ฯ

4.1 ผลจากการคัดเลือกระดับความปลอดภัยให้แก่อุปกรณ์สุดท้ายในฟังก์ชันนิรภัย

จากการคัดเลือกระดับความปลอดภัย SIL ให้แก่อุปกรณ์สุดท้ายในฟังก์ชันนิรภัย เพื่อทำการสร้างตารางในการซ่อมบำรุงให้แก่อุปกรณ์สุดท้ายที่ประกอบไปด้วยโซลินอยล์วาล์ว และวาล์เปิดปิด ทำการประเมินอุปกรณ์สุดท้ายทุกตัวที่อยู่ภายในระบบนิรภัยทั้ง 2 ระบบที่ใช้งานอยู่ ได้แก่ ระบบ Triconex และระบบ FSC ด้วยตารางการประเมินระดับความปลอดภัยตามวิธีลัดของไทยออยล์ฯ จะได้ผลลัพธ์ระดับความปลอดภัยของอุปกรณ์ควบคุมสุดท้ายเป็นจำนวนทางสถิติแสดงได้ดังตารางที่ 4.1

ตารางที่ 4.1 ผลจากการคัดกรองระดับความปลอดภัยแก่วาล์วเปิด/ปิด

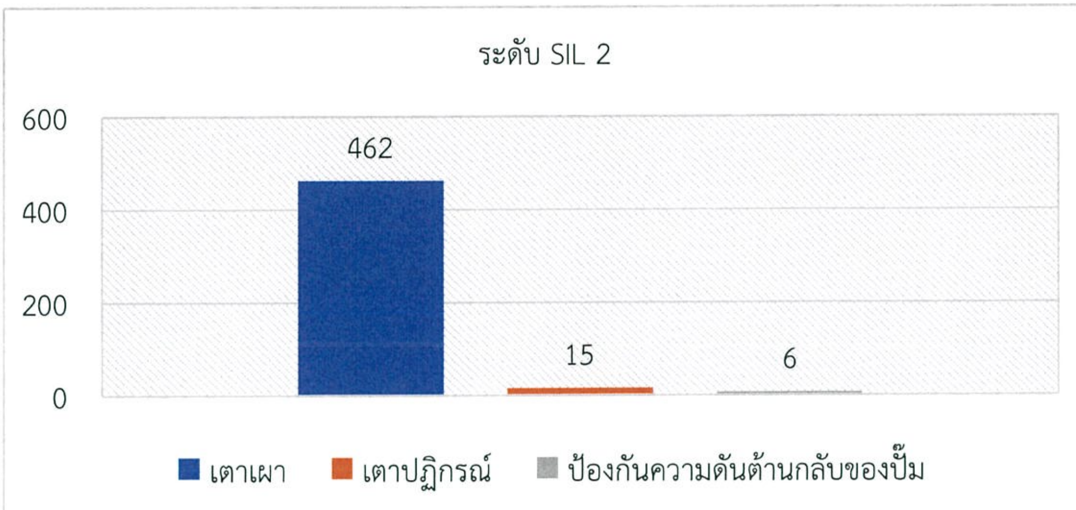
ระดับความปลอดภัย	จำนวน
SIL 2	483
SIL 1	850
Non SIL	298
รวม	1631

4.1.1 ผลจากการคัดเลือกระดับความปลอดภัย SIL 2

จากตารางที่ 4.1 ระดับความปลอดภัยของอุปกรณ์สุดท้ายที่ถูกคัดเลือดให้มีระดับ SIL 2 นั้นมีจำนวน 483 ตัว และสามารถพิจารณาได้ว่ากระบวนการที่ถูกติดตั้งอยู่นั้นถูกวิเคราะห์ความเสี่ยงแล้วว่ามีความอันตรายของผลกระทบต่อชีวิตของผู้ปฏิบัติงาน สิ่งแวดล้อม และทรัพย์สินที่ค่อนข้างสูง ทำให้มีการเลือกใช้รูปแบบการติดตั้งของอุปกรณ์ที่มีความเชื่อมั่นสูง และมีการทดสอบฟังก์ชันที่บ่อยครั้งกว่า โดยผลลัพธ์ในการประเมินที่ระดับ SIL 2 นั้นจะถูกแบ่งออกได้ดังตารางที่ 4.2 และแจกแจงข้อมูลเป็นกราฟทางสถิติของอุปกรณ์ระดับ SIL 2 ได้ดังรูปที่ 4.1

ตารางที่ 4.2 รูปแบบของอุปกรณ์สุดท้ายในระดับความปลอดภัย SIL 2

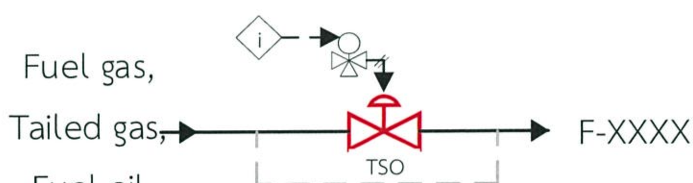
รูปแบบของการติดตั้ง (ระยะการซ่อมบำรุง)	คำอธิบาย	จำนวนอุปกรณ์สุดท้าย
เตาเผา (5 ปี)	ท่อเชื้อเพลิงแก๊ส น้ำมัน แก๊สทิ้ง	462
เตาปฏิกรณ์ (5 ปี)	ท่อไฮดรอเจน น้ำมันร้อน	15
ป้องกันความดันต้านกลับของปั๊ม (5 ปี)	ท่อขาออกของปั๊ม	6



รูปที่ 4.1 กราฟสถิติจากการประเมินในระดับ SIL 2

4.1.1.1 วาล์วเปิด/ปิดในการทำงานของเตาเผา

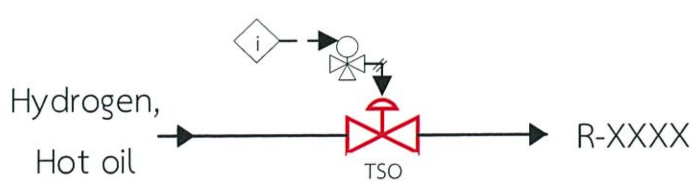
ในการทำงานของเตาเผา จะเป็นการติดตั้งวาล์วบนท่อเชื้อเพลิงน้ำมัน เชื้อเพลิงแก๊ส อากาศในการเผาไหม้ แก๊สทิ้ง ซึ่งเป็นส่วนประกอบที่ช่วยในการเผาไหม้ของเตาเผาและห้องเผาไหม้ ซึ่งจะเห็นว่ามีจำนวนมากในระดับความปลอดภัย SIL 2 เนื่องจากความร้อนนั้นเป็นองค์ประกอบสำคัญของการกลั่นน้ำมัน โดยการติดตั้งอุปกรณ์สุดท้ายสามารถแสดงการเชื่อมต่อแบบไม่ละเอียดได้ดังรูปที่ 4.2 ซึ่งเป็นการเชื่อมต่อแบบ 1oo1 voting แต่โดยปกติแล้วจะมีการเชื่อมต่อท่อ Bypass หรือเป็นการเชื่อมต่อแบบ 2oo2 voting บนเส้นปะในรูปที่ 4.2 เพื่อทำการสลับใช้งานเมื่อต้องการซ่อมบำรุงโดยที่ไม่ต้องการหยุดกระบวนการ



รูปที่ 4.2 การติดตั้งวาล์วเปิด/ปิดในฟังก์ชันนิรภัยของเตาเผา

4.1.1.2 วาล์วเปิด/ปิดในการทำงานของเตาปฏิกรณ์

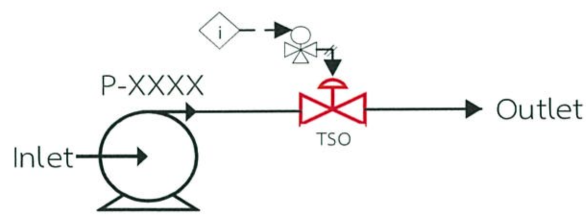
ในการทำงานเป็นการติดตั้งวาล์วบนท่อส่งไฮโดรเจน น้ำมันร้อน ที่จะถูกนำเข้าไปทำปฏิกิริยาในเตาปฏิกรณ์ จะเห็นว่ามีปริมาณการติดตั้งน้อยเนื่องจากจะติดตั้งบนกระบวนการที่อันตรายกว่าเตาปฏิกรณ์ปกติ การติดตั้งอุปกรณ์สุดท้ายสามารถแสดงได้ดังรูปที่ 4.3



รูปที่ 4.3 การติดตั้งวาล์วเปิด/ปิดในฟังก์ชันนิรภัยของเตาปฏิกรณ์

4.1.1.3 วาล์วเปิด/ปิดในการป้องกันความดันต้านกลับของปั๊ม

ในการป้องกันความดันต้านกลับของปั๊ม (Pump Back Flow Protection) การติดตั้งวาล์วจะถูกติดตั้งอยู่ด้านหลังของปั๊ม เพื่อป้องกันของไหลในท่อเกิดแรงดันสวนกลับมาจากปลายทางและสร้างความเสียหายแก่ปั๊ม การติดตั้งอุปกรณ์สุดท้ายแสดงได้ดังรูปที่ 4.4



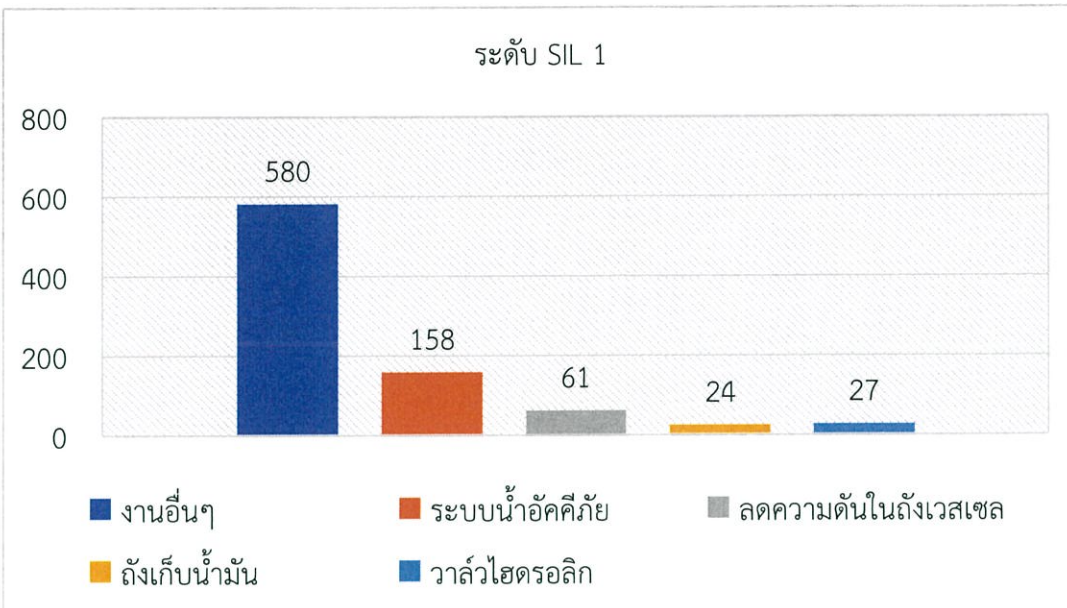
รูปที่ 4.4 การติดตั้งวาล์วเปิด/ปิดในฟังก์ชันนิรภัยของการป้องกันความดันต้านกลับของปั๊ม

4.1.2 ผลจากการคัดเลือกระดับความปลอดภัย SIL 1

จากตารางที่ 4.1 ระดับความปลอดภัยของอุปกรณ์ควบคุมสุดท้ายที่ถูกคัดเลือกให้มีระดับความปลอดภัย SIL 1 มีจำนวน 850 ตัว และสามารถพิจารณาได้ว่ากระบวนการที่ถูกติดตั้งอยู่นั้นถูกวิเคราะห์ความเสี่ยงแล้วว่ามีความอันตรายของผลกระทบต่อชีวิตของผู้ปฏิบัติงาน สิ่งแวดล้อมและทรัพย์สินที่ค่อนข้างต่ำ ทำให้มีการเลือกใช้รูปแบบการติดตั้งของอุปกรณ์ที่มีความเชื่อมั่นน้อยลงมาจากระดับความปลอดภัย SIL 2 และมีการทดสอบฟังก์ชันที่น้อยครั้งกว่า โดยผลลัพธ์ในการประเมินที่ระดับ SIL 1 จะถูกแบ่งออกได้ดังตารางที่ 4.3 และสามารถแจกแจงข้อมูลเป็นกราฟทางสถิติของอุปกรณ์ระดับ SIL 1 ได้ดังรูปที่ 4.5

ตารางที่ 4.3 รูปแบบของอุปกรณ์สุดท้ายในระดับความปลอดภัย SIL 1

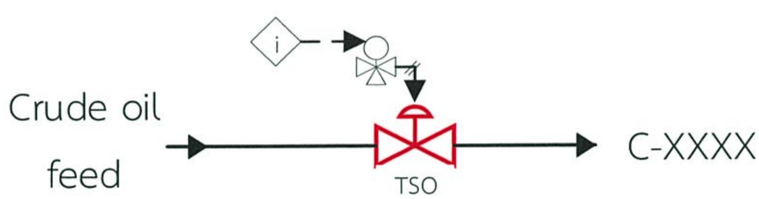
การติดตั้ง (ระยะการซ่อมบำรุง)	คำอธิบาย	จำนวนอุปกรณ์
การทำงานอื่น ๆ (5 ปี)	ท่อขาเข้าของฟีทสู่หอกลั่น และอื่น ๆ	580
สเปรย์น้ำป้องกันอัคคีภัย (2 ปี)	ท่อน้ำดับเพลิงในระบบนิรภัย	158
การลดความดันในถังเวสเซล (5 ปี)	ท่อด้านบนของถังเวสเซล	61
ถังเก็บน้ำมัน (2 ปี)	ท่อขาเข้าของถังเก็บน้ำมันและแก๊ส	24
วาล์วไฮดรอลิก (2 ปี)	วาล์วที่ควบคุมโดยใช้แรงไฮดรอลิก	27



รูปที่ 4.5 ผลจากการประเมินในระดับ SIL 1

4.1.2.1 วาล์วเปิด/ปิดในการทำงานอื่น ๆ

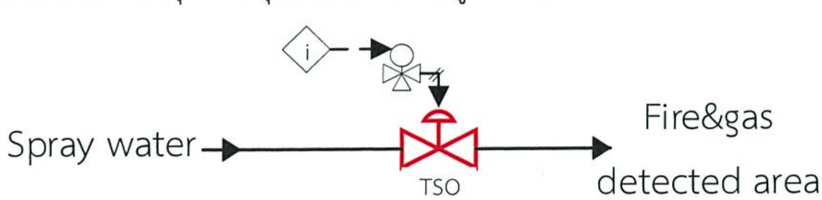
ในการทำงานอื่น ๆ ของฟังก์ชันวัดตุมนิรภัยจะมีการติดตั้งวาล์วอยู่ในที่ต่าง ๆ ได้แก่ ป้องกันหอกลั่นมีความดันสูงโดยติดตั้งวาล์วที่ท่อขาเข้าของฟีต ป้องกันระดับของถังเวสเซลสูงเกินไปโดยติดตั้งไว้ที่ขาเข้าของฟีต หรือการป้องกันที่อยู่นอกเหนือจากในตารางการคัดเลือกด้วยวิธีลัด การติดตั้งอุปกรณ์สุดท้ายแสดงได้ดังรูปที่ 4.6



รูปที่ 4.6 การติดตั้งวาล์วเปิด/ปิดในฟังก์ชันนิรภัยของการป้องกันหอกลั่นมีระดับสูง

4.1.2.2 วาล์วเปิด/ปิดในระบบสเปรย์น้ำป้องกันอัคคีภัย

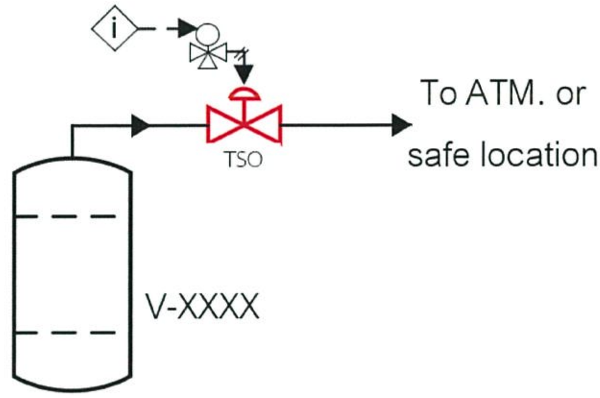
ในการทำงานของระบบสเปรย์น้ำ จะเป็นการติดตั้งของวาล์วควบคุมระบบเปิด (Deluge Valve) ที่ท่อส่งน้ำ โดยจะทำงานเพื่อป้องกันการเกิดเพลิงไหม้และการลุกลามของไฟหากเกิดเขม่าควัน การติดตั้งอุปกรณ์สุดท้ายแสดงได้ดังรูปที่ 4.7



รูปที่ 4.7 การติดตั้งวาล์วเปิด/ปิดในฟังก์ชันนิรภัยของระบบสเปรย์น้ำป้องกันอัคคีภัย

4.1.2.3 วาล์วเปิด/ปิดในการลดความดันในถังเวสเซล

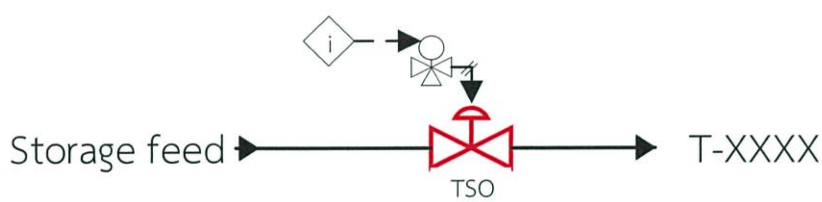
ในการลดความดันในถังเวสเซล จะติดตั้งของวาล์วไว้ที่ด้านบนของถังเวสเซลเพื่อทำการปล่อยกระบวนการด้านในออกเพื่อป้องกันความดันที่สูงเกินกว่าที่ถังเวสเซลสามารถรับได้ จะทำการเปิดเมื่อถังเวสเซลมีความดันสูง การติดตั้งอุปกรณ์สุดท้ายแสดงได้ดังรูปที่ 4.8



รูปที่ 4.8 การติดตั้งวาล์วเปิด/ปิดในฟังก์ชันนิรภัยของการลดความดันในถังเวสเซล

4.1.2.4 วาล์วเปิด/ปิดในการทำงานของถังเก็บน้ำมัน

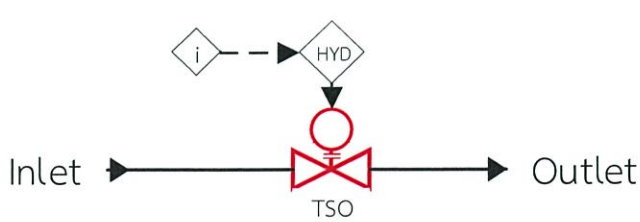
ในการติดตั้งวาล์ในการทำงานของถังเก็บน้ำมันหรือแก๊สนั้น จะเป็นการป้องกันไม่ให้ระดับของของเหลวหรือแก๊สภายในถังมีระดับสูงเกินไป เพื่อป้องกันการล้นถังของน้ำมันหรือการรั่วไหลของแก๊สภายในถังทรงกลม การติดตั้งอุปกรณ์สุดท้ายแสดงได้ดังรูปที่ 4.9



รูปที่ 4.9 การติดตั้งวาล์วเปิด/ปิดในฟังก์ชันนิรภัยของถังเก็บน้ำมัน

4.1.2.5 วาล์วเปิด/ปิดในการทำงานของวาล์วไฮดรอลิก

ในบางส่วนนั้นการติดตั้งจะเป็นการใช้รูปแบบของวาล์วแบบไฮดรอลิกหรือ Remote Operating Valve (ROV) ซึ่งจะนิยมใช้ในการติดตั้งแบบเก่า โดยจะทำงานด้วยแรงดันลมแบบไฮดรอลิก การติดตั้งอุปกรณ์สุดท้ายแสดงได้ดังรูปที่ 4.10



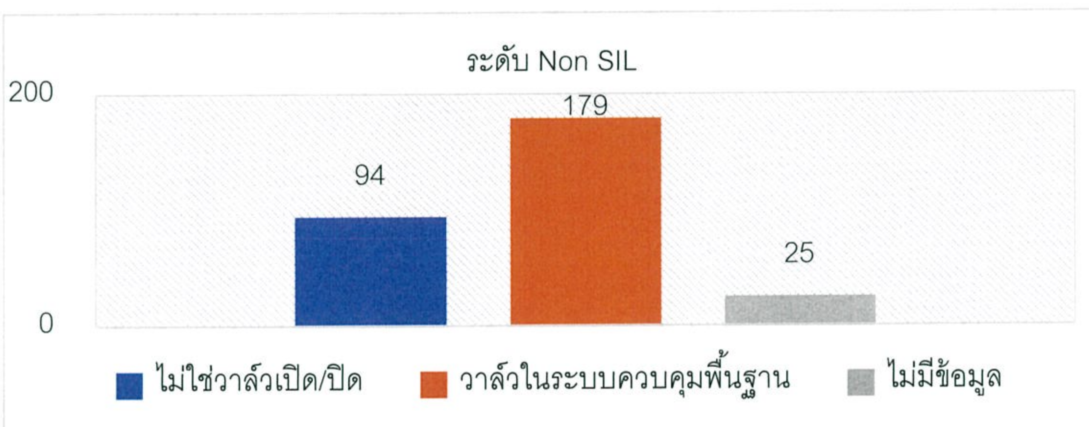
รูปที่ 4.10 การติดตั้งวาล์วเปิด/ปิดในฟังก์ชันนิรภัยด้วยวาล์วไฮดรอลิก

4.1.3 ผลจากการคัดเลือกระดับความปลอดภัย Non SIL

จากตารางที่ 4.1 ระดับความปลอดภัยของอุปกรณ์สุดท้ายที่ถูกคัดเลือดให้มีระดับ Non SIL หรือไม่ใช่วาล์วเปิด/ปิด นั้นมีจำนวน 298 ตัว ข้อมูลในส่วนนี้จะไม่ถูกนำไปสร้างเป็นตารางการบำรุงรักษาเนื่องจากบางส่วนไม่ใช่วาล์วเปิดปิดและบางส่วนไม่ใช่อุปกรณ์สุดท้าย โดยผลลัพธ์ในการประเมินที่ระดับ Non SIL นั้นจะถูกแบ่งออกดังตารางที่ 4.4 และสามารถแจกแจงข้อมูลเป็นกราฟทางสถิติของอุปกรณ์ระดับ Non SIL ดังรูปที่ 4.11

ตารางที่ 4.4 รูปแบบของอุปกรณ์สุดท้ายในระดับความปลอดภัย Non SIL

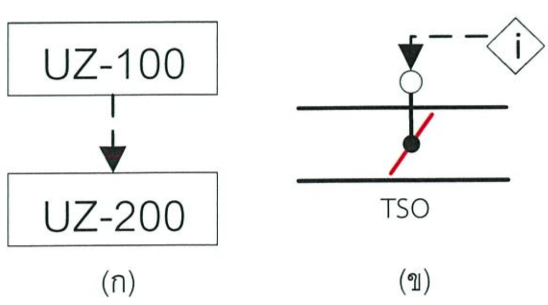
รูปแบบของการติดตั้ง	คำอธิบาย	จำนวน
ไม่ใช่วาล์วเปิด/ปิด	เป็นอุปกรณ์ประเภทอื่น สัญญาณลอจิก	94
วาล์วในระบบควบคุมพื้นฐาน	วาล์วควบคุมที่นำมาใช้	179
เป็น Tags ที่ไม่มีข้อมูล	ไม่สามารถค้นหาเจอ	25



รูปที่ 4.11 ผลจากการประเมินในระดับ Non SIL

4.1.3.1 ไม่ใช่วาล์วเปิด/ปิด

ผลจากการคัดกรองที่ไม่ใช่วาล์วหรือเป็นแค่เพียงชื่อของสัญญาณ เช่น สัญญาณจากลอจิกไปหาลอจิก วาล์วแบบพิเศษอย่างไดเวิทแดมเปอร์ (Divert Damper) ที่ปล่องปล่อยแก๊สเสีย เป็นต้น การติดตั้งอุปกรณ์สุดท้ายแสดงได้ดังรูปที่ 4.12



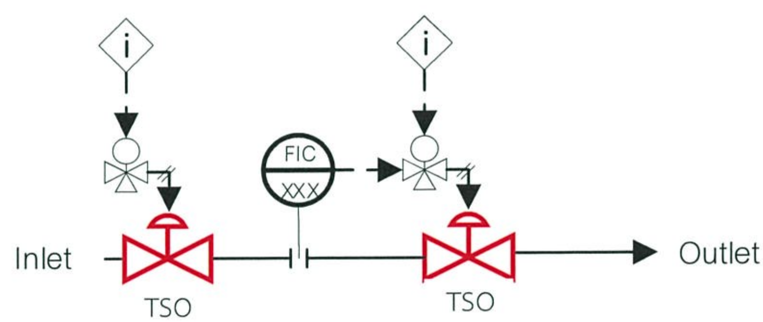
รูปที่ 4.12 รูปของ Tags ที่ทำการคัดกรองแล้วไม่ใช่วาล์วเปิด/ปิด

(ก) สัญญาณลอจิกไปสู่ลอจิก (ข) วาล์วแบบ Divert Damper

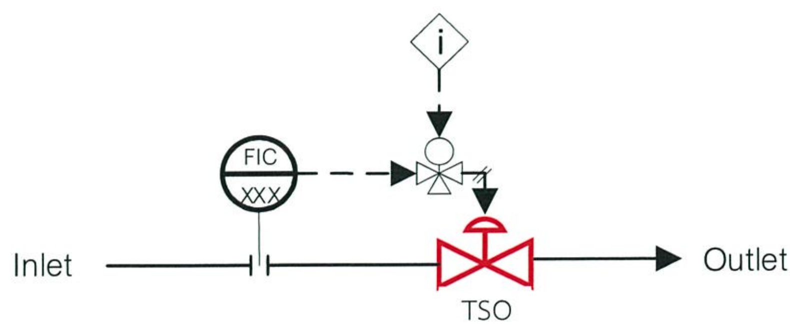
4.1.3.2 วาล์วที่ใช้ในระบบควบคุมพื้นฐาน

วาล์วควบคุมที่อยู่ในการประเมินจะถูกแบ่งออกเป็น 2 ประเภท ได้แก่

1) วาล์วควบคุมที่ต่อแบบอนุกรมอยู่กับวาล์วเปิด/ปิด (Series with On/Off Valve) โดยการเชื่อมต่อในลักษณะนี้สามารถอธิบายได้ว่ากระบวนการนั้นต้องการที่จะเพิ่มระดับความปลอดภัยให้สูงขึ้น การเชื่อมต่อแบบนี้ไม่จำเป็นต้องสร้างตารางการซ่อมบำรุงเพิ่มเติม เนื่องจากทำการซ่อมบำรุงวาล์วเป็นประจำ แสดงการติดตั้งได้ดังรูปที่ 4.13
2) วาล์วควบคุมที่ไม่ได้ต่ออนุกรมอยู่กับวาล์วเปิด/ปิด (Not Series with On/Off Valve) โดยการเชื่อมต่อในลักษณะนี้สามารถอธิบายได้ว่ากระบวนการนั้นต้องการระดับความปลอดภัยที่ไม่สูงมาก หรือไม่ต้องการเลยซึ่งเป็นการนำวาล์วควบคุมมาปฏิบัติหน้าที่ในฟังก์ชันนิรภัยแทนการใช้งานของวาล์วเปิด/ปิด การเชื่อมต่อแบบนี้ไม่จำเป็นต้องสร้างตารางการซ่อมบำรุงเพิ่มเติมเนื่องจากมีผลกระทบน้อย และวาล์วควบคุมบางตัวมีตารางการทดสอบอยู่แล้ว แสดงการติดตั้งได้ดังรูป 4.14



รูปที่ 4.13 รูปของวาล์วควบคุมที่ต่อแบบอนุกรมอยู่กับวาล์วเปิด/ปิด



รูปที่ 4.14 รูปของวาล์วควบคุมที่ไม่ได้ต่อแบบอนุกรมอยู่กับวาล์วเปิด/ปิด

4.1.3.3 เป็นอุปกรณ์ที่ไม่มีข้อมูล

เป็นรายชื่อของอุปกรณ์ที่ไม่สามารถหาข้อมูลได้ในโปรแกรม INTools และแผนภาพ P&ID โดยอาจจะเป็นข้อมูลที่ตกหล่นจากการบันทึก

4.2 ผลจากการศึกษาการปรับปรุงระยะเวลาในการทดสอบฟังก์ชันใน CDU-3

จากการคำนวณระยะเวลาการทดสอบใหม่ ให้ตรงตามระดับความปลอดภัยที่ถูกพิจารณา จะได้ผลลัพธ์ของระยะเวลาการทดสอบฟังก์ชันในแต่ละฟังก์ชันวัดคุมนิรภัยดังต่อไปนี้

4.2.1 ระยะเวลาทดสอบของฟังก์ชันนิรภัยในเตาเผา F-1001

จากการพิจารณาฟังก์ชันวัดคุมนิรภัยในระบบของเตาเผา F-1001 ในหน่วยกลั่น CDU-3 และจากสมการการคำนวณระดับความปลอดภัย จะได้ผลลัพธ์จากการคำนวณเป็นระยะเวลาการทดสอบฟังก์ชันในแต่ละอุปกรณ์ ซึ่งจะแสดงผลและแสดงการปรับระยะเวลาการทดสอบที่คำนวณได้ตามมาตรฐานของไทยออยล์ฯ ดังตารางที่ 4.5

ตารางที่ 4.5 ผลการคำนวณระยะเวลาการทดสอบฟังก์ชันนิรภัยในเตาเผา F-1001

ลำดับ	อุปกรณ์ในฟังก์ชันนิรภัย	ระดับ SIL	ระยะเวลาการทดสอบ (เก่า)	ระยะเวลาทดสอบจากการคำนวณ (ใหม่)	ระยะเวลาการทดสอบที่ควรเลือก (ใหม่)
1-8	FZA-001 – 008 LL	SIL 1	3 ปี	508.992 ปี	3 ปี
9	PZA-302 HH	SIL 1	3 ปี	66.667 ปี	3 ปี
10	LZA-205 HH	SIL 1	3 ปี	16.667 ปี	3 ปี
11	LZA-203 HH	SIL 1	3 ปี	16.667 ปี	3 ปี
12	PZA-201 HH	SIL 1	3 ปี	66.667 ปี	3 ปี
13	PZA-202 LL	SIL 2	1.5 ปี	6.667 ปี	3 ปี
14	PZA-301 HH	SIL 1	3 ปี	66.667 ปี	3 ปี
15	FZA-204 LL	SIL 2	1.5 ปี	2.375 ปี	2 ปี
-	หน่วยประมวลผล	SIL 2	ทุก ๆ ครั้งที่มีการเปลี่ยนแปลงระบบ	13.175 ปี	13 ปี หรือทุก ๆ ครั้งที่มีการเปลี่ยนแปลงระบบ
-	อุปกรณ์สุดท้าย	SIL 2	1.5 ปี	1.25 ปี	1 ปี

4.2.2 ระยะเวลาทดสอบของฟังก์ชันนิรภัยในหอกลั่น C-1001

จากการพิจารณาฟังก์ชันนิรภัยในระบบของหอกลั่น C-1001 ในหน่วยกลั่น CDU-3 และจากสมการการคำนวณระดับความปลอดภัย จะได้ผลลัพธ์จากการคำนวณเป็นระยะเวลาการทดสอบฟังก์ชันแสดงภายในตารางที่ 4.6

ตารางที่ 4.6 ผลการคำนวณระยะเวลาการทดสอบฟังก์ชันนิรภัยในหอกลั่น C-1001

ลำดับ	อุปกรณ์ในฟังก์ชันนิรภัย	ระดับ SIL	ระยะเวลาการทดสอบ (เก่า)	ระยะเวลาทดสอบจากการคำนวณ (ใหม่)	ระยะเวลาการทดสอบที่ควรเลือก (ใหม่)
13	PZA-301 HH	SIL 1	3 ปี	66.667 ปี	3 ปี
-	หน่วยประมวลผล	SIL 2	ทุก ๆ ครั้งที่มีการเปลี่ยนแปลงระบบ	13.175 ปี	13 ปี หรือ ทุก ๆ ครั้งที่มีการเปลี่ยนแปลงระบบ
-	อุปกรณ์สุดท้าย	SIL 1	3 ปี	12.5 ปี	3 ปี

4.2.3 ระยะเวลาทดสอบของฟังก์ชันนิรภัยในหม้อพักน้ำ V-1007

จากการพิจารณาฟังก์ชันนิรภัยในระบบของหม้อพักน้ำ V-1007 ในหน่วยกลั่น CDU-3 และจากสมการการคำนวณระดับความปลอดภัย จะได้ผลลัพธ์จากการคำนวณเป็นระยะเวลาการทดสอบฟังก์ชันแสดงภายในตารางที่ 4.7

ตารางที่ 4.7 ผลการคำนวณระยะเวลาการทดสอบฟังก์ชันนิรภัยในหม้อพักน้ำ V-1007

ลำดับ	อุปกรณ์ในฟังก์ชันนิรภัย	ระดับ SIL	ระยะเวลาการทดสอบ (เก่า)	ระยะเวลาทดสอบจากการคำนวณ (ใหม่)	ระยะเวลาการทดสอบที่ควรเลือก (ใหม่)
14	LZA-308 LL และ HH	SIL 1	3 ปี	66.667 ปี	3 ปี
-	หน่วยประมวลผล	SIL 2	ทุก ๆ ครั้งที่มีการเปลี่ยนแปลงระบบ	13.175 ปี	13 ปี หรือ ทุก ๆ ครั้งที่มีการเปลี่ยนแปลงระบบ
-	อุปกรณ์สุดท้าย	SIL 1	1.5 ปี	12.5 ปี	3 ปี

บทที่ 5
สรุปผลการดำเนินการและข้อเสนอแนะ

ในบทนี้จะกล่าวถึงการสรุปผลที่ได้จากการดำเนินงาน การศึกษาปัญหาทั้งหมดและอุปสรรคในการดำเนินงาน รวมถึงแนวทางหรือข้อเสนอแนะในการแก้ไขปัญหาต่าง ๆ ที่พบเพื่อให้ผลของการดำเนินงานสำเร็จลุล่วงตามที่กำหนดไว้

5.1 สรุปผลการดำเนินงาน

ในการดำเนินงานจะถูกแบ่งเป็น 2 ส่วนคือ ส่วนในการคัดเลือกระดับความปลอดภัยให้แก่วาล์วเปิดปิดในฟังก์ชันวัดคุมนิรภัยและส่วนการศึกษา พัฒนา ระยะเวลาการทดสอบของฟังก์ชันนิรภัยในหน่วยกลั่นน้ำมันดิบ CDU-3 สามารถสรุปการดำเนินงานได้ดังนี้

จากการคัดเลือกระดับความปลอดภัยให้แก่วาล์วเปิดปิดในฟังก์ชันวัดคุมนิรภัย เพื่อนำมาสร้างเป็นตารางเวลาในการทดสอบและซ่อมแซมในช่วงเวลาการซ่อมบำรุงของหน่วยกลั่นนั้น ๆ โดยการขนย้ายวาล์วมาทำการทดสอบจะอยู่ในช่วงเวลาตามตาราง คือ 2 ปี และ 5 ปี วาล์วที่ถึงช่วงเวลาการซ่อมบำรุงจะถูกนำมาทำความสะอาดและเปลี่ยนแปลงอุปกรณ์ด้านใน เช่น หน้าวาล์ว แหวนบ่าวาล์ว หรือแพ็คกิ้ง เป็นต้น พร้อมทั้งทดสอบฟังก์ชันการทำงานและทำการทดสอบการรั่วไหลตามระดับการรั่วไหลที่ต้องการ เพื่อไม่ให้วาล์วมีการเสียหายและเกิดความผิดพลาดในการปฏิบัติหน้าที่นิรภัย

จากการศึกษาการพัฒนาระยะเวลาการทดสอบของฟังก์ชันวัดคุมนิรภัยในหน่วยกลั่น CDU-3 จะเห็นได้ว่าต้องทำการรวบรวมข้อมูลความเสียหายของอุปกรณ์ ข้อมูลระดับความปลอดภัยที่คัดกรอง และข้อมูลในการเลือกระยะเวลาในการทดสอบ ซึ่งผลลัพธ์จากข้อมูลในตารางที่ 4.5 4.6 และ 4.7 แสดงให้เห็นว่าผลจากการคำนวณมีบางส่วนที่มีระยะนานเกินจริง ส่งผลมาจากข้อมูลการเสียหายเก่าที่ถูกบันทึกอย่างไม่ถูกต้องและบางส่วนสูญหายไปตามกาลเวลา อัตราความผิดพลาดที่ทำการสำรวจจึงมีค่าที่ไม่ถูกต้องทั้งนี้ผลลัพธ์ที่ได้เป็นการใช้ข้อมูลความเสียหายในปี ค.ศ. 2014 ถึง 2017 รวม 4 ปี แต่โรงกลั่นน้ำมันไทยออยล์ฯ มีระยะการดำเนินงานมากว่า 50 ปี ทำให้ยังไม่สามารถใช้งานได้จริงเนื่องจากข้อมูลไม่เพียงพอ จึงต้องมีการพัฒนาการสำรวจเพิ่มเติมในระยะต่อ ๆ ไปโดยการเก็บรวบรวมข้อมูลความเสียหายอย่างต่อเนื่อง ซึ่งจะทำให้องค์กรมีข้อมูลความเสียหายของอุปกรณ์ที่มีความถูกต้องใช้ในการพิจารณาระยะเวลาในการทดสอบ ข้อมูลบางส่วนจากการศึกษาที่มีระยะการทดสอบจากการคำนวณเกินข้อกำหนด 3 ปี ตามมาตรฐานของไทยออยล์ฯ จะสามารถสรุปได้ว่าฟังก์ชันนั้นสามารถใช้งานได้ดีในระดับความปลอดภัยที่ตั้งไว้ ไม่ต้องมีการเปลี่ยนแปลงระยะเวลาทดสอบเพิ่มเติม

5.2 ปัญหาและอุปสรรค

1) ความรู้ที่ศึกษามาไม่เพียงพอต่อการทำรายงาน
2) ไม่มีประสบการณ์จากหน้างานจริงมาก่อน จึงทำให้เกิดความสับสนในการทำงาน
3) ในการทำงานมีข้อมูลรายละเอียดต่าง ๆ ที่ค่อนข้างเยอะสามารถเกิดความผิดพลาดได้
4) ต้องทำการฝึกงานในแผนกอื่น ๆ ไปพร้อมกับการทำรายงาน จึงทำให้เกิดความล่าช้า

5.3 แนวทางการแก้ปัญหา

1) ศึกษาข้อมูลที่ใช้ในรายงานอย่างละเอียด เพื่อให้เกิดความเข้าใจแนวทางการวิเคราะห์และสร้างระบบนิรภัย
2) ออกไปสำรวจหน้างานกับฝ่ายซ่อมบำรุง เพื่อสร้างความเข้าใจในรูปแบบการติดตั้งฟังก์ชันนิรภัยและลักษณะผลกระทบจากอุปกรณ์ต่าง ๆ
3) ดำเนินการเก็บข้อมูลอย่างรอบคอบและเป็นระเบียบ พร้อมให้พี่ที่ทำงานตรวจสอบความถูกต้อง
4) แบ่งเวลาในการทำงานเพื่อที่จะสามารถทำรายงานให้สำเร็จและได้ความรู้ในแผนกอื่นไปพร้อมกัน

5.4 ข้อเสนอแนะ

ในการปฏิบัติสหกิจศึกษาครั้งนี้ ทางบริษัทสามารถนำข้อมูลที่ได้จากการศึกษาของนักศึกษานอกจากจะประยุกต์ใช้งานเพื่อพัฒนาระบบการแยกประเภทความเสียหายภายในองค์กร ทั้งในส่วนงานฝ่ายปฏิบัติการและช่างซ่อมบำรุงแล้ว ยังสามารถพัฒนาระยะเวลาในการซ่อมบำรุงและทดสอบอุปกรณ์ในฟังก์ชันนิรภัยเพื่อให้มีความถูกต้องตามข้อมูลทางสถิติยิ่งขึ้นในอนาคต

บรรณานุกรม

[1] ทวิช ชูเมือง. (2551). *การกำหนดค่าระดับความปลอดภัยสำหรับฟังก์ชันนิรภัย*. กรุงเทพฯ: วีพรินท์.

[2] William M. Goble and Harry Cheddie. (2548). *Safety Instrumented Systems Verification: Practical Probabilistic Calculations*. North Carolina: ISA – The Instrumentation, Systems and Automation Society.

[3] Edward M. Marszal and Eric Scharpf, (2545). *Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis*. North Carolina: ISA – The Instrumentation, Systems and Automation Society.

[4] TR84.00.02 PART 1-2 (2545). Safety Instrumented Function (SIF) – Safety Integrity Level (SIL) Evaluation Techniques. North Carolina: ISA – The Instrumentation, Systems and Automation Society.

[5] ทวิช ชูเมือง. (2554). *อัตราความผิดพลาดสำหรับเครื่องมือวัดแบบเครื่องกล*. เข้าถึงได้จาก : http://www.thailandindustry.com. (วันที่ค้นข้อมูล : 7 พฤศจิกายน 2560).

ภาคผนวก

ผลการประเมินค่าปัจจัยจากสาเหตุร่วม (Common Cause)

จากมาตรฐาน IEC 61508 Part 6, Annex D สามารถแสดงตาราง D.1 ซึ่งใช้ในการประเมินค่าปัจจัยจากสาเหตุร่วม (β : Common Cause) ของทรานสมิตเตอร์วัดอัตราการไหล ที่ใช้งานอยู่ในฟังก์ชันนิรภัยภายใต้หน่วยกลั่นน้ำมันดิบที่ 3 (CDU-3) ด้วยการประเมินด้วยข้อมูลของวิศวกรความปลอดภัย สามารถพิจารณาข้อมูลจากทรานสมิตเตอร์วัดอัตราการไหลแบบ 2oo8 voting ในฟังก์ชันของเตาเผา F-1001 ลำดับที่ 1-8 ได้ดังนี้

ตารางผลการประเมินคะแนนของค่าปัจจัยจากสาเหตุร่วมของทรานสมิตเตอร์อัตราการไหล

การใช้งาน	คะแนน		ข้อมูลปัจจุบัน	คะแนนผลลัพธ์ (S)
	X_{SA}	Y_{SA}		$X_{SA} + Y_{SA}$
การเดินสายสัญญาณของอุปกรณ์มีการแยกเส้นทางกันหรือไม่ ?	1.0	2.0	มีการเดินสายแยกจากกัน	3.0
อุปกรณ์วัด/อุปกรณ์สุดท้ายมีการติดตั้งบนแผงบอร์ดวงจรแยกกันหรือไม่ ?	2.5	1.5	มีการติดตั้งแยกจากกัน	4.0
อุปกรณ์วัด/อุปกรณ์สุดท้ายมีการติดตั้งสายเคเบิลในตู้ Cabinets แยกกันหรือไม่ ?	2.5	0.5	อยู่ในตู้แยกจากกัน	3.0
อุปกรณ์มีหลักการที่ใช้ในการวัดแตกต่างกันหรือไม่ ?	7.5	-	ไม่แตกต่าง (ความดันแตกต่าง)	0
อุปกรณ์มีการออกแบบ/เทคโนโลยี/ผู้จัดจำหน่ายต่างกันหรือไม่ ?	5.5	-	ไม่แตกต่าง (Rosemount 1151)	0
ลักษณะของการออกแบบอุปกรณ์สำรอง (Redundancy) MooN, N > M+2 หรือไม่ ?	2.0	0.5	8 > 4	2.5
ลักษณะของการออกแบบอุปกรณ์สำรอง (Redundancy) MooN, N = M+2 หรือไม่ ?	1.0	0.5	8 = 4	0
อุปกรณ์มีการทดสอบที่แตกต่างกันและมีการใช้งานอุปกรณ์อีกตัวขณะการปฏิบัติงานหรือไม่ ?	1.0	1.0	ไม่	2.0
การซ่อมบำรุงมีการปฏิบัติโดยผู้ดูแลคนละคนในเวลาที่ต่างกันหรือไม่ ?	2.5	-	ไม่	2.5
ช่องสัญญาณของอุปกรณทั้งสองมีการส่งข้อมูลแยกกันหรือไม่ ?	0.5	0.5	ใช่ ส่งสัญญาณแยกจากกัน	1.0
การออกแบบของอุปกรณ์มีการใช้งานอย่างสำเร็จลุล่วงมากกว่า 5 ปีหรือไม่ ?	1.0	1.0	มีการใช้งานมามากกว่า 5 ปี	2.0

ตารางผลการประเมินคะแนนของค่าปัจจัยจากสาเหตุร่วมของทรานสมิตเตอร์อัตราการไหล (ต่อ)

การใช้งาน	คะแนน		ข้อมูลปัจจุบัน	คะแนนผลลัพธ์ (S)
	X_{SA}	Y_{SA}		$X_{SA} + Y_{SA}$
อุปกรณ์มีการใช้งานมากกว่า 5 ปี ในสภาพแวดล้อมเดียวกันหรือไม่ ?	1.5	1.5	มีการใช้งานมามากกว่า 5 ปี	3.0
มีการป้องกันการลัดวงจรและกระแสเกินในอินพุต/เอาต์พุตหรือไม่ ?	1.5	0.5	มีการป้องกันในอุปกรณ์	2.0
อุปกรณ์ทุกตัวมีการกำหนด Conservative rated จากผู้ผลิตหรือไม่ ?	2.0	-	มีการกำหนดจากผู้ผลิต	2.0
การวิเคราะห์ความผิดพลาดและการประเมินค่าปัจจัยสาเหตุร่วมกันถูกพิจารณามาก่อนการออกแบบ ?	-	3.0	ไม่มีการพิจารณา	0
ค่าปัจจัยสาเหตุร่วมกันมีการประเมินและส่งข้อมูลใช้งานให้การออกแบบหรือไม่ ?	-	3.0	ไม่มีการพิจารณา	0
ความผิดพลาดในการติดตั้งมีการพิจารณาในการออกแบบหรือไม่ ?	0.5	3.5	มีการพิจารณาก่อนการติดตั้ง	4.0
มีระบบในการสืบค้นต้นตอของปัญหาหรือไม่ ?	0.5	1.5	ไม่ มีเพียงระบบแจ้งเตือนและการทดสอบระบบ	0
มีกระบวนการในการยืนยันการซ่อมบำรุง รวมถึงการสอบเทียบและปรับแต่ง หรือไม่ ?	2.0	1.0	มี	3.0
ทั้งระบบของอุปกรณ์สำรอง (เช่น สายเคเบิล) ที่มีการอิสระต่อกันจะไม่ถูกเคลื่อนย้ายหลังจากการซ่อมบำรุงหรือไม่ ?	0.5	0.5	ไม่เคลื่อนย้าย	1.0
การซ่อมบำรุงของแผงวงจรในอุปกรณ์ถูกปฏิบัติการโดยศูนย์ซ่อมบำรุงและถูกทดสอบอย่างเต็มรูปแบบหรือไม่ ?	0.5	1.5	ใช่	2.0
ระบบแจ้งเตือนสามารถค้นหาความผิดพลาดในระดับสัญญาณหรือโมดูลได้หรือไม่ ?	1.0	1.0	หน่วยประมวลผลสามารถตรวจพบได้	2.0

ตารางผลการประเมินคะแนนของค่าปัจจัยจากสาเหตุร่วมของทรานสมิตเตอร์อัตราการไหล (ต่อ)

ผู้ออกแบบถูกอบรมและเข้าใจถึงปัญหาและผลกระทบของ Common cause หรือไม่ ?	2.0	3.0	ผู้ออกแบบถูกอบรม	5.0
ผู้ซ่อมบำรุงถูกอบรมและเข้าใจถึงปัญหาและผลกระทบของค่าปัจจัยสาเหตุร่วมกันหรือไม่ ?	0.5	4.5	ผู้ซ่อมบำรุงไม่ถูกอบรม	0
บริเวณการเข้าถึงอุปกรณ์ถูกจำกัดหรือไม่ ?	0.5	2.5	จำกัดเพียงแค่ผู้ปฏิบัติงาน	3.0
โดยปกติอุปกรณ์ทำงานที่อุณหภูมิ ความชื้น ฝุ่น การกัดกร่อน การสั่นสะเทือนหรือสภาพแวดล้อมอื่น ๆ ที่อยู่ในย่านที่ถูกทดสอบโดยไม่ต้องมีตัวควบคุมสภาพแวดล้อมหรือไม่ ?	3.0	1.0	เงื่อนไขของสภาพแวดล้อมถูกยืนยันในการติดตั้ง	4.0
สายสัญญาณและสายไฟแยกออกจากกันในทุก ๆ จุดหรือไม่ ?	2.0	1.0	แยกจากกัน	3.0
ระบบถูกทดสอบสำหรับการต้านทานของสภาพแวดล้อมต่าง ๆ ที่ถูกกำหนดในมาตรฐานหรือไม่ ?	10.0	10.0	ถูกทดสอบโดยมาตรฐาน	20.0
คะแนนรวม	55	46.5	$S = X_{SA} + Y_{SA}$	74.0

จากตาราง จะได้คะแนนรวม S เท่ากับ 74.0 ซึ่งจากตารางที่ 2.10 จะสามารถพิจารณาหาค่าของปัจจัยสาเหตุร่วมกันได้โดยค่าที่อยู่ระหว่างช่วง 70 ถึง 120 คะแนน ทรานสมิตเตอร์จะมีค่าปัจจัยสาเหตุร่วมกัน ที่ 2 % หรือ 0.02 ซึ่งจะนำไปคำนวณในการกำหนดระยะเวลาการทดสอบฟังก์ชันต่อไป

ประวัติผู้เขียน

ชื่อ – นามสกุล	นายพงศพล จิตตโสภาวดี
วัน เดือน ปีเกิด	9 พฤษภาคม 2539
ที่อยู่	88/160 หมู่ 12 ต.บางแก้ว อ.บางพลี จ.สมุทรปราการ 10540
Email	Phongsapon_Jitta@hotmail.com
โทรศัพท์	064-9351201

ประวัติการศึกษา

- พ.ศ. 2554 - 2556 ระดับมัธยมศึกษาตอนปลาย โรงเรียนอัสสัมชัญสมุทรปราการ
- พ.ศ. 2557 - ปัจจุบัน วิศวกรรมศาสตร์บัณฑิต สาขาวิชาวิศวกรรมการวัดคุม คณะวิศวกรรมศาสตร์สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ประสบการณ์

- นักศึกษาฝึกงาน แผนก Engineering Construction and Modification (ECM) บริษัท ปตท. สำรวจและผลิตปิโตรเลียม จำกัด (มหาชน)
- นักศึกษาโครงงานสหกิจศึกษา แผนก Engineering Instrument Specialist (ENIS) บริษัท ไทยออยล์ จำกัด (มหาชน)