

ความปลอดภัยเชิงระบบ

Bahr (1997) กล่าวว่า “ความปลอดภัยเชิงระบบเป็นชื่อเรียกที่เป็นทางการสำหรับการตรวจสอบ (Examination) ที่สมบูรณ์รอบด้าน (Comprehensive) และเป็นระบบต่อการออกแบบทางวิศวกรรมหรือต่อการปฏิบัติการ (Operation) และการควบคุมอันตรายใดๆ ก็ตาม ที่อาจทำให้คนบาดเจ็บหรืออุปกรณ์เสียหาย”

ในเอกสาร MIL-STD-882B ของกระทรวงกลาโหม สหรัฐอเมริกา (1984) ได้ให้นิยามของความปลอดภัยเชิงระบบ เพื่อทำให้เกิดความปลอดภัยสูงสุดภายใต้ข้อจำกัดของประสิทธิภาพการดำเนินงาน (Operational Effectiveness) เวลา และค่าใช้จ่าย ในทุก ๆ ระยะของวงจรชีวิตของระบบ”

สรุปความปลอดภัยเชิงระบบ จึงมีความหมายว่า เป็นการดำเนินงานด้วยวิธีทางวิศวกรรมและบริหารจัดการที่จะวิเคราะห์ว่าอันตรายใดบ้างในระบบที่วิเคราะห์นั้น แล้วทำการป้องกันควบคุมอันตรายที่จะทำให้คนบาดเจ็บและ/หรือทรัพย์สินเสียหาย

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 กำหนดการออกแบบและผลลัพธ์ที่คาดหวัง

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

ระยะที่ 3 การผลิต (Production Phase) เป็นระยะการผลิตสิ่งที่ต้องการ ให้ได้ผลลัพธ์ตามเป้าหมาย

ระยะที่ 4 การดำเนินการ (Operations Phase) นำผลลัพธ์ที่ได้มาใช้งาน สิ่งอำนวยความสะดวก อุปกรณ์เครื่องมือ หรือบริการ จะเห็นว่าการทำเรื่องความปลอดภัยเชิงระบบได้ผลอย่างไร ถ้าพบอันตรายก็ต้องปรับปรุงแก้ไข แต่จะแก้ไขยากกว่า ควรทำ3 ระยะแรกอย่างมีคุณภาพ

ระยะที่ 5 การกำจัด (Disposal Phase) กากผลิตภัณฑ์หรือของเสียที่เกิดขึ้น จะต้องได้รับการวิเคราะห์ ควบคุมอันตรายด้วย

ความแตกต่างระหว่างความปลอดภัยเชิงระบบกับการดำเนินการด้านความปลอดภัยแบบดั้งเดิม

- ความปลอดภัยแบบดั้งเดิม ทำงานแบบแก้ไขเฉพาะหน้า คือเมื่อเกิดอุบัติเหตุขึ้นมาก็แก้ไขกัน เน้นระยะสั้นแก้ไขแบบเชิงรับ ยกตัวอย่างพนักงานเช็ดกระจก

- ความสมบูรณ์แบบรอบด้านและความเป็นระบบ(Comprehensive and Systematic) ในการจัดการกับอันตราย หากโรงงานดำเนินงานด้านความปลอดภัยทั่วไป ในการมองปัญหา (คือขีปนาวุธอันตราย) จะมองเฉพาะอันตรายนั้นจะแก้ไข ป้องกัน และควบคุมอย่างไร แล้วตัดสินใจลงมือทำ ในขณะที่โรงงานดำเนินการตามหลักวิชาด้านความปลอดภัยเชิงระบบจะต้องมองอันตรายที่มีตั้งแต่เริ่มการออกแบบ (Design) การพัฒนา (Development) การทดสอบ (Test) การผลิต (Production) และกากของเสียที่เกิดขึ้น การทำเรื่องความปลอดภัยเชิงระบบต้องทำการวิเคราะห์อันตรายที่มีตลอดวงจรชีวิตของระบบนั้นๆ

- เครื่องมือที่ใช้ขีปนาวุธและวิเคราะห์อันตราย ทั่วไปแบบเดิมจะใช้ แบบตรวจความปลอดภัย แบบสำรวจหรือ Checklist

ความปลอดภัยเชิงระบบจะใช้เครื่องมือขีปนาวุธ และเทคนิคการวิเคราะห์อันตรายที่สลับซับซ้อนกว่า บางเทคนิคต้องอาศัยทีมงาน

- การประมาณระดับความเสี่ยง

- การดำเนินงานในลักษณะทีมงาน

Checklists แบบสำรวจ เป็นเทคนิคหนึ่งที่สามารถนำมาใช้วิเคราะห์อันตรายในกระบวนการผลิต ไม่ยุ่งยาก ง่ายต่อการนำไปใช้ ในการจัดทำ Checklists ควรให้ผู้ที่มีความรู้และประสบการณ์เกี่ยวกับกระบวนการผลิตนั้นๆ มาตรฐานแนวปฏิบัติ และกฎหมายที่เกี่ยวข้อง วิธีการทำงาน และนโยบายความปลอดภัยของบริษัท มากำหนดรายการที่จะวิเคราะห์ ซึ่งจะมีความละเอียดมากขึ้นขึ้นอยู่กับอันตรายหรือ ความเสี่ยงที่มี และความสลับซับซ้อนของระบบ

ยกตัวอย่างหน้า 11-29 (ตัวหนังสือสีส้มคือ คู่มือในหนังสือประกอบ)

ตัวอย่าง Checklists อันตรายทางกลของเครื่องจักร			
คำพรรณนาเกี่ยวกับเครื่องจักร			
.....			
อันตรายที่อาจมี	ใช่	ไม่ใช่	การป้องกัน/แก้ไขที่ควรทำ
ส่วนของเครื่องจักรที่หมุน/เคลื่อนที่ จุดหนีบ ความดันสูง/ต่ำ อุณหภูมิสูง/ต่ำ เสียงดัง สารเคมี ไฟฟ้า รังสี อักเสบ การยศาสตร์ ขั้นตอนการดำเนินงาน(Operating Procedure) ขั้นตอนการบำรุงรักษา มาตรฐานที่เกี่ยวข้อง (ANSI,NFPA,ASME) อื่น ๆ			
ทบทวน โดย วันที่			

What – If เป็นเทคนิคที่อาศัยทีมวิเคราะห์จากหลายสาขาวิชาชีพ ร่วมกันวิเคราะห์ว่ามีเหตุการณ์ใดบ้างที่เกิดขึ้นที่เป็นอันตราย หรือ เหตุการณ์ใดที่เกิดความผิดพลาดและหากเกิดขึ้น จะส่งผลกระทบตามมา ผลนั้นมีโอกาสเกิดขึ้นมากน้อยเพียงใด มีความรุนแรงมากน้อยเพียงใด ท้ายสุดก็พิจารณาเสนอแนวทางป้องกันมิให้เหตุการณ์นั้นๆเกิดขึ้นอีก

โดยทั่วไปทีมวิเคราะห์ What – If จะประกอบด้วย ผู้ที่มาจากฝ่ายผลิตและซ่อมบำรุง ผู้ออกแบบหรือวิศวกรควบคุมฝ่ายผลิต คนที่มีความรู้เฉพาะที่เกี่ยวข้องกับกระบวนการผลิตที่กำลังจะถูกวิเคราะห์

ผลจากการทำ What – If จะได้บัญชีรายการคำถาม ซึ่งชี้บ่งอันตรายที่เกี่ยวข้อง สภาพการที่เป็นอันตรายหรืออุบัติเหตุที่มีหรือสามารถเกิดขึ้นได้ ในทีมวิเคราะห์อาจจะกำหนดให้คนหนึ่งคนใดไปประเมินเกี่ยวกับผลลัพธ์ที่เกิดขึ้น มาตรการป้องกันที่มีอยู่ และทางเลือกที่เป็นไป

ได้ในการลดความเสี่ยงหลังจากนั้นที่ผู้วิเคราะห์จะร่วมกันพิจารณาเพื่อตรวจสอบรายงานและข้อเสนอแนะ และใช้เป็นบันทึกผลในการวิเคราะห์อันตรายในขบวนการผลิต

1. การเตรียมการเพื่อการวิเคราะห์ กำหนดขอบเขตของการวิเคราะห์ จัดหาแผนภูมิ P&ID และข้อมูลปฏิบัติการ ข้อมูลวิธีการบำรุงรักษา ข้อมูลรายละเอียดของการออกแบบและข้อมูลมาตรฐาน แนวปฏิบัติ และกฎหมายที่เกี่ยวข้อง

2. การดำเนินการวิเคราะห์

2.1 การตั้งคำถาม What – If ที่วิเคราะห์ควรพิจารณาข้อมูลจากเอกสารต่างๆ รวมทั้งนำความรู้และประสบการณ์ที่มีอยู่ มาวิเคราะห์หาอันตรายโดยการตั้งคำถามในลักษณะว่า**จะเกิดอะไรขึ้น ถ้า.....**

- ไม่ได้ปฏิบัติตามเอกสารขั้นตอนการทำงาน หรือทำผิดพลาดจากที่กำหนด
- ขั้นตอนการดำเนินงานผิดพลาด
- ไม่ได้ปฏิบัติตามขั้นตอนการทำงานฉบับล่าสุด
- ผู้ปฏิบัติงานไม่ได้ตั้งใจทำงาน
- ผู้ปฏิบัติงานไม่ได้รับการฝึกอบรม
- อุปกรณ์ทำงานผิดพลาด
- ไม่ได้ทำการสอบเทียบอุปกรณ์
- ความล้มเหลวของยูทิลิตี้ที่มีอยู่ เช่น พลังงาน ไอน้ำ ก๊าซ
- มีสิ่งแวดล้อมภายนอกที่ไม่ดี เช่น สภาพอากาศ อากาศ
- หลายๆเหตุการณ์ข้างต้นเกิดขึ้นต่อเนื่อง เช่น อุปกรณ์หลายชิ้นทำงานผิดพลาด
- ปีมัหมายเลข 2 หยุดขณะเริ่มเดินเครื่อง
- คนงานเปิดวาล์วB แทนที่จะเปิดวาล์ว A

2.2 พิจารณาคำตอบให้กับคำถาม What – If ว่าจะเกิดอะไรขึ้น คำตอบที่ได้คืออันตรายที่มีอยู่ในขบวนการผลิตที่กำลังวิเคราะห์

2.3 การประเมินโอกาสเกิด (Likelihood) และความรุนแรง (Consequences) ของอันตราย และเสนอแนะแนวทางป้องกัน

แบบวิเคราะห์อันตรายด้วยเทคนิค What - If				
การปฏิบัติการ <u>ผสมสารเคมีที่เป็นผงเล็กกับกรด</u> แผนก <u>ผสม</u>				
ทีมวิเคราะห์ 1.นายมานะ ขยันเรียน 2.นายปิติ ยินดีด้วย 3.นางจุใจ ไสสะอาด วันที่ 24 กันยายน 2550				
What - If	คำตอบ	โอกาสเกิด	ความรุนแรง	แนวทางป้องกัน
1.ถึงบรรจุผงเล็กๆ - ตัดฉลาก ผิด	1.เกิดปัญหาคุณภาพสินค้า	Remote	เสียหาย (Serious)	ปรับปรุงการติดฉลากจากผู้ส่ง
2.ในถึงบรรจุมีผงคนละชนิด	2.ถ้าเปียกอาจเกิดปฏิกิริยา การให้ความร้อนขึ้น	ไม่น่าเกิด (Unlikely)	เล็กน้อย (Minor)	เพิ่มขั้นตอนการตรวจตราในเอกสารขั้นตอนการดำเนินงาน
3.ถึงบรรจุสุกก่อน	3. การปนเปื้อนเหล็ก ถึงรั่ว และอาจทำให้บาดเจ็บ	Remote	เสียหาย (Serious)	ไม่ต้องทำอะไร
4.ระบบระบายอากาศเสีย	4.ฝุ่นฟุ้ง ผู้ปฏิบัติหายใจ เข้าร่างกาย	ไม่น่าเกิด (Unlikely)	เล็กน้อย (Minor)	เพิ่มขั้นตอนการตรวจสอบระบบ ระบายอากาศในขั้นตอนการทำงาน (Work Instruction)

5.ระดับความสูงของกรดอยู่สูง เกินขีดที่กำหนด	5.กรดกระเด็นใส่ตัว และเกิดปัญหาคุณภาพ สินค้า	ห่างไกล	รุนแรงมาก (Remote)	ใช้แว่นตาและเอี๊ยม
--	--	---------	---------------------------	--------------------

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

HAZOP เป็นวิธีหรือเทคนิคการซึ่งอย่างเป็นทางการเป็นระบบถึงสิ่งที่จะเบี่ยงเบน (Deviation) ไปจากระบบหรือกระบวนการผลิตที่ได้จากการออกแบบระบบหรือกำหนดไว้แล้ว การวิเคราะห์ว่าจะเบี่ยงเบนหรือไม่อย่างไร จะใช้วิธีกำหนดคำ เรียกว่า Guide Words

ดังตาราง การทำ HAZOP ต้องเป็นทีมที่ประกอบด้วยผู้เชี่ยวชาญในเรื่องระบบที่จะวิเคราะห์ เข้าใจในรายละเอียดของแบบที่กำหนด (Design Requirement) และแผน ไลอะแกรมแสดงท่อและอุปกรณ์ที่ติดตั้งในระบบ (Piping and Instrument Diagram : P&ID และเข้าใจเทคนิคการทำ HAZOP

HAZOP Guide Words และความหมายของแต่ละคำ

Guide words	ความหมาย
No	การเป็นไปตามที่ออกแบบไว้ - "ไม่มีส่วนใดที่ออกแบบไว้เกิดขึ้นหรือ"ได้รับตามที่ควรจะเป็นและไม่มีอะไรเกิดขึ้น
Less	การลดลงเชิงปริมาณ - อ้างถึงปริมาณและคุณสมบัติ เช่น การไหล อุณหภูมิและความดัน
More	การเพิ่มขึ้นเชิงปริมาณ - เช่นเดียวกับกรณี Less (แต่เป็นการเพิ่มขึ้น "ไม่ใช่ลดลง")
Part of	การเพิ่มขึ้นเชิงคุณภาพ - มีเพียงบางส่วนที่ได้ออกแบบไว้ที่เกิดขึ้นหรือเป็นไปตามที่ออกแบบไว้ แต่บางส่วนก็"ไม่เป็นไปตามแบบ
As well as	การเพิ่มขึ้นเชิงคุณภาพ - ทุกส่วนที่ออกแบบไว้ "ได้เป็นไปตามนั้นรวมทั้งมีบางส่วนเพิ่มเข้ามาด้วย
Reverse	ตรงกันข้ามกับที่ได้ตั้งใจไว้ - ประยุกต์กับกิจกรรมเช่นการไหล
Other than	การทดแทนที่สมบูรณ์ - "ไม่มีส่วนใดที่ออกแบบไว้เกิดขึ้นหรือ"ได้รับตามที่ควรจะเป็น 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 สถานีบรรจุก๊าซ

ยกตัวอย่างหน้า 4-43

ภาพที่ 4.20 ตารางที่ 4.9

HAZOP								
ระบบ Ammonia fill station	ทีมวิเคราะห์	1.มานะ	2. ปิติ	3.ซูโจ				
วันที่ 31/08/2550	P&IDที่ หมายเลข C-121							
Node Design Description การเก็บบรรจุแอมโมเนียจำนวนมาก และแบ่งถ่ายไปยังถังขนาดเล็กเพื่อใช้ในกระบวนการผลิต								
Node Component ถังบรรจุขนาด 200 ตัน ถังบรรจุขนาดเล็ก 15,000 ปอนด์ ปัม วาล์ว ระบบท่อในไฮดรเจน และท่อต่างๆ								
Guide Word	สาเหตุ	ผล	ชนิด (Type)	วิธีป้องกัน ในขณะนี้	ดัชนีความเสี่ยง(HRI) ก่อน	วิธีป้องกันที่ ควรทำเพิ่ม	ดัชนีความเสี่ยง (HRI) หลัง	สถานะ
No/less flow	ท่อแตกหรือรั่ว เนื่องจากการสั่นสะเทือน	แอมโมเนียรั่วไหล ในบริเวณนั้น	สิ่งแวดล้อม	การป้องกันเพียงพอ	2D	เพิ่มตัวเซ็นเซอร์ ความดัน ระหว่างCV-1และ CV2 เพื่อปิดปัม ถ้าตรวจพบว่า มีการสูญเสียความดัน	2D	อยู่ระหว่างการ ติดตั้ง
No/less flow	CV-1 หรือ CV-2 ปิด ขณะมีการทำงานอยู่	ไม่มีการแบ่งถ่าย แอมโมเนียไปยังถัง ขนาดเล็กและอาจ เกิดปัญหาความดันสูงไป	ความปลอดภัย	มี Work instruction	3C	มีการทวนสอบการทำงานของพนักงานและติดตั้ง relief valve ระหว่าง CV-1, CV-2 และปัม	3D	อยู่ระหว่างการ ติดตั้ง
More pressure	Block valves ปิดขณะที่ปัมทำงาน	ความดันสูงในระบบ	ความปลอดภัย/ การทำงาน	มี work instruction การแจ้งให้เปิดวาล์ว	1B	ติดตั้ง relief valves ระหว่าง block valves ทุกตัว และเพิ่ม block valves ในระบบด้วย		

Failure Mode and Effect Analysis FMEA

เป็นเทคนิคที่ใช้ใน Reliability Engineering ต่อมาจึงมีการนำมาใช้ในงานความปลอดภัยเชิงระบบ โดยมีวัตถุประสงค์เพื่อการชี้บ่งอันตราย ด้วยการวิเคราะห์ว่าแต่ละส่วนของระบบจะมีโอกาสทำงานผิดพลาดได้อย่างไร (Failure Mode) และมีผลกระทบต่อทั้งระบบอย่างไร (Effect Analysis) แต่ละส่วนที่ทำกรวิเคราะห์ส่วนใหญ่จะเป็นอุปกรณ์ เช่น ปัม วาล์ว ดังนั้นทีมที่ทำ FMEA จึงควรมีผู้มีความรู้ความเข้าใจเกี่ยวกับการทำงานของอุปกรณ์อยู่ในทีมด้วย FMEA จะเน้นที่อุปกรณ์ ไม่ใช่เน้นที่คน ดังนั้นจึงไม่มีการวิเคราะห์เรื่องความผิดพลาดของคน (Human Failure)

ขั้นตอนการทำ FMEA

1. กำหนดอุปกรณ์ที่จะวิเคราะห์พร้อมรายละเอียด ทีมวิเคราะห์ FMEA ต้องพิจารณาจาก P&ID (Piping and Instrument Diagram) หรือแผนภูมิกระบวนการผลิต จัดทำรายการอุปกรณ์ที่ใช้ในการผลิต พร้อมคำอธิบายเกี่ยวกับการทำงานอุปกรณ์นั้นๆ ควรกำหนดรหัสอุปกรณ์เพื่อสะดวกในการอ้างอิง เช่น ลิน โซลินอยด์นักรักสำหรับไอน้ำร้อน รหัส V-123
2. พิจารณาความผิดพลาด (Failure Mode) ที่อาจเกิดขึ้น ซึ่งต้องเป็นอุปกรณ์ที่อาจเกิดขึ้นจริงของอุปกรณ์นั้นๆ เช่น ลินนักรักไม่เปิดทำงานเมื่อแรงดันเกิน หรือปัมจ่ายน้ำยังทำงานอยู่ทั้งที่มีสัญญาณให้หยุด
3. พิจารณาผลที่จะเกิดขึ้นจากความผิดพลาดนั้น โดยพิจารณาไปที่ละความผิดพลาด
4. กำหนดระดับความเสี่ยง โดยพิจารณาในประเด็น โอกาสเกิดและความรุนแรงที่จะเกิดขึ้น
5. กำหนดวิธีป้องกัน โดยพยายามอิงวิธีทางวิศวกรรมหรือเทคโนโลยีเป็นสำคัญ

ตัวอย่าง ระบบจ่ายน้ำให้กับที่ล้างตาฉุกเฉิน หน้า 4-27

Failure Mode and Effect Analysis					
ระบบ ระบบการจ่ายน้ำให้กับที่ล้างตาฉุกเฉิน		ผู้วิเคราะห์ 1.นายมานะ ชัยเย็น			
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: วาล์วนิรภัย โซลินอยส์สำหรับ ไอน้ำร้อน-เปิด(ทางาน) ตามปกติ	1. วาล์วปิดอย่างไม่คาดคิด ขณะทางาน	1. สูญเสียการควบคุม น้ำเข้า มีน้ำเย็น เข้ามาในระบบ	1. ไม่น่าเกิด	เล็กน้อย	1. ทาโปรแกรม บำรุงรักษา ป้องกันอย่างจริงจัง
	2. วาล์วไม่เปิดแม้จะมี สัญญาณให้เปิด (Sticks Closed)	2. เหมือนข้อ 1.	2. น้อย	เล็กน้อย	2. เหมือนข้อ 1
	3. วาล์วไม่ปิดแม้จะมี สัญญาณให้ปิด (Sticks Open)	3. ตาอาจถูกไอน้ำลวก	3. ไม่น่าเกิด	รุนแรงมาก	3. ตั้งตั้งอุปกรณ์ เตือนภัยที่อุณหภูมิสูง
	4. วาล์วมีรอยรั่วทำให้มี การรั่วไหลไปบริเวณรอบๆ	4. ไอน้ำจะรั่วไหล ในบริเวณเล็กๆ ที่ถูกปิดล้อมไว้	4. ไม่ธรรมดา แต่เป็น ไปได้	เล็กน้อย	4. เหมือนข้อ 1

สรุป FMEA เป็นเครื่องมือที่เหมาะสมกับการชี้บ่งว่า อุปกรณ์ เครื่องมือที่ใช้อยู่ในกระบวนการผลิตมีโอกาสจะทำงานผิดพลาดอะไรได้บ้างเช่น วาล์วอาจไม่เปิด (ทั้งที่มีสัญญาณแจ้งมาแล้ว) หรือวาล์วอาจปิดในขณะที่ทางานอยู่โดยไม่คาดคิด การทำ FMEA จึงต้องมีทีมงานที่มีความเข้าใจในเทคนิค FMEA และเข้าใจกระบวนการผลิตและการทำงานของอุปกรณ์

ขั้นตอนการทำ FMEA ทีมงานต้องทำการวิเคราะห์ความผิดพลาด (Failure Mode) กำหนดระดับความเสี่ยงและกำหนดมาตรการป้องกันที่เน้นวิธีการทางวิศวกรรม หรือเทคโนโลยี

Fault Tree Analysis FTA

การวิเคราะห์แบบฟอลท์ ทรี เป็นวิธีหนึ่งของการวิเคราะห์เพื่อความปลอดภัย คิดค้นพัฒนาโดย W.A.W Watson พ ศ 2505 กองทัพอากาศสหรัฐอเมริกา ให้ช่วยแก้ปัญหา เกิดการระเบิดของจรวด การชนกันของเครื่องบินบังคับ วิธีนี้ถูกนำไปใช้มากในอุตสาหกรรมด้าน อวกาศ และอุตสาหกรรมเคมี และต้องการความมั่นใจสูงว่าจะไม่เกิดอุบัติเหตุในระหว่างการทำงาน

ความหมายของสัญลักษณ์ต่างๆ

- รูปวงกลม (Circle)** สัญลักษณ์ตัวแทนของเหตุการณ์ที่เกิดจากความบกพร่องหรือไม่สมบูรณ์ของตัวมันเอง(Basic Fault Event) ไม่ต้องวิเคราะห์ต่อไปอีก เหตุการณ์อยู่ระดับต่ำสุด เช่น ดวงไฟสัญญาณไม่ทำงานเนื่องจากความเสื่อมสภาพของไส้หลอด
- รูปสี่เหลี่ยมขนมเปียกปูนหรือรูปเพชร (Diamond)** สัญลักษณ์ของเหตุการณ์ที่เป็นสาเหตุที่ทำให้เกิดเหตุการณ์ที่อยู่ในตำแหน่งที่สูงกว่า เช่น เหตุการณ์ ข และ ค เป็นสาเหตุทำให้เกิดเหตุการณ์ ก เหตุการณ์จะไม่ถูกวิเคราะห์ต่อไปอีก อาจจะไม่มีข้อมูลเพียงพอในการวิเคราะห์ ขณะนั้นหรือเหตุการณ์นั้นไม่มีความสำคัญ อย่างไรก็ตามผู้วิเคราะห์ตั้งใจจะวิเคราะห์ต่อไปอีกถ้ามีข้อมูลเพิ่มเติม ตัวอย่างเหตุการณ์แบบนี้ เช่น ผู้ปฏิบัติงาน ไม่ได้ยินสัญญาณเตือนภัย
- รูปสี่เหลี่ยมผืนผ้า (Rectangle)** สัญลักษณ์ตัวแทนของเหตุการณ์ที่เป็นผลจากเหตุการณ์หรือสาเหตุต่างๆ ที่อยู่ได้ช่องทางผ่าน (Gate) ของมัน เหตุการณ์ที่อยู่ในลักษณะนี้จะต้องทำการวิเคราะห์ต่อไปเสมอ
- แอนด์เกต (And Gate)** แทนให้เห็นว่าเหตุการณ์หนึ่งที่เกิดขึ้น (คือผล-Effect or Output) เป็นผลเนื่องมาจากทุกเหตุการณ์ (Input) ที่เกี่ยวข้องที่เขียนอยู่ได้ช่องทางผ่านของเหตุการณ์นั้น เช่น เหตุการณ์ A จะเกิดขึ้นได้ต้องมีสาเหตุมาจากเหตุการณ์ B1 , B2และ Bn ซึ่งเกิดขึ้นพร้อมกัน แอนด์เกตนี้ใช้ตอบคำถามจำพวก เหตุการณ์อะไรบ้างที่ต้อง (Must) เกิดขึ้นจึงทำให้เกิดผลเช่นนี้
- ออร์เกต (Or Gate)** ใช้แทนเหตุการณ์หนึ่งจะเกิดขึ้นมีสาเหตุมาจากเหตุการณ์ใดเหตุการณ์หนึ่งก็ได้อย่างน้อยหนึ่งเหตุการณ์ ใช้ตอบคำถาม เหตุการณ์ อะไรบ้างที่อาจเกิดขึ้นแล้วทำให้เกิดเหตุการณ์นี้
- ทรานซ์เฟอร์เกต (Transfer Gate)** ใช้แทนสัญลักษณ์หลักเกี่ยวกับการวิเคราะห์ซ้ำ

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

ขั้นตอนการสร้างโครงสร้างฟอลต์ ทรี

1. กำหนดและเลือกทอปอีเวนต์ (Top Event) หัวข้อในการพิจารณาที่อันตรายมากที่สุด เป็นรูปสี่เหลี่ยมผืนผ้า
2. ประมวลหาสาเหตุ เริ่มสร้างฟอลต์ ทรี พิจารณาว่าทอป อีเวนต์มาจากสาเหตุอะไรบ้าง ใช้ความรู้ทางวิชาการ พิจารณาในเชิงตรรก (Logic) เท่านั้น จึงจะทำให้ได้โครงสร้างที่ถูกต้องและเป็นประโยชน์ต่อการนำไปใช้วิเคราะห์จากผลไปหาเหตุ คล้ายกับรากของต้นไม้
3. สาเหตุพื้นฐาน เป็นระดับได้สุดของแต่ละสายของโครงสร้างฟอลต์ ทรี สาเหตุหรือ เหตุการณ์พื้นฐาน (Basic Fault Event) จะใช้สัญลักษณ์รูปวงกลมหรือรูปเพชรเท่านั้น

ตัวอย่างหน้า 4-30

Event Tree Analysis ETA

คือการกำหนดเหตุการณ์ที่เป็นอันตราย (Initiating Event) ที่อาจเกิดขึ้นจากความผิดพลาดของอุปกรณ์ เครื่องมือ หรือความผิดพลาดของมนุษย์ แล้วพิจารณาว่าในมาตรการความปลอดภัยที่มีอยู่จะสามารถจัดการได้หรือไม่ หากได้หรือไม่ได้ ผลลัพธ์ที่ตามมาจะเป็นอย่างไร หากได้ (Success) หรือไม่ได้ (Failure) ก็วิเคราะห์ต่อ ถึงมาตรการความปลอดภัยที่ 2 ที่ 3 เป็นลำดับ เส้นแสดงการวิเคราะห์เส้นบน ได้ผล เส้นล่างไม่ได้ผล

วิธีการวิเคราะห์ ETA

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

เหตุการณ์ อันตราย	มาตรการความปลอดภัยที่ 1 อุปกรณ์เตือนภัยเสียงดัง ที่อุณหภูมิ x	มาตรการความปลอดภัยที่ 2 ผู้ปฏิบัติงานปรับอัตราไหล ของน้ำหล่อเย็นใหม่	มาตรการความปลอดภัยที่ 3 ระบบปิดทำงาน	ผลลัพธ์
การสูญเสีย น้ำหล่อเย็น ในเตาปฏิริยา	สำเร็จ	[]	[]	สถานการณ์ปลอดภัย เหตุการณ์กลับสู่ปกติ
			[]	สถานการณ์ปลอดภัย ระบบปิดอัตโนมัติ
	ล้มเหลว	[]	[]	สถานการณ์ไม่ปลอดภัย ปฏิริยาเกิดขึ้นต่อเนื่อง ผู้ปฏิบัติงานรับรู้ปัญหา
			[]	สถานการณ์ปลอดภัย ระบบปิดอัตโนมัติ
			[]	สถานการณ์ไม่ปลอดภัย ปฏิริยาเกิดขึ้นต่อเนื่อง ผู้ปฏิบัติงานไม่รับรู้ปัญหา

ตัวอย่าง การทำETA ที่ผู้วิเคราะห์ ได้กำหนดเหตุการณ์เริ่มต้นคือ การสูญเสียน้ำหล่อเย็นในเตาปฏิริยาออกซิเดชั่น ซึ่งทางโรงงานได้กำหนด มาตรการความปลอดภัยไว้ 3 มาตรการคือ

- 1) อุปกรณ์เตือนเรื่องอุณหภูมิสูงในเตาปฏิริยาออกซิเดชั่น จะส่งเสียงเตือนผู้ปฏิบัติงานที่อุณหภูมิ x
- 2) ผู้ปฏิบัติงานจะปรับอัตราไหลของน้ำหล่อเย็นใหม่
- 3) ระบบปิดการทำงาน โดยอัตโนมัติที่อุณหภูมิ y

การประมาณระดับความเสี่ยง ตารางหน้า 4-11 ถึง 4-13 กระดาษกราฟโหมสหรือได้นำเสนอ

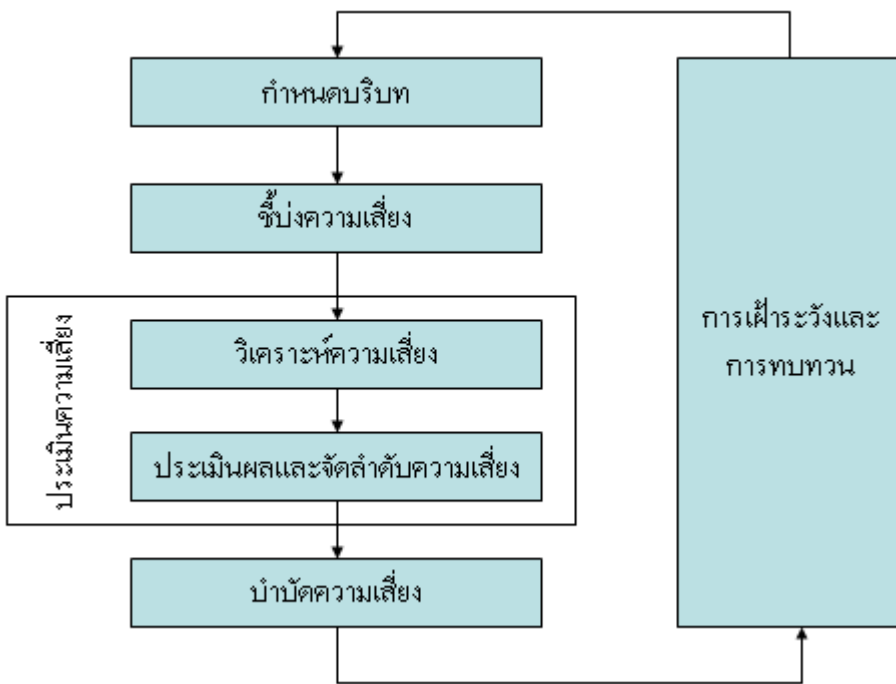
การจัดการความเสี่ยง

การวิเคราะห์ความเสี่ยงและการประเมินผลความเสี่ยง

การวิเคราะห์ความเสี่ยง (Risk Analysis) เป็นการประมาณระดับความเสี่ยงว่ายอมรับได้หรือไม่ได้มีการวิเคราะห์เชิงคุณภาพและเชิงปริมาณในโรงงานที่มีอันตรายมากจะใช้การวิเคราะห์เชิงปริมาณจะแม่นยำกว่า

ข้อกำหนดและกระบวนการจัดการความเสี่ยง มาตรฐาน AS/NZS 4360: 1998 ประกอบด้วยข้อกำหนดหลัก 6 ข้อ

แต่ละข้อจะมีความสัมพันธ์ในเชิงกระบวนการจัดการความเสี่ยงตามภาพข้างล่างนี้ คือเริ่มจากการกำหนดบริบทของการจัดการความเสี่ยง แล้วตามด้วยการชี้บ่งความเสี่ยง การวิเคราะห์ความเสี่ยง การประเมินผลและจัดลำดับความเสี่ยงและการบำบัดความเสี่ยง ในขณะเดียวกันในทุกๆ ข้อกำหนดจะมีการเฝ้าระวังและการทบทวนการดำเนินการควบคู่กันไปด้วย



กระบวนการจัดการความเสี่ยง

การกำหนดบริบท ควรมีการกำหนดบริบทให้ชัดเจนถึงความสัมพันธ์ทั้งเชิงบวกและเชิงลบระหว่างโรงงานและสิ่งที่เกี่ยวข้องซึ่งอาจเป็นเศรษฐกิจ สังคม ผู้มีส่วนได้ส่วนเสีย แผนพัฒนาองค์กร สิ่งแวดล้อม บริบทที่ควรกำหนดและพิจารณาแบ่งออกเป็น 3 ด้านคือ

1. การกำหนดบริบทด้านยุทธศาสตร์ ผู้บริหารต้องกำหนด ความสัมพันธ์ชัดเจน โรงงานกับสิ่งแวดล้อม อาจมีการทำ SWOT Analysis เพื่อทบทวนจุดแข็งจุดอ่อน โอกาสและสิ่งคุกคาม จะทำให้โรงงานมองเห็นความเสี่ยงให้ครอบคลุม ได้แก่ องค์กร เจ้าของ บุคลากร ลูกค้า ผู้รับเหมา ผู้ส่งมอบ ชุมชนท้องถิ่น และสังคมโดยรวม บริบทที่ควรพิจารณาได้แก่ 1) การเงิน 2) การปฏิบัติการ 3) การแข่งขัน 4) การเมือง (การยอมรับของสาธารณะ ภาพพจน์) 5) สังคม 6) วัฒนธรรม 7) กฎหมาย
2. การกำหนดบริบทด้านองค์กร โรงงานศึกษาตนเองให้เข้าใจก่อนดำเนินงานจัดการความเสี่ยงเหตุผลสำคัญคือ
 1. การจัดการความเสี่ยงเป็นการป้องกันความล้มเหลวที่จะไม่บรรลุวัตถุประสงค์ขององค์กร
 2. นโยบายและเป้าหมายองค์กร จะช่วยทำให้สามารถกำหนดเกณฑ์ได้ถูกต้องเหมาะสมว่าความเสี่ยงนั้นๆ สามารถยอมรับได้หรือไม่
3. การกำหนดบริบทด้านการจัดการความเสี่ยง
 1. กำหนดความชัดเจนของโครงการและกิจกรรม รวมถึงเป้าหมายและวัตถุประสงค์
 2. กำหนดขอบเขตความครอบคลุม ของโครงการ ระยะเวลา และสถานที่
 3. ชี้บ่งความต้องการการศึกษาอื่นๆที่จำเป็น เช่นทรัพยากรที่ต้องใช้ในโครงการนี้ แหล่งของความเสี่ยงที่จะมี ผลกระทบของความเสี่ยง

นั้นๆ

4. บทบาทความรับผิดชอบของส่วนอื่น ๆ ในองค์กร ที่มีส่วนเกี่ยวข้องกับการจัดการความเสี่ยง

5. ความสัมพันธ์ระหว่างโครงการนี้กับโครงการอื่นๆ หรือส่วนอื่นๆ ขององค์กร

4. การกำหนดเกณฑ์เพื่อการประเมินผลความเสี่ยง พิจารณากำหนดเกณฑ์ (Criteria) เพื่อใช้ในการประเมินความเสี่ยงเกณฑ์ที่กำหนดขึ้นแต่ ละโรงงานจะมีความแตกต่างกันเพราะ มีนโยบาย เป้าหมาย วัตถุประสงค์ วัฒนธรรม องค์กร ตลอดจนความสนใจของผู้มีส่วนได้ส่วนเสีย แตกต่างกัน และนำสิ่งเหล่านี้มาเป็นปัจจัยในการพิจารณาด้วยคือ การปฏิบัติการ (Operation) เทคนิค การเงิน กฎหมาย สังคม ความเป็นมนุษย์ และอื่น ๆ

5. การกำหนดโครงสร้าง การกำหนดกิจกรรมหรือโครงการต่างๆ ให้แยกเป็นหมวดหมู่หรือโครงสร้างที่ชัดเจน จะทำให้การชี้แจงและวิเคราะห์ สามารถทำได้อย่างดี

การชี้แจงความเสี่ยง เป็นเรื่องที่สำคัญดำเนินการทุกๆ ความเสี่ยงที่มีให้จัดทำเป็นรายการความเสี่ยงรวมถึงความเสี่ยงที่ยอมรับได้ด้วยควรรใช้ เทคนิคและการชี้แจงที่เป็นระบบเช่น แบบตรวจสอบ (Checklist) , Event Tree, FMEA, FTA, HAZOP

1.การวิเคราะห์ความเสี่ยงเชิงคุณภาพของ มาตรฐาน SA/SNZ 4360 (Standards Australia/Standards New Zealand) มีวิธีวิเคราะห์ ดังนี้

1.1 ความเป็นไปได้แบ่งออกเป็น 5 ระดับ

ระดับ	Descriptor	ความหมาย
A	มีความเป็นไปได้มาก	เหตุการณ์นี้คาดว่าจะเกิดขึ้นในกรณีต่างๆ
B	มีความเป็นไปได้	เหตุการณ์นี้เป็นไปได้ที่เกิดขึ้นในกรณีต่างๆ
C	มีความเป็นไปได้ปานกลาง	เหตุการณ์นี้อาจเกิดขึ้นบางครั้ง
D	มีความเป็นไปได้น้อย	เหตุการณ์นี้อาจเกิดขึ้นได้ในบางครั้ง
E	มีความเป็นไปได้น้อยมาก	เหตุการณ์นี้อาจเกิดขึ้นได้ในกรณีพิเศษเท่านั้น

ความรุนแรง แบ่งออกเป็น 5 ระดับ

ระดับ	Descriptor	ความหมาย
1	ไม่รุนแรง	ไม่เกิดการบาดเจ็บ สูญเสียด้านเงินน้อย
2	เล็กน้อย	ปฐมพยาบาล มีการรั่วไหลภายในโรงงาน สูญเสียเงินปานกลาง
3	ปานกลาง	ได้รับการรักษาทางการแพทย์ มีการรั่วไหลภายในโรงงาน และต้องอาศัยความช่วยเหลือจากภายนอก
4	มาก	บาดเจ็บรุนแรงมาก สูญเสียความสามารถในการผลิต มีการรั่วไหลสู่ภายนอกแต่ไม่เกิดอันตราย สูญเสียเงินมาก
5	ความหายนะ	ตาย มีการรั่วไหลสู่ภายนอกเกิดเป็นอันตราย สูญเสียเงินมหาศาล

ระดับความเสี่ยง เป็นผลที่ได้จากการวิเคราะห์ความเป็นไปได้ออกกับความรุนแรง

ความเป็นไปได้	ความรุนแรง				
	1-ไม่รุนแรง	2-เล็กน้อย	3-ปานกลาง	4-มาก	5-ความหายนะ
A-มีความเป็นไปได้มาก	S	S	H	H	H
B-มีความเป็นไปได้	M	S	S	H	H
C-มีความเป็นไปได้ปานกลาง	L	M	S	H	H
D-มีความเป็นไปได้น้อย	L	L	M	S	H
E-มีความเป็นไปได้น้อยมาก	L	L	M	S	S

ความหมาย

H = ความเสี่ยงสูงมาก (High Risk) ผู้บริหารระดับสูงต้องการการวิจัยและวางแผน การจัดการ

S = ความเสี่ยงสูง (Significant Risk) ผู้บริหารระดับสูงต้องให้ความสนใจ

M = ความเสี่ยงปานกลาง (Moderate Risk) ต้องมีการกำหนดหน้าที่ความรับผิดชอบของระดับบริหาร

L = ความเสี่ยงต่ำ (Low Risk) มีการจัดการด้วยขั้นตอนการดำเนินงานตามปกติ

2. การวิเคราะห์ความเสี่ยงเชิงคุณภาพของ สมอ. และ BSI (British Standard Institute)

ในมาตรฐาน มอก . 18004 : 2544 มาตรฐาน BS 8800: 1996 และมาตรฐาน OHSAS : 1999 เสนอแนะวิธีวิเคราะห์ความเสี่ยงดังนี้

2.1 โอกาสที่จะเกิดแบ่งเป็น 3 ระดับ คือ ไม่น่าจะเกิด เกิดขึ้นได้น้อย และเกิดขึ้นได้มาก ประเด็นที่ใช้ในการพิจารณา เช่น คน ความถี่และช่วงระยะเวลาสัมผัสอันตราย การสัมผัส การกระทำที่ไม่ปลอดภัย ความล้มเหลวระบบสาธารณสุขโลก

2.2 ความรุนแรง แบ่งเป็น 3 ระดับคือ อันตรายเล็กน้อย อันตรายปานกลาง อันตรายร้ายแรง พิจารณาความรุนแรงดังนี้

1) ส่วนของร่างกายที่ได้รับผลกระทบ

2) ลักษณะของการบาดเจ็บหรือเจ็บป่วย โดยเรียงลำดับจากน้อยไปหามาก

- การบาดเจ็บหรือเจ็บป่วยขั้นปฐมพยาบาล
- การบาดเจ็บหรือเจ็บป่วยแต่ไม่สูญเสียอวัยวะหรือพิการ
- การบาดเจ็บหรือเจ็บป่วยร้ายแรง สูญเสียอวัยวะ พิการ ทุพพลภาพ หรือ เสียชีวิต

กรณีทรัพย์สินเสียหายควรพิจารณาทั้งทางตรงและทางอ้อม

ระดับความเสี่ยง

โอกาสที่จะเกิด	ระดับความรุนแรงของอันตราย		
	อันตรายเล็กน้อย	อันตรายปานกลาง	อันตรายร้ายแรง
ไม่น่าจะเกิด	ความเสี่ยงเล็กน้อย	ความเสี่ยงที่ยอมรับได้	ความเสี่ยงปานกลาง
เกิดขึ้นได้น้อย	ความเสี่ยงที่ยอมรับได้	ความเสี่ยงปานกลาง	ความเสี่ยงสูง
เกิดขึ้นได้มาก	ความเสี่ยงปานกลาง	ความเสี่ยงสูง	ความเสี่ยงที่ยอมรับไม่ได้

ดูตารางที่ 5.6 หน้า 5-31 ประกอบ

ความเสี่ยงที่ยอมรับได้มาจากโอกาสการเกิดน้อย มีอันตรายน้อย

ความเสี่ยงปานกลางขึ้นไปต้องมีมาตรการป้องกัน เพื่อให้เป็นระดับความเสี่ยงที่ยอมรับได้

ดู หน้า 5-31 ถึง 5-34 เพิ่มเติม

สรุป การวิเคราะห์ความเสี่ยงเป็นการประมาณระดับความเสี่ยงว่าอยู่ในระดับที่ยอมรับได้หรือไม่ หากยอมรับได้แสดงว่ามาตรการ/วิธีการควบคุมที่มีอยู่เพียงพอแล้วต่อการจัดการความเสี่ยงนั้น สิ่งที่ต้องดำเนินการคือการรักษา (Maintain) ให้มาตรการ/วิธีการเหล่านั้นมีการปฏิบัติจริง กรณีผลวิเคราะห์พบว่าเป็นความเสี่ยงที่ยอมรับไม่ได้ โรงงานต้องหาทางจัดการด้วยวิธีการต่างๆ คือการบำบัดความเสี่ยง หลีกเลี่ยงความเสี่ยง โยกย้ายความเสี่ยง (ทำประกัน)

ระบบการจัดการอาชีวอนามัยและความปลอดภัย

กล่าวถึงมาตรฐาน มอก 18000 มอก 18001 ข้อกำหนด วัตถุประสงค์ 3 ข้อ มี 6 ข้อกำหนดหลัก

1. การทบทวนสถานะ
2. นโยบายอาชีวอนามัยและความปลอดภัย
3. การวางแผน
4. การนำไปใช้และปฏิบัติ
5. การตรวจสอบและแก้ไข
6. การทบทวนการจัดการ

ดูรายละเอียดข้อกำหนดเพิ่มเติม

มาตรฐาน ILO – OSH 2001 มี 5 ข้อกำหนด

ความหมายของระบบการจัดการสิ่งแวดล้อมตามมาตรฐานสากล ISO 14001 คือ การดูแลปัญหาสิ่งแวดล้อมขององค์กร ด้วยระบบการจัดการตามข้อกำหนดของมาตรฐานสากลที่เรียกว่า ISO 14001 มี 5 ข้อกำหนด

เอกสารมี 4 ระดับ

คู่มือการทำงาน manual

ระเบียบวิธีปฏิบัติ Procedure

วิธีปฏิบัติงาน WI

เอกสารสนับสนุน เช่น ข้อกำหนด เอกสารอ้างอิง