การออกแบบระบบควบคุมกระบวนการและระบบวัดคุมนิรภัยสำหรับแท่นขุดเจาะน้ำมันและก๊าซ(กรณีศึกษา)

PROCESS CONTROL & SAFETY INSTRUMENTED SYSTEM DESIGN FOR UPSTREAM OIL AND GAS INDUSTRY (CASE STUDY)

ชลิต อยู่สำราญ
CHARLIT YOOSAMRAN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมการวัดคุม
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2562
KMITL-2019-EN-M-060-103

การออกแบบระบบควบคุมกระบวนการและระบบวัดคุมนิรภัยสำหรับแท่นขุดเจาะน้ำมันและก๊าซ(กรณีศึกษา)

PROCESS CONTROL & SAFETY INSTRUMENTED SYSTEM DESIGN FOR UPSTREAM OIL AND GAS INDUSTRY (CASE STUDY)

ชลิต อยู่สำราญ

CHARLIT YOOSAMRAN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมการวัดคุม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2562

KMITL-2019-EN-M-060-103

การออกแบบระบบควบคุมกระบวนการและระบบวัดคุมนิรภัยสำหรับแท่นขุดเจาะน้ำมันและก๊าซ(กรณีศึกษา)

PROCESS CONTROL & SAFETY INSTRUMENTED SYSTEM DESIGN FOR UPSTREAM OIL AND GAS INDUSTRY (CASE STUDY)

ชลิต อยู่สำราญ

CHARLIT YOOSAMRAN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมการวัดคุม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2562

KMITL-2019-EN-M-060-103

PROCESS CONTROL & SAFETY INSTRUMENTED SYSTEM DESIGN FOR UPSTREAM OIL AND GAS INDUSTRY (CASE STUDY)

CHARLIT YOOSAMRAN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN INSTRUMENTATION ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2019

KMITL-2019-EN-M-060-103

คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การออกแบบระบบควบคุมกระบวนการและระบบวัดคุมนิรภัยสำหรับแท่นขุดเจาะน้ำมันและก๊าซ (กรณีศึกษา)

Thesis Title Process Control & Safety Instrumented System Design for Upstream Oil and Gas Industry (Case Study)

นักศึกษา นายชลิต อยู่สำราญ

รหัสประจำตัว 57601220

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมการวัดคุม

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.สักรียา ชิตวงศ์

หมายเลขวิทยานิพนธ์ KMITL-2019-EN-M-060-103

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.ฟูศักดิ์	ชีวสุวิทย์	
รศ.ดร.วิทยา	ทิพย์สุวรรณพร	
รศ.ดร.อาจินต์	น่วมสำราญ	
ผศ.ดร.พงษ์ชัย	นิลาศ	
รศ.สักรียา	ชิตวงศ์	

วัน / เดือน/ ปี ที่สอบ วันพุธที่ 24 กรกฎาคม พ.ศ. 2562 เวลา 11.00-13.00 น.
สถานที่สอบ ณ ห้องประชุม 4 ชั้น 5 อาคาร A

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร. คมสัน มาลีสี)

คณบดี คณะวิศวกรรมศาสตร์

วันที่ 24 กรกฎาคม พ.ศ. 2562

หัวข้อวิทยานิพนธ์	การออกแบบระบบควบคุมกระบวนการและระบบวัดคุมนิรภัย สำหรับแท่นขุดเจาะน้ำมันและก๊าซ (กรณีศึกษา)
นักศึกษา	นายชลิต อยู่สำราญ
รหัสประจำตัว	57601220
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมการวัดคุม
พ.ศ.	2562
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.สักรียา ชิตวงศ์

บทคัดย่อ

วัตถุประสงค์ของวิทยานิพนธ์ฉบับนี้จัดทำเพื่อสำหรับคนที่มีความสนใจในอุตสาหกรรมแท่นขุดเจาะน้ำมันและก๊าซ โดยจะเป็นภาพรวมของการควบคุมกระบวนการผลิตและการออกแบบระบบวัดคุมนิภัยสำหรับอุตสาหกรรมน้ำมันและก๊าซ ซึ่งระบบควบคุมกระบวนการจะใช้ในการตรวจสอบข้อมูลและควบคุมอุปกรณ์ทั้งหมดที่อยู่บนแท่นขุดเจาะและผลิต วัตถุประสงค์ของระบบนี้คือจะทำการอ่านค่าจากเซ็นเซอร์ที่มีจำนวนมากแล้วเรียกใช้งานโปรแกรมเพื่อตรวจสอบสถานะกระบวนการผลิต เพื่อทำการควบคุมค่ากระบวนการและแสดงสัญญาณเตือนต่อผู้ปฏิบัติงานให้ได้ทราบข้อมูล ระบบวัดคุมนิรภัย คือ ระบบที่ทำการควบคุมและป้องกันเหตุการณ์ไม่พึงประสงค์เมื่อกระบวนการและสิ่งอำนวยความสะดวกไม่สามารถใช้งานได้อีกต่อไปภายใต้สภาวะการทำงานปกติ ฟังก์ชั่นของระบบวัดคุมนิรภัยเป็นส่วนหนึ่งของความปลอดภัยโดยรวมของระบบที่ขึ้นอยู่กับการตอบสนองที่ถูกต้องของระบบความปลอดภัย โดยการตอบสนองต่ออินพุตรวมไปถึงการจัดการข้อผิดพลาดของผู้ปฏิบัติงาน ความผิดพลาดของอุปกรณ์และการเปลี่ยนแปลงด้านสิ่งแวดล้อม วัตถุประสงค์ของระบบวัดคุมนิรภัย คือเพื่อปกป้องผู้คน สิ่งแวดล้อมและทรัพย์สินจากเหตุการณ์อันตรายที่จะเกิดขึ้นโดยการลดความน่าจะเป็นของเหตุการณ์อันตรายที่จะเกิดขึ้นตามมาตรฐานสากล IEC61508 และ IEC61511

คำสำคัญ : ระบบควบคุมแบบกระจายส่วน, ระบบวัดคุมนิรภัย

Title	Process Control & Safety Instrumented System design for upstream Oil and Gas Industry (Case Study)
Student	Mr.Charlit Yoosamran
Student ID.	57601220
Degree	Master of Engineering
Program	Instrumentation Engineering
Year	2019
Thesis Advisor	Assoc.Prof.Sakreya Chitwong

Abstract

This paper has been compiled for people with an interest in the upstream oil and gas industry. It is an overview of the main processes control and safety instrumented system design for upstream oil and gas industry. A process control system is used to monitor data and control all equipment on the Wellhead Processing Platform (WPP). The purpose of this system is to read values from a large number of sensors, run programs to monitor the process and control valves etc. to control the process values, alarms are presented to the operator and command inputs accepted. The safety instrumented systems (SIS) is to take control and prevent an undesirable event when the process and the facility are no longer operating within normal operating conditions. The function of safety system is the part of the overall safety of a system that depends on the correct response of the safety system response to its inputs, including safe handling of operator errors, hardware failures and environmental changes (fires, lightning, etc.). The purpose of an SIS is to protect people, the environment, and assets from the consequences of accidents by reducing the probability of incidents occurring base on safety standard IEC61508 and IEC61511.

Keywords : Distributed Control System; Safety Instrumented Systems

กิตติกรรมประกาศ

การออกแบบระบบควบคุมกระบวนการและระบบวัดคุมนิรภัยสำหรับแท่นขุดเจาะน้ำมันและก๊าซ (กรณีศึกษา) สำเร็จลุลวงไปได้ เนื่องจากได้รับความกรุณาจากคณาจารย์ซึ่งคอยให้การสนับสนุนและให้ปรึกษาแนะนำแนวทางในการดำเนินงาน แนวทางในการแก้ไขปัญหาที่เกิดขึ้นในการทำโครงงานพิเศษซึ่งเป็นประโยชน์อย่างยิ่งในการจัดทำโครงงานพิเศษครั้งนี้

ขอขอบพระคุณ รศ.สักรียา ชิตวงศ์ และอาจารย์ประจำภาควิชาวิศวกรรมการวัดคุมทุกท่านเป็นอย่างสูง ซึ่งคอยให้คำแนะนำและให้คำปรึกษาในการแก้ไขปัญหาที่เกิดขึ้นในโครงงานพิเศษตลอดจนข้อแนะแนวต่างๆ

สุดท้ายนี้ขอขอบพระคุณ บิดา มารดา ภรรยา และอาจารย์ทุกท่านที่คอยให้การสนับสนุนคอยให้ความช่วยเหลือด้านต่างๆ และคอยเป็นกำลังที่สำคัญอย่างยิ่งในการจัดทำโครงงานพิเศษนี้ให้สำเร็จลุล่วงไปด้วยดี

นายชลิต อยู่สำราญ

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญรูป

หน้า

สารบัญรูป

หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

อุตสาหกรรมกระบวนการผลิตน้ำมันดิบและก๊าซธรรมชาตินั้นได้มีการใช้งานแท่นขุดเจาะและผลิต เพื่อสำหรับทำการผลิตน้ำมันดิบและก๊าซธรรมชาติ ซึ่งแท่นขุดเจาะและผลิตนี้นั้นจะมีกระบวนการในการขุดเจาะเพื่อสูบน้ำมันดิบและก๊าซธรรมชาติขึ้นมาจากใต้พื้นโลกและได้มีกระบวนการสำหรับแยกสิ่งต่างๆที่ไม่ต้องการใช้งาน เช่น น้ำ และ ทราย ออกมาจากน้ำมันดิบและก๊าซธรรมชาติ ซึ่งในระหว่างขั้นตอนการผลิตนี้นั้นได้มีการใช้งานระบบควบคุมแบบกระจายส่วน (Distributed Control System) สำหรับทำการควบคุมการทำงานของเครื่องจักรและอุปกรณ์ต่างๆ เพื่อทำให้ระบบการผลิตนั้นสามารถทำงานได้อย่างมีประสิทธิภาพ และนอกจากนี้ก็ได้มีการใช้งานระบบวัดคุมนิรภัย (Safety Instrumented System) สำหรับทำหน้าที่ในการควบคุมและยับยั้งเหตุการณ์อันตรายต่างๆที่อาจจะเกิดขึ้นในระหว่างกระบวนการผลิต เพื่อทำให้ระบบการผลิตนั้นอยู่ในสภาวะที่ปลอดภัยตลอดเวลาและพนักงานที่ปฏิบัติงานมีความปลอดภัยในการทำงาน รวมถึงอุปกรณ์ต่างๆ ที่อยู่ในกระบวนการผลิตไม่เสียหายและไม่ส่งผลกระทบต่อสิ่งแวดล้อมที่อยู่รอบๆ กระบวนการผลิต

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

วัตถุประสงค์ของการศึกษาเป็นการออกแบบระบบควบคุมกระบวนการแบบกระจายส่วน (Distributed Control System) และระบบวัดคุมนิรภัย (Safety Instrumented System) สำหรับแท่นขุดเจาะและผลิตน้ำมันดิบหรือก๊าซธรรมชาติ ตามมาตรฐานสากล IEC61508 และ IEC61511 เพื่อศึกษาวิธีการออกแบบและวีธีการทำงานของระบบควบคุมแบบกระจายส่วนและระบบวัดคุมนิรภัยที่ทำงานร่วมกันในระบบการผลิต จากที่ได้ศึกษาบทวิจัยพบว่าเป็นการวิจัยแบบกรณีศึกษาเท่านั้น ซึ่งผู้ที่สนใจสามารถใช้วิธีการและแนวทางความรู้ดังกล่าวไปประยุกต์ใช้งานในวงการอุตสาหกรรมที่เกี่ยวข้องต่อไปได้

1. เพื่อศึกษาวิธีการออกแบบและหลักการทำงานของระบบควบคุมแบบกระจายส่วน (Distributed Control System) สำหรับแท่นขุดเจาะและผลิตปิโตรเลียม

2. เพื่อศึกษาวิธีการออกแบบและหลักการทำงานของระบบวัดคุมนิรภัย (Safety Instrumented System) สำหรับแท่นขุดเจาะและผลิตปิโตรเลียมตามมาตรฐานสากล IEC61508 และ IEC 61511

1.3 สมมุติฐานของการศึกษา

1. การทำงานของระบบควบคุมแบบกระจายส่วน (Distributed Control System) จะช่วยทำให้ระบบการผลิตน้ำมันดิบหรือก๊าซธรรมชาติทำงานได้อย่างมีประสิทธภาพ โดยมีการแสดงผลค่าพารามิเตอร์ต่างๆที่จำเป็นต่อการควบคุมเพื่อให้ผู้ใช้งานได้ทราบข้อมูลและสั่งงานอุปกรณ์ต่างๆที่อยู่ในกระบวนการผลิตได้ตลอดเวลา

2. การทำงานของระบบวัดคุมนิรภัย (Safety Instrumented System) จะมีฟังก์ชั่นนิรภัย (Safety Instrument Function) สำหรับช่วยควบคุมและยับยั้งเหตุการณ์อันตรายต่างๆ ที่อาจจะเกิดขึ้นในระหว่างกระบวนการผลิตให้อยู่ในสภาวะที่ปลอดภัยโดยอ้างอิงตามค่าระดับความปลอดภัย (Safety Integrity Level) ที่ได้ออกแบบไว้ในตอนเริ่มต้นของโครงการ

1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย

การทำวิจัยครั้งนี้เริ่มขึ้นจากการศึกษาวิธีการออกแบบและหลักการทำงานของระบบควบคุมในกระบวนการผลิตน้ำมันดิบและก๊าซธรรมชาติซึ่งจะทำงานร่วมกันกับระบบวัดคุมนิรภัย โดยระบบได้ใช้การจำลองค่าพารามิเตอร์ต่างๆ หรือฟังก์ชั่นนิรภัยต่างๆตามข้อมูลเอกสาร ซึ่งเหตุการณ์จริงอาจไม่ได้เป็นไปตามข้อมูลเอกสารทั้งหมดเพื่อเป็นกรณีศึกษาสำหรับผู้ที่สนใจหรือผู้ที่เริ่มต้นทำงานในวงการอุตสากรรมที่เกี่ยวข้อง

1.5 ขอบเขตการวิจัย

ในการออกแบบระบบควบคุมกระบวนการแบบกระจายส่วน (Distributed Control System) และระบบวัดคุมนิรภัย (Safety Instrumented System) ได้มีการอ้างอิงตามมาตรฐานสากล IEC 61508 และ IEC 61511 โดยได้มีส่วนของการแสดงผลที่เป็นกราฟฟิกซึ่งจะแสดงค่าพารามิเตอร์ต่างๆ และสถานะการทำงานของเครื่องจักรที่จำเป็นต่อการควบคุมกระบวนการจึงทำให้ผู้ใช้งานได้ทราบถึงข้อมูลของกระบวนการผลิต ณ เวลาขณะนั้นเพื่อทำการวิเคราะห์ข้อมูลและสามารถสั่งงานเครื่องจักรทำงานได้อย่างมีประสิทธิภาพ ซึ่งการจำลองระบบควบคุมแบบกระจายส่วนนั้นได้มีการใช้งานโปรแกรม Centum VP R5.04 และการจำลองระบบวัดคุมนิรภัยได้ใช้โปรแกรม ProSafe-RS R3.02 ของบริษัทโยโกกาวา สำหรับช่วยในการออกแบบฟังก์ชั่นและพัฒนาระบบการทำงานเพื่อทำการทดลองและเก็บผลการทดลอง และนำมาวิเคราะห์เพื่อสรุปผลต่อไป

1.6 ขั้นตอนของการศึกษา

ขั้นตอนที่ 1 ศึกษาค้นคว้าทฤษฎีระบบระบบควบคุมแบบกระจายส่วน (Distributed Control System) ที่ใช้งานและแสดงผลการทำงานของเครื่องจักรในระบบกระบวนการผลิตของแท่นจุดเจาะและผลิตน้ำมันดิบ

ขั้นตอนที่ 2 ศึกษาค้นคว้าทฤษฎีระบบวัดคุมนิรภัย (Safety Instrumented System) ที่ใช้งานและแสดงผลสถานะการทำงานของฟังก์ชั่นนิรภัยต่างๆ ในระบบกระบวนการผลิตของแท่นจุดเจาะและผลิตปิโตรเลียม ตามมาตรฐานสากล IEC 61508 และ IEC 61511

ขั้นตอนที่ 3 ทำการออกแบบระบบควบคุมแบบกระจายส่วน (Distributed Control System) ในส่วนของการแสดงผลค่าพารามิตเตอร์และแสดงสถานะการทำงานของเครื่องจักรและอุปกรณ์ต่างๆ ในกระบวนการผลิต

ขั้นตอนที่ 4 ทำการออกแบบระบบวัดคุมนิรภัย (Safety Instrumented System) ในส่วนของการกำหนดค่าระดับความปลอดภัย (Safety Integrity Level) ให้กับฟังก์ชั่นนิรภัย (Safety Instrument Function) ที่ใช้งานในกระบวนการผลิต

ขั้นตอนที่ 5 ทำการจำลองการทำงานของระบบควบคุมแบบกระจายส่วน (Distributed Control System) ที่ทำงานร่วมกับระบบวัดคุมนิรภัย (Safety Instrumented System)

ขั้นตอนที่ 6 สรุปงานวิจัยและแนวทางในการพัฒนาต่อไป

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 งานวิจัยที่เกี่ยวข้อง

ในอุตสาหากรรมแท่นขุดเจาะและผลิตน้ำมันดิบและก๊าซธรรมชาตินั้นจะต้องมีการวัดและควบคุมตัวแปรต่างๆ เช่น การไหล (Flow), ระดับ (Level), ความดัน (Pressure) และอุณหภูมิให้อยู่ในค่าที่ต้องการและเพื่อทำให้ผลิตภัณฑ์ที่ได้มีคุณสมบัติตามที่ต้องการ ดังนั้นเพื่อทำให้บรรลุวัตถุประสงค์ในการควบคุมตัวแปรต่างๆเหล่านี้ จึงต้องมีการจัดเตรียมระบบการวัดและควบคุมขึ้นในกระบวนการผลิตซึ่งจะเห็นได้ว่าฟังก์ชันการควบคุมนั้น ผู้ใช้งานสามารถทำการเปลี่ยนแปลงค่า Set point ได้ตามที่ต้องการเพื่อสั่งงานไปยังอุปกรณ์ควบคุมตัวสุดท้าย (Final Element) ให้มีการทำงานอยู่ตลอดเวลา ซึ่งเมื่อมีการใช้งานไปในระยะเวลานานๆก็อาจทำให้เกิดการสึกหรอหรือเกิดการผิดปกติขึ้นในอุปกรณ์การวัดและควบคุมและอาจจะส่งผลทำให้ค่าตัวแปรที่ต้องการควบคุมนั้นไม่สามารถควบคุมได้หรืออาจทำให้ค่าตัวแปรในกระบวนการผลิตมีค่าสูงกว่าที่อุปกรณ์ในกระบวนการจะทนได้ ซึ่งเหตุการณ์นี้อาจทำให้เกิดการรั่วไหลของน้ำมันดิบและก๊าซธรรมชาติออกมายังภายนอกและอาจทำให้เกิดการลุกไหม้หรืออาจจะทำให้เกิดอันตรายต่อผู้ปฏิบัติงานที่อยู่ในบริเวณนั้น, เกิดความเสียหายต่อทรัพย์สินหรืออุปกรณ์ต่างๆ หรือเกิดความเสียหายต่อสิ่งแวดล้อมภายนอกได้

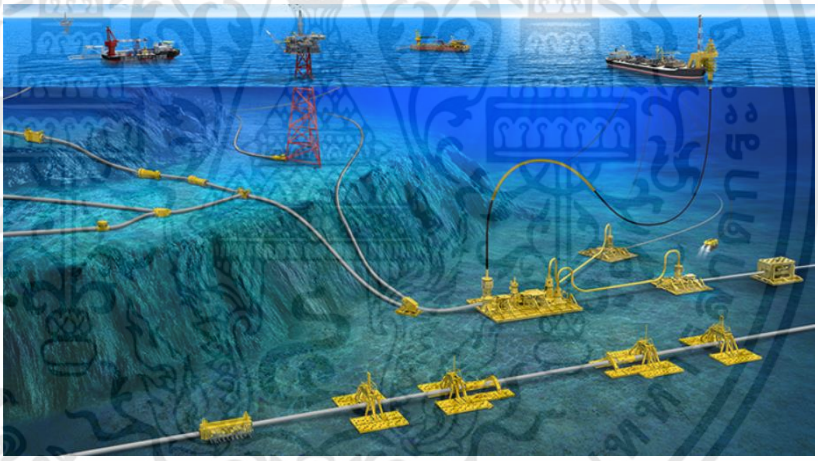
ด้วยเหตุนี้การป้องกันหรือการยับยั้งการเกิดเหตุการณ์เหล่านี้สามารถทำได้โดยการติดตั้งระบบป้องกัน (Protection System) เข้าไปในระบบการผลิต เช่น ระบบวัดคุมนิรภัย (Safety Instrumented System) เป็นต้น ซึ่งจะมีอุปกรณ์ทางไฟฟ้า,ทางอิเล็กทรอนิกส์และการโปรแกรมอิเล็กทรอนิกส์สำหรับฟังก์ชันนิรภัย (Safety Instrument Function) เป็นส่วนประกอบของระบบตามมาตรฐานสากล IEC 61508 และ IEC 61511

2.2 ทฤษฎี

2.2.1 การผลิตปิโตรเลียมของแท่นขุดเจาะและผลิต (Wellhead Processing Platform)

การผลิตปิโตรเลียมของแท่นขุดเจาะและผลิต (Wellhead Processing Platform) ดังรูปที่ 2.1 นั้นจะมีกระบวนการหลักๆคือการสูบปิโตรเลียมขึ้นมาจากหลุมผลิตต่างๆ ผ่านระบบท่อใต้ทะเลดังรูปที่ 2.2 เพื่อส่งปิโตรเลียมขึ้นมาเข้ากระบวนการผลิตที่อยู่บนแท่นขุดเจาะและผลิต

รูปที่ 2.1 แท่นขุดเจาะและผลิต (Wellhead Processing Platform)
ที่มา : Google (2H)



รูปที่ 2.2 ระบบท่อใต้ทะเล (Subsea Pipline)
ที่มา : Google (Oil States)

ซึ่งก่อนที่จะถูกนำมาใช้ประโยชน์ในรูปของน้ำมันดิบ, ก๊าซธรรมชาติ และก๊าซธรรมชาติเหลวได้นั้น จะต้องนำมาผ่านขบวนการผลิตต่างๆ เพื่อให้ได้ผลิตภัณฑ์ที่มีคุณสมบัติตรงตามความต้องการเสียก่อน ขบวนการผลิตน้ำมันดิบและก๊าซธรรมชาติโดยทั่วไปตามแหล่งต่างๆ ทั้งบนบกและในทะเลจะประกอบด้วยระบบต่างๆ ดังนี้คือ

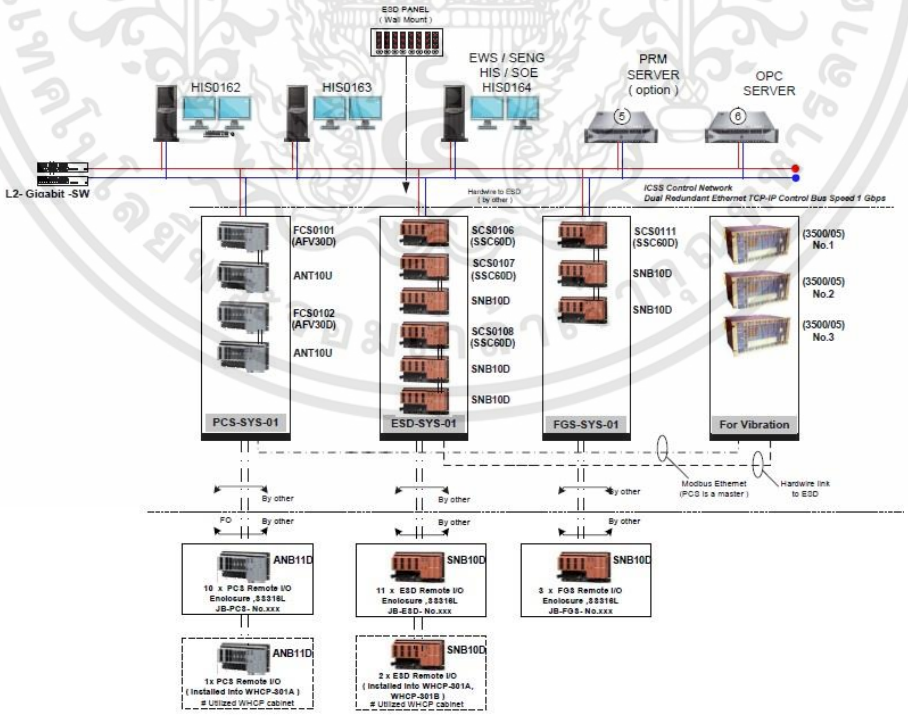
- ระบบแยกสถานะ (Gas/Liquid Separator)
- ระบบเพิ่มแรงดันก๊าซ (Gas Compression)
- ระบบดูดความชื้นก๊าซ (Gas Dehydration)

- ระบบคงสภาพก๊าซธรรมชาติเหลว (Condensate Stabilizer)
- ระบบคงสภาพและกักเก็บน้ำมันดิบ (Crude/oil Tank System)
- ระบบบำบัดน้ำทิ้ง (Water Treatment & Disposal System)
- ระบบมาตรวัด (Metering)

ปิโตรเลียมจากหลุมผลิตถูกส่งไปแยกสถานะที่ระบบแยกสถานะเพื่อทำการแยกก๊าซธรรมชาติเหลว น้ำมันและน้ำออกจากกันซึ่งก๊าซที่ได้จะถูกส่งไปเพิ่มแรงดันและดูดความชื้นที่ระบบเพิ่มแรงดันก๊าซและระบบดูดความชื้นก๊าซตามลำดับ ก่อนที่จะทำการซื้อขายโดยผ่านระบบมาตรวัดก๊าซ ส่วนก๊าซธรรมชาติเหลวหรือน้ำมันที่ได้จากระบบแยกสถานะจะถูกส่งไปยังระบบคงสภาพ ก่อนที่จะส่งไปกักเก็บเพื่อรอการขนถ่าย น้ำที่ผลิตได้ทั้งหมดจากขบวนการผลิตจะถูกส่งไปบำบัดเพื่อให้ได้มาตรฐานน้ำทิ้งก่อนปล่อยลงสู่ทะเล หรืออัดกลับลงไปในหลุมเพื่อให้มีผลกระทบต่อสิ่งแวดล้อมน้อยที่สุด

2.2.2 ระบบควบคุมแบบกระจายส่วน (Distributed Control System)

ระบบควบคุมแบบกระจายส่วน (Distributed Control System) นั้นเป็นระบบการควบคุมพื้นฐาน (Basic Process Control System: BPCS) ที่ใช้งานกันอย่างกว้างขวางสำหรับอุตสาหกรรมกระบวนการผลิตน้ำมันดิบและก๊าซธรรมชาติ ซึ่งสามารถแสดงตัวอย่างโครงสร้างของระบบควบคุมดังรูปที่ 2.3



รูปที่ 2.3 โครงสร้างของระบบควบคุมแบบกระจายส่วน

จากรูปที่ 2.3 ระบบควบคุมแบบกระจายส่วน (Distributed Control System) จะเป็นระบบที่ใช้สำหรับควบคุมการทำงานกระบวนการผลิตน้ำมันดิบและก๊าซธรรมชาติโดยผ่านอุปกรณ์เครื่องมือวัดไฟฟ้าและอุปกรณ์อื่นๆ ในกระบวนการผลิตเพื่อให้กระบวนการผลิตทำงานเป็นไปตามที่ได้ออกแบบไว้ โดยจะมีส่วนประกอบหลักๆ ดังต่อไปนี้

2.2.2.1 อุปกรณ์การวัด (Sensing Device) เป็นอุปกรณ์ที่ใช้สำหรับเปลี่ยนตัวแปรต่างๆ ในกระบวนการผลิต (Process Parameter) เช่น อัตราการไหลในกระบวนการ, ระดับของไหลในถัง, ความดันที่จุดต่างๆในกระบวนการ, อุณหภูมิตามจุดต่างๆที่อยู่ในกระบวนการให้เป็นสัญญาณกระแสไฟฟ้ามาตรฐาน 4-20 mA ที่แรงดันไฟฟ้ากระแสตรง 24 VDC หรือสัญญาณมาตรฐานชนิดอื่นๆ เพื่อส่งข้อมูลของตัวแปรต่างๆไปยังอินพุตของตัวควบคุม (Controller) และใช้แสดงค่าที่หน่วยแสดงผลอุปกรณ์การวัดต่อไป

2.2.2.2 ตัวควบคุม (Controller) เป็นส่วนใช้สำหรับประมวลผลโดยตัวควบคุมจะประกอบด้วยอุปกรณ์หลักๆ ดังนี้เช่นแหล่งจ่ายพลังงาน (Power Supply), ตัวประมวลผลกลาง (Central Processing Unit), ส่วนรับส่งสัญญาณ (Input and Output Cards) ส่วนการติดต่อสื่อสาร (Communication Port) และโปรแกรมที่ใช้ในการควบคุมกระบวนการผลิต (Control Function) ซึ่งตัวควบคุมในระบบการควบคุมพื้นฐานจะมีให้เลือกใช้งานอยู่หลายชนิดซึ่งจะขึ้นอยู่กับความต้องการในการควบคุม เช่น การควบคุมแบบปิดเปิด (On-Off Control) หรือ การควบคุมแบบ PID (Proportional-Intregral-Derivative Control) เป็นต้น

2.2.2.3 อุปกรณ์สุดท้าย (Final Element) เป็นอุปกรณ์ที่ใช้สำหรับเปลี่ยนสัญญาณไฟฟ้ามาตรฐาน 4-20 mA จากเอาต์พุตของตัวควบคุมไปเป็นการควบคุมตัวแปรกระบวนการผลิต ตัวอย่างของอุปกรณ์สุดท้ายจะเป็น วาล์วควบคุม (Control Valve) ซึ่งจะทำการเปิดและปิดของไหลตามสัญญาณเอาต์พุตของตัวควบคุม

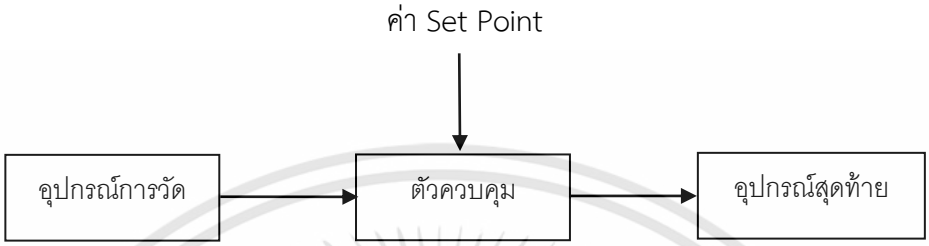
2.2.2.4 เครือข่ายสื่อสารหลัก (Backbone Network) เป็นระบบสื่อสารหลักที่ใช้ในการส่งผ่านข้อมูลระหว่างอุปกรณ์ต่างๆ ของระบบควบคุม ซึ่งในปัจจุบันเครือข่ายสื่อสารหลักของระบบควบคุมการผลิตสามารถสื่อสารที่อัตราความเร็วสูงถึง 1Gb

2.2.2.5 ส่วนการติดต่อกับผู้ปฏิบัติการ (Human Machine Interface) จะเป็นส่วนที่ใช้สำหรับแสดงแผนภาพ (Graphic Display) กระบวนการผลิตและแสดงค่าตัวแปรต่างๆ ของกระบวนการผลิตสำหรับใช้เป็นส่วนติดต่อหรือรับคำสั่งจากผู้ปฏิบัติงานในการควบคุมระบบการผลิตและนอกจากนี้ยังใช้เป็นส่วนแสดงสัญญาณเตือนต่างๆที่มาจากหน่อยการควบคุมอื่นๆ เช่น ระบบวัดคุมนิรภัยและระบบตรวจจับไฟไหม้และก๊าซรั่ว เป็นต้น

2.2.2.6 ส่วนพิมพ์รายงาน (Printer) เป็นเครื่องพิมพ์ส่วนกลางที่ติดตั้งอยู่บนเครือข่ายหลักเพื่อสำหรับใช้ในการพิมพ์รายงานหรือสัญญาณเตือนต่างๆในระบบการผลิต

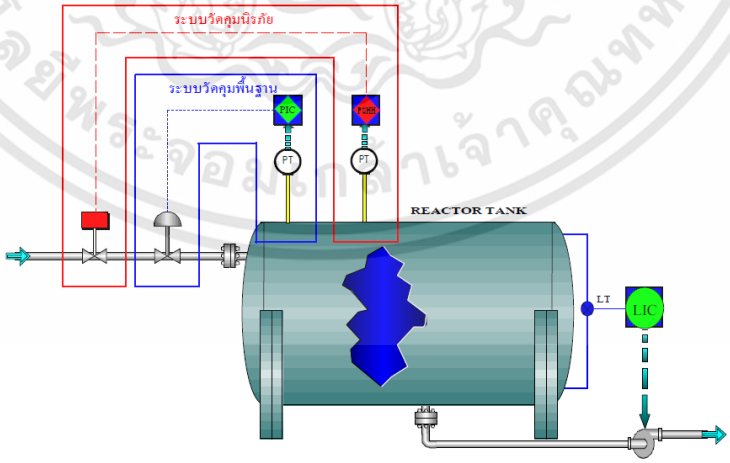
2.2.2.7 Engineering Unit เป็นหน่วยที่ใช้ในการกำหนดคำสั่งการทำงาน โดยหน่วยนี้จะมีความจำเป็นตั้งแต่เริ่มทำโครงการสร้างระบบควบคุมการผลิตตลอดไปจนถึงการซ่อมบำรุงระบบการ

ในการควบคุมตัวแปรต่างๆในกระบวนการผลิตนั้นสามารถแบ่งการควบคุมย่อยๆออกได้เป็นฟังก์ชันควบคุม (Control Function) ซึ่งในกระบวนการหนึ่งๆ จะมีฟังก์ชันการควบคุมได้หลายฟังก์ชัน ซึ่งแต่ละฟังก์ชันการควบคุมจะประกอบไปด้วยอุปกรณ์พื้นฐาน 3 ส่วนดังนี้ อุปกรณ์การวัด (Sensing Element), ตัวควบคุม (Controller) และอุปกรณ์สุดท้าย (Final Element) ดังแสดงในรูปที่ 2.4



รูปที่ 2.4 ฟังก์ชันการควบคุม
ที่มา : ชาญวิทย์ (2553)

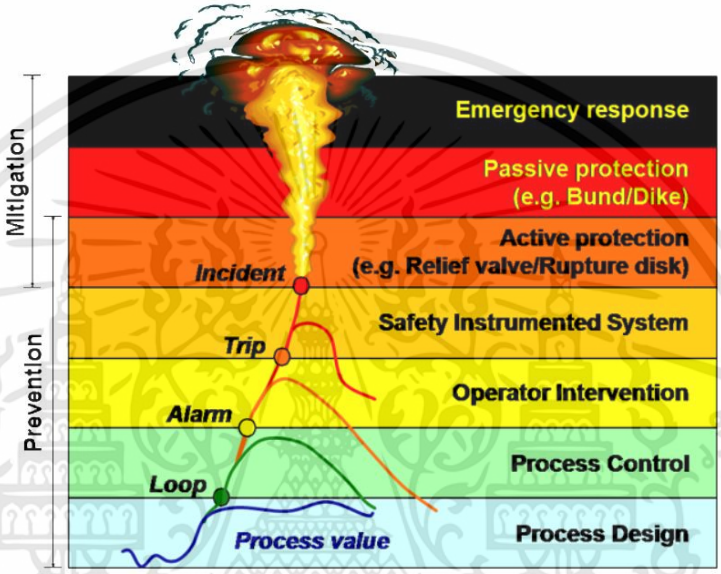
จากรูปที่ 2.4 ผู้ปฏิบัติงานสมารถควบคุมตัวแปรของกระบวนการผลิตได้ด้วยการปรับค่า Set Point ที่ตัวควบคุม จากนั้นตัวควบคุมจะทำการอ่านค่าตัวแปรที่มาจากอุปกรณ์การวัดแล้วจากนั้นตัวควบคุมจะทำการเปรียบเทียบค่าที่วัดได้กับค่า Set Point ซึ่งถ้าหากว่าค่าที่อ่านได้จากอุปกรณ์การวัดมีค่ามากกว่าหรือน้อยกว่าค่า Set Point ตัวควบคุมจะส่งสัญญาณไปยังอุปกรณ์สุดท้ายให้ทำการปรับค่าตัวแปรกระบวนการจนกระทั่งตัวแปรที่อ่านได้จากอุปกรณ์การวัดมีค่าเท่ากับ Set Point ที่กำหนด ตัวอย่างฟังก์ชันการควบคุมความดันและระดับแสดงได้ดังรูปที่ 2.5



รูปที่ 2.5 ฟังก์ชันการควบคุมความดันและระดับ
ที่มา : สุนทร (2552)

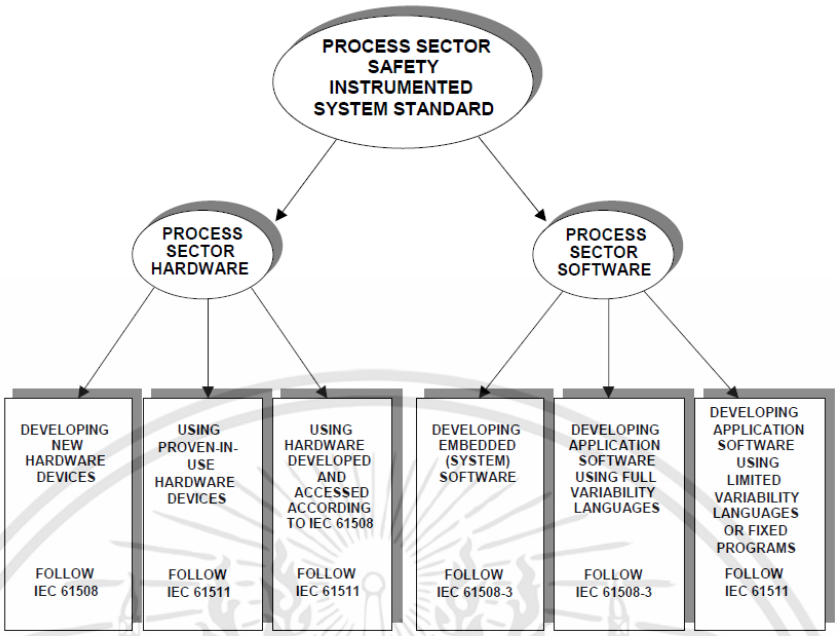
2.2.3 มาตรฐานระบบวัดคุมนิรภัย (Safety Instrumented System Standard)

ในกระบวนการผลิตน้ำมันดิบและก๊าซธรรมชาตินั้นมีความเสี่ยงและโอกาสที่จะเกิดสภาวะอันตรายได้สูงอันเนื่องมาจากขั้นตอนในการผลิตซึ่งอาจก่อให้เกิดความเสียหายต่อทุกๆส่วนที่เกี่ยวข้อง เช่น อาจก่อให้เกิดอันตรายกับผู้ปฏิบัติงาน, เกิดความเสียหายต่ออุปกรณ์ต่างๆในกระบวนการผลิต และอาจส่งผลกระทบต่อสิ่งแวดล้อมดังแสดงในรูปที่ 2.6



รูปที่ 2.6 ชั้นการป้องกันเหตุการณ์อันตรายในกระบวนการผลิต
ที่มา : Google (AIChE)

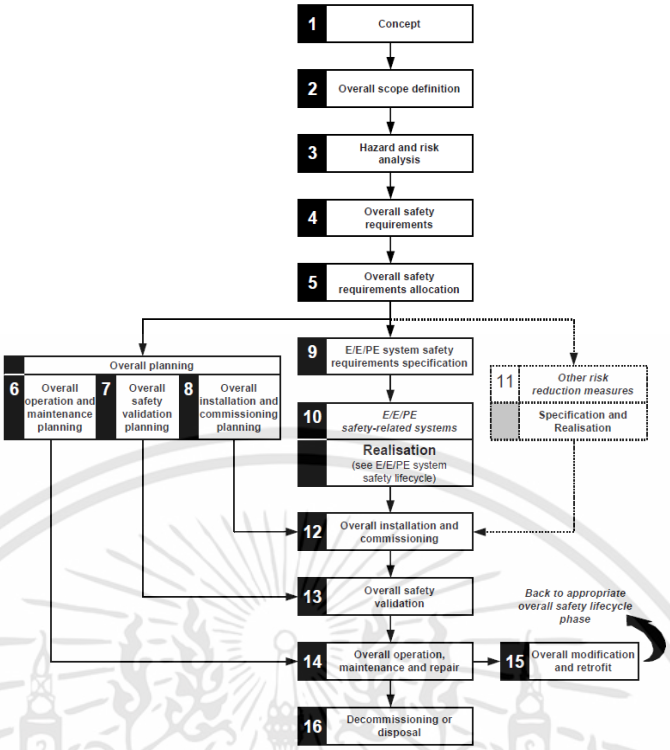
ดังนั้นจึงมีการทำให้ความเสี่ยงที่จะเกิดเหตุการณ์อันตรายเหล่านี้ลดลงอยู่ในค่าที่ยอมรับได้ ซึ่งระบบวัดคุมนิรภัยจึงเป็นทางเลือกที่จะนำมาใช้งานในการทำให้ความเสี่ยงลดลงอยู่ในค่าที่ยอมรับได้ ดังนั้นระบบวัดคุมนิรภัยที่จะนำมาใช้งานจึงต้องมีความน่าเชื่อถือสูง (High Reliability) และทำงานได้อย่างถูกต้องตามที่ได้ออกแบบไว้ ซึ่งมาตรฐานสำหรับการออกแบบระบบวัดคุมนิรภัยที่ครอบคลุมตั้งแต่ขั้นตอนการออกแบบไปจนถึงขั้นตอนการใช้งานนั้นก็คือมาตรฐานสากล IEC 61508 และ IEC 61511 ดังแสดงในรูปที่ 2.7



รูปที่ 2.7 การใช้งานมาตรฐานสากล IEC61508 และ IEC 61511

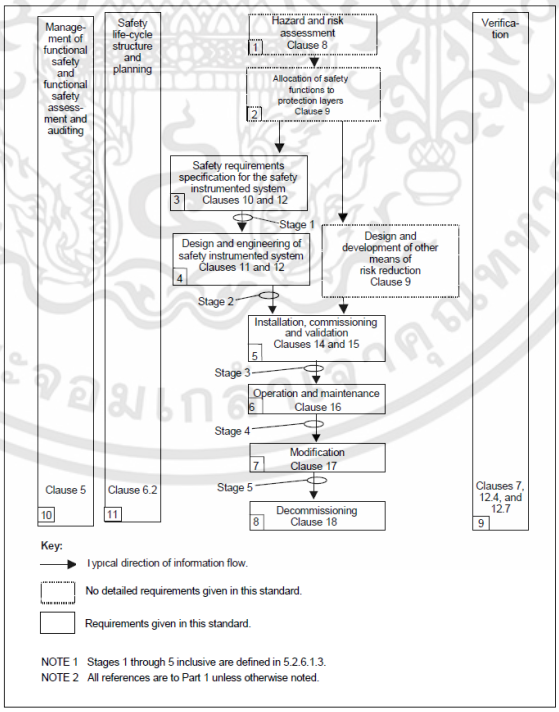
ที่มา : มาตรฐาน IEC 61511 Part 1 (2003)

มาตรฐานสากล IEC 61508 และ IEC 61511 ได้กำหนดลำดับขั้นตอนสำหรับการออกแบบระบบวัดคุมนิรภัยที่มีส่วนประกอบทางอิเล็กทรอนิกส์และโปรแกรมทางอิเล็กทรอนิกส์ (Electrical/Electronic/Programmable Electronic Systems: E/EPESs) ลำดับขั้นตอนดังกล่าวจะเรียกว่า วงรอบความปลอดภัย (Safety Life Cycle) ดังแสดงในรูปที่ 2.8 และรูปที่ 2.9 โดยวงรอบความปลอดภัยของมาตรฐาน IEC 61511 จะเริ่มตั้งแต่ขั้นตอนการกำหนดรายละเอียดของระบบวัดคุมนิรภัย ซึ่งจะแตกต่างจากมาตรฐาน IEC 61508 ที่จะเริ่มตั้งแต่การแสดงรายละเอียดการทำงานของระบบการผลิตและการกำหนดแหล่งกำเนิดสิ่งที่เป็นอันตราย เป็นต้น



รูปที่ 2.8 รูปวงรอบความปลอดภัยของมาตรฐานสากล IEC61508

ที่มา : มาตรฐาน IEC 61508 Part 1 (2010)



รูปที่ 2.9 รูปวงรอบความปลอดภัยของมาตรฐานสากล IEC61511

ที่มา : มาตรฐาน IEC 61511 Part 1 (2003)

2.2.4 การประเมินความเสี่ยงต่อเหตุการณ์อันตราย (Risk Assessment)

การประเมินความเสี่ยงของฟังก์ชันนิรภัยในระบบวัดคุมนิรภัยจะเป็นกิจกรรมหลักในเฟสที่ 3 บนวงรอบความปลอดภัยของมาตรฐานสากล IEC61508 ซึ่งจะเป็นการประเมินความเสี่ยงต่อเหตุการณ์อันตรายและผลกระทบที่อาจเกิดขึ้น อันเนื่องมาจากความผิดปกติของอุปกรณ์ภายใต้การควบคุมหรือในฟังก์ชันการคบคุม ซึ่งหลังจากการประเมินแล้วผลลัพธ์ที่ได้จะเป็นค่าระดับความปลอดภัยที่ถูกกำหนดให้กับฟังก์ชันนิรภัยนั้นต่อไป ซึ่งก่อนเริ่มทำการประเมินความเสี่ยงต่อเหตุการณ์อันตรายเพื่อกำหนดค่าระดับความปลอดภัยนั้นจำเป็นต้องทำความเข้าใจกับเป้าหมายและวัตถุประสงค์ของการประเมินเพื่อให้การตัดสินใจในขั้นตอนการประเมินมีประสิทธิภาพและถูกต้องมากที่สุด ซึ่งวัตถุประสงค์ของการประเมินนั้นก็เพื่อให้แน่ใจว่าระบบวัดคุมนิรภัยที่ออกแบบไว้นั้นสามารถทำให้โอกาสที่จะเกิดเหตุการณ์อันตรายและผลกระทบที่จะตามมานั้นลดลงได้เท่ากับเกณฑ์ความเสี่ยงที่ยอมรับได้ โดยวิธีการที่จะบรรลุวัตถุประสงค์ดังกล่าวนั้นสามารถแสดงได้ 3 ทางดังนี้

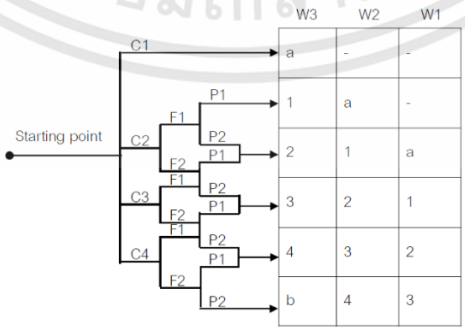
2.2.4.1 กำหนดหรือตั้งเกณฑ์ความเสี่ยงที่ยอมรับได้

2.2.4.2 ประเมินความเสี่ยงที่เกี่ยวข้องกับอุปกรณ์ภายใต้การควบคุม

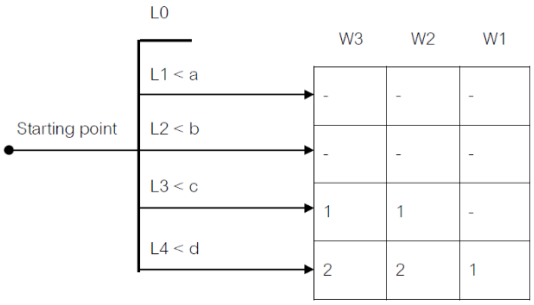
2.2.4.3 หาวิธีที่จะลดความเสี่ยงลงให้เท่ากับเกณฑ์ความเสี่ยงที่ยอมรับได้

2.2.5 กราฟความเสี่ยง (Risk Graph)

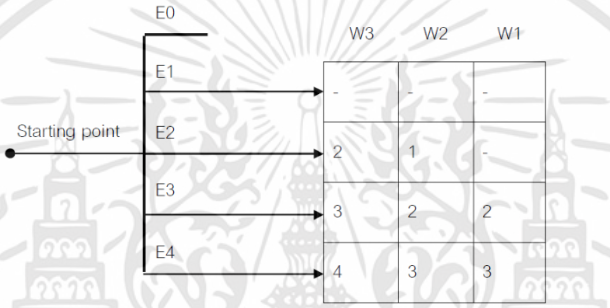
มาตรฐานสากล IEC61508 ได้นำเสนอแนงทางการประเมินความเสี่ยงต่ออันตรายโดยใช้กราฟความเสี่ยง (Risk Graph) เพื่อนำผลลัพธ์ที่ได้ไปทำการเลือกใช้หรือออกแบบระบบวัดคุมนิรภัยที่จะทำให้ความเสี่ยงต่อเหตุการณ์อันตรายลดลงอยู่ในค่าที่กำหนดโดยการประเมินนั้นจะกระทำในทุกๆ ฟังก์ชันนิรภัยซึ่งผลลัพธ์ที่ได้จากการประเมินจะเป็นค่าระดับความปลอดภัย (Safety Integrity Level) จะถูกกำหนดให้กับฟังก์ชันนิรภัยนั้นซึ่งกราฟความเสี่ยงนั้นจะประกอบด้วยกราฟที่สำคัญอยู่ 3 กราฟ คือ กราฟความสูญเสียต่อสิ่งมีชีวิต, กราฟความเสี่ยงสูญเสียต่อทรัพย์สิน และกราฟสูญเสียต่อสิ่งแวดล้อม ดังแสดงในรูปที่ 2.10, 2.11 และ 2.12 ตามลำดับ



รูปที่ 2.10 กราฟความสูญเสียต่อสิ่งมีชีวิต
ที่มา : ทวิช (2548)



รูปที่ 2.11 กราฟความสูญเสียต่อทรัพย์สิน
ที่มา : ทวิช (2548)



รูปที่ 2.12 กราฟความสูญเสียต่อสิ่งแวดล้อม
ที่มา : ทวิช (2548)

2.2.5.1 อัตราการเกิดเหตุการณ์ (Demand rate, W) ในที่นี้ได้แบ่งอัตราการเกิดเหตุการณ์ (W) ออกเป็น 3 ระดับ ดังนี้

W1 หมายถึง อัตราการเกิดเหตุการณ์ที่อาจเกิดขึ้นเมื่อเวลาเกิน 10 ปี แต่ไม่เกิน 100 ปี (Very low)

W2 หมายถึง อัตราการเกิดเหตุการณ์ที่อาจเกิดขึ้นในช่วงเวลา 1 ปี แต่ไม่เกิน 10 ปี (Low)

W3 หมายถึง อัตราการเกิดเหตุการณ์ที่อาจเกิดขึ้นในเวลาภายใน 1 ปี (High)

2.2.5.2 ผลกระทบต่อชีวิตคน (Consequences Concerning People, C) ในที่นี้ได้แบ่งผลการระทบต่อชีวิต (C) เป็น 4 ระดับ ดังนี้

C1 หมายถึง บาดเจ็บเล็กน้อย (Minor injury)

C2 หมายถึง บาดเจ็บมากหรือเสียชีวิตหนึ่งคน Serious permanent injury, death to one people

C3 หมายถึง เสียชีวิต 2-3 คน (Death to several people)

C4 หมายถึง เสียชีวิตหลายคน (Many People Killed)

2.2.5.3 ระยะเวลาในบริเวณอันตราย (Frequency of Exposure Time, F) ในที่นี้ได้แบ่งระยะเวลาในบริเวณอันตราย (F) เป็น 2 ระดับ ดังนี้

F1 หมายถึง การมีผู้ปฏิบัติงานและผู้เกี่ยวข้องอยู่ในบริเวณที่อาจจะเกิดเหตุการณ์น้อยกว่าครึ่งวัน (Half of the Around)

F2 หมายถึง การมีผู้ปฏิบัติงานและผู้เกี่ยวข้องอยู่ในบริเวณที่อาจจะเกิดเหตุการณ์มากกว่าครึ่งวัน (Always People Around)

2.2.5.4 การหลีกเลี่ยงจากบริเวณอันตราย (Possibility of Avoiding, P) ในที่นี้ได้แบ่งการหลีกเลี่ยงจากบริเวณอันตราย (P) เป็น 2 ระดับ ดังนี้

P1 หมายถึง สามารถที่จะหลีกเลี่ยงเหตุการณ์ที่จะเกิดขึ้นได้ (Possible Under Certain Conditions)

P2 หมายถึง ไม่สามารถที่จะหลีกเลี่ยงจากเหตุการณ์ที่จะเกิดขึ้นได้ (Almost Impossible)

2.2.5.5 ความสูญเสียต่อทรัพย์สิน (Asset & Production Loss, L) ความสูญเสียต่อทรัพย์สินรวมถึง ค่าใช้จ่ายที่ต้องทำการซ่อมหรือเปลี่ยน, ค่าแรงในการซ่อมหรือเปลี่ยนอุปกรณ์ ค่าสูญเสียผลผลิต และค่าสูญเสียคุณภาพของผลผลิต รวมทั้งค่าปรับที่ไม่สามารถส่งผลิตภัณฑ์ให้ลูกค้าได้ ในที่นี้ได้แบ่งความสูญเสียต่อทรัพย์สิน (L) เป็น 5 ระดับ

L0 หมายถึง ไม่มีการสูญเสีย (No Operation Upset/ No Damage to Equipment)

L1 หมายถึง สูญเสียเล็กน้อย (Minor Operation Upset/ Moderate Damage to Equipment)

L2 หมายถึง สูญเสียมากแต่ไม่ต้องหยุดกระบวนการผลิต (Moderate Operation Upset/ Major Damage to Equipment)

L3 หมายถึง สูญเสียมากและต้องหยุดกระบวนการผลิตช่วงเวลาสั้นๆ (Major Operation Upset / Major Damage to Equipment)

L4 หมายถึง สูญเสียมากและต้องหยุดกระบวนการผลิตเป็นเวลานาน (Major Damage to Essential Equipment)

2.2.5.6 ความเสียหายต่อสิ่งแวดล้อม (Environmental damage, E) ในที่นี้ได้แบ่งความเสี่ยหายต่อสิ่งแวดล้อม (E) เป็น 5 ระดับดังนี้

E0 หมายถึง ไม่มีผลกระทบต่อสิ่งแวดล้อม (No Release / No Effect)

E1 หมายถึง กระทบต่อสิ่งแวดล้อมเล็กน้อย (Release with Minor Damage to Environment)

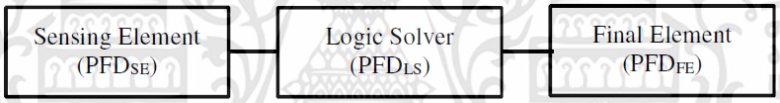
E2 หมายถึง กระทบต่อสิ่งแวดล้อมชั่วคราวอยู่ภายในขอบเขต
(Release within Fence Significant Damage to Environment)

E3 หมายถึง กระทบต่อสิ่งแวดล้อมชั่วคราวแต่ออกไปภายนอกขอบเขต (Release outside Fence Moderate with Temporary Damage to Environment)

E4 หมายถึง กระทบต่อสิ่งแวดล้อมถาวรและออกไปภายนอกขอบเขต (Release outside Fence Major with Permanent Major Damage to Environment)

2.2.6 ระบบวัดคุมนิรภัย (Safety Instrumented System)

ระบบวัดคุมนิรภัย (Safety Instrumented System) ได้ถูกนำมาใช้เพื่อควบคุมความเสี่ยงของกระบวนการผลิตที่ได้มีการวิเคราะห์ความเสี่ยงของกระบวนการผลิตมาแล้วซึ่งจะประกอบไปด้วยฟังก์ชันนิรภัย (Safety Function) สำหรับทำหน้าที่ในการป้องกันอันตราย ซึ่งฟังก์ชันนิรภัยนั้นจะประกอบไปด้วยส่วนสำคัญ 3 ส่วน ดังนี้ อุปกรณ์การวัด (Sensing Element), ส่วนประมวลผล (Logic Solver) และอุปกรณ์สุดท้าย (Final Element) ดังแสดงในรูปที่ 2.13



รูปที่ 2.13 ส่วนประกอบของฟังก์ชันนิรภัย
ที่มา : มาตรฐาน IEC 61508 Part 6 (2010)

โดยในแต่ละส่วนประกอบของฟังก์ชันนิรภัยนั้นจะมีค่าความผิดพลาดอันตราย (Dangerous Failure) ของตัวเองจากนั้นจะนำค่าความผิดพลาดอันตรายของอุปกรณ์ในทุกๆส่วนมารวมกัน ซึ่งผลลัพธ์ที่ได้นั้นต้องมีค่าเฉลี่ยความผิดพลาดอันตรายในระดับความปลอดภัยที่กำหนดในตอนเริ่มต้นโครงการโดยสามารถแสดงผลรวมค่าเฉลี่ยความผิดพลาดได้ดังสมการที่ (2.1)

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

เมื่อ

$PFD_{(AVG)}$ = ผลรวมค่าเฉลี่ยความผิดพลาดอันตรายของฟังก์ชันนิรภัย

$PFD_{(SE)}$ = ค่าเฉลี่ยความผิดพลาดอันตรายของอุปกรณ์การวัด

$PFD_{(LS)}$ = ค่าเฉลี่ยความผิดพลาดอันตรายของส่วนประมวลผล

$PFD_{(FE)}$ = ค่าเฉลี่ยความผิดพลาดอันตรายของอุปกรณ์สุดท้าย

2.2.7 ค่าระดับความปลอดภัย (Safety Integrity Level: SIL)

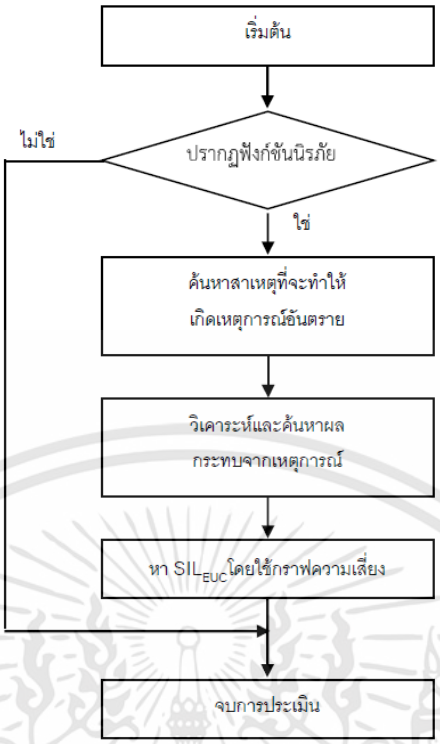
มาตรฐานสากล IEC61508 ได้มีการกำหนดค่าเฉลี่ยความผิดพลาดอันตรายของฟังก์ชันนิรภัยต่างๆที่อยู่ในระบบวัดคุมนิรภัย โดยค่าความปลอดภัยนั้นจะถูกแบ่งออกได้เป็น 4 ระดับ ตามช่วงค่าเฉลี่ยความผิดพลาดอันตรายของอุปกรณ์ในเวลาที่ต้องการ (Probability of a Failure on Demand: PFD) ซึ่งเวลาที่ต้องการนั้นเป็นสภาวะที่เกินจุดกำหนดความปลอดภัยของตัวแปรที่วัดได้จากกระบวนการผลิต ถ้าเวลาที่ต้องการเกิดขึ้นและระบบไม่สามารถทำงานได้ในเวลาที่กำหนดอันตรายจากเหตุการณ์นั้นก็จะเกิดขึ้น จากตาราง 2.1 จะแสดงค่าระดับความปลอดภัย 4 ระดับของการใช้งานในกระบวนการผลิตที่มีการเกิดเหตุการณ์อันตรายต่ำ (Low Demand Rate) ซึ่งเป็นสภาวะที่ใช้งานในอุตสาหกรรมการผลิตทั่วไป

ตาราง 2.1 ค่าระดับความปลอดภัยที่อัตราการเกิดเหตุการณ์อันตรายต่ำ
ที่มา : มาตรฐาน IEC 61508 Part 1 (2010)

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

2.2.8 การกำหนดค่าระดับความปลอดภัย (SIL Specification)

การกำหนดค่าระดับความปลอดภัยจำเป็นต้องทำความเข้าใจกับเป้าหมายและวัตถุประสงค์ของการประเมินเพื่อทำให้การตัดสินใจในขั้นตอนของการประเมินนั้นมีประสิทธิภาพและมีความถูกต้องมากที่สุด โดยในระหว่างขั้นตอนการประเมินนั้น เราจะต้องรู้ความผิดพลาดของอุปกรณ์ภายใต้การควบคุมที่อาจจะเกิดขึ้นและมีโอกาสจะก่อให้เกิดเหตุการณ์อันตรายต่อสิ่งมีชีวิตทรัพย์สิน และสิ่งแวดล้อมโดยแสดงลำดับขั้นตอนการประเมินความเสี่ยงดังรูปที่ 2.14 ซึ่งข้อมูลที่ได้นี้จะถูกวิเคราะห์และเก็บรวบรวมบันทึกไว้ในเอกสารการประเมินเพื่อนำไปใช้อ้างอิงสำหรับการออกแบบระบบวัดคุมนิรภัยต่อไป



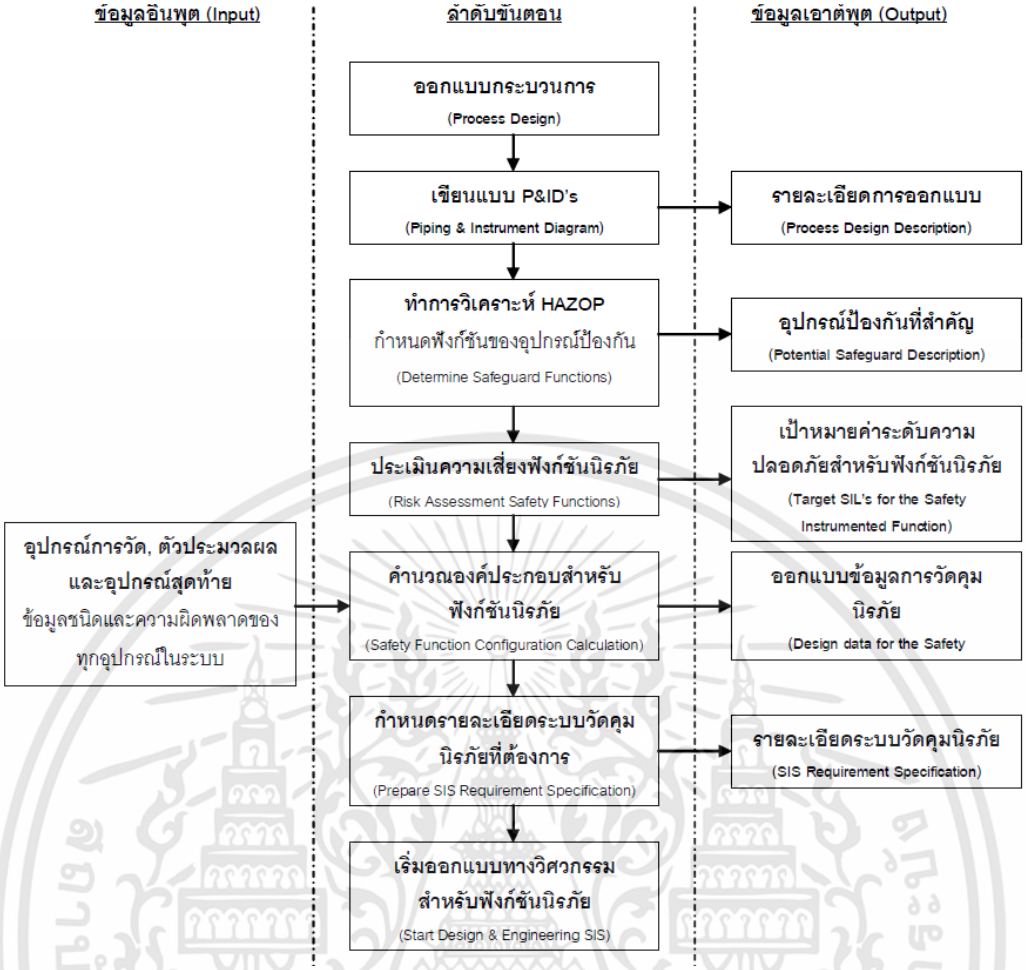
รูปที่ 2.14 ขั้นตอนการประเมินความเสี่ยง
ที่มา : ดัดแปลงมาจากชาญวิทย์ (2553)

2.2.9 การออกแบบระบบวัดคุมนิรภัย (Safety Instrumented System Design)

การออกแบบระบบวัดคุมนิรภัยดังแสดงในรูปที่ 2.15 นั้นจะมีข้อกำหนดต่างๆที่ต้องพิจารณาและต้องมีการกำหนดเป็นรายละเอียดสำหรับนำไปใช้งานในการปฏิบัติงานกับระบบวัดวัดคุมนิรภัย เพื่อทำให้ระบบนั้นสามารถทำงานได้ตามข้อกำหนดที่ต้องการ ซึ่งข้อกำหนดต่างๆที่ต้องพิจารณามีดังนี้

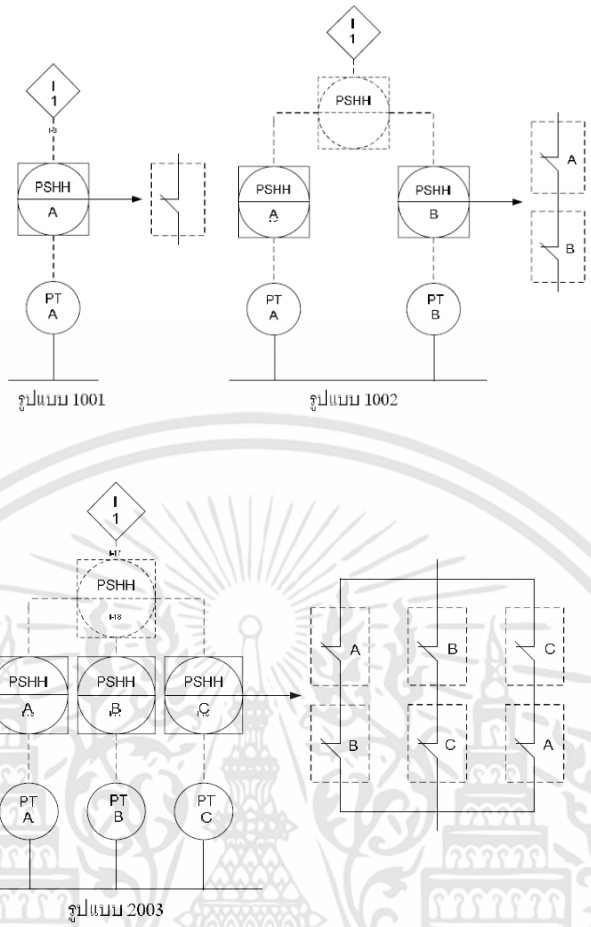
- ระบบนิรภัยต้องทำงานเร็วกว่าเวลาปลอดภัยของกระบวนการผลิต
- อุปกรณ์ทุกๆส่วนต้องทำงานอย่างสมบูรณ์
- การเปลี่ยนแปลงตัวแปรต่างๆต้องมีการป้องกันอย่างเพียงพอ

โดยขั้นตอนการออกแบบระบบวัดคุมนิรภัยนั้นจะเป็นการเลือกใช้รูปแบบและชนิดของอุกรณ์ต่างๆที่จะนำไปใช้งานเพื่อทำให้ระบบมีค่าระดับความปลอดภัยตรงกับความต้องการ ซึ่งในการออกแบบจะต้องพิจารณาตั้งแต่อุปกรณ์การวัด (Sensing Element) ไปจนถึงอุปกรณ์สุดท้าย (Final Element) จากนั้นนำค่าความผิดพลาดอันตรายของอุปกรณ์เหล่านั้นมารวมกันและค่าที่ได้นั้นจะต้องมีค่าน้อยกว่าค่าที่กำหนดไว้ในแต่ละระดับความปลอดภัย



รูปที่ 2.15 การออกแบบระบบวัดคุมนิรภัย
ที่มา : ชาญวิทย์ (2553)

2.2.9.1 อุปกรณ์การวัด (Sensing Element) อุปกรณ์การวัดสามารถเลือกใช้เหมือนกับระบบการควบคุมโดยทั่วไปแต่จะต้องมีคุณลักษณะที่เหมาะสมกับค่าระดับความปลอดภัยของฟังก์ชันนิรภัยที่ได้ออกแบบไว้ตอนเริ่มต้นโครงการด้วย ซึ่งอุปกรณ์ที่มีการใช้งานนั้นจะมีอยู่ 2 รูปแบบให้ผู้ใช้ได้เลือกใช้งาน คือ อุปกรณ์ Type A และอุปกรณ์ Type B โดยอุปกรณ์ Type A นั้นเป็นอุปกรณ์การวัดที่เป็นแบบต่อเนื่องทั่วไป โดยสามารถใช้งานได้เป็นเวลานานและสามารถทำการทดสอบได้อย่างสมบูรณ์ เช่น สวิตช์ระดับ (Level Switch) หรือ สวิตช์ความดัน (Pressure Switch) ส่วนอุปกรณ์ Type B นั้นเป็นอุปกรณ์การวัดที่ไม่สามารถใช้งานได้เป็นเวลานานและไม่สามารถทำการทดสอบได้อย่างสมบูรณ์ เช่น อุปกรณ์การวัดแบบชาญฉลาด (Smart Transmitter) นอกจากนี้เรายังสามารถจัดรูปแบบอุปกรณ์การวัดที่เป็นรูปแบบพื้นฐานดังแสดงในรูปที่ 2.16 ได้ดังนี้



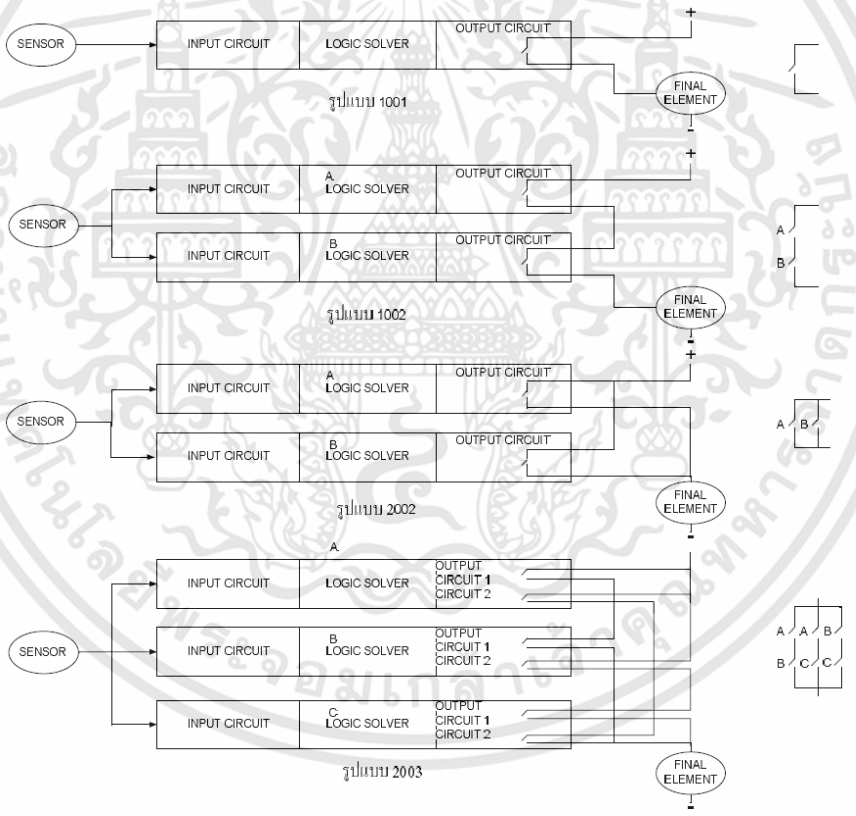
รูปที่ 2.16 รูปแบบของอุปกรณ์การวัด
ที่มา : ทวิช (2548)

2.2.9.1.1 อุปกรณ์การวัดรูปแบบ 1oo1 (One out of One Voting) ใช้อุปกรณ์ในการวัดหนึ่งตัวเท่านั้นแล้วนำไปใช้งานรวมกับระบบวัดคุมนิรภัย ดังแสดงในรูปที่ 2.16 การวัดรูปแบบนี้เป็นรูปแบบพื้นฐานสำหรับระบบวัดคุมนิรภัย โดยการทำงานนั้นถ้าอุปกรณ์การวัดทำการตรวจจับความผิดปกติได้หรือถึงจุดที่อุปกรณ์การวัดทำงานตามที่ได้กำหนดไว้ก็จะทำให้ระบบวัดคุมนิรภัยทำงานทันที

2.2.9.1.2 อุปกรณ์การวัดรูปแบบ 1oo2 (One out of Two Voting) ใช้อุปกรณ์ในการวัดสองตัวแล้วนำไปใช้งานรวมกับระบบวัดคุมนิรภัย ดังแสดงในรูปที่ 2.16 การวัดรูปแบบนี้เป็นการใช้อุปกรณ์การวัดสองตัวต่อร่วมกันแบบอนุกรม โดยการทำงานนั้นถ้าอุปกรณ์ตัวใดตัวหนึ่งวัดค่าความผิดปกติได้หรือถึงจุดทำงานที่กำหนดไว้ก็จะทำให้ระบบวัดคุมนิรภัยทำงานทันที แต่ถ้าเกิดความผิดพลาดอันตรายในตัวอุปกรณ์การวัดตัวใดตัวหนึ่งและระบบวัดคุมนิรภัยไม่สามารถตรวจจับความผิดพลาดที่เกิดขึ้นนั้นได้ก็ยังมีอุปกรณ์การวัดอีกหนึ่งตัวที่ยังคงทำหน้าที่ต่อไปได้

2.2.9.1.3 อุปกรณ์การวัดรูปแบบ 2oo3 (Two out of Three Voting) ใช้อุปกรณ์ในการวัดสามตัวแล้วนำไปใช้งานรวมกับระบบวัดคุมนิรภัย ดังแสดงในรูปที่ 2.16 การวัดรูปแบบนี้เป็นการใช้อุปกรณ์การวัดสามตัวต่อร่วมกันแบบอนุกรม และขนานกัน โดยการทำงานเป็นแบบลงมติ (Voting) ระบบวัดคุมนิรภัยจะทำงานก็ต่อเมื่ออุปกรณ์การวัดสองตัววัดค่าความผิดปกติได้ แต่ถ้าเกิดความผิดพลาดอันตรายในอุปกรณ์การวัดตัวใดตัวหนึ่งและระบบวัดคุมนิรภัยไม่สามารถตรวจจับความผิดพลาดนั้นได้จะมีอุปกรณ์ตัวที่สองและตัวที่สามยังคงทำหน้าที่ต่อไปได้

2.2.9.2 ส่วนประมวลผล (Logic Solver) ระบบวัดคุมนิรภัยจะใช้ Safety Controller เป็นตัวประมวลผลซึ่งจะมีการใช้งานร่วมกับฟังก์ชันนิรภัยที่มีค่าระดับความปลอดภัยที่แตกต่างกัน ดังนั้นส่วนประมวลผลจะถูกเลือกใช้ที่ค่าระดับความปลอดภัยสูงสุด โดยจะมีรูปแบบของตัวประมวลผลดังแสดงในรูปที่ 2.17



รูปที่ 2.17 รูปแบบของตัวประมวลผล
ที่มา : IEC-61511

2.2.9.2.1 ตัวประมวลรูปแบบ 1oo1 (One out of One Voting) รูปแบบนี้จะเป็นระบบประมวลผลที่มีเพียงชุดเดียว ดังแสดงในรูปที่ 2.17 โดยชุดระบบประมวลผลประกอบด้วยตัวประมวลผล (Central Processing Unit) ส่วนรับสัญญาณ (Input) และส่วนขับสัญญาณ (Output) รูปแบบ 1oo1 จะเป็นรูปแบบที่ไม่มีระบบการตรวจสอบความผิดพลาดที่อาจจะเกิดขึ้นได้

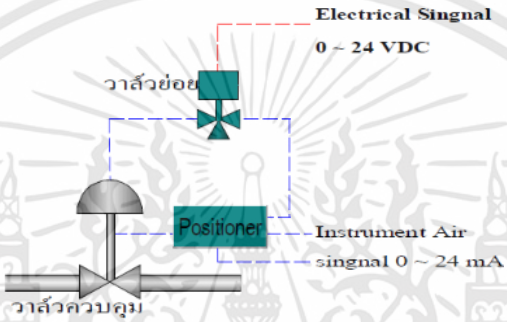
2.2.9.2.2 ตัวประมวลรูปแบบ 1oo2 (One out of Two Voting) รูปแบบนี้จะใช้ระบบประมวลผลสองชุดที่เชื่อมต่อการทำงานร่วมกันแบบอนุกรม ดังแสดงในรูปที่ 2.17 เพื่อนำไปใช้กับระบบนิรภัยที่ต้องการลดผลกระทบที่เกิดจากความผิดพลาดอันตราย สำหรับระบบนิรภัยที่ถูกออกแบบให้ทำงานโดยการหยุดจ่ายพลังงาน (Deenergize to Trip) เพื่อใช้ในการช่วยลดผลกระทบที่เกิดจากความผิดพลาดอันตราย

2.2.9.2.3 ตัวประมวลรูปแบบ 2oo2 (Two out of Two Voting) รูปแบบนี้จะเป็นการนำเอาระบบประมวลผลสองชุดเชื่อมต่อการทำงานร่วมกัน ดังแสดงในรูปที่ 2.17 เพื่อใช้กับระบบนิรภัยที่ไม่ต้องการให้เกิดผลกระทบจากความผิดพลาดนิรภัย (Safe Failure) กับกระบวนการผลิต เพราะจะเป็นสาเหตุให้ค่าความพร้อมใช้งาน (Availability) ของกระบวนการผลิตมีค่าลดลง ระบบการประมวลผลรูปแบบนี้จะถูกนำไปใช้งานกับระบบนิรภัยที่ต้องการให้ส่วนขับสัญญาณจ่ายพลังงานออกไปในสภาวะการทำงาน (Energize to Trip)

2.2.9.2.4 ตัวประมวลรูปแบบ 2oo3 (Two out of Three Voting) รูปแบบนี้จะเป็นการนำเอาระบบประมวลผลสามชุดเชื่อมต่อการทำงานร่วมกัน ดังแสดงในรูปที่ 2.17 โดยในการทำงานของระบบต้องการอุปกรณ์ทำงาน 2 ชุด จากอุปกรณ์ 3 ชุด (รูปแบบนี้สามารถทำให้การทำงานมีความเชื่อมั่นสูง)

2.2.9.3 อุปกรณ์สุดท้าย (Final Element) อุปกรณ์สุดท้ายสามารถจะใช้เป็นวาล์วนิรภัย (Shut Down Valve) หรือชุดขับมอเตอร์ (Motor Control Center) ซึ่งการใช้งานสามารถเลือกใช้ได้เหมือนกับอุปกรณ์การวัดได้ดังนี้

- SIL 1 สามารถใช้วาล์วนิรภัยเพียงตัวเดียวหรืออาจใช้วาล์วย่อยร่วมกันกับวาล์วควบคุม แสดงดังในรูปที่ 2.18
- SIL 2 สามารถใช้วาล์วนิรภัยเพียงตัวเดียวแยกออกจากระบบควบคุม
- SIL 3 จะใช้วาล์วนิรภัยสองตัวต่อกันในลักษณะ 1oo2 (One out of Two Voting)



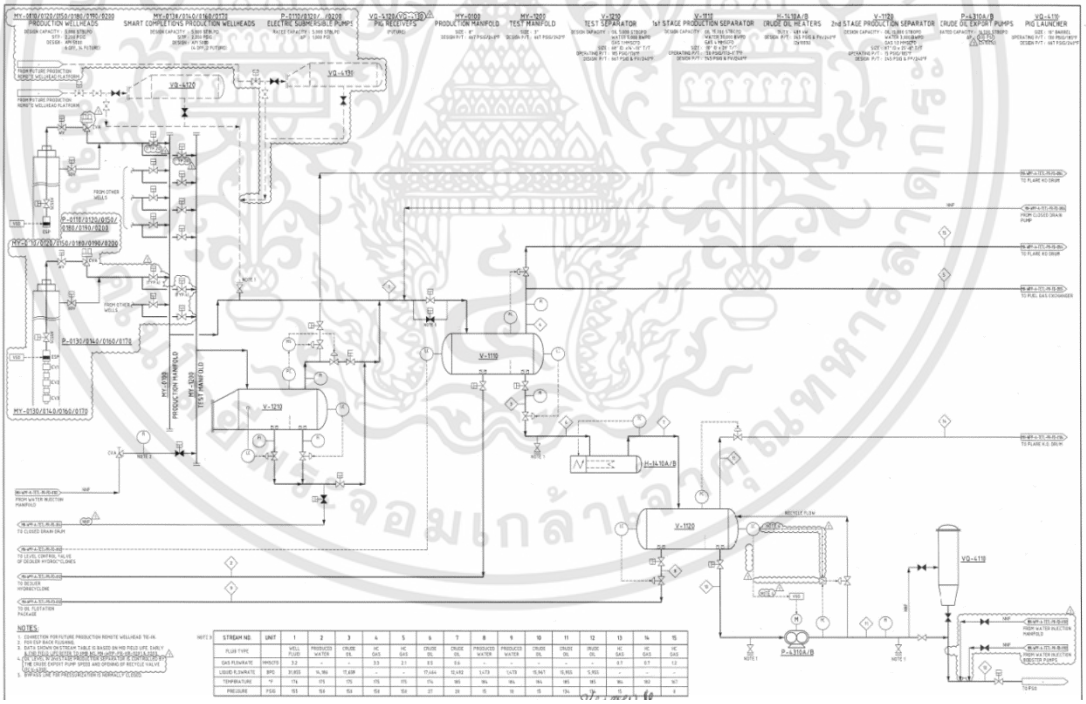
รูปที่ 2.18 วาล์วย่อยกับวาล์วควบคุมที่ใช้เป็นวาล์วนิรภัย
ที่มา : ชาญวิทย์ (2553)

บทที่ 3
วิธีการดำเนินงานวิจัย

การดำเนินงานวิจัยในหัวข้อการออกแบบระบบควบคุมกระบวนการและระบบวัดคุมนิรภัยสำหรับแท่นขุดเจาะน้ำมันและก๊าซ (กรณีศึกษา) นั้นสามารถแบ่งวิธีการดำเนินงานวิจัยได้ ดังหัวข้อต่อไปนี้

3.1 ศึกษาไดอะแกรมของระบบการผลิตน้ำมันดิบและก๊าซธรรมชาติ (Process flow diagram for oil processing)

ในขั้นตอนการออกแบบระบบควบคุมกระบวนการผลิตและระบบวัดคุมนิรภัยนั้นเราจำเป็นที่จะต้องศึกษาไดอะแกรมหรือภาพรวมของระบบการผลิตและส่วนประกอบหลักๆ ของอุปกรณ์ต่างๆ ที่อยู่ในกระบวนการผลิตดังแสดงในรูปที่ 3.1 เสียก่อนเพื่อจะได้มีความเข้าใจภาพรวมของระบบการทำงานและช่วยในการออกแบบฟังก์ชั่นการทำงานของระบบได้อย่างถูกต้อง



รูปที่ 3.1 ไดอะแกรมของระบบการผลิตน้ำมันดิบและก๊าซธรรมชาติ

3.2 จำลองการประเมินความเสี่ยงโดยใช้วิธีกราฟความเสี่ยง

การจำลองการประเมินความเสี่ยงของเหตุการณ์อันตรายที่อาจจะเกิดขึ้นในระหว่างกระบวนการผลิตน้ำมันดิบและก๊าซธรรมชาตินั้น ได้ใช้วิธีการกราฟความเสี่ยงมาช่วยในการพิจารณา โดยมีขั้นตอนของการจำลองดังต่อไปนี้

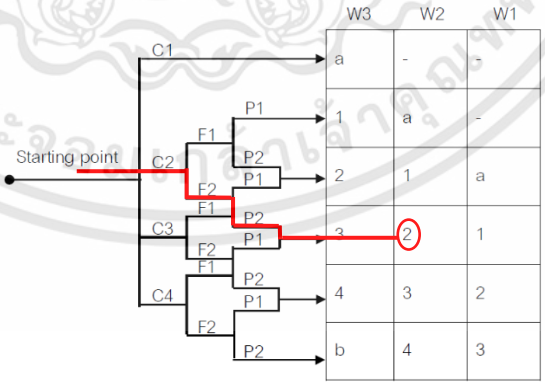
ขั้นตอนที่ 1 กำหนดให้อัตราการเกิดสาเหตุที่นำไปสู่เหตุการณ์อันตรายอันเนื่องมาจากการทำงานที่ผิดพลาดของอุปกรณ์เครื่องมือวัดไฟฟ้า โดยกำหนดให้จะเกิดขึ้นหนึ่งครั้งเมื่อระยะเวลาเกิน 1 ปี แต่ไม่ถึง 10 ปี จากกราฟความเสี่ยง อัตราการเกิดสาเหตุนี้จะได้เป็นตัวแปร W2

ขั้นตอนที่ 2 ทำการประเมินหาค่าระดับความปลอดภัยโดยใช้กราฟความสูญเสียต่อชีวิต โดยกำหนดให้เมื่อเกิดความผิดปกติเกิดขึ้นจะมีผู้ปฏิบัติงานเข้าไปทำการตรวจสอบอย่างน้อย 1 คน ซึ่งเมื่อเกิดเหตุการณ์ผิดปกติขึ้นในระหว่างที่ผู้ปฏิบัติงานกำลังตรวจสอบอยู่นั้นอาจจะทำให้บาดเจ็บหรือเสียชีวิตได้ 1 คน อัตราการสูญเสียต่อชีวิตจะได้เป็น C2

ขั้นตอนที่ 3 ทำการพิจารณาระยะเวลาที่ผู้ปฏิบัติงานต้องเข้าไปทำงานในบริเวณที่เกิดเหตุการณ์นานเพียงใด โดยกำหนดให้ฝ่ายซ่อมบำรุงต้องเข้าไปทำงานเกินกว่าครึ่งวัน จากกราฟความเสี่ยงจะได้เป็น F2

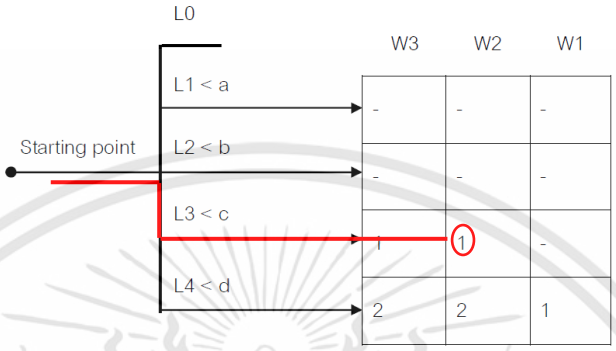
ขั้นตอนที่ 4 ทำการพิจารณาความสามารถในการหลบหลีกออกจากบริเวณที่เกิดเหตุการณ์ผิดปกติขึ้น โดยการจำลองนี้กำหนดให้ผู้ปฏิบัติงานไม่สามารถหลบออกจากบริเวณนั้นได้ จากกราฟความเสี่ยงจะได้เป็น P2

จากการประเมินลำดับเหตุการณ์ต่างๆ จะได้ตัวแปรไปใช้ในกราฟความสูญเสียต่อชีวิต ดังนี้ W2, C2, F2, P2 และเมื่อนำไปลากเส้นลงในกราฟความปลอดภัยดังกล่าวจะได้เป็นค่าระดับความปลอดภัยระดับ 2 ดังแสดงในรูปที่ 3.2



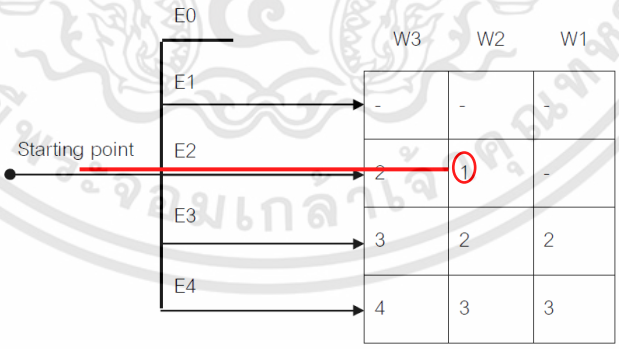
รูปที่ 3.2 ผลลัพธ์ที่ได้จากการประเมินความสูญเสียต่อชีวิต

ขั้นตอนที่ 5 ทำการประเมินมูลค่าความเสียหาย โดยกำหนดให้หลังจากที่เกิดเหตุการณ์อันตรายแล้วนั้นทำให้มีความสูญเสียเกิดขึ้นมากและต้องหยุดกระบวนการผลิตในระยะสั้น จากกราฟความเสี่ยงจะได้เป็น L3 จากนั้นนำค่าตัวแปรที่ได้มาลากเส้นลงในกราฟความสูญเสียต่อทรัพย์สินจะได้เป็นค่าระดับความปลอดภัยระดับ 1 ดังแสดงในรูปที่ 3.3



รูปที่ 3.3 ผลลัพธ์ที่ได้จากการประเมินความสูญเสียต่อทรัพย์สิน

ขั้นตอนที่ 6 ทำการประเมินความสูญเสียต่อสิ่งแวดล้อม โดยกำหนดให้หลังจากที่เกิดเหตุการณ์อันตรายแล้วนั้นทำให้มีผลกระทบต่อสิ่งแวดล้อมชั่วคราวและอยู่ในขอบเขตที่จำกัด จากกราฟความเสี่ยงจะได้เป็น E2 จากนั้นนำค่าตัวแปรที่ได้มาลากเส้นลงในกราฟความสูญเสียต่อสิ่งแวดล้อมจะได้เป็นค่าระดับความปลอดภัยระดับ 1 ดังแสดงในรูปที่ 3.4

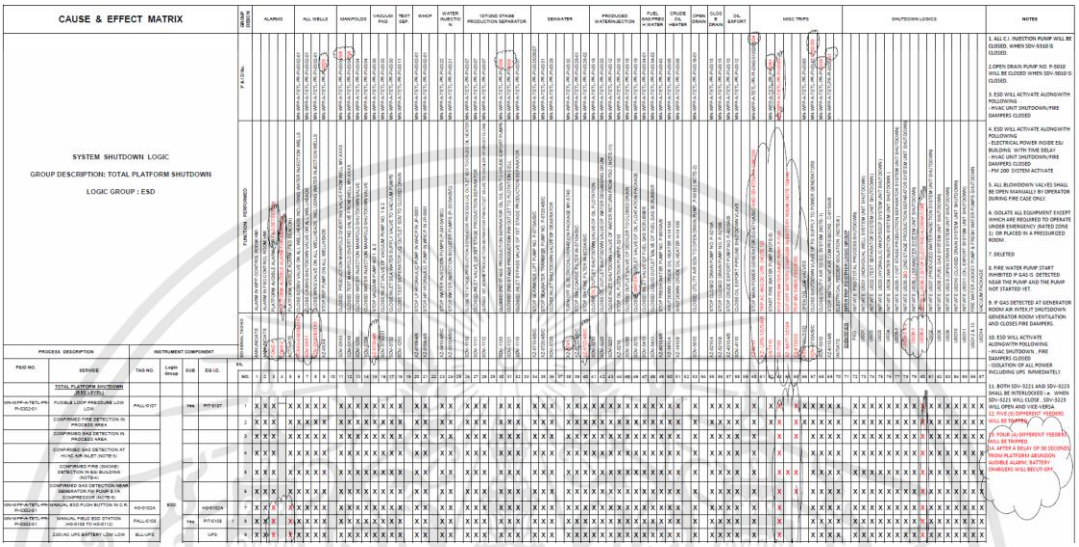


รูปที่ 3.4 ผลลัพธ์ที่ได้จากการประเมินความสูญเสียต่อสิ่งแวดล้อม

ขั้นตอนที่ 7 ทำการสรุปค่าระดับความปลอดภัยของฟังก์ชันนิรภัยที่พิจารณา โดยเมื่อประเมินความเสี่ยงต่อความเสียหายครบทั้ง 3 กราฟแล้ว จากนั้นเราก็จะเลือกค่าระดับความปลอดภัยที่สูงสุดเป็นผลลัพธ์ของฟังก์ชันนิรภัย ดังนั้นจะมีค่าระดับความปลอดภัยระดับ 2

3.3 จำลองการทำงานของฟังก์ชันนิรภัยผ่านตาราง ESD Cause & Effect

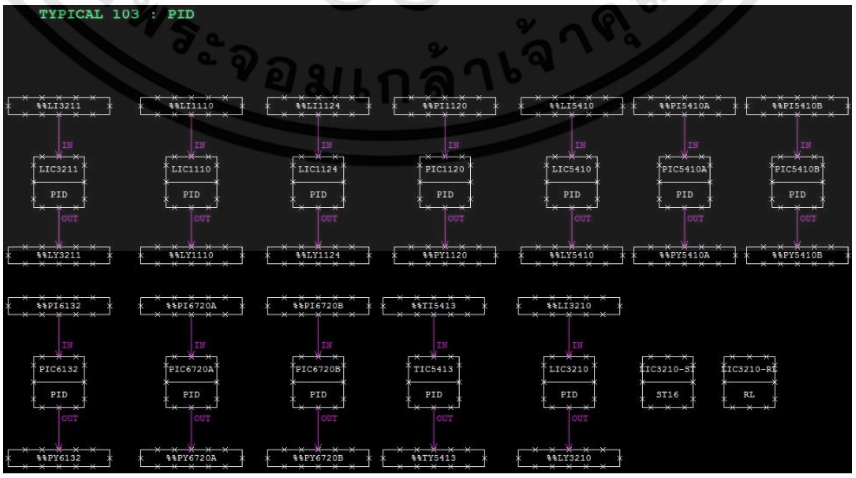
ในการทำงานของฟังก์ชันนิรภัยที่อยู่ในกระบวนการผลิตนั้นจะใช้ตาราง ESD Cause & Effect เป็นตัวอ้างอิงและตรวจสอบการทำงานของฟังก์ชั่นนิรภัยต่างๆที่อยู่ในระบบวัดคุมนิรภัย ดังแสดงในรูปที่ 3.5



รูปที่ 3.5 ตาราง ESD Cause & Effect

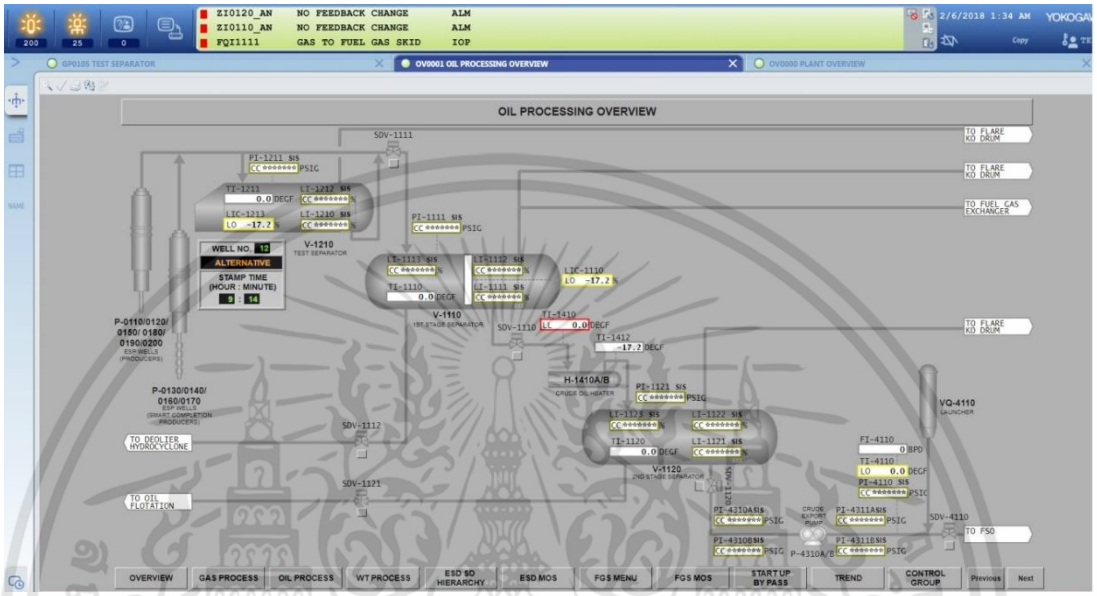
3.4 จำลองการออกแบบระบบควบคุมการผลิตแบบกระจายส่วนและการแสดงผล

ในส่วนของระบบควบคุมการผลิตนั้นได้มีการใช้งานโปรแกรม Centum VP R5.04 ของบริษัทโยโกกาวา ในการออกแบบลูปควบคุมค่าพารามิเตอร์ต่างๆของกระบวนการที่เป็นแบบ PID ดังแสดงในรูปที่ 3.6

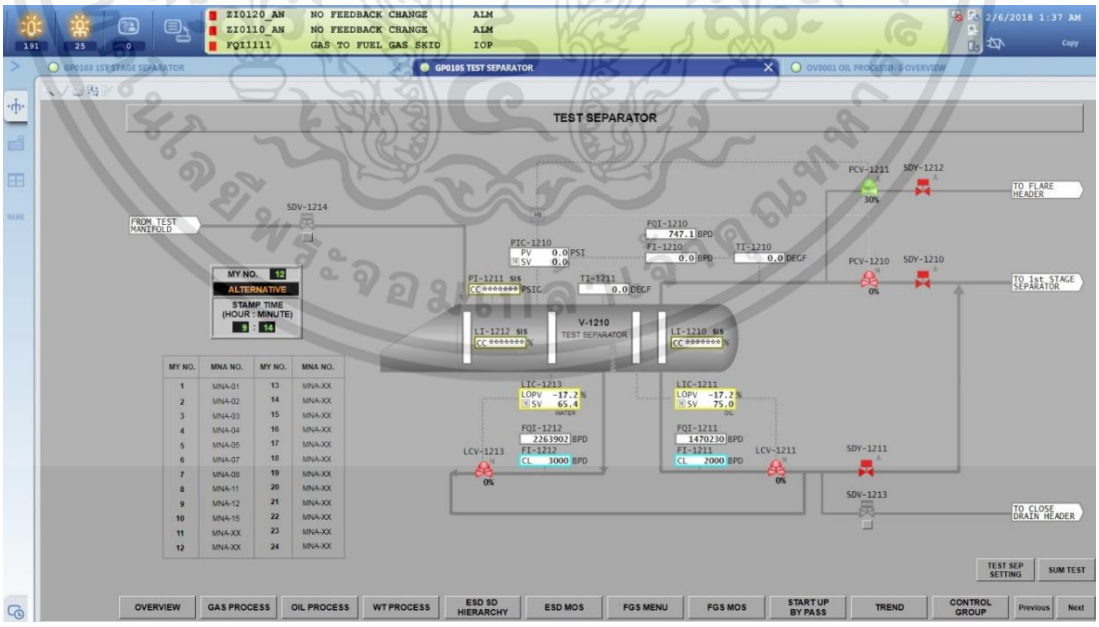


รูปที่ 3.6 PID Function blocks

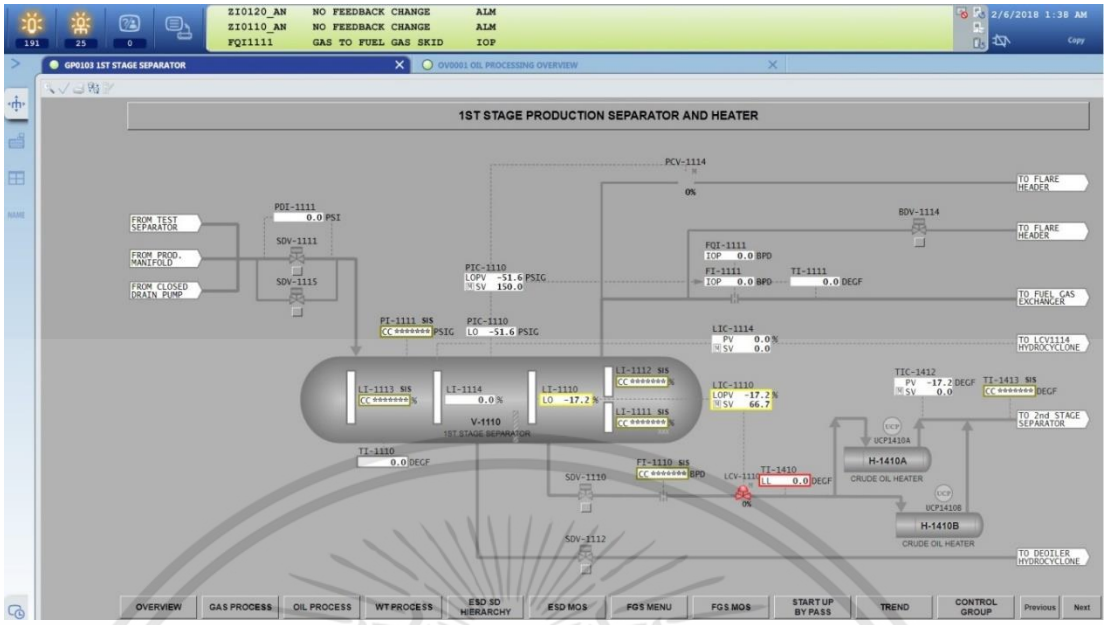
3.4.1 ส่วนของกราฟฟิก (Graphic Display) หลังจากที่ได้ศึกษาไดอะแกรมของระบบการผลิตน้ำมันดิบและก๊าซธรรมชาติหรือแผนภาพ P&ID แล้วนั้น จากนั้นเราก็จะมาทำการออกแบบกราฟฟิกเพื่อการแสดงข้อมูลของระบบการผลิตให้ผู้ปฏิบัติงานได้ทราบข้อมูลค่าพารามิเตอร์ต่างๆ หรือข้อความเตือนต่างๆ ที่อยู่ในกระบวนการผลิตดังแสดงในรูปที่ 3.7 ถึงรูปที่ 3.10 ตามลำดับ



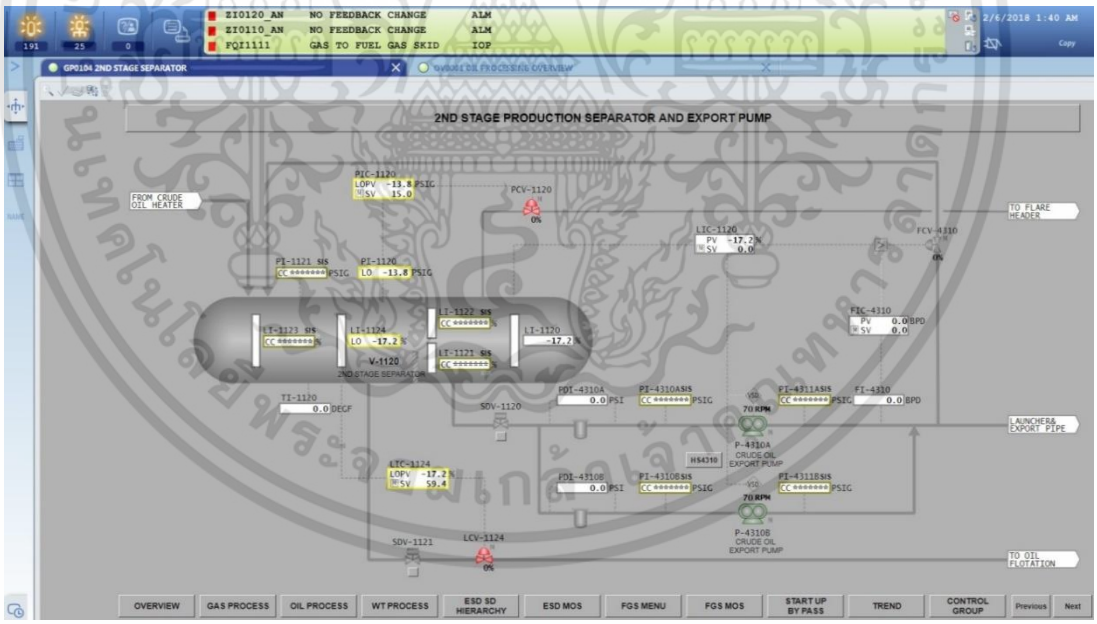
รูปที่ 3.7 กราฟฟิกสำหรับภาพรวมของระบบการผลิต



รูปที่ 3.8 กราฟฟิกสำหรับ Test Separator



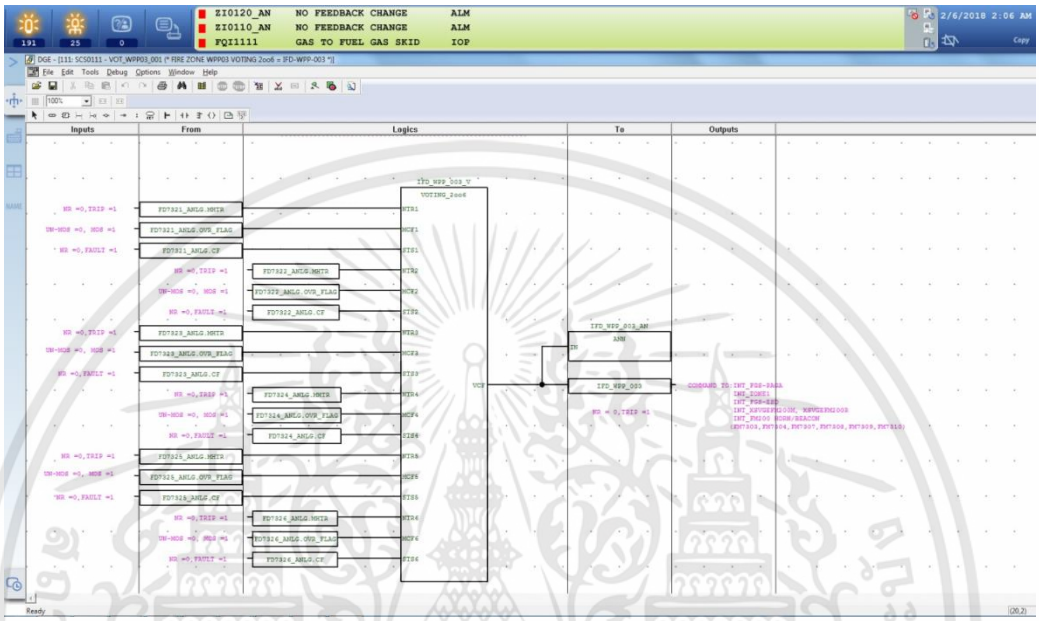
รูปที่ 3.9 กราฟฟิกสำหรับ 1st stage production separator and heater.



รูปที่ 3.10 กราฟฟิกสำหรับ 2nd stage production separator and export pump.

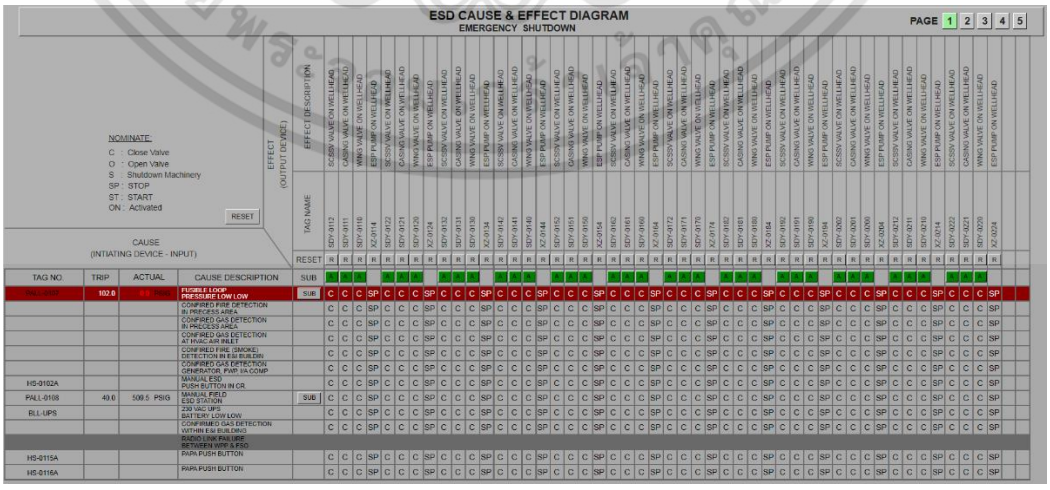
3.5 จำลองการออกแบบฟังก์ชันนิรภัยและการแสดงผล

ในส่วนของการออกแบบฟังก์ชันนิรภัยนั้นได้มีการใช้งานโปรแกรม ProSafe-RS R3.02 ของบริษัทโยโกกาวา เพื่อทำการออกแบบและทดสอบการทำงานของฟังก์ชันนิรภัยต่างๆ ดังแสดงในรูปที่ 3.11



รูปที่ 3.11 รูปแบบของฟังก์ชันนิรภัย

โดยเมื่อเราทำการออกแบบและทดสอบการทำงานของฟังก์ชั่นนิรภัยเสร็จแล้ว เราก็จะนำค่าสถานะการทำงานของฟังก์ชั่นนิรภัยนั้นมาแสดงผลที่กราฟฟิกด้วยเช่นเดียวกับการแสดงสถานะการทำงานของระบบควบคุมกระบวนการผลิต ดังแสดงในรูปที่ 3.12



รูปที่ 3.12 กราฟฟิกสำหรับ ESD Cause & Effect diagram.

บทที่ 4
การประยุกต์ใช้งานระบบควบคุมแบบกระจายส่วนร่วมกับระบบวัดคุมนิรภัยสำหรับแท่นขุดเจาะและผลิตน้ำมันและก๊าซ

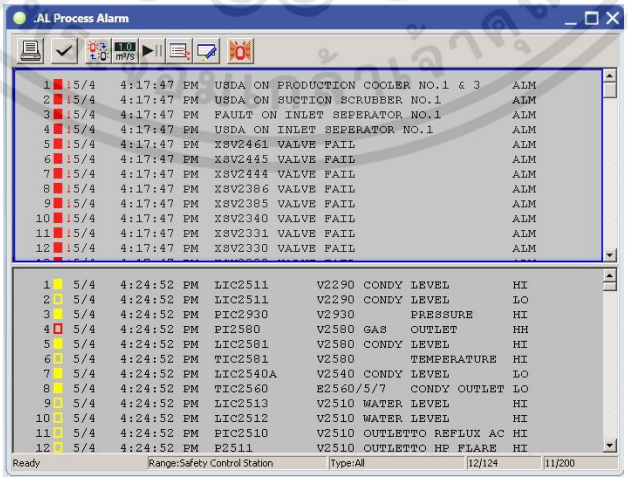
ในการทำวิจัยนี้ได้มีการจำลองการออกแบบกราฟฟิกเพื่อแสดงผลการทำงานของระบบควบคุมแบบกระจายส่วนให้ผู้ใช้งานได้ทราบข้อมูลในกระบวนผลิตโดยการแสดงค่าพารามิเตอร์ต่างๆ และนอกจากนี้ก็ยังมีส่วนของการแสดงผลสถานะการทำงานของฟังก์ชันนิรภัยต่างๆ ร่วมด้วย ซึ่งผลของการดำเนินงานมีดังนี้

4.1 ฟังก์ชันของระบบควบคุมแบบกระจายส่วนที่ใช้ในติดต่อสื่อสารกับผู้ใช้งาน

4.1.1 แถบเมนูแสดงข้อความบอกสถานะของระบบ (System Message Banner) ซึ่งจะอยู่ด้านบนของหน้าจอเมื่อรันโปรแกรม Centum VP R 5.02 ขึ้นมาใช้งานดังแสดงในรูปที่ 4.1

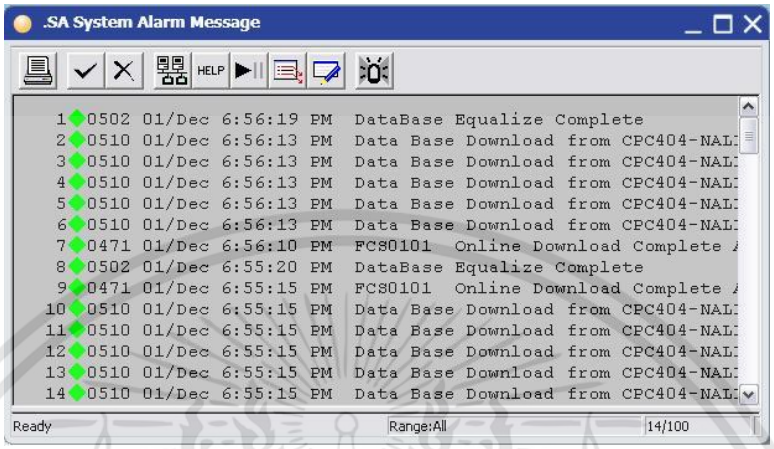
รูปที่ 4.1 แถบเมนูแสดงข้อความบอกสถานะของระบบ

4.1.2 ข้อความแสดงสถานะของกระบวนการ (Process Alarm) โดยจะทำหน้าที่แจ้งสถานะค่าพารามิเตอร์ต่างๆของกระบวนการว่ามีค่าปกติ (Normal) หรือมีการแจ้งเตือน (Alarm) เกิดขึ้น ดังแสดงในรูปที่ 4.2



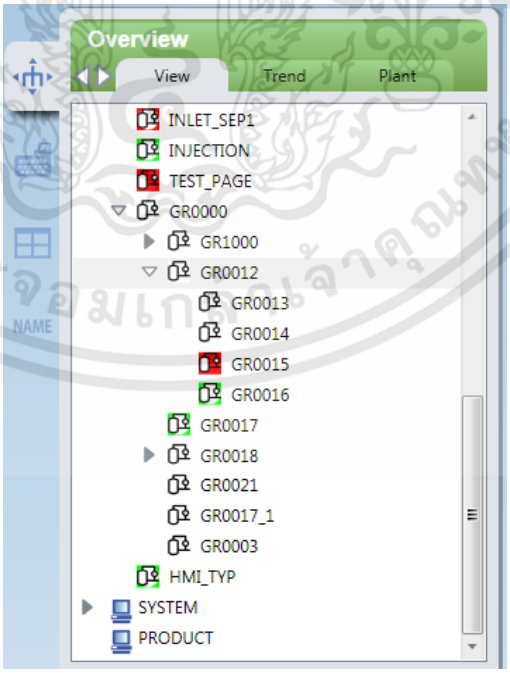
รูปที่ 4.2 ข้อความแสดงสถานะของกระบวนการ (Process Alarm)

4.1.3 ข้อความแสดงสถานะของระบบ (System Alarm) โดยจะทำหน้าที่แจ้งสถานะของระบบว่าตอนนี้ระบบมีสถานะเป็นอย่างไรบ้าง เช่น มีการโหลดโปรแกรมอยู่ หรือมีการ์ดอินพุต/เอาต์พุตบางการ์ดนั้นไม่ทำงาน เป็นต้น ดังแสดงในรูปที่ 4.3



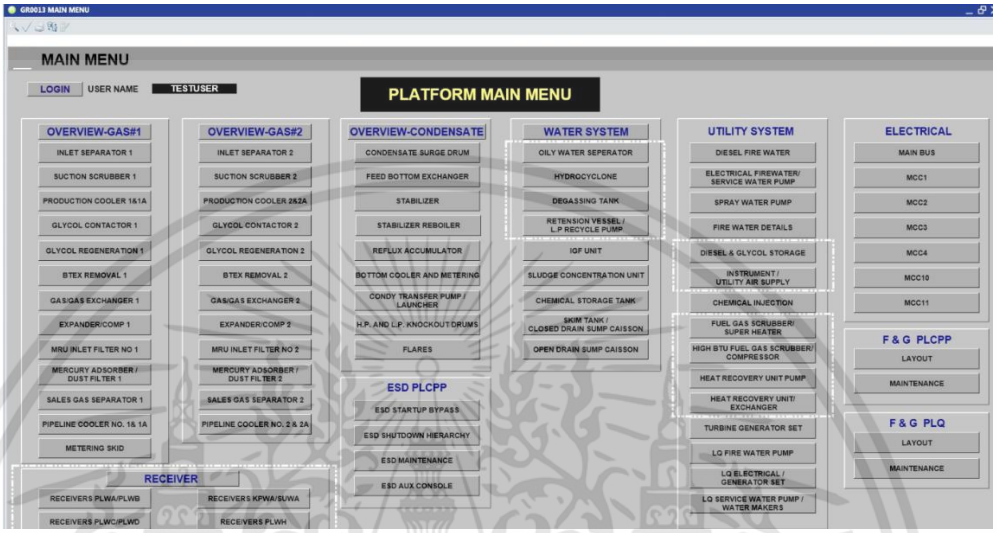
รูปที่ 4.3 ข้อความแสดงสถานะของระบบ (System Alarm)

4.1.4 ส่วนของกล่องเครื่องมือ (Overview Toolbox) โดยจะทำหน้าที่สำหรับให้ผู้ใช้งานได้เลือกหน้ากราฟฟิกที่ต้องการแสดงผลปรากฏขึ้นมาได้หรือการดูเทรนของค่าพารามิเตอร์ต่างๆ เป็นต้น ดังแสดงในรูปที่ 4.4

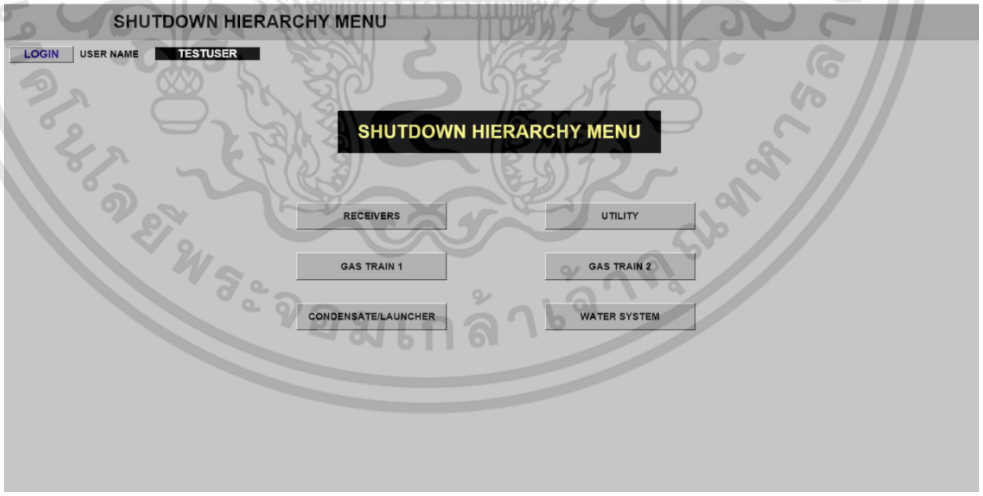


รูปที่ 4.4 ส่วนของกล่องเครื่องมือ (Overview Toolbox)

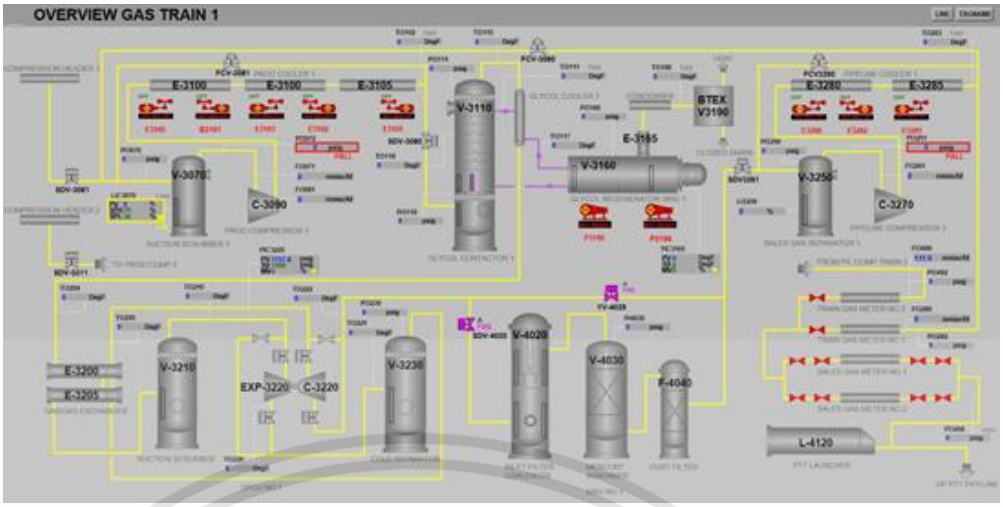
4.1.5 ส่วนของการแสดงกราฟฟิกของระบบควบคุม โดยได้มีการอ้างอิงและออกแบบมาจากข้อมูลไดอะแกรมของกระบวนการผลิต (Process Flow Diagram) ดังแสดงในรูปตัวอย่างที่ 4.5 ถึง 4.7 ตามลำดับ



รูปที่ 4.5 รูปตัวอย่างกราฟฟิกของระบบควบคุมเมนูหลัก

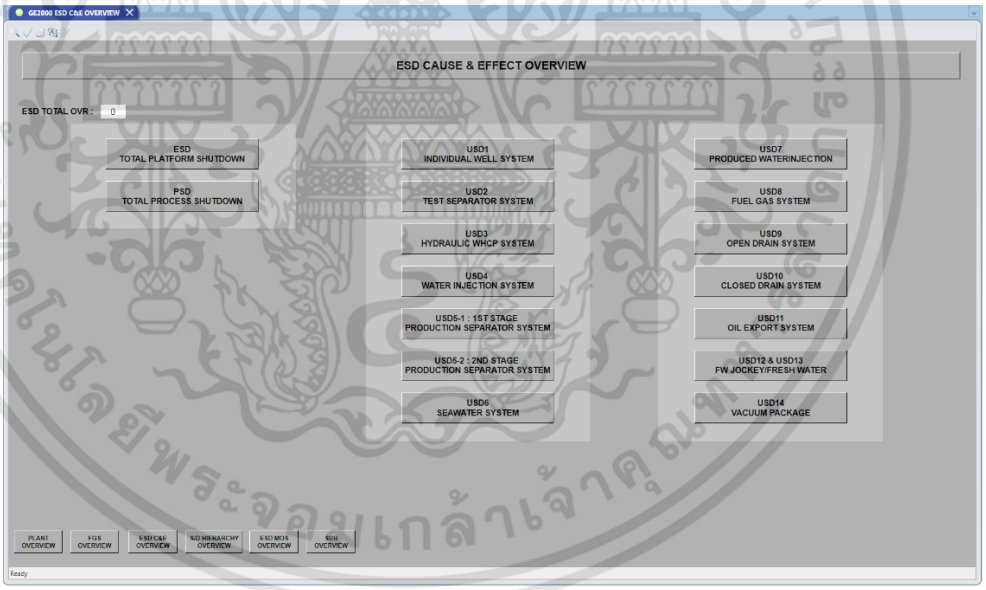


รูปที่ 4.6 รูปตัวอย่างกราฟฟิกของระบบควบคุมเมนูย่อย

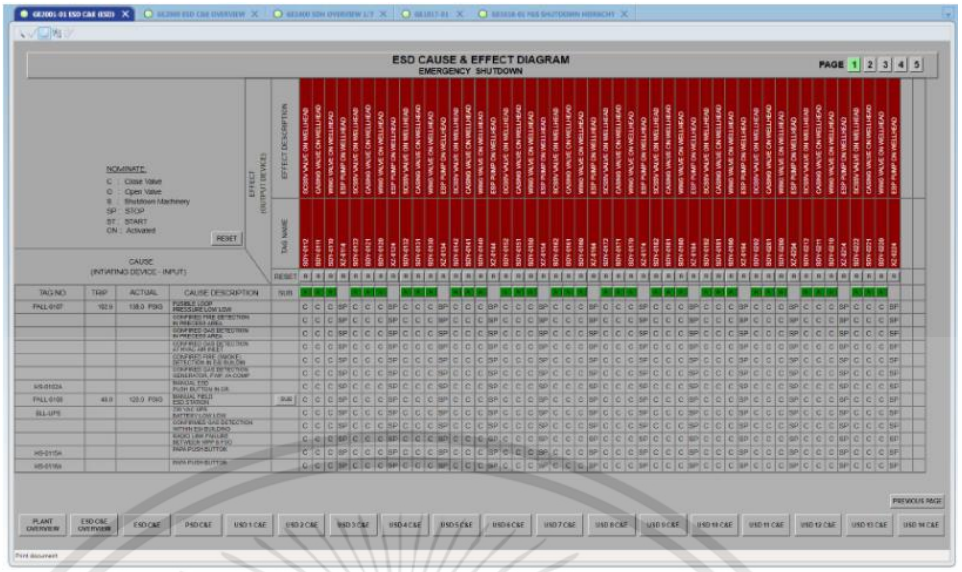


รูปที่ 4.7 รูปตัวอย่างกราฟฟิกโดยรวมของระบบการผลิต

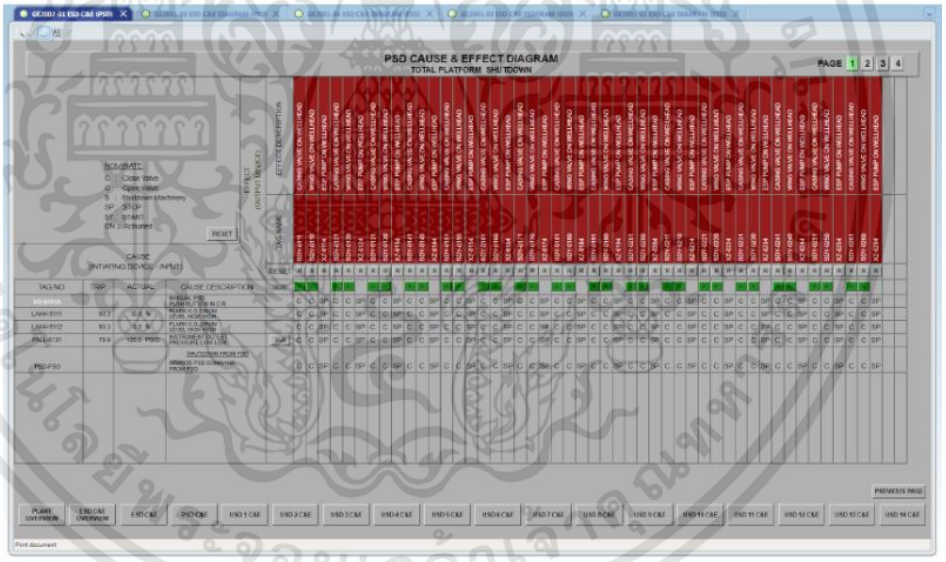
4.1.6 ส่วนของการแสดงกราฟฟิกของระบบวัดคุมนิรภัย โดยได้มีการอ้างอิงและออกแบบมาจากข้อมูลตาราง ESD Cause & Effect ดังแสดงในรูปตัวอย่างที่ 4.8 ถึง 4.11 ตามลำดับ



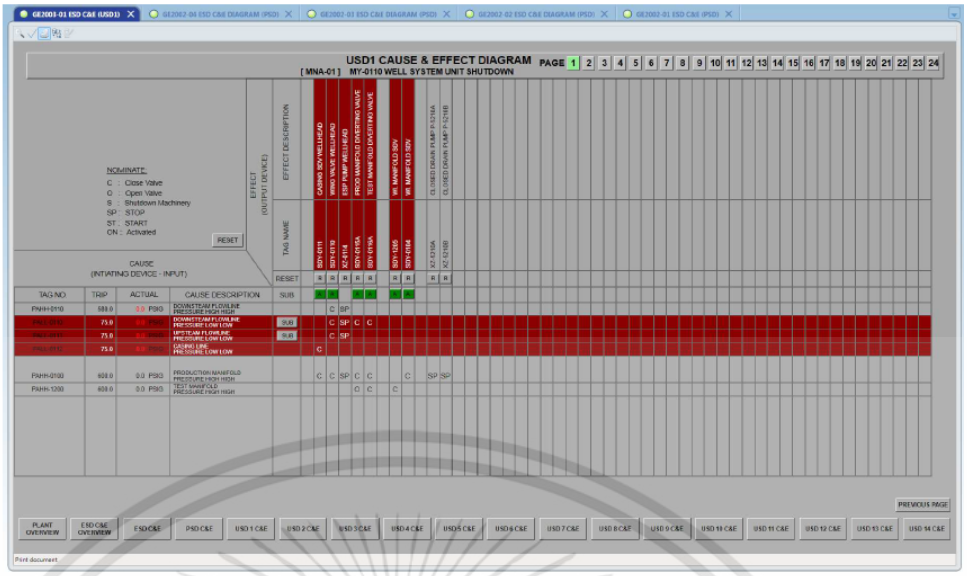
รูปที่ 4.8 รูปตัวอย่างกราฟฟิกระบบวัดคุมนิรภัยเมนูหลัก



รูปที่ 4.9 รูปตัวอย่างกราฟฟิก ESD Total Platform Shutdown



รูปที่ 4.10 รูปตัวอย่างกราฟฟิก PSD Total Process Shutdown



รูปที่ 4.11 รูปตัวอย่างกราฟฟิก USD Individual Well System

4.2 กำหนดขั้นตอนการทำงานฟังก์ชันนิรภัยของระบบวัดคุมนิรภัย

ในการกำหนดขั้นตอนการทำงานฟังก์ชันนิรภัยสำหรับระบบวัดคุมนิรภัยนี้นั้นได้มีการจำลองข้อมูลขึ้นมา ดังตาราง 4.1

ตาราง 4.1 การทำงานของฟังก์ชันนิรภัย

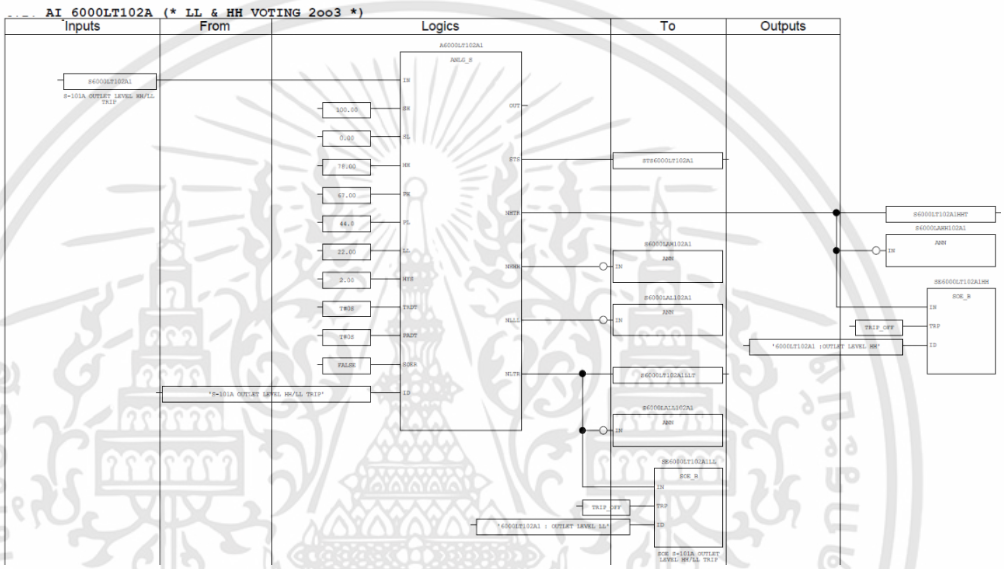
Step No.	Test description	SIS Function Result				Remark
		Condition / Status of 3 Analog Voting			Action Result from Group Voting	
1	2oo3 Voting Function (3 Tag AI are Normal Status)	AI-1 = "TRIP"	AI-2 = "TRIP"	AI-3 = "NORMAL"	Trip Condition	"TRIP" = High-HightTrip or Low-Low Trip
		AI-1 = "TRIP"	AI-2 = "NORMAL"	AI-3 = "TRIP"	Trip Condition	
		AI-1 = "NORMAL"	AI-2 = "TRIP"	AI-3 = "TRIP"	Trip Condition	
2	Degraded Voting from 2oo3 to 1oo2 by 1 Tag AI Fault	AI-1 = "FAULT"	AI-2 = "TRIP"	AI-3 = "NORMAL"	Trip Condition	"FAULT" = IOP+ or IOP-
		AI-1 = "FAULT"	AI-2 = "NORMAL"	AI-3 = "TRIP"	Trip Condition	
		AI-1 = "TRIP"	AI-2 = "FAULT"	AI-3 = "NORMAL"	Trip Condition	
		AI-1 = "NORMAL"	AI-2 = "FAULT"	AI-3 = "TRIP"	Trip Condition	
		AI-1 = "TRIP"	AI-2 = "NORMAL"	AI-3 = "FAULT"	Trip Condition	
		AI-1 = "NORMAL"	AI-2 = "TRIP"	AI-3 = "FAULT"	Trip Condition	
3	Degraded Voting from 2oo3 to Trip Condition by 2 Tag AI Fault	AI-1 = "FAULT"	AI-2 = "FAULT"	AI-3 = "NORMAL"	Trip Condition	"FAULT" = IOP+ or IOP-
		AI-1 = "FAULT"	AI-2 = "NORMAL"	AI-3 = "FAULT"	Trip Condition	
		AI-1 = "NORMAL"	AI-2 = "FAULT"	AI-3 = "FAULT"	Trip Condition	
4	Degraded Voting from 2oo3 to 1oo2 by 1 Tag AI = Override	AI-1 = "OVR"	AI-2 = "TRIP"	AI-3 = "NORMAL"	Trip Condition	"OVR" = OVERRIDE
		AI-1 = "OVR"	AI-2 = "NORMAL"	AI-3 = "TRIP"	Trip Condition	
		AI-1 = "TRIP"	AI-2 = "OVR"	AI-3 = "NORMAL"	Trip Condition	
		AI-1 = "NORMAL"	AI-2 = "OVR"	AI-3 = "TRIP"	Trip Condition	
		AI-1 = "TRIP"	AI-2 = "NORMAL"	AI-3 = "OVR"	Trip Condition	
		AI-1 = "NORMAL"	AI-2 = "TRIP"	AI-3 = "OVR"	Trip Condition	
5	Degraded Voting from 2oo3 to Trip Condition by 1 Tag AI= Fault and 1 Tag AI = Override	AI-1 = "OVR"	AI-2 = "FAULT"	AI-3 = "NORMAL"	Trip Condition	As per SRS Rev.A1 Function Override or Fault are same Function for Degraded Voting.
		AI-1 = "OVR"	AI-2 = "NORMAL"	AI-3 = "FAULT"	Trip Condition	
		AI-1 = "FAULT"	AI-2 = "OVR"	AI-3 = "NORMAL"	Trip Condition	
		AI-1 = "NORMAL"	AI-2 = "OVR"	AI-3 = "FAULT"	Trip Condition	
		AI-1 = "FAULT"	AI-2 = "NORMAL"	AI-3 = "OVR"	Trip Condition	
		AI-1 = "NORMAL"	AI-2 = "FAULT"	AI-3 = "OVR"	Trip Condition	

4.3 เขียนโปรแกรมฟังก์ชันนิรภัย (Programming for Safety Function)

ในการเขียนโปรแกรมฟังก์ชันนิรภัยนั้นได้มีการใช้งานโปรแกรม ProSafe-RS R3.02 เป็นตัวคอนโทรลเลอร์ในการรันและทดสอบโปรแกรมโดยมีขั้นตอนหลักๆ ดังต่อไปนี้

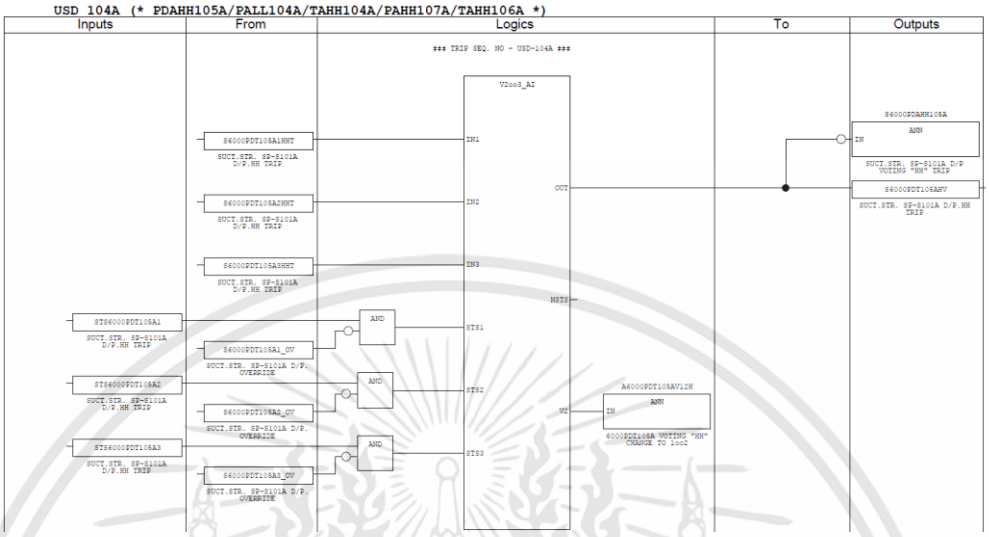
4.3.1 การกำหนดชื่อตัวแปรอินพุต/เอาต์พุตจากเครื่องมือวัดไฟฟ้าและอุปกรณ์ตัวสุดท้ายต่างๆ ลงในโปรแกรมฟังก์ชันนิรภัย

4.3.2 การทำสเกลลิ่งค่าตัวแปรต่างๆ ที่ได้รับสัญญาณไฟฟ้ามาจากอุปกรณ์เครื่องมือวัดโดยใช้งานฟังก์ชันบล๊อกที่ภายโปรแกรมดังแสดงในรูปที่ 4.12



รูปที่ 4.12 ตัวอย่างการทำสเกลลิ่งค่าตัวแปรต่างๆ

4.3.3 ทำการเขียนเงื่อนไขสำหรับฟังก์ชันนิรภัยเพื่อทำการสั่งงานอุปกรณ์ตัวสุดท้ายดังแสดงในรูปที่ 4.13



รูปที่ 4.13 ตัวอย่างแสดงเงื่อนไขสำหรับฟังก์ชันนิรภัย

บทที่ 5
ผลการวิจัยและอภิปรายผล

5.1 ผลการวิจัย

จากบทที่ 4 ได้กล่าวถึงวิธีการใช้งานฟังก์ชันของระบบควบคุมแบบกระจายส่วนที่ใช้ในการติดต่อสื่อสารกับผู้ใช้งานและการกำหนดขั้นตอนการทำงานฟังก์ชันนิรภัยของระบบวัดคุมนิรภัยไปแล้วนั้น ในตัวบทที่ 5 บทนี้กล่าวถึงผลการทดลองเพื่อทดสอบการทำงานของโปรแกรมตามที่ได้ออกแบบไปในขั้นต้น โดยมีรายละเอียดของผลของการทดสอบ ดังตาราง 5.1

ตาราง 5.1 ผลการทดสอบการทำงานของฟังก์ชั่นระบบควบคุมและระบบวัดคุมนิรภัย

ระบบ	หัวข้อที่ทำการทดสอบ	เกณฑ์การทดสอบ	ผ่าน	ไม่ผ่าน	หมายเหตุ
DCS	ฟังก์ชั่นการควบคุมเครื่องจักร/อุปกรณ์	สั่งงาน เปิด/ปิด อุปกรณ์ได้	√		-
DCS	กราฟฟิกแสดงการทำงาน	กราฟฟิกแสดงสีสถานะได้ถูกต้อง	√		มีบางจุดที่ได้ทำการแก้ไข
DCS	ตัวแสดงผลค่าพารามิเตอร์ (Indicator)	แสดงผลของการวัดได้อย่างถูกต้อง	√		-
DCS	การแสดงข้อความเตือน (Alarm)	มีข้อความเตือนขึ้นมาให้เห็น	√		
SIS	การทำงานของฟังก์ชันนิรภัยต่างๆ	ตารางในรูปที่ 4.12 (ในบทที่ 4)	√		-
SIS	กราฟฟิกแสดงการทำงาน	กราฟฟิกแสดงสีสถานะได้ถูกต้อง	√		-
SIS	ตัวแสดงผลค่าพารามิเตอร์ (Indicator)	แสดงผลของการวัดได้อย่างถูกต้อง	√		-
SIS	การแสดงข้อความเตือน (Alarm)	มีข้อความเตือนขึ้นมาให้เห็น	√		-

บทที่ 6
สรุปผลวิจัยและข้อเสนอแนะ

เมื่อทำการออกแบบระบบควบคุมกระบวนการแบบกระจายส่วนและระบบวัดคุมนิรภัยสำหรับแท่นขุดเจาะน้ำมันและก๊าซและทำการทดสอบการทำงานของโปรแกรมเป็นที่เรียบร้อยแล้วนั้น ทำให้ทราบถึงปัญหาและอุปสรรคในการดำเนินงานโดยมีการสรุปผลวิจัยและข้อเสนอแนะดังนี้

6.1. สรุปผลการดำเนินงาน

6.2. ข้อจำกัดของระบบ

6.3. ข้อเสนอแนะ

6.1 สรุปผลการดำเนินงาน

จากผลการทดลองและประเมินการทำงานของโปรแกรมระบบควบคุมกระบวนการและระบบวัดคุมนิรภัยนั้นพบว่าฟังก์ชั่นนิรภัยนั้นสามารถทำงานได้ตามที่กำหนดไว้จึงสามารถช่วยทำให้ระบบกระบวนการผลิตนั้นกลับเข้าสู่สภาวะปกติได้ โดยเมื่อเกิดเหตุการณ์ค่าพารามิตเตอร์ตัวแปรในกระบวนการผลิตเช่น ค่าความดัน มีค่าสูงเกินผิดปกติและอาจจะทำให้เกิดเหตุการณ์อันตรายขึ้นได้ เมื่อมีกรณีนี้เกิดขึ้นฟังก์ชั่นนิรภัยก็จะทำการสั่งงานไปที่อุปกรณ์ควบคุมสุดท้ายเพื่อทำการหยุดระบบการผลิตต่อไป

6.2 ข้อจำกัดของระบบ

ระบบนี้ยังทำได้แค่จำลองเหตุการณ์ความผิดปกติของกระบวนการผลิตตามข้อมูลเอกสาร ซึ่งเหตุการณ์จริงอาจไม่ได้เป็นไปตามข้อมูลเอกสารทั้งหมด

6.3 ข้อเสนอแนะ

งานวิจัยนี้ได้ทำการออกแบบระบบควบคุมกระบวนการแบบกระจายส่วนและระบบวัดคุมนิรภัยที่ทำหน้าที่หยุดระบบการผลิตในกรณีฉุกเฉินสำหรับแท่นขุดเจาะน้ำมันและก๊าซสำหรับผู้ที่สนใจหรือผู้ที่กำลังจะเข้ามาทำงานในอุตสาหกรรมที่เกี่ยวข้องนี้ ซึ่งในอนาคตอาจจะมีการเพิ่มเติมระบบตรวจจับควันและไฟไหม้ (Fire and Gas System) เพื่อทำให้ระบบมีความปลอดภัยและน่าเชื่อถือเพิ่มขึ้น

เอกสารอ้างอิง

เอกสารอ้างอิง

[1] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related system.

[2] IEC 61511, Functional safety-safety instrumented system for the process industry sector.

[3] Paul Gruhn, P.E., CFSE and Harry Cheddie, P.Eng., CFSE., “SAFETY INSTRUMENTED SYSTEMS:Design, Analysis, and Justification,” 2nd Edition.

[4] William M. Goble and Harry Cheddie., “Safety Instrumented Systems Verification:Practical Probabilistic Calculations”.

[5] Havard Devold., “Oil and gas production handbook,” Edition 3.0 Oslo, August 2013.

[6] http://dmf.go.th/public/list/data/detail/id/5835/menu/621/page/1/mainmenu/915

[7] ทวิช ชูเมือง , ระบบวัดคุมนิรภัยในอุตสาหกรรมกระบวนการผลิต, ISBN 974-212-172-9, บริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน), 2548

[8] ชาญวิทย์ เลาหอุดมโชค, การศึกษาความเสี่ยงและระบบวัดคุมนิรภัยของเตาเผาแยกสารไฮโดรคาร์บอน: กรณีศึกษาโรงงานโอเลฟินส์, 2553

[9] สุนทร แสงแก้ว, การประยุกต์ใช้ Human Machine Interface เพื่อวิเคราะห์ระบบวัดคุมนิรภัย, 2552

[10] Arthur M. Dowell III, “Layer of protection analysis for determining safety integrity level”, ISA Transactions, pp. 155-165, 1998.

[11] Curt Miller, Lindsey Bredemyer, “Innovative safety valve selection techniques and data”, Journal of Hazardous Materials, pp.685-688, 2007.

[12] Sung Kyu Kim, Yong Soo Kim, “An evaluation approach using a HARA and FMEDA for the hardware SIL”, Journal of Loss Prevention in the Process Industries, pp. 1-9, 2013.

[13] M. Catelani, L. Ciani, V. Luongo, “A simplified procedure for the analysis of Safety Instrumented Systems in the process industry application”, Microelectronics Reliability, pp.1503-1507, 2011.

[14] Charlit Yoosamran, Sakreya Chitwong, Phongchai Nilas, “Process Control & Safety Instrumented system design for upstream Oil and Gas Industry (Case Study)”, Proceedings of the SICE Annual Conference 2018, pp. 125-129, 2018.

ภาคผนวก

Proceedings of the SICE Annual Conference 2018
September 11-14, 2018, Nara, Japan

Process Control & Safety Instrumented system design for upstream Oil and Gas Industry (Case Study)

Charlit Yoosamran Sakreya Chitwong and Phongchai Nilas

Department of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
(E-mail: charlit_yoosamran@hotmail.com, sakreya.ch@kmitl.ac.th, phongchai.ni@kmitl.ac.th)

Abstract: This paper has been compiled for people with an interest in the upstream oil and gas industry. It is an overview of the main processes control and safety instrumented system design for upstream oil and gas industry. A process control system is used to monitor data and control all equipment on the Wellhead Processing Platform (WPP). For the installations distributed control system (DCS) may be used. The purpose of this system is to read values from a large number of sensors, run programs to monitor the process and control valves, switches etc. to control the process values, alarms, reports and other information are also presented to the operator and command inputs accepted. The safety instrumented systems (SIS) is to take control and prevent an undesirable event when the process and the facility are no longer operating within normal operating conditions. The function of safety system is the part of the overall safety of a system that depends on the correct response of the safety system response to its inputs, including safe handling of operator errors, hardware failures and environmental changes (fires, lightning, etc.). The purpose of a SIS is to protect people, the environment, and assets from the consequences of accidents by reducing the probability of incidents occurring base on safety standard IEC61508 and IEC61511.

Keywords: Process control system, Distributed control system, Safety instrumented systems

1. INTRODUCTION

The upstream oil and gas industry is the process equipment that takes the product from the wellhead manifolds and delivers stabilized marketable products, in the form of crude oil, condensates or gas. Components of the process also exist to test products and clean waste products such as produced water. During routine operation in Fig. 1 of upstream oil and gas industry distributed control system (DCS) may be used to monitor data and control equipment on the platform and Including the protective system or safety instrumented systems (SIS) show in Fig. 2 to protect people, the environment, and assets from the consequences of accidents by reducing the probability of incidents occurring base on safety standard IEC61508 and IEC61511.

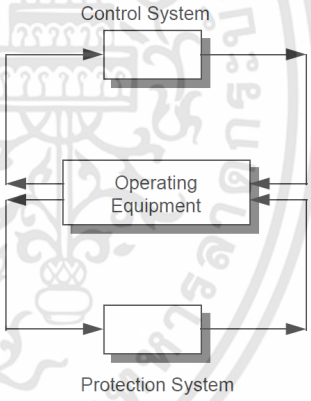


Fig.1 Overview of control with protective system.

2. DISTRIBUTED CONTROL SYSTEM

A Distributed control system is used to controls all normal operating process equipment on the platform. Very small installations may use hydraulic or pneumatic control systems, but larger plants with many input and output signals to and from the process require a dedicated distributed control system. This system is operated from a central control room (CCR) with a combination of graphical process displays, alarm lists and historical data curves. Smaller personal screens are often used in combination with large wall screens. The purpose of this system is to read values from a large number of sensors, run programs to monitor the process and control valves, switches to control the process. Values and other information are also presented to the operator and command inputs accepted.

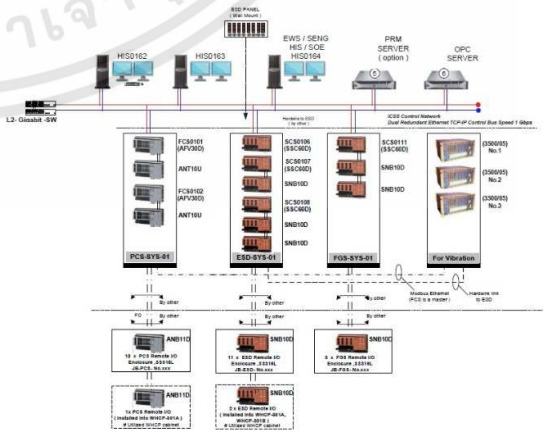


Fig.2 Control with protective system configuration.

1.1 DISTRIBUTED CONTROL SYSTEMS CONSIST OF THE FOLLOWING COMPONENTS:

- Field instrumentation: sensors and switches that sense process conditions such as temperature, pressure, level or flow. These are connected over single and multiple pair electrical cables (hardwired) or communication bus systems called fieldbus.
- Final elements, such as actuators for valves, electrical switchgear and drives or indicators are also hardwired or connected over fieldbus.
- Controllers execute the control algorithms so that the desired actions can be taken. The controllers also generate events and alarms based on changes of state and alarm conditions, and prepare data for operators and information systems.
- A number of servers perform the data processing required for data presentation, historical archiving, alarm processing and engineering changes.
- Clients, such as operator stations and engineering stations, are provided for human interfaces to the control system.
- The communication can be laid out in many different configurations, often including connections to remote facilities, remote operations support and other similar environments.

The main function of the control system is to make sure the production, processing and utility systems operate efficiently within design constraints and alarm limits. The control system is typically specified in programs as a combination of logic and control function blocks, such as AND, ADD and PID Function blocks in Fig. 3 For a particular system, a library of standard solutions such as level control loops and motor control blocks are defined. This means that the system can be specified with combinations of typical loop templates, consisting of one or more input devices, function blocks and output devices. This allows much if not all of the application to be defined based on engineering databases and templates rather than formal programming.

The basic functionality of control system can be used for more advanced control and optimization functions as following:

- Open/close control valves in manual mode.
- Start/stop pumps in manual mode.
- Initiate start-up bypass for inputs which are in the shutdown state during start-up.
- Reset the shutdown logic provided the inputs initiating the shutdown return to the normal state.
- Change set points of control loops.
- Monitor status indications and acknowledge alarms.
- Initiate logs and reports.
- Change Process graphic displays.
- Initiate individual well shutdowns.
- Initiate process shutdown via hardwired push-button.
- Initiate Emergency shutdown via hardwired push-button.
- Close the ESD valves manually from the consoles under all conditions.

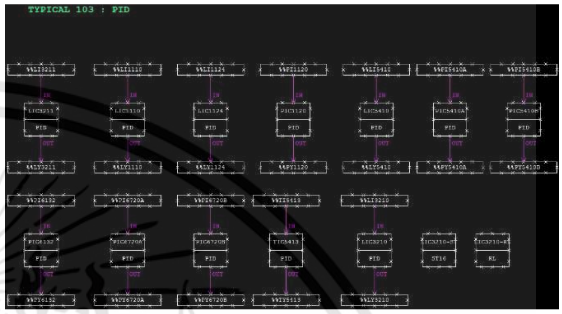


Fig.3 PID Function blocks of the control systems.

3. SAFETY INSTRUMENTED SYSTEM

The function of safety systems is to take control and prevent an undesirable event when the process and the facility are no longer operating within normal operating conditions show in Fig. 4 Functional safety is the part of the overall safety of a system that depends on the correct response of the safety system response to its inputs, including safe handling of operator errors, hardware failures and environmental changes (fires, lightning, etc.). The definition of safety is “freedom from unacceptable risk” of physical injury or of damage to the health of people, either directly or indirectly. It requires a definition of what is acceptable risk, and who should define acceptable risk levels. This involves several concepts, including:

- Identifying what the required safety functions are, meaning that hazards and safety functions have to be known. A process of function reviews, formal hazard identification studies (HAZID), hazard and operability (HAZOP) studies and accident reviews are applied to identify the risks and failure modes.
- Assessment of the risk-reduction required by the safety function. This will involve a safety integrity level (SIL) assessment. A SIL applies to an end-to-end safety function of the safety-related system, not just to a component or part of the system.

- Ensuring the safety function performs to the design intent, including under conditions of incorrect operator input and failure modes. Functional safety management defines all technical and management activities during the lifecycle of the safety system. The safety lifecycle is a systematic way to ensure that all the necessary activities to achieve functional safety are carried out, and also to demonstrate that the activities have been carried out in the right order. Safety needs to be documented in order to pass information to different engineering disciplines.

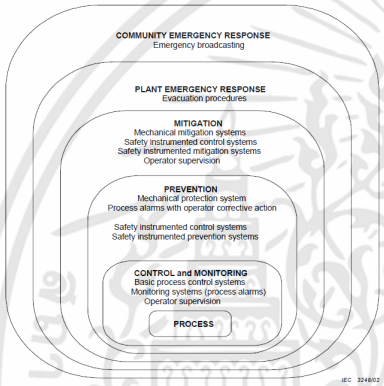


Fig.4 Typical risk reduction methods found in process plants.

For the upstream oil and gas industry, safety standards comprise a set of corporate, national and international laws, guidelines and standards. Some of the primary international standards are:

- IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems.
- IEC 61511 Functional safety - Safety instrumented systems for the process industry sector.

A safety integrity level show in Table 1 is not directly applicable to individual subsystems or components. It applies to a safety function carried out by the safety instrumented system (end-to-end: sensor, controller and final element).

Table 1 - Safety integrity levels.

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

The SIS is a collection of sensors, controllers and final elements that execute one or more SIFs/safety loops in Fig. 5 that are implemented for a common purpose. Each SIF has its own safety integrity level (SIL) and all sensors, controllers and final elements in one SIF must comply with the same SIL. When safety system is used in demand mode the standard requires that its $PFD_{(AVG)}$ calculation of SIF in Eq. (1).

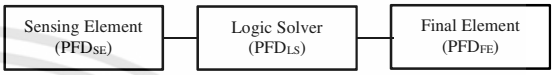


Fig.5 Typical of Safety Instrumented Functions (SIF).

$$PFD_{(AVG)} = PFD_{(SE)} + PFD_{(LS)} + PFD_{(FE)}, \quad (1)$$

The SIS is typically divided into the following subsystems:

- Emergency shutdown system (ESD) to handle emergency conditions (High criticality shutdown levels).
- Process shutdown system (PSD) to handle non-normal but less critical shutdown levels.

3.1 EMERGENCY SHUTDOWN (ESD) AND PROCESS SHUTDOWN (PSD)

The emergency shutdown and process shutdown (PSD) systems will take action when the process goes into a malfunction or dangerous state. For this purpose, the system maintains four sets of limits for a process value, LowLow (LL), Low (L), High (H) and HighHigh (HH). L and H are process warning limits which alert to process disturbances. LL and HH are alarm conditions and detect that the process is operating out of range and there is a chance of undesirable events and malfunction. The emergency shutdown actions are defined in a Cause and effect chart show in Fig. 6 based on a HAZOP of the process. Thus, a typical ESD function might require a SIL 2 or even SIL 3 level, while PSD loops could be SIL 1 or SIL 2.

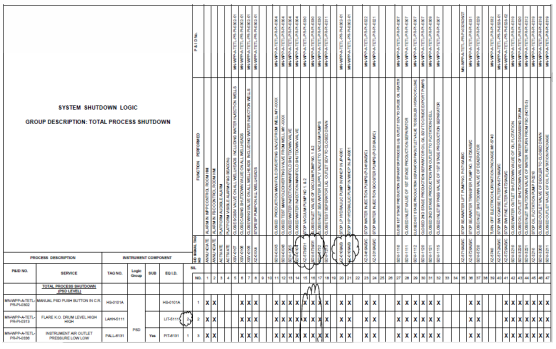


Fig.6 Cause and effect chart.

4. CASE STUDY FOR PROCESS CONTROL SYSTEM AND SAFETY INSTRUMENTED SYSTEM DESIGN FOR WELLHEAD PROCESSING PLATFORM (WPP)

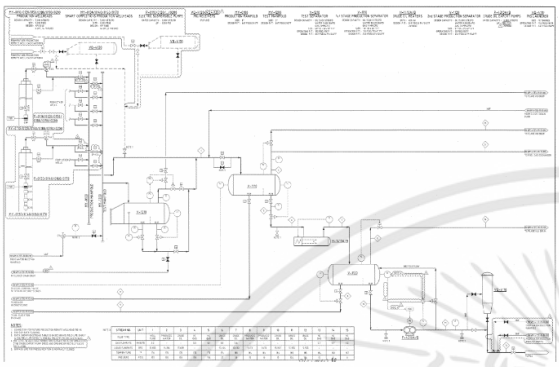


Fig.7 Process flow diagram for WPP.

5. RESULTS

A process control system for Wellhead Processing Platform (WPP) show in Fig. 7 are implemented by Yokogawa's Centum VP which its use for operate and monitoring the status of equipment under control via graphic of Human Machine Interface (HMI) in Fig.8. The safety instrumented systems are implemented by Yokogawa's ProSafe-RS which its use for logic interlocking of ESD system and PSD system show in Figs.9 to 11.

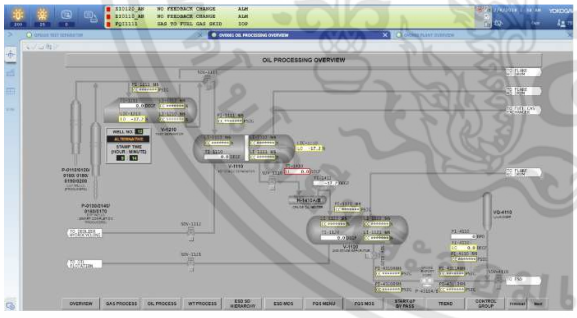


Fig.8 HMI's Graphic for oil processing overview.

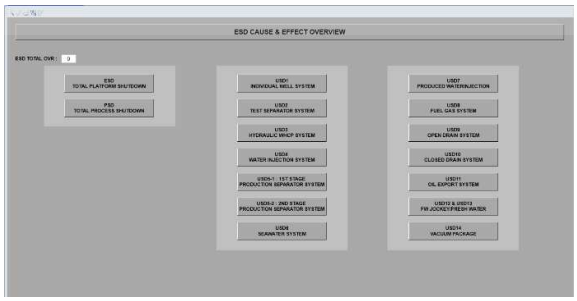


Fig.9 HMI's Graphic for ESD Cause & Effect overview.

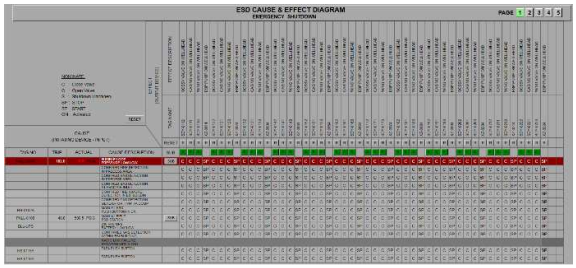


Fig.10 HMI's Graphic for ESD Cause & Effect diagram.

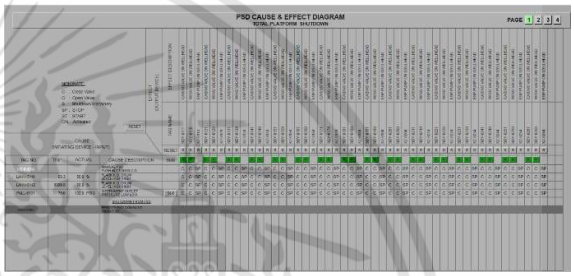


Fig.11 HMI's Graphic for PSD Cause & Effect diagram.

For the application programming language of logic interlock for ESD & PSD show in Fig.11, In this case study function block programming is used. In additional, for the logic concept of ESD & PSD system, field devices should be "fail safe." In most cases this means that the devices are normally energized (logic 1), output solenoid valves should be supplied with latching mechanisms so that when a trip condition (logic 0) occurs the valves will be go to safe state (Shutdown process).

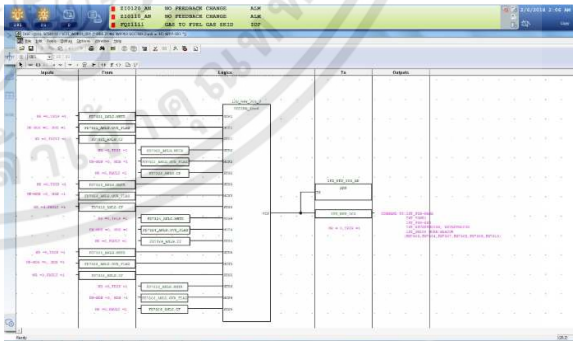


Fig.11 Logic interlocking for ESD & PSD.

6. CONCLUSIONS

In this paper, We have proposed overview of the main processes control and safety instrumented system design for upstream oil and gas industry with two main system: (1) Distributed control system .(2) Safety instrumented systems for guideline to people with an interest in the upstream oil and gas industry.

REFERENCES

[1] Paul Gruhn, P.E., CFSE and Harry Cheddie, P.Eng., CFSE., “SAFETY INSTRUMENTED SYSTEMS: Design, Analysis, and Justification,” 2nd Edition.
[2] William M. Goble and Harry Cheddie., “Safety Instrumented Systems Verification:Practical Probabilistic Calculations”.
[3] IEC 61508-1:2010., “Functional safety of electrical/ electronic/programmable electronic safety-related systems”.
[4] IEC 61511-1:2016., “Functional safety Safety instrumented systems for the process industry sector”.
[5] Havard Devold., “Oil and gas production handbook,” Edition 3.0 Oslo, August 2013.

Technical Information

Safety Instrumented System
ProSafe-RS
System Overview

TI 32R01B10-01E

YOKOGAWA
Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan
Tel.: 81-422-52-5634 Fax.: 81-422-52-9802

TI 32R01B10-01E

7th Edition Sep. 2013 (YK)

Introduction

ProSafe-RS is a safety instrumented system conforming to IEC 61508. This manual explains the various features and functions of safety instrumented systems that ProSafe-RS provides.

Structure of This Manual

This manual provides an overview of the ProSafe-RS system. After reading this manual, see the other documents, such as General Specifications, Instruction Manuals, and so forth, for more detailed coverage of various topics.

This manual consists of 7 chapters. Chapter 1 explains Safety Instrumented System, from Chapter 2 to Chapter 7 explains respectively Features, System Configuration, Safety Control Station (SCS), Test Functions, Related Packages and HIS Operation and Monitoring of ProSafe-RS.

Reference Documents

As for the configuration of whole system, refer to the following document.

- Integrated Production Control System CENTUM VP System Overview (General Overview) (TI 33K01A10-50E)
- 2, “System Configuration” in CENTUM CS 3000 Integrated Production Control System System Overview (TI 33Q01B10-01E)

Target Readership for This Manual

This manual is mainly intended for:

- Managers who are planning to purchase a new safety instrumented system.
- Instrumentation, Power and Computer Engineers who are evaluating ProSafe-RS for purchase or who will be in charge of installation.

Representation of Drawings in This Manual

- Drawings are represented in this manual as illustrations; some features may be emphasized, and some simplified or omitted.
- The drawing illustrations are to help you understand the functions; dimensions, labels and visible features may differ slightly from those of actual drawings.

Trademarks

- ProSafe, CENTUM and Vnet/IP are registered trademarks of Yokogawa Electric Corporation.
- All other company and product names mentioned in this document are trademarks or registered trademarks of their respective companies.
- We do not use TM or ® mark to indicate those trademarks or registered trademarks in this document.

1. Safety Instrumented System (ProSafe-RS)

This chapter explains the positioning of safety instrumented system, safety lifecycle and safety evaluation.

Protection Layers of Plant and Safety Instrumented System

IEC 61511 utilizes the concept of protection layers in order to achieve safety, freedom from unacceptable risk. Each protection layer is required to set quantitative risk reduction goals as well as means of achieving these goals independently without interfering with other layers.

According to this idea of protection layers, safety instrumented system is positioned within the mitigation and prevention layers.

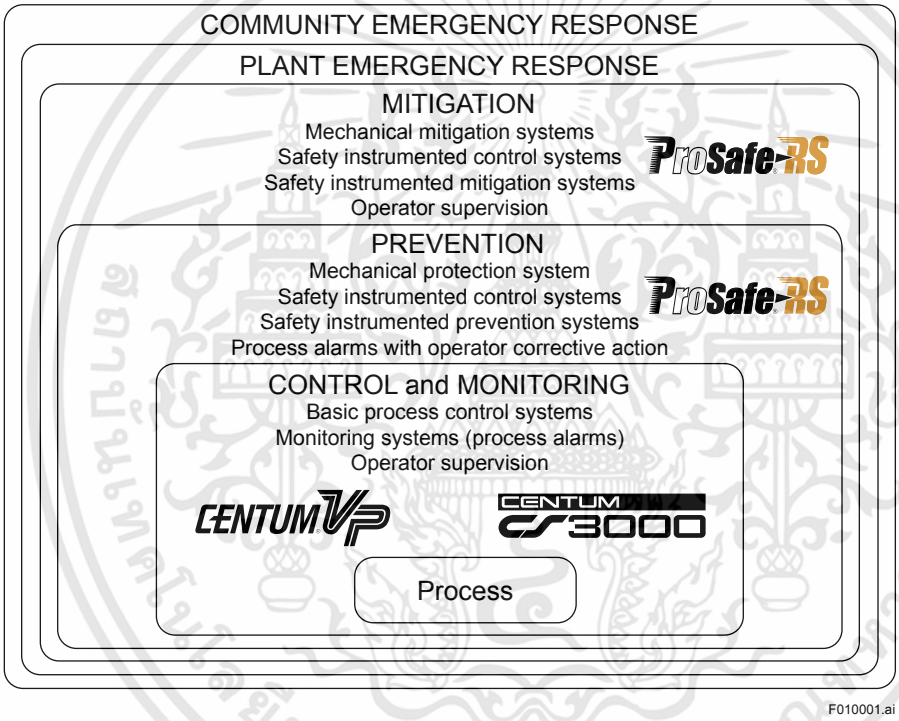


Figure Protection Layers and Positioning of Safety Instrumented Systems

Safety Life Cycle

IEC 61508 specifies the management of safety-related systems in terms of lifecycles. In the safety lifecycle, the tasks involved, from the conceptual stage in which a basic safety instrumented system is designed to the decommissioning of the system, are divided into 16 phases as shown in the figure below, and the required tasks to be achieved in each phase are defined. The purpose of these definitions is to minimize the likelihood of human-induced errors. For example, “Hazard and risk analysis” shown in the third frame sets requirements to clarify the hazards and hazardous events that may occur in a plant and its control devices (e.g., DCS).

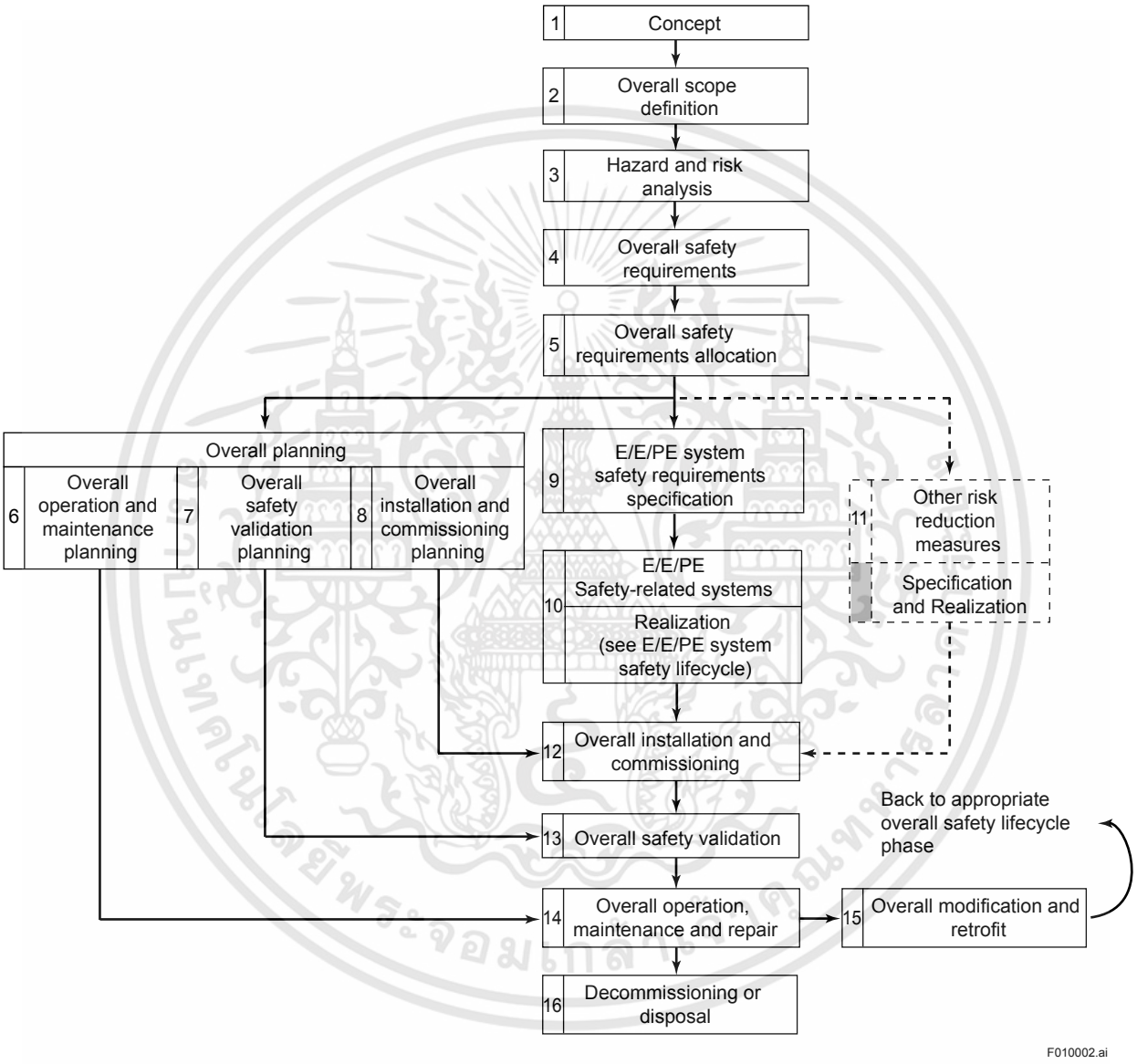


Figure Safety Lifecycle

2. Features of ProSafe-RS

ProSafe-RS is a safety instrumented system conforming to safety rating SIL3 as defined by IEC 61508. It not only satisfies requirements to be used in safety instrumentation by itself, but also achieves higher efficiency of operations through integration with CENTUM VP or CENTUM CS 3000 R3 (hereinafter, "CENTUM VP/CS 3000").

Implementation of Control System Technologies

ProSafe-RS employs the CENTUM VP/CS 3000 architecture in its base technologies. Because of this, the following advantages can be expected.

- Basic concepts, such as hardware installation and maintenance methods, can be shared with CENTUM VP/CS 3000.
- Since connection via Vnet/IP or V net is possible, system construction and interface design are made simpler, allowing an improvement of the total engineering efficiency, including design and installation costs.

Achievement of Safety Rating SIL3 with Single Configuration

ProSafe-RS has built-in dual-redundant system matching and self-diagnosis mechanisms embedded within one CPU module and one input/output module, thus making it conform to SIL3 as defined by IEC 61508 in a single component. This allows implementing SIL3 safety loop in a single configuration together with the CPU module and input/output module.

Achievement of High Availability by Redundancy

ProSafe-RS allows selecting dual-redundant module configurations in order to achieve high availability. Since it achieves SIL3 with a single configuration, the safety level of SIL3 can be maintained even if a CPU module or input/output module on one side fails in the dual-redundant configuration.

Security Measures

ProSafe-RS is equipped with the security functions described below.

- Security by using a password for a project database and/or SCS (Safety Control Station)
- The IT security function based on Windows security feature (Revision R2.01 or later)
- Security by giving the control access permission to the user in the CENTUM VP/CS 3000 integration

Integrated Monitoring with CENTUM VP/CS 3000

ProSafe-RS realizes integration with CENTUM VP/CS 3000 and provides a communication to establish access with ProSafe-RS's SCS via Vnet/IP or V net from HIS and FCS. This function allows monitoring SCS operation using the same interface (view or window) as of monitoring FCS from HIS. FCS can read data of SCS. This can be done by the same interface (tag name) as of reading data of one FCS from other FCS.

3. System Configuration of ProSafe-RS

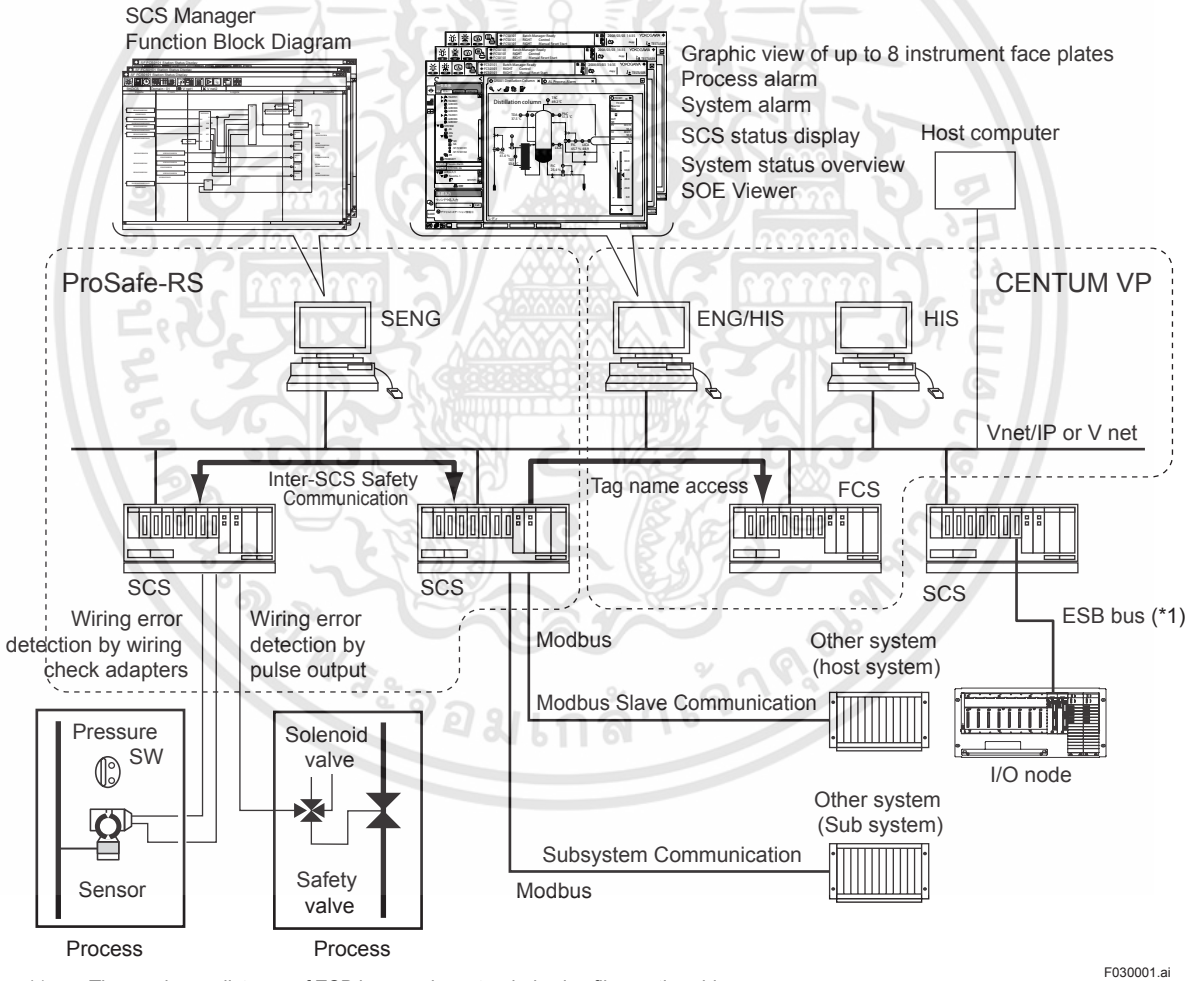
ProSafe-RS is comprised of SENGs (safety engineering PCs) equipped with engineering and maintenance functions and controller SCSs (safety control stations) for safety. The available configurations are described below.

- **The configuration in which ProSafe-RS is integrated with CENTUM VP/CS 3000**
- **The configuration in which ProSafe-RS is connected to systems other than CENTUM VP/CS 3000 via Modbus**

System Overview

In ProSafe-RS, CPU modules and input/output modules comprising an SCS are placed in single configuration and can be applied to applications of up to IEC 61508 SIL3. If it is desired to improve the availability, modules in required areas are made dual-redundant.

By using inter-SCS safety communication, it is possible to configure SIL3 safety loops across multiple SCSs via Vnet/IP or V net.



*1: The maximum distance of ESB bus can be extended using fiber optic cable.

Figure ProSafe-RS System Configuration (Example of CENTUM VP Integration Structure)

- In a CENTUM VP/CS 3000 integration structure, it is possible to monitor operations of both FCS and SCS with HIS.

- SCS engineering is performed from SENG. FCS and HIS engineering are performed from ENG (engineering station for CENTUM VP/CS 3000). Engineering of CENTUM VP/CS 3000 integration function is performed from both SENG and ENG.
  SENG, ENG and HIS software can be installed together in a single PC or separately in several PCs. (*1)
- Host computer that performs production control can access data of FCSs and SCSs via an OPC interface by installing the Exaopc OPC interface package of CENTUM VP or CS 3000 (for HIS).
  By using the SOE OPC interface package of ProSafe-RS, it is also possible to access SOE information of SCS from a host computer.
- In a CENTUM VP/CS 3000 integration structure on V net, it is necessary to connect SENG, ENG and HIS via Ethernet during the engineering.
- In a CENTUM VP/CS 3000 integration structure, it is possible to connect only HIS to ProSafe-RS. In this case, the configuration is the same as the above system configuration without FCS.
- Using the external communication function blocks prepared in ProSafe-RS, it is possible to communicate with external devices without interfering the safety functions of an SCS. In case of a CENTUM VP/CS 3000 integration structure, it is possible to write data in an SCS from HIS and FCS.

  Note that external communication function blocks are required when writing data to an SCS from external devices.
- It is possible to connect an SCS with other systems using Modbus communication functions. SCSs support subsystem communication functions that allow the SCS side to connect to other systems as a communication master, and Modbus slave communication functions that allow other systems to establish connections as Modbus communication masters. In both cases, communication modules are mounted on SCS nodes and used to connect with other systems.
  Note that Modbus communication functions cannot be used in safety loops. They shall be used as interference-free applications.

*1: When ProSafe-RS R2.xx and CENTUM VP R4.02 or later software are installed in the same PC, ProSafe-RS must be R2.03 or later. In the integration of ProSafe-RS R3 and CS 3000, SENG functions and ENG functions, or SENG functions and HIS functions cannot be installed in the same PC. For more detail, please contact our sales representative or your local distributor.

5. Test Functions

The test functions of ProSafe-RS are used for effective debugging of applications, and useful in debugging when you create or change applications.

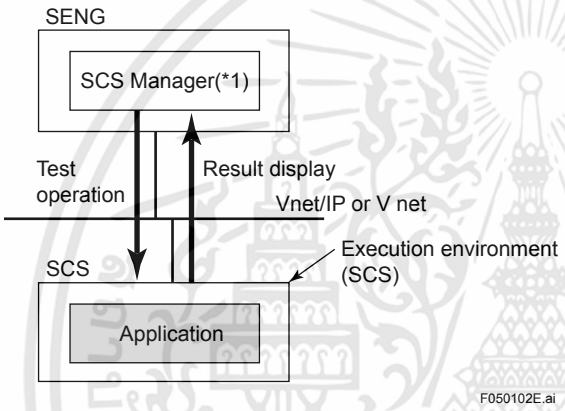
There are three types of tests, target tests, SCS simulation tests and logic simulation tests.

Target Tests

In a target test, an application is executed on an actual SCS.

It is possible to execute tests in a status where inputs/outputs are disconnected, i.e., without any input/output modules connected, using the forcing function.

In a target test, the test according to each SCS security level can be executed.



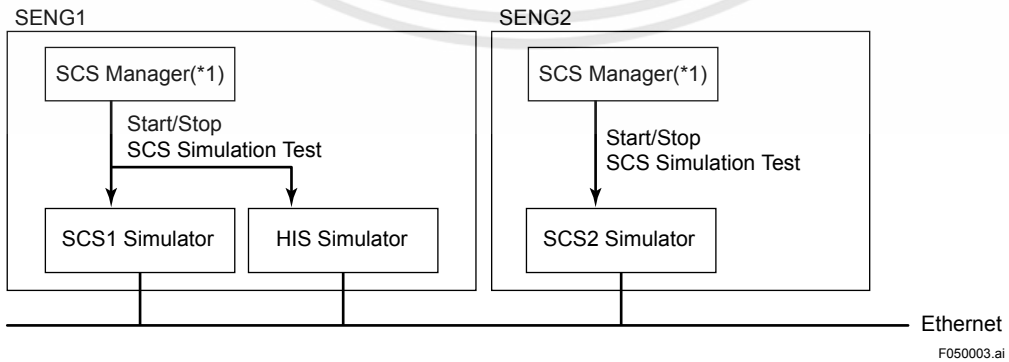
*1: A function that controls system engineering and maintenance tasks of an SCS, such as definition of applications to be executed on the SCS, database generation test functions, etc.

Figure Target Test

SCS Simulation Tests

In an SCS simulation test, an application is executed on an SCS simulator on an SENG. The integrated operation environment for CENTUM VP/CS 3000 is required.

If you use two or more SCS simulators, the test for inter-SCS safety communication can be executed. In an SCS simulation test, the test according to each SCS security level can be executed.

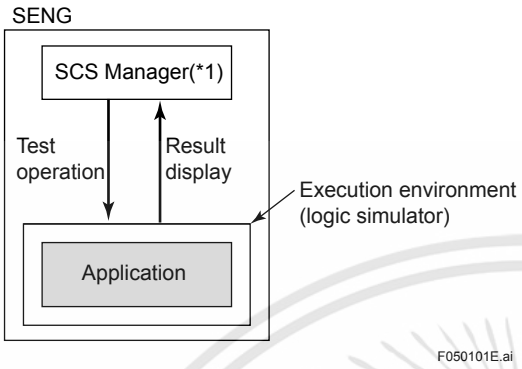


*1: A function that controls system engineering and maintenance tasks of an SCS, such as definition of applications to be executed on the SCS, database generation test functions, etc.

Figure SCS Simulation Tests

Logic Simulation Tests

In a logic simulation test, an application is executed using a logic simulator on an SENG, which allows debugging application logic of each SCS. In a logic simulation test, the test regardless of each SCS security level can be executed.



*1: A function that controls system engineering and maintenance tasks of an SCS, such as definition of applications to be executed on the SCS, database generation test functions, etc.

Figure Logic Simulation Test

Technical Information

Integrated Production Control System
CENTUM VP
System Overview (General Overview)

TI 33J01A10-01EN

[Release 6]

YOKOGAWA
Yokogawa Electric Corporation
2-9-32, Nakacho, Musashino-shi, Tokyo, 180-8750 Japan

1. CENTUM VP Overview

Yokogawa is the world's first company that introduced the distributed control system (DCS) in 1975 - the first series of CENTUM Systems. Ever since, Yokogawa kept developing and enhancing the CENTUM series systems by complying with what customers (managers, operators, engineers, and so on) requirements. As the generations of CENTUM advanced Yokogawa kept improving its product quality achieving the highest level of reliability in the market. CENTUM systems have been adopted by customers around the world to control and monitor their industrial plants.

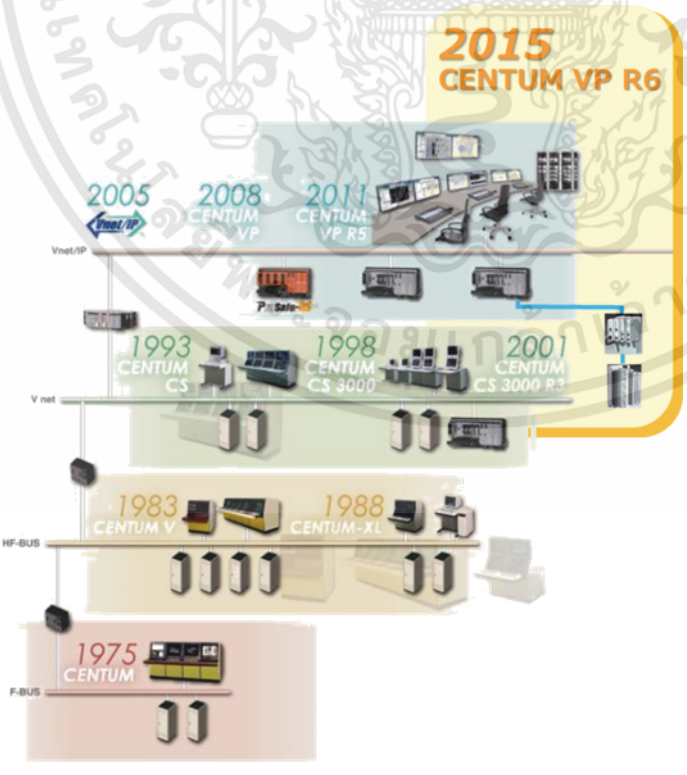
1.1 History of CENTUM

Innovations of operation in the process industries have come a long way since the age of panel-mounted loop controllers. In early 1970s, a panel operator was assigned for operation per panel. However, by the introduction of a DCS, operators' ways of working have drastically changed. Operators can grasp the plant-wide operation by sitting in a central control room (CCR). And their work scope has largely been extended.

The CENTUM systems kept evolving to increase productivity and improve plant operations in the past 40 years, and CENTUM VP is the 8th generation of the CENTUM Series. Yokogawa has adopted the latest state-of-the-art technologies of the time to develop the systems, keeping return on the investment (ROI) and the total cost of ownership (TCO) in minds.

Yokogawa has always been offering a smooth upgrade path from an existing CENTUM system into the latest one. It provides customers the benefits of using the existing system as long as they wish yet allows them to adopt the latest technologies with a minimum investment. Yokogawa's CENTUM systems have been replaced with the latest ones smoothly with minimum shutdown time.

Yokogawa continually endeavors to meet customers' needs by providing highly reliable control systems based on the leading edge technology.



F010101.ai

Figure History of CENTUM

1.2 CENTUM at Work

Yokogawa has sold over 25,000 CENTUM projects in all kinds of industrial plants worldwide such as oil and gas, petrochemicals, chemicals, power, pulp and paper, pharmaceuticals, food, iron and steel, waste, and water and sewage treatment. The majority of the customers are from oil and gas, and petrochemical industries. It means that once the CENTUM system is delivered and start its operation, it has to be in operation non-stop.

In the past 40 years of experience, Yokogawa is reputed with the high reliability of the CENTUM system winning customer satisfactions. Yokogawa is engaged in the global purchase agreements with world major customers as their sole instrumentation supplier. Yokogawa needs only one project to convince customers of our capability and win trust. Once Yokogawa system is delivered, customers stay with Yokogawa.

As of March, 2015

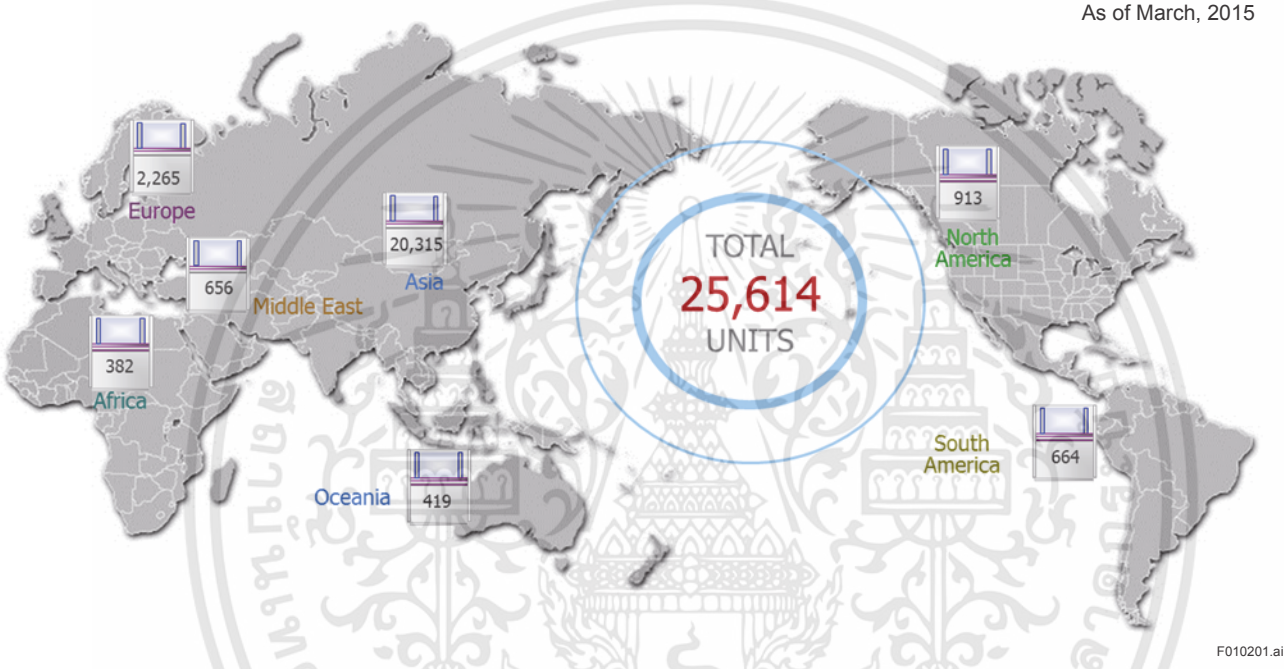


Figure CENTUM at work

1.3 CENTUM VP Advantages

For Operations

- **Safe and unified plant operations**

  Universal interface for control, safety, and asset intelligence.
  Embedded mechanisms to prevent information overload

- **Non-stop improvement**

  Continuous systemization of operational best practices and context specific operational advisories.

For Engineering

- **Flexible system design is enabled by the new engineering environment**

  Automation Design Suite (AD Suite) is a new integrated engineering environment released from CENTUM VP R6, which enables to design and configure control applications independently from configurations of FCSs or I/O module assignments. The I/O design can also flexibly be changed even after designing the control applications.

For Controllers

- **Highly-reliable controllers**

  CENTUM's FCS is highly reliable: it hardly fails, keeps operating normally even if it is failed, and quickly recovers from failures. These features are the foundation of the long and stable operations of the plant.

  With CENTUM VP R6, a new controller complying with the N-IO (*1) has been released.

*1: A single type of I/O module handles all DI, DO, AI, and AO signals which are changeable by the software. For details, refer to System Overview (for FCS) (TI 33J01A12-01EN).

For Production Management

- **Faster Plan, Do, Check, and Act cycle for agile adaptation**

  MES and enterprise system integration is enabled by using S95 andB2MML standards

- **Secure and standard-based information integration**

  Built-in control network security certified by experts

For Maintenance

- **Continuous evolution without compromising asset availability**

  Evergreen evolution with online upgrades and modifications. It is the most reliable platform with no single point of failure

- **Long-term investment protection**

  Upgrade paths is incorporated before any new release. We have over 40 years of backward compatibility.

For Project

- **Faster project execution with fewer integration risks**

  Single-source integrated solutions for control system (DCS), safety instrumented system (SIS), embedded plant information management system (PIMS), intelligent RTU & SCADA, and turbine controller.

2. System Configuration

CENTUM VP has a simple & common architecture consisting of human machine interfaces called human interface station (HIS), field control stations (FCS), and a control network. These three basic components support facilities from the tiny to very large and complex with up to 1,000,000 tags.

The Design Concept of CENTUM VP System Configuration

CENTUM VP is designed based on the concept to keep the plant operation availability high. Customers expect Yokogawa products to perform its functions without failure so that the plant operations shall not stop. Yokogawa developed our own FCSs so that we can meet up with the customers' expectations. Quite a number of FCSs are still in operation even after 20 or more years passed since those are originally installed. It is owing to the high quality of the products themselves that has been supported by the total serviceability such as skilled manufacturing, quality control, after sales service and appropriate training.

Self-independent Controller

CENTUM VP's FCSs are designed to work without HIS. The fundamental controls can be done only by the FCSs, and all the process data, control logic, and procedures are contained in the controllers. HIS works only as a monitor screen under the normal condition. In Yokogawa's system configuration, FCSs are acting like servers and HISs as clients. The hardware availability of FCS (=server) is 99.99999% which comes from the basic policy in product designs. Our FCSs are designed; (a) not causing failures easily (fault-avoidance), (b) to continue controlling the plant even it fails (fault-tolerant), and (c) to recover from failures as quickly as possible (maintainability). It is the crystallization of Yokogawa's leading edge technology.

Why CENTUM VP does not have Client-Server Concept?

In a typical server-client configuration, when the server fails, all the client HMIs come to stop. It means that all the controls and the data of the plant are lost until the server is recovered. This is certainly not an acceptable situation for plant operations in reality. In order to prevent server down as much as possible, an expensive server machine is needed or to have a redundant configuration.

CENTUM VP's Field Control Stations (FCSs) are far superior to the PC servers on account of availability, even those with redundant configuration. Each FCS runs independently that hedges the risk of causing serious damage to the plant by a single failure.

PC servers become obsolete in a few years of cycles, but FCSs with appropriate maintenance runs for many years. The robustness of FCS saves the cost of repairs and damages to the plants as the plant does not fail. In the viewpoint of total cost of ownership (TCO), Yokogawa's FCS is more economical.

CENTUM VP Components

In this section, a term “PC” means an Intel x86-based computer which has inherited IBM PC/AT compatible machine, and it runs on the Microsoft Windows OS. The PC means not only a personal computer but also a workstation and a server.

Human Interface Station (HIS)

CENTUM VP uses a PC for its human machine interface. It is called HIS when the software packages for Operation and Monitoring Functions are installed there.

Engineering Station (ENG)

ENG is a computer with Engineering Function software packages of AD Suite. AD Suite consists of Automation Design Server (AD Server), Automation Design Organizer (AD Organizer), and VP Builder. ENG allows you to use AD Organizer and VP Builder of AD Suite.
For details on AD Server, AD Organizer, and VP Builder, refer to Chapter 3.

Field Control Station (FCS)

FCS is a high reliability controller designed and manufactured by Yokogawa. It performs control computation functions for each function block and input/output functions for process and software inputs/outputs. FCS hardware can be selectable from a cabinet type or a rack-mountable type. It consists of a field control unit (FCU) and node units to mount input/output modules. It enables to configure a scalable system by connecting several node units in a FCS in accordance with the I/O points.

Generic Subsystem Gateway (GSGW)

GSGW is a station for operation and monitoring subsystems. By using a PC as a platform, it establishes subsystem communications via OPC DA(*1) interface defined by the OPC Foundation. Subsystem data is assigned to the GSGW’s function blocks to be controlled and monitored via HIS in the same manners as other control stations.

*1: Open Product Connectivity, Data Access

System Integration OPC Station (SIOS)

SIOS is a station to integrate CENTUM VP and the third-party process control systems (PCSs). It enables CENTUM VP to exchange data with and receives alarms and events from the third-party PCS via OPC interface.

Unified Gateway Station (UGS/UGS2)

UGS/UGS2 is a station exclusively used for Vnet/IP to integrate CENTUM VP and subsystem controllers such as STARDOM controllers (FCN/FCJ) and other third-party programmable logic controllers (PLCs). Its standard function allows CENTUM VP to communicate with subsystem controllers via various communication protocols such as OPC DA, OPC A&E (*1), Modbus, Ethernet/IP, or IEC 61850 IED. UGS/UGS2 enables CENTUM VP to control and monitor those subsystems in the same way as CENTUM VP FCS. UGS/UGS2 can be configured in dual-redundant using 2 computers.

*1: Open Product Connectivity, Alarms and Events

Advanced Process Control Station (APCS)

APCS performs advanced control and computation functions for improving plant operation efficiencies.

Bus Converter (BCV)

BCV relays CENTUM VP communications with other CENTUM VP and older CENTUM systems such as CENTUM CS 3000, CENTUM CS 1000, CENTUM CS, CENTUM-XL, CENTUM V, and μXL.

V net Router (AVR)

AVR connects and transmits control communications between the Vnet/IP and V net domains. The control data can be sent and received in both ways between the Vnet/IP and V net domains. It enables control and monitoring of the control stations among other domains.

Wide Area Communication Router (WAC Router)

WAC Router is a relay equipment to connect 2 Vnet/IP domains via Wide Area Network (WAN). Operations and monitoring that are distributed in remote areas can be realized.
Satellite communication can also be used as a WAN.

Layer 2 Switch (L2SW)

L2SW relays communications among devices connected to the Vnet/IP network. The Vnet/IP domain refers to the Vnet/IP system area connected by L2SW. Use L2SW with 1 Gbps communication speed in the Vnet/IP domain.

Layer 3 Switch (L3SW)

L3SW relays communications among Vnet/IP domains. Use L3SW with 1 Gbps communication speed.

Control Network (Vnet/IP)

“Vnet/IP” is an IEEE802.3 Ethernet compliant, 1Gbps redundant network. The control network links stations such as HIS, FCS and BCV. It incorporates Yokogawa’s technology to achieve deterministic, reliable, and secure communications.

Digital Fieldnetworks

CENTUM VP supports FOUNDATION fieldbus, HART, PROFIBUS-DP, DeviceNet, Modbus, Modbus/TCP, Ethernet/IP, and ISA100.11a field wireless network.

Network-based Control System (STARDOM)

Yokogawa’s intelligent-hybrid remote telecommunication controllers are ideal for the oil and gas upstream market. They can be seamlessly integrated, via the UGS, to CENTUM VP.

- **Autonomous Controller (FCN/FCJ)**

  These controllers utilize the global Standard IEC 61131-3 as the engineering tool.

- **Versatile Data Server Software (ASTMAC VDS)**

  VDS is a SCADA software which uses Web browser (Internet Explorer) for HMI display.

Safety Instrumented System (ProSafe-RS)

This is Yokogawa's TÜV SIL3 certified premier safety instrumented system. It incorporates Yokogawa's own Pair and Spare and Vnet/IP technologies and offers unprecedented synergy with CENTUM VP.

- **Safety Control Station (SCS)**

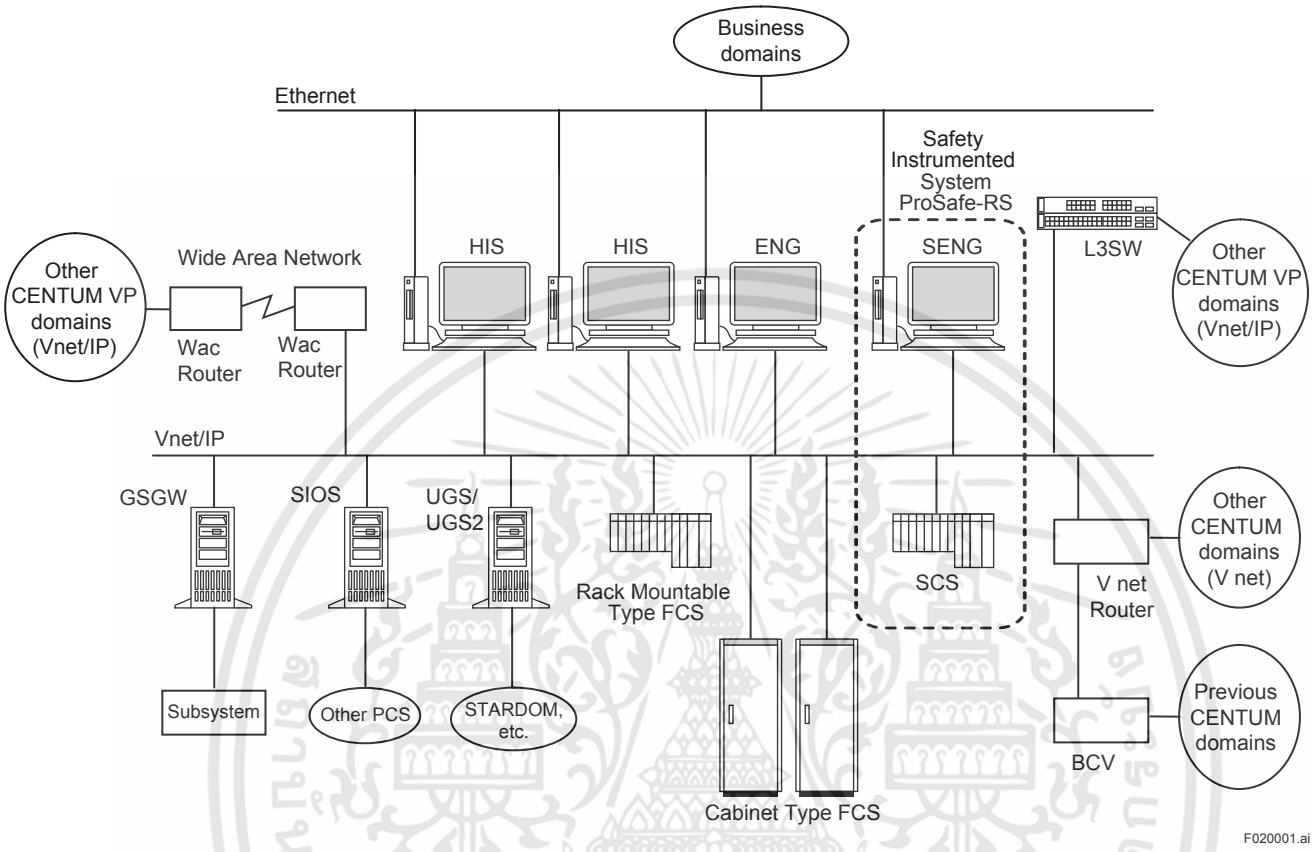
  SCS is a Yokogawa manufactured safety controller that executes logics for systems including interlock, emergency shutdown and fire and gas protection.

- **Safety Engineering Station (SENG)**

  An off-the-shelf PC that performs SCS generation and maintenance management.

Overall System Configuration

The below drawing shows an overall system configuration of the CENTUM VP integrating previous CENTUM system, the ProSafe-RS safety instrumented system, and other subsysems.



CENTUM VP system specifications are shown below.

- Number of tags that can be monitored: 100,000 tags
- Number of stations that can be connected: 256 stations

CENTUM VP can expand the specifications for a very large system.

- Number of tags that can be monitored: 1,000,000 tags
  (When using VP6H4000 Million Tag Handling Package. See GS 33J05K10-01EN.)

If an expansion of the number of stations is required, please contact to Yokogawa's sales representative.

Control Logic Dependency Analysis

A list of tag names connection destination of analysis keys is displayed in the control logic dependency analysis. Furthermore, a list of destination beyond the connection destinations can also be displayed using the connection destinations as new analytical keys in a hierarchical format. Each of the dependency elements displayed in a hierarchical format can be collapsed or expanded as needed.

Analysis key (control logic dependency)

- Tag name
- Tag name.data item name
- User-defined label name

The dependency is displayed in a hierarchical format with the analysis key on the top as shown in the following figure.

<Tag name> (Analysis key)
- <Tag name>.<Data item name> (Item related to the analysis key)
- <Element name>.<Data item name> (Item related to the analysis key)

<Tag name> (Analysis key)
- <Tag name>.<Data item name> (Item related to the analysis key)

<Tag name>.<Data item name> (Analysis key)
- <Tag name>.<Data item name> (Item related to the analysis key)
- <Element name>.<Data item name> (Item related to the analysis key)

<Tag name> (Analysis key)
- <Tag name>.<Data item name> (Item related to the analysis key)
- <Element name>.<Data item name> (Item related to the analysis key)

F030503.ai

Logical and Physical Relationship Analysis

The logical attributes and physical assignment of I/Os can be displayed in a logical and physical analysis function view.

Analysis key (logical and physical relationship)

- Application module name
- Tag name
- P&ID tag name
- Station name
- I/O module name

The table below shows the items displayed in a logical and physical relationship view.

Table Display Items in Logical and Physical Relationship View

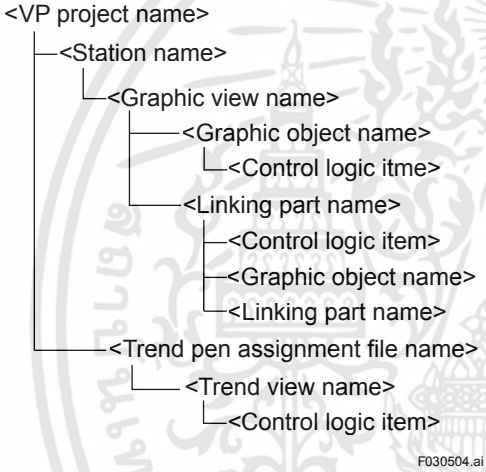
Category	Display item	Description
Logic	Flag display	Displays the cause flag and impact flag.
	P&ID tag	Displays the P&ID tag name.
	I/O tag name	Displays the I/O tag name or user-defined label name.
	Module	Displays the application module name to which the I/O is connected.
Physical	Flag display	Displays the cause flag and impact flag.
	VP project	Displays the VP project name.
	Station	Displays the station name.
	Train	Displays “IOM” for the I/O of an FIO module. N-IO Displays “IOM2” for the I/O of an N-IO module.
	Node	Displays the node number.
	I/O module	Displays the model of the I/O module.
	Unit	Displays the unit number. Blank for the I/O of an FIO module.
	Terminal	Displays the terminal number.

Graphic Dependency Analysis

The following graphic objects including the analytical key can be displayed in a hierarchical format in a graphic dependency analysis view in the same way as with the control logic dependency analysis.

- Analysis key (graphic dependency)
- VP project name
- Station name
- Window name
- Trend file name
- Tag name
- Graphic object name

The graphic objects including the analyticalsis key are displayed in a hierarchical format as follows.



ประวัติผู้เขียน

ชื่อ-นามสกุล	นายชลิต อยู่สำราญ
วัน เดือน ปีเกิด	4 เมษายน 2529
ที่อยู่	เลขที่ 7 ซอยสุขสวัสดิ์ 15/1 แขวงบางปะกอก เขตราษฎร์บูรณะ 10140
ประวัติการศึกษา	2552 วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมระบบควบคุมและเครื่องมือวัด TH SarabunPSKมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี