

หน่วยที่ 4 ความปลอดภัยเชิงระบบ

1. ความเป็นมา ก่อนทศวรรษที่ 1940 การดำเนินงานด้านความปลอดภัยแบบลองผิดลองถูกเกิดเหตุแล้วแก้ไข เช่นเครื่องบินตกแล้วแก้ไข ตกอีกแล้วแก้ไขบินต่ออีก จึงมีคนในวงการบินกล่าวว่า บิน-แก้ไข – บิน (Fly-Fix-Fly)

- 1962 กองทัพอากาศสหรัฐอเมริกาจัดพิมพ์ System Safety Engineering For the Development to Air Force Ballistic Missles
- 1963 กองทัพอากาศอเมริกา จัดพิมพ์ MIL-S-38130 General Requirements for Safety Engineering of System and Associated Subsystems and Equipment
- 1963 มีการก่อตั้งสมาคมเชิงระบบ (System Safety Society)
- 1966 กระทรวงกลาโหม สหรัฐอเมริกา ปรับปรุง MIL-S-38130 เป็น MIL-S-381308A
- 1969 มีการปรับปรุง MIL-S-38130 เป็น MIS-STD-882B System Safety Program Requirements

ต่อมาในช่วงทศวรรษที่ 1970-1980 ความก้าวหน้าในการทำ System Safety ของหน่วยงานที่สำคัญ ยังคงเน้นหนักไปที่อุตสาหกรรมที่มีอันตรายร้ายแรง

- 1970 – NASA จัดทำเอกสาร NHB 1700 (V3) System Safety
- 1973 – Atomic Energy Commission (AEC) จัดทำเอกสาร MORT-The Management Oversight and Risk Tree
- 1974 – จัดตั้ง System Safety Development Center ศูนย์ดังกล่าวได้ปรับปรุงเพิ่มเติมให้ MORE มีความเหมาะสมมากยิ่งขึ้น
- 1970 มีหลายหน่วยงานความปลอดภัยเชิงระบบแตกต่างกัน AEC จึงปรับปรุงนำส่วนที่ดีมารวมกันให้ผู้รับเหมาะช่วงนำไปใช้
- 1980 แนวคิดความปลอดภัยเชิงระบบถูกนำไปใช้ในอุตสาหกรรมทั่วไปโดยเฉพาะอุตสาหกรรมเคมี
- 1985 สถาบันวิศวกรเคมีแห่งสหรัฐอเมริกา(American Institute Of Chemical Engineers: AIChE) ได้จัดทำเอกสาร Guidelines of Hazard Evaluation Procedures ซึ่งเป็นเครื่องมือวิเคราะห์ความปลอดภัยเชิงระบบหลายเครื่องมือ อาทิ Hazard and Operability Study (HAZOP) Fault Tree Analysis (FTA)และ Failure Mode Effects, and Criticality Analysis (FMEA)
- ประเทศไทยพัฒนาอุตสาหกรรมในภาคตะวันออก นิคมมาบตาพุด ได้นำเครื่องมือเหล่านี้มาใช้ เรียนรู้กับผู้เชี่ยวชาญต่างประเทศ
- 2542 กระทรวงอุตสาหกรรมเห็นความจำเป็นโรงงานที่มีอันตรายสูงต้องใช้เครื่องมือเหล่านี้จึงออกกฎหมายบังคับใช้คือ ประกาศกระทรวงอุตสาหกรรม ฉบับที่ 3 เรื่องมาตรการคุ้มครองความปลอดภัยในการดำเนินงานที่ให้กำหนดหลักเกณฑ์การชั่งอันตราย การประเมินความเสี่ยง และการจัดทำแผนงานบริหารจัดการความเสี่ยง

2. ความปลอดภัยเชิงระบบ มีความหมายว่า เป็นการดำเนินงานด้วยวิธีทางวิศวกรรมและบริหารจัดการที่จะวิเคราะห์ว่ามีอันตรายใดบ้างในระบบที่วิเคราะห์นั้น แล้วทำการป้องกันควบคุมอันตรายที่จะทำให้คนบาดเจ็บและ/หรือทรัพย์สินเสียหาย

3. ความสำคัญของความปลอดภัยเชิงระบบ

- ให้ความสำคัญกับการชั่งอันตรายที่รอบด้านด้วยเครื่องมือหรือเทคนิคต่างๆ พิจารณาตลอดวงจรชีวิตของผลิตภัณฑ์และโครงการ
- โรงงานที่นำความปลอดภัยเชิงระบบมาใช้ จะได้รับความสมบูรณ์และบูรณาการ มาตรการเชิงรุกมากกว่าเชิงรับ

- การดำเนินงานด้านอาชีวอนามัยและความปลอดภัยของโรงงานที่นำเรื่องความปลอดภัยเชิงระบบมาใช้จะมีขอบเขตความปลอดภัยมากกว่าแบบดั้งเดิมที่ยึดการปฏิบัติตามกฎหมาย ซึ่งเป็นมาตรฐานขั้นต่ำเท่านั้น

แนวคิดของความปลอดภัยเชิงระบบ

1.องค์ประกอบของระบบ (System)



2. การวิเคราะห์อันตรายตลอดวงจรชีวิตผลิตภัณฑ์หรือโครงการ (Product or Project Lift Cycle) แบ่งออกเป็น 5 ระยะ

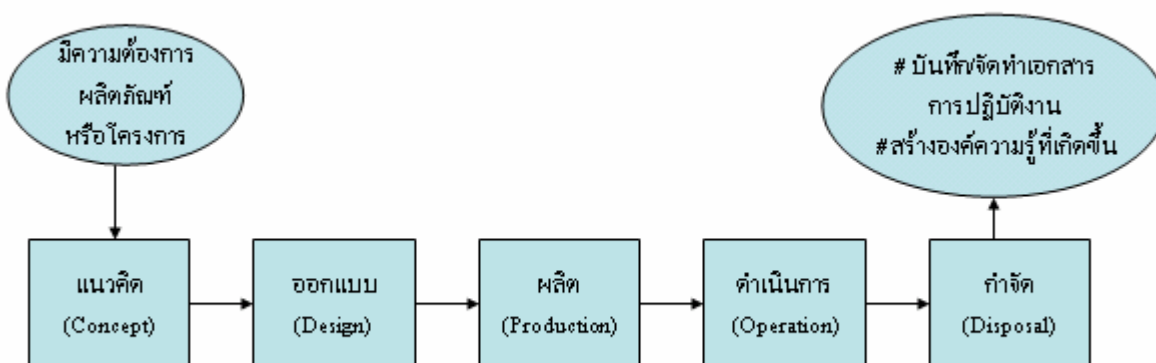
ระยะที่ 1 แนวคิด (Concept Phase) เป็นระยะของการพิจารณาความต้องการผลิตภัณฑ์หรือโครงการ เช่น โครงการใหม่ ผลิตภัณฑ์ใหม่ หรือเพิ่มสายการผลิต แล้วนำมากำหนดเป้าหมาย วัตถุประสงค์โครงการ พรรณนาโครงการ กำหนดการออกแบบ และผลลัพธ์ที่คาดหวัง

ระยะที่ 2 การออกแบบ (Design Phase) ชัดเจนมากยิ่งขึ้น การวาดผัง (Drawing) วางแผนงาน

ระยะที่ 3 การผลิต (Production Phase) เป็นระยะการผลิตสิ่งที่ต้องการให้ได้ผลลัพธ์ตามเป้าหมาย

ระยะที่ 4 การดำเนินการ (Operations Phase) นำผลลัพธ์ที่ได้มาใช้งาน สิ่งอำนวยความสะดวก อุปกรณ์เครื่องมือ หรือบริการ จะเห็นว่าการทำเรื่องความปลอดภัยเชิงระบบได้ผลอย่างไร ถ้าพบอันตรายก็ต้องปรับปรุงแก้ไข แต่จะแก้ไขยากกว่า ควรทำระยะแรกอย่างมีคุณภาพ

ระยะที่ 5 การกำจัด (Disposal Phase) กากผลิตภัณฑ์หรือของเสียที่เกิดขึ้น จะต้องได้รับการวิเคราะห์ ควบคุมอันตรายด้วย



3. การประมาณระดับความเสี่ยง เป็นตารางที่ปรากฏในเอกสาร MIL-STD-882 B,1984 ที่กระทรวงกลาโหมสหรัฐอเมริกาใช้ในการระบุว่าอันตรายนั้นเป็นความเสี่ยงที่ยอมรับได้หรือไม่ เรียกว่า **ดัชนีความเสี่ยง (Hazard Risk Index : HRI)**

4. ลำดับของการควบคุม (System Safety Precedence) ความเสี่ยงที่ยอมรับไม่ได้ วิธีการควบคุมอันตรายตาม MIL-STD-882 B1

1. ออกแบบเพื่อลดความเสี่ยงให้น้อยที่สุด
2. ใช้อุปกรณ์ความปลอดภัย
3. การใช้อุปกรณ์เตือนภัย
4. การจัดทำขั้นตอนการทำงาน (Procedure) และการฝึกอบรม
5. การยอมรับความเสี่ยง

การประยุกต์ความปลอดภัยเชิงระบบในการบริหารงานอาชีวอนามัยและความปลอดภัย

1. ความแตกต่างระหว่างความปลอดภัยเชิงระบบกับการดำเนินการด้านความปลอดภัยแบบดั้งเดิม

- ความปลอดภัยแบบดั้งเดิม ทำงานแบบแก้ไขปัญหาเฉพาะหน้า คือเมื่อเกิดอุบัติเหตุขึ้นมาก็แก้ไขกัน เน้นระยะสั้นแก้ไขแบบเชิงรับ
- ความสมบูรณ์แบบรอบด้านและความเป็นระบบ(Comprehensive and Systematic) ในการจัดการกับอันตราย หากโรงงานดำเนินงานด้านความปลอดภัยต่างๆ ไป ในการมองปัญหา (คือชี้บ่งอันตราย) จะมองเฉพาะอันตรายนั้นจะแก้ไข ป้องกัน และควบคุมอย่างไร แล้วตัดสินใจลงมือทำ ในขณะที่โรงงานดำเนินการตามหลักวิชาด้านความปลอดภัยเชิงระบบจะต้องมองอันตรายที่มีตั้งแต่เริ่มการออกแบบ (Design) การพัฒนา (Development) การทดสอบ (Test) การผลิต (Production) และภาคของเสียที่เกิดขึ้น การทำเรื่องความปลอดภัยเชิงระบบต้องทำการวิเคราะห์อันตรายที่มีตลอดวงจรชีวิตของระบบนั้นๆ
- เครื่องมือที่ใช้ชี้บ่งและวิเคราะห์อันตราย ทั้งไปแบบเดิมจะใช้ แบบตรวจความปลอดภัย แบบสำรวจหรือ Checklist ความปลอดภัยเชิงระบบจะใช้เครื่องมือชี้บ่งอันตราย และเทคนิคการวิเคราะห์อันตรายที่สลับซับซ้อนกว่า บางเทคนิคต้องอาศัยทีมงาน
 - การประมาณระดับความเสี่ยง
 - การดำเนินงานในลักษณะทีมงาน

2. แนวทางประยุกต์เรื่องความปลอดภัยเชิงระบบในโรงงาน

1. ทำให้โรงงานเข้าใจหลักการพื้นฐานของความปลอดภัย นั่นคือ
 - ผู้บริหารต้องมีเจตจำนง ที่จะมีการจัดการความปลอดภัยขึ้นในโรงงาน
 - ความปลอดภัยเป็นความรับผิดชอบของสายงานหลัก เช่นสายการผลิต การชี้แนะ แนะนำของฝ่ายปลอดภัยถือเป็นสายงานสนับสนุน
 - ความปลอดภัยเป็นเรื่องที่สร้างมูลค่าให้โรงงาน เนื่องจากการทำงานที่ปลอดภัยตั้งแต่แรกและทุกครั้งที่ทำงาน ย่อมมีโอกาสน้อยมากที่จะเกิดความสูญเสีย ลดการเกิดอุบัติเหตุ ก็ลดวันหยุดงานของพนักงาน ลดความสูญเสียในแง่การผลิตทั้งแรงงานและวัตถุดิบ
2. ทำการชี้บ่งอันตราย (Hazard Identification) ที่มีอยู่ในระบบ และต้องทำอย่างรอบคอบ
3. ใช้อุปกรณ์ต่างๆ ที่ถูกต้องเหมาะสม และมีการบำรุงรักษาอย่างเหมาะสม
4. พัฒนาและขั้นตอนการดำเนินงาน (Procedure) ด้านความปลอดภัยเชิงระบบขึ้นในโรงงานและต้องผสมผสานเป็นส่วนหนึ่งของระบบการบริหารของโรงงาน ปัจจุบันระบบการจัดการอาชีวอนามัยและความปลอดภัยที่เป็นที่รู้จักในโรงงานคือ มอก/OHSAS 18001
5. ฝึกอบรมบุคลากรให้มีความรู้และความสามารถในการเรื่องความปลอดภัยเชิงระบบ

6. เฝ้าระวังและตรวจประเมินระบบ (Monitoring and Auditing) เพื่อความมั่นใจว่าการดำเนินงานด้านความปลอดภัยได้ดำเนินการตามแนวคิดของความปลอดภัยเชิงระบบ

เครื่องมือที่ใช้ในความปลอดภัยเชิงระบบ

Preliminary Hazard Analysis (PHA)

PHA นิยมทำเป็นตารางที่มีหัวข้อสำหรับการวิเคราะห์

Preliminary Hazard Analysis					
เรื่อง (Element) <u>บ่อกำจัดไขมัน</u>					
ระบบ (System) <u>ห้องกำจัดไขมัน</u>		ส่วนย่อยของระบบ (Subsystem) <u>บ่อกำจัดไขมัน</u>			
ผู้วิเคราะห์ 1. นายมานะ		2. นายปิติ		วันที่	
ลักษณะเสี่ยงอันตราย (Hazard description)	สาเหตุ (causes)	ผล (effects)	ดัชนีความเสี่ยง (HRI)	แนวทางป้องกัน	ดัชนีความเสี่ยง (หลังป้องกัน)
การชน	เครนทำงานผิดพลาด	คนงานบาดเจ็บ บ่ออุปกรณ์เสียหาย	2A	ติดตั้งกลไกหยุดเครน	4C
การชน	เครนทำงานผิดพลาด	บางส่วนของเครนเสียหาย เพราะสัมผัสกับสารในบ่อ	2B	ติดตั้งกลไกหยุดเครน	4C
โครงสร้าง	การเชื่อมบ่อทำไม่ดี	สารเคมีรั่วไหล	3D	1. ใช้บ่อที่ผ่านการเชื่อมมาอย่างดี 2. ตรวจสอบรอยเชื่อมก่อนการติดตั้ง	4D

ตัวอย่างการทำ PHP สำหรับการออกแบบงานกำจัดไขมัน (Vapor Degreaser) ที่ใช้คนยกเครนย้ายชิ้นงาน ผลการวิเคราะห์อาจจะมีรูปแบบที่แตกต่างกันบ้างของแต่ละหน่วยงานแต่โดยหลัก ๆ แล้วหัวข้อสำหรับวิเคราะห์ PHP ประกอบด้วย

1. ลักษณะอันตราย
2. สาเหตุของอันตราย
3. ผลที่อาจเกิดขึ้น
4. ความรุนแรง โอกาสเกิด และค่าดัชนีความเสี่ยง
5. ข้อเสนอแนะวิธีป้องกัน
6. ผลที่ตามมาหลังทำตามข้อเสนอแนะนั้นๆ

ควรนำ PHA มาใช้ในระบะแนวคิดและระบะออกแบบ เพื่อชี้บ่งอันตรายที่อาจมีจากการผลิต ผลิตภัณฑ์นั้นๆ จะได้หาทางป้องกันควบคุม หรือแก้ไขแบบก่อนที่จะดำเนินการในระบะอื่นต่อไป

PHL (Preliminary Hazard List : PHL) คือบัญชีรายการอันตรายเพื่อความปลอดภัยในการชี้บ่งอันตราย เช่น

รายการอันตราย

1. การชน/ ความเสียหายทางกล (Collision/Mechanical Damage)
2. การปนเปื้อน (Contamination)
3. การกัดกร่อน (Corrosion) เป็นต้น

Failure Mode and Effect Analysis FMEA

เป็นเทคนิคที่ใช้ใน Reliability Engineering ต่อมาจึงมีการนำมาใช้ในงานความปลอดภัยเชิงระบบ โดยมีวัตถุประสงค์เพื่อการชี้บ่งอันตรายด้วยการวิเคราะห์ว่าแต่ละส่วนของระบบจะมีโอกาสทำงานผิดพลาดได้อย่างไร (Failure Mode) และมีผลกระทบต่อทั้งระบบอย่างไร (Effect Analysis) แต่ละส่วนที่ทำการวิเคราะห์ส่วนใหญ่จะเป็นอุปกรณ์ เช่น ปัมป์ วาล์ว ดังนั้นทีมที่ทำ FMEA จึงควรมีผู้มีความรู้ความเข้าใจเกี่ยวกับการทำงานของอุปกรณ์อยู่ในทีมด้วย FMEA จะเน้นที่อุปกรณ์ ไม่ใช่เน้นที่คน ดังนั้นจึงไม่มีการวิเคราะห์เรื่องความผิดพลาดของคน (Human Failure)

ขั้นตอนการทำ FMEA

- กำหนดอุปกรณ์ที่จะวิเคราะห์พร้อมรายละเอียด ทีมวิเคราะห์ FMEA ต้องพิจารณาจาก P&ID (Piping and Instrument Diagram) หรือแผนภูมิกระบวนการผลิต จัดทำรายการอุปกรณ์ที่ใช้ในการผลิต พร้อมคำอธิบายเกี่ยวกับการทำงานอุปกรณ์นั้นๆ ควรกำหนดรหัสอุปกรณ์เพื่อสะดวกในการอ้างอิง เช่น ลินโซลินอยด์นิกซ์สำหรับไอน้ำร้อน รหัส V-123
- พิจารณาความผิดพลาด (Failure Mode) ที่อาจเกิดขึ้น ซึ่งต้องเป็นอุปกรณ์ที่อาจเกิดขึ้นจริงของอุปกรณ์นั้นๆ เช่น ลินนิกซ์ไม่เปิดทำงานเมื่อแรงดันเกิน หรือปัมป์จ่ายน้ำยังทำงานอยู่ทั้งที่มีสัญญาณให้หยุด
- พิจารณาผลที่จะเกิดขึ้นจากความผิดพลาดนั้น โดยพิจารณาไปที่ความผิดพลาด
- กำหนดระดับความเสี่ยง โดยพิจารณาในประเด็น โอกาสเกิดและความรุนแรงที่จะเกิดขึ้น
- กำหนดวิธีป้องกัน โดยพยายามอิงวิธีทางวิศวกรรมหรือเทคโนโลยีเป็นสำคัญ

Failure Mode and Effect Analysis					
ระบบ ระบบการจ่ายน้ำให้กับที่ล้างตาฉุกเฉิน		ผู้วิเคราะห์ 1. นายมานะ ชัยนเรียม			
ส่วนของระบบ P & ID หมายเลข A-123		วันที่ 30 สิงหาคม 2550			
ส่วนโรง A		หน้าที่ 1 ใน 4			
ลักษณะของส่วน/ อุปกรณ์	ความผิดพลาด	ผล	ระดับความเสี่ยง		วิธีป้องกัน
			โอกาสเกิด	ความรุนแรง	
A-451: วาล์วนิกซ์โซลินอยด์สำหรับไอน้ำร้อน-เปิด(ทำงาน)ตามปกติ	1. วาล์วปิดอย่างไม่คาดคิดขณะทำงาน	1. สูญเสียการควบคุมน้ำเข้า มีน้ำเย็นเข้ามาในระบบ	1. ไม่น่าเกิด	เล็กน้อย	1. ทำโปรแกรมบำรุงรักษาป้องกันอย่างจริงจัง
	2. วาล์วไม่เปิดแม้จะมีสัญญาณให้เปิด (Sticks Closed)	2. เหมือนข้อ 1.	2. น้อย	เล็กน้อย	2. เหมือนข้อ 1
	3. วาล์วไม่ปิดแม้จะมีสัญญาณให้ปิด (Sticks Open)	3. อาจถูกไอน้ำลวก	3. ไม่น่าเกิด	รุนแรงมาก	3. ตั้งตั้งอุปกรณ์เตือนภัยที่อุณหภูมิสูง
	4. วาล์วมักรอยรั่วทำให้มีการรั่วไหลไปบริเวณรอบๆ	4. ไอน้ำจะรั่วไหลในบริเวณเล็กๆ ที่ถูกปิดล้อมไว้	4. ไม่ธรรมดา แต่เป็นไปได้	เล็กน้อย	4. เหมือนข้อ 1

ตัวอย่างบางส่วนของ การวิเคราะห์ FMEA ระบบจ่ายน้ำให้กับที่ล้างตาฉุกเฉิน

สรุป FMEA เป็นเครื่องมือที่เหมาะสมกับการชี้บ่งว่า อุปกรณ์ เครื่องมือที่ใช้อยู่ในกระบวนการผลิตมีโอกาสจะทำงานผิดพลาดอะไรได้บ้าง เช่น วาล์วอาจไม่เปิด (ทั้งที่มีสัญญาณแจ้งมาแล้ว) หรือวาล์วอาจปิดในขณะที่ทำงานอยู่โดยไม่คาดคิด การทำ FMEA จึงต้องมีทีมงานที่มีความเข้าใจในเทคนิค FMEA และเข้าใจกระบวนการผลิตและการทำงานของอุปกรณ์

ขั้นตอนการทำ FMEA ทีมงานต้องทำการวิเคราะห์ความผิดพลาด (Failure Mode) กำหนดระดับความเสี่ยงและกำหนดมาตรการป้องกันที่เน้นวิธีการทางวิศวกรรม หรือเทคโนโลยี

Fault Tree Analysis FTA

การวิเคราะห์แบบฟอลต์ ทรี เป็นวิธีหนึ่งของการวิเคราะห์เพื่อความปลอดภัย คิดค้นพัฒนาโดย W.A.W Watson พ.ศ. 2505 กองทัพอากาศสหรัฐฯ เพื่อให้ช่วยแก้ปัญหา เกิดการระเบิดของจรวด การชนกันของเครื่องบินบังคับ วิธีนี้ถูกนำไปใช้มากในอุตสาหกรรมด้านอวกาศ และอุตสาหกรรมเคมี และต้องการความมั่นใจสูงว่าจะไม่เกิดอุบัติเหตุในระหว่างการทำงาน

ความหมายของสัญลักษณ์ต่างๆ

1. รูปวงกลม (Circle) สัญลักษณ์ตัวแทนของเหตุการณ์ที่เกิดจากความบกพร่องหรือไม่สมบูรณ์ของตัวมันเอง(Basic Fault Event) ไม่ต้องวิเคราะห์ต่อไปอีก เหตุการณ์อยู่ระดับต่ำสุด เช่น ดวงไฟสัญญาณไม่ทำงานเนื่องจากความเสื่อมสภาพของไส้หลอด

2. รูปสี่เหลี่ยมขนมเปียกปูนหรือรูปเพชร (Diamond) สัญลักษณ์ของเหตุการณ์ที่เป็นสาเหตุที่ทำให้เกิดเหตุการณ์ที่อยู่ในตำแหน่งที่สูงกว่า เช่น เหตุการณ์ ข และ ค เป็นสาเหตุทำให้เกิดเหตุการณ์ ก เหตุการณ์จะไม่ถูกวิเคราะห์ต่อไปอีก อาจจะไม่มีการพิจารณาในการวิเคราะห์ขณะนั้นหรือเหตุการณ์นั้นไม่มีความสำคัญ อย่างไรก็ตามผู้วิเคราะห์ที่ตั้งใจจะวิเคราะห์ต่อไปอีกถ้ามีข้อมูลเพิ่มเติม ตัวอย่างเหตุการณ์แบบนี้ เช่น ผู้ปฏิบัติงานไม่ได้ยื่นสัญญาณเตือนภัย

3. รูปสี่เหลี่ยมผืนผ้า (Rectangle) สัญลักษณ์ตัวแทนของเหตุการณ์ที่เป็นผลจากเหตุการณ์หรือสาเหตุต่างๆ ที่อยู่ได้ช่องทางผ่าน (Gate) ของมัน เหตุการณ์ที่อยู่ในลักษณะนี้จะต้องทำการวิเคราะห์ต่อไปเสมอ

4. แอนด์เกต (And Gate) แทนให้เห็นว่าเหตุการณ์หนึ่งที่เกิดขึ้น (คือผล-Effect or Output) เป็นผลเนื่องมาจากทุกเหตุการณ์ (Input) ที่เกี่ยวข้องที่เขียนอยู่ได้ช่องทางผ่านของเหตุการณ์นั้น เช่น เหตุการณ์ A จะเกิดขึ้นได้ต้องมีสาเหตุมาจากเหตุการณ์ B1 , B2และ Bn ซึ่งเกิดขึ้นพร้อมกัน แอนด์เกตนี้ใช้ตอบคำถามจำพวก เหตุการณ์อะไรบ้างที่ต้อง (Must) เกิดขึ้นจึงทำให้เกิดผล เช่นนี้

5. ออร์เกต (Or Gate) ใช้แทนเหตุการณ์หนึ่งจะเกิดขึ้นมีสาเหตุมาจากเหตุการณ์ใดเหตุการณ์หนึ่งก็ได้อย่างน้อยหนึ่งเหตุการณ์ ใช้ตอบคำถาม เหตุการณ์ อะไรบ้างที่อาจเกิดขึ้นแล้วทำให้เกิดเหตุการณ์นี้

6. ทรานซ์เฟอร์เกต (Transfer Gate) ใช้แทนสัญลักษณ์หลีกเลี่ยงการวิเคราะห์ซ้ำ

7. อินฮิบิตเกต (Inhibit Gate) แทนการเกิดเหตุการณ์ที่เป็นผล (Effect or Output) นั้นจะเกิดขึ้นได้ต่อเมื่อมีเหตุการณ์ที่เป็นเงื่อนไข (Condition) หรือข้อจำกัด (Restriction) ที่เขียนอยู่ติดกับสัญลักษณ์นี้เกิดขึ้นมาด้วยควบคู่กับเหตุการณ์ที่เป็นตัวสาเหตุ (Input)

ขั้นตอนการสร้างโครงสร้างฟอลต์ ทรี

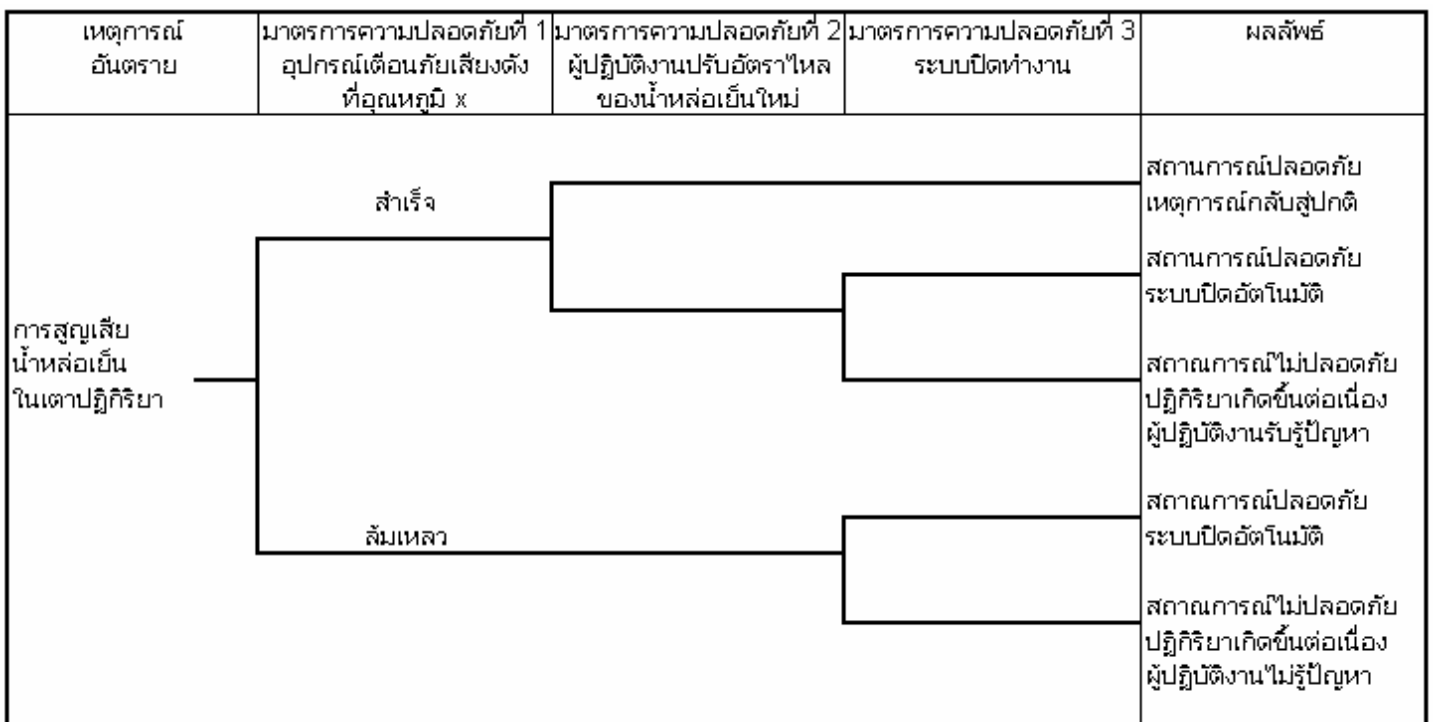
- 1. กำหนดและเลือกทอปอีเวนท์ (Top Event)** หัวข้อในการพิจารณาที่อันตรายมากที่สุด เป็นรูปสี่เหลี่ยมผืนผ้า
- 2. ประมวลผลสาเหตุ** เริ่มสร้างฟอลต์ ทรี พิจารณาว่าทอป อีเวนท์มาจากสาเหตุอะไรบ้าง ใช้ความรู้ทางวิชาการ พิจารณาในเชิงตรรก (Logic) เท่านั้น จึงจะทำให้ได้โครงสร้างที่ถูกต้องและเป็นประโยชน์ต่อการนำไปใช้ วิเคราะห์จากผลไปหาเหตุ คล้ายกับรากของต้นไม้
- 3. สาเหตุพื้นฐาน** เป็นระดับต่ำสุดของแต่ละสายของโครงสร้างฟอลต์ ทรี สาเหตุหรือ เหตุการณ์พื้นฐาน (Basic Fault Event) จะใช้สัญลักษณ์รูปวงกลมหรือรูปเพชรเท่านั้น

Event Tree Analysis ETA

คือการกำหนดเหตุการณ์ที่เป็นอันตราย (Initiating Event) ที่อาจเกิดขึ้นจากความผิดพลาดของอุปกรณ์ เครื่องมือ หรือความผิดพลาดของมนุษย์ แล้วพิจารณาว่าในมาตรการความปลอดภัยที่มีอยู่จะสามารถจัดการได้หรือไม่หากได้หรือไม่ได้ ผลลัพธ์ที่ตามมาจะเป็นอย่างไรหากได้ (Success) หรือไม่ได้ (Failure) ก็วิเคราะห์ต่อ ถึงมาตรการความปลอดภัยที่ 2 ที่ 3 เป็นลำดับ เส้นแสดงการวิเคราะห์เส้นบนได้ผล เส้นล่างไม่ได้ผล

วิธีการวิเคราะห์ ETA

1. กำหนดเหตุการณ์เริ่มต้น ซึ่งถือเป็นเหตุการณ์อันตราย(Hazard) สำคัญของการทำงาน ที่จะนำไปสู่อุบัติเหตุร้ายแรง
2. กำหนดซึ่งมาตรการความปลอดภัย
3. จัดทำเส้นแสดงการวิเคราะห์



ตัวอย่าง การทำETA ที่ผู้วิเคราะห์ ได้กำหนดเหตุการณ์เริ่มต้นคือ การสูญเสียน้ำหล่อเย็นในเตาปฏิกรณ์ออกซิเดชัน ซึ่งทางโรงงานได้กำหนดมาตรการความปลอดภัยไว้ 3 มาตรการคือ

- 1) อุปกรณ์เตือนเรื่องอุณหภูมิสูงในเตาปฏิกรณ์ออกซิเดชัน จะส่งเสียงเตือนผู้ปฏิบัติงานที่อุณหภูมิ x
- 2) ผู้ปฏิบัติงานจะปรับอัตราไหลของน้ำหล่อเย็นใหม่
- 3) ระบบปิดการทำงานโดยอัตโนมัติที่อุณหภูมิ y

HAZOP (Hazard and Operability Study) พัฒนขึ้นในปี 1960 โดยบริษัท Imperial Chemical Industry (ICI) ประเทศอังกฤษ ในประเทศไทยนั้นวิธีการวิเคราะห์นิยมใช้ในโรงงานที่มีอันตรายมาก (Major Hazard Industries)

HAZOP เป็นวิธีหรือเทคนิคการซึ่งอย่างเป็นระบบถึงสิ่งที่จะเบี่ยงเบน (Deviation) ไปจากระบบหรือกระบวนการผลิตที่ได้จากการออกแบบระบบหรือกำหนดไว้แล้ว การวิเคราะห์ว่าจะเบี่ยงเบนหรือไม่ อย่างไร จะใช้วิธีกำหนดคำ เรียกว่า Guide Words

ดังตาราง การทำ HAZOP ต้องเป็นทีมที่ประกอบด้วยผู้เชี่ยวชาญในเรื่องระบบที่จะวิเคราะห์ เข้าใจในรายละเอียดของแบบที่กำหนด (Design Requirement) และแผนไดอะแกรมแสดงท่อและอุปกรณ์ที่ติดตั้งในระบบ (Piping and Instrument Diagram : P&D และเข้าใจเทคนิคการทำ HAZOP

HAZOP Guide Words และความหมายของแต่ละคำ

Guide words	ความหมาย
No	การเป็นไปตามที่ออกแบบไว้ - "ไม่มีส่วนใดที่ออกแบบไว้เกิดขึ้นหรือได้รับตามที่ควรจะเป็นและไม่มีอะไรเกิดขึ้น"
Less	การลดลงเชิงปริมาณ - อ้างถึงปริมาณและคุณสมบัติ เช่น การไหล อุณหภูมิและความดัน
More	การเพิ่มขึ้นเชิงปริมาณ - เช่นเดียวกับกรณี Less (แต่เป็นการเพิ่มขึ้น "ไม่ใช่ลดลง")
Part of	การเพิ่มขึ้นเชิงคุณภาพ - มีเพียงบางส่วนของได้ออกแบบไว้ที่เกิดขึ้นหรือเป็นไปตามที่ออกแบบไว้ แต่บางส่วนก็"ไม่เป็นไปตามแบบ"
As well as	การเพิ่มขึ้นเชิงคุณภาพ - ทุกส่วนของออกแบบไว้ "ได้เป็นไปตามนั้นรวมทั้งมีบางส่วนเพิ่มเข้ามาด้วย"
Reverse	ตรงกันข้ามกับที่ได้ตั้งใจไว้ - ประยุกต์กับกิจกรรมเช่นการไหล
Other than	การทดแทนที่สมบูรณ์ - "ไม่มีส่วนใดที่ออกแบบไว้เกิดขึ้นหรือได้รับตามที่ควรจะเป็น และบางสิ่งที่แตกต่างก็เกิดขึ้น"

ข้อมูลและแบบที่ใช้วิเคราะห์ HAZOP

1. แบบ P & ID
2. แผนผังโรงงาน
3. วิธีปฏิบัติงาน (Operation Procedure)
4. ผลการวิเคราะห์อันตรายและรายงานอื่นๆ
5. รายงานเกี่ยวกับอุบัติเหตุในอดีต
6. พารามิเตอร์ขณะปฏิบัติงาน (Operating Parameter)
7. ข้อมูลจำเพาะของอุปกรณ์ (Equipment Specifications)
8. Instrumentation Set Parameters
9. ผลการทำ HAZOP ของระบบที่คล้ายกัน ตัวอย่าง ผลการทำ HAZOP สถานีบรรจุแอมโมเนีย

ระบบ Ammonia fill station		ทีมวิเคราะห์		HAZOP				
วันที่ 31/08/2550		P&IDที่ หมายเลข C-121		1.มานะ	2. ปิติ	3.ชูใจ		
Node Design Description		การเก็บบรรจุแอมโมเนียจำนวนมาก และแบ่งถ่ายไปยังถังขนาดเล็กเพื่อใช้ในกระบวนการผลิต		4.มานี				
Node Component		ถังบรรจุขนาด 200 ตัน ถังบรรจุขนาดเล็ก 15,000 ปอนด์ ปีบ วาล์ว ระบบท่อในไฮดรเจน และท่อต่างๆ						
Guide Word	สาเหตุ	ผล	ชนิด (Type)	วิธีป้องกันในขณะนี้	ดัชนีความเสี่ยง (HRI) ก่อน	วิธีป้องกันที่ควรทำเพิ่ม	ดัชนีความเสี่ยง (HRI) หลัง	สถานะ
No/less flow	ท่อแตกหรือรั่ว เนื่องจาก การสิ้นชะเทือน	แอมโมเนียรั่วไหล ในบริเวณนั้น	สิ่งแวดล้อม	การป้องกันเพียงพอ	2D	เพิ่มตัวเซ็นเซอร์ ความดัน ระหว่าง CV-1 และ CV2 เพื่อปิดปั๊ม ถ้าตรวจพบว่า มีการสูญเสียความดัน	2D	อยู่ระหว่างการติดตั้ง
No/less flow	CV-1 หรือ CV-2 ปิด ขณะมีการทำงานอยู่	ไม่มีการแบ่งถ่าย แอมโมเนียไปยังถังขนาดเล็กและอาจ เกิดปัญหาแก๊มดันสูงไป	ความปลอดภัย	มี Work instruction	3C	มีการทวนสอบการทำงานของพนักงานและติดตั้ง relief valve ระหว่าง CV-1, CV-2 และปั๊ม	3D	อยู่ระหว่างการติดตั้ง
More pressure	Block valves ปิดขณะ เต็มทำงาน	ความดันสูงในระบบ	ความปลอดภัย/การทำงาน	มี work instruction การแจ้งให้เปิดวาล์ว	1B	ติดตั้ง relief valves ระหว่าง block valves ทุกตัว และเพิ่ม block valves ในระบบด้วย		