การประยุกต์ใช้มาตรฐานความปลอดภัยสากล EN ISO 13849 กับเครื่องจักรในอุตสาหกรรมยางรถยนต์

IMPLEMENTATION OF INTERNATIONAL SAFETY STANDARD EN ISO 13849 INTO MACHINERY OF TYRE INDUSTRY

ณภัทร วงศ์พิริยโยธา

NAPAT WONGPIRIYAYOTHAR

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมการวัดคุม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2560

KMITL-2017-EN-M-060-083

การประยุกต์ใช้มาตรฐานความปลอดภัยสากล EN ISO 13849 กับเครื่องจักรในอุตสาหกรรมยางรถยนต์

IMPLEMENTATION OF INTERNATIONAL SAFETY STANDARD EN ISO 13849 INTO MACHINERY OF TYRE INDUSTRY

ณภัทร วงศ์พิริยโยธา
NAPAT WONGPIRIYAYOTHAR

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมการวัดคุม
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2560
KMITL-2017-EN-M-060-083

IMPLEMENTATION OF INTERNATIONAL SAFETY STANDARD EN ISO 13849 INTO MACHINERY OF TYRE INDUSTRY

NAPAT WONGPIRIYAYOTHAR

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
2017

KMITL-2017-EN-M-060-083

คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การประยุกต์ใช้มาตรฐานความปลอดภัยสากล EN ISO 13849 กับเครื่องจักรในอุตสาหกรรมยางรถยนต์

Thesis Title Implementation of International Safety Standard EN ISO 13849 into Machinery of Tyre Industry

นักศึกษา นายณภัทร วงศ์พิริยโยธา

รหัสประจำตัว 56601429

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมการวัดคุม

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.สักรียา ชิตวงศ์

หมายเลขวิทยานิพนธ์ KMITL-2017-EN-M-060-083

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.ฟูศักดิ์	ชีวสุวิทย์	
รศ.ดร.วิทยา	ทิพย์สุวรรณพร	
ผศ.ดร.พงษ์ชัย	นิลาศ	
รศ.วิริยะ	กองรัตน์	
รศ.สักรียา	ชิตวงศ์	

วัน / เดือน/ ปี ที่สอบ วันพุธที่ 14 มิถุนายน พ.ศ. 2560 เวลา 10.00-12.00 น.
สถานที่สอบ ณ อาคาร A ชั้น 5 ห้องประชุม 3

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร. คมสัน มาลีสี)
คณบดี คณะวิศวกรรมศาสตร์
วันที่ 14 มิถุนายน พ.ศ. 2560

หัวข้อวิทยานิพนธ์	การประยุกต์ใช้มาตรฐานความปลอดภัยสากล EN ISO 13849 กับเครื่องจักรในอุตสาหกรรมยางรถยนต์
นักศึกษา	นายณภัทร วงศ์พิริยโยธา
รหัสประจำตัว	56601429
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมการวัดคุม
พ.ศ.	2560
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.สักรียา ชิตวงศ์

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้ จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อศึกษาและประยุกต์ใช้มาตรฐานความปลอดภัยสากล EN ISO 13849 ในการออกแบบระบบควบคุมความเสี่ยง SRP/CS (Safety-Related Parts of Control System) ให้กับเครื่องจักรในอุตสาหกรรมยางรถยนต์ โดยในกระบวนการประเมินความเสี่ยง (Risk assessment process) จะใช้วิธีกราฟความเสี่ยง (Risk graph method) ในการหาค่าระดับความปลอดภัยที่ต้องการ PLr (Performance Level required) ในส่วนของกระบวนการลดความเสี่ยง (Risk reduction process) จะออกแบบระบบควบคุมความเสี่ยง SRP/CS ด้วยพารามิเตอร์ Category, MTTFd, DC และ CCF ซึ่งค่าระดับความปลอดภัยของระบบ PL (Performance Level) และค่าโอกาสในการล้มเหลวของระบบ PFHDavg (Average Probability of Dangerous Failure per hour) สามารถหาได้จากตารางความสัมพันธ์ของพารามิเตอร์ดังกล่าว จากนั้นจะทำการเปรียบเทียบค่าระดับความปลอดภัยที่ได้จากการออกแบบระบบ PL กับค่าระดับความปลอดภัยที่ต้องการ PLr ว่าเป็นไปตามที่มาตรฐานความปลอดภัยกำหนดหรือไม่ ค่าระดับความปลอดภัยที่ยอมรับได้ตามที่มาตรฐานกำหนด คือ PL ต้องมากกว่าหรือเท่ากับ PLr (PL ≥ PLr, Acceptable level) ซึ่งในกรณีที่ค่าระดับความปลอดภัย PL น้อยกว่า PLr (PL < PLr, Non acceptable level) จะต้องกลับไปพิจารณากระบวนการประเมินความเสี่ยงและลดความเสี่ยงอีกครั้ง เพื่อปรับปรุงค่าระดับความปลอดภัยของระบบ PL ให้อยู่ในระดับที่ยอมรับได้ จึงจะสามารถรับประกันความปลอดภัยให้กับผู้ใช้งานเครื่องจักรได้

Thesis	Implementation of International Safety Standard EN ISO 13849 into Machinery of Tyre Industry
Student	Mr. Napat Wongpiriyayothar
Student ID.	56601429
Degree	Master of Engineering
Program	Instrumentation Engineering
Year	2017
Thesis Advisor	Assoc. Prof. Sakreya Chitwong

ABSTRACT

This thesis aims to study and implement international safety standard EN ISO 13849 in design SRP/CS (Safety-Related Parts of Control System) for machinery of tyre industry. This standard recommends us to use risk graph method for the risk assessment process and determine PLr (Performance Level required). Then, perform the risk reduction process by design SRP/CS following these concerned parameters Category, MTTFd, DC and CCF. Then, evaluate PL (Performance Level) and PFHDavg (Average Probability of Dangerous Failure per hour) of SRP/CS by referring from relation table of these parameters as mentioned on international safety standard. After that evaluate the performance level of SRP/CS whether can be acceptable or not by comparing PL and PLr. It means acceptable level if PL is greater than or equal to PLr ($PL \geq PLr$). On the other hand, It means non-acceptable level if PL is less than PLr ($PL < PLr$). In case of PL is non-acceptable level, all processes of the risk assessment and risk reduction must be reconsidered in order to improve PL into acceptable level and to guarantee that SRP/CS can build safe working environment for machine user.

กิตติกรรมประกาศ

วิทยานิพนธ์เล่มนี้สำเร็จได้ด้วยความกรุณาจากอาจารย์ที่ปรึกษา รศ.สักรียา ชิตวงศ์ ที่ให้ความช่วยเหลือ ให้คำชี้แนะในการแก้ปัญหาตลอดจนให้ความรู้และประสบการณ์ที่ดีแก่ข้าพเจ้า

ขอขอบคุณคณาจารย์คณะวิศวกรรมศาสตร์ สาขาการวัดคุม ที่ให้ความช่วยเหลือทางด้านความรู้เฉพาะทางในด้านต่างๆ แนะนำแนวทางของการทำงานวิจัยและแหล่งค้นคว้าข้อมูลในระหว่างการศึกษา

ขอขอบคุณเพื่อนมหาบัณฑิตคณะวิศวกรรมศาสตร์ สาขาการวัดคุม ทุกท่าน ที่ได้ให้ความช่วยเหลือ แบ่งปันความรู้และแลกเปลี่ยนประสบการณ์ในระหว่างการศึกษา

สำหรับคุณงามความดีอันใดที่เกิดจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบให้กับบิดา มารดา ซึ่งเป็นที่รักและเคารพยิ่ง ตลอดจนครูบาอาจารย์ที่เคารพทุกท่านที่ได้ประสิทธิประสาทวิชาความรู้และถ่ายทอดประสบการณ์ที่ดีให้แก่ข้าพเจ้า

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์เล่มนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

ณภัทร วงศ์พิริยโยธา

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

รายการสัญลักษณ์

SRP/CS	=	ระบบควบคุมความเสี่ยง (Safety Related Parts of Control System)
PLr	=	ค่าระดับความปลอดภัยที่ต้องการในการออกแบบระบบควบคุมความเสี่ยง SRP/CS (Performance Level required)
PL	=	ค่าระดับความปลอดภัยของระบบควบคุมความเสี่ยง SRP/CS (Performance Level)
Category	=	โครงสร้างของระบบควบคุมความเสี่ยง มีอยู่ 5 ประเภท Category B, 1, 2, 3, 4
MTTFd	=	ค่าแสดงอัตราการล้มเหลวของอุปกรณ์หรือระบบ (Mean Time to dangerous failure), หน่วยเป็นปี
DC	=	ค่าแสดงอัตราการตรวจพบความผิดปกติของอุปกรณ์หรือระบบ (Diagnostic coverage), หน่วยเป็นเปอร์เซ็นต์
CCF	=	ค่าแสดงปัจจัยในการล้มเหลวของอุปกรณ์ที่มาจากสาเหตุเหมือนๆกัน (Common cause failure), หน่วยเป็นคะแนน
PFHD	=	ค่าแสดงโอกาสในการล้มเหลวของอุปกรณ์หรือระบบ (Probability of Dangerous Failure per hour), หน่วยเป็นครั้งต่อชั่วโมง
B_{10d}	=	จำนวนครั้งโดยเฉลี่ยที่อุปกรณ์สามารถทำงานได้
n_{op}	=	จำนวนครั้งโดยเฉลี่ยที่อุปกรณ์สามารถทำงานได้ใน 1 ปี
d_{op}	=	จำนวนวันโดยเฉลี่ยที่อุปกรณ์สามารถทำงานได้ใน 1 ปี
h_{op}	=	จำนวนชั่วโมงโดยเฉลี่ยที่อุปกรณ์สามารถทำงานได้ใน 1 วัน
t_{cycle}	=	เวลาเฉลี่ยที่อุปกรณ์ทำงานใน 1 รอบ (หน่วยเป็นวินาที)
E-Stop	=	อุปกรณ์ส่วนอินพุท ประเภทสวิทช์แบบกดสำหรับหยุดแบบฉุกเฉิน (Emergency Stop)
LC	=	อุปกรณ์ส่วนอินพุท ประเภทม่านแสงนิรภัย (Safety Light Curtain)
K	=	อุปกรณ์ส่วนเอาท์พุท ประเภท Magnetic Contactor
MRS	=	อุปกรณ์ส่วนชุดควบคุม ประเภท Master Relay for Control Safety Devices
EN ISO 12100	=	มาตรฐานความปลอดภัยสากลเกี่ยวกับเครื่องจักร มุ่งเน้นในเรื่องการประเมินความเสี่ยง (Risk assessment) และการลดความเสี่ยง (Risk reduction)
EN 954-1	=	มาตรฐานความปลอดภัยสากลเกี่ยวกับเครื่องจักร มุ่งเน้นในเรื่องการออกแบบระบบควบคุมความเสี่ยง SRP/CS
EN ISO 13849-1	=	มาตรฐานความปลอดภัยสากลเกี่ยวกับเครื่องจักร มุ่งเน้นในเรื่องการออกแบบระบบควบคุมความเสี่ยง SRP/CS (ปรับปรุงเพื่อมาแทนมาตรฐาน EN 954-1)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

จากรายงานข้อมูลทางสถิติของสำนักงานประกันสังคมกระทรวงแรงงานประเทศไทย (Social Security Office Ministry Of Labor, Thailand) ตั้งแต่ปี พ.ศ. 2551 ถึง พ.ศ. 2558 พบว่าการเกิดอุบัติเหตุจากการทำงานที่ทำให้สูญเสียอวัยวะหรือเสียชีวิตมาจาก 5 สาเหตุหลักๆ ซึ่งเรียงลำดับจากมากไปน้อยได้ดังนี้ เครื่องจักร (Machine), วัตถุ สิ่งของ (Object/Stuff/Material), ยานพาหนะ (Vehicle), เครื่องมือ อุปกรณ์ (Equipment/Tooling) และ สภาพแวดล้อมการทำงาน (Working Environment) จะพบว่าสถิติของการเกิดอุบัติเหตุตั้งแต่อดีตจนถึงปัจจุบันไม่ได้มีแนวโน้มที่ลดลง โดยที่อัตราการเกิดอุบัติเหตุสูงสุดมาจากเครื่องจักร (Machine) แสดงดังภาคผนวก ข ซึ่งปัจจัยที่ทำให้เกิดสภาวการณ์ที่อันตรายได้แก่

1. การออกแบบเครื่องจักรที่ไม่ถูกต้องตามมาตรฐานความปลอดภัย และไม่ได้มีการประเมินความเสี่ยงที่จะเกิดขึ้นอย่างครอบคลุม
2. การที่พนักงานไม่มีความรู้ ความเข้าใจเกี่ยวกับการใช้งานเครื่องจักรอย่างถูกต้อง

ในปัจจุบัน มีอุตสาหกรรมจำนวนมากที่ใช้เครื่องจักรในกระบวนการผลิต มีความเสี่ยงและโอกาสสูงที่จะนำไปสู่การเกิดเหตุการณ์อันตรายต่อผู้ใช้งานเครื่องจักรได้ เช่น การบาดเจ็บ การสูญเสียอวัยวะ หรือร้ายแรงที่สุดถึงขั้นเสียชีวิตได้ อีกทั้งค่าใช้จ่ายที่เพิ่มขึ้นที่องค์กรจะต้องรับผิดชอบต่อเหตุการณ์อันตรายที่เกิดขึ้น เช่น การรักษาเยียวยาพนักงานที่ได้รับบาดเจ็บ สูญเสียอวัยวะ หรือเสียชีวิตจากการทำงาน อีกทั้งการขาดแคลนบุคลากรอันเนื่องมาจากการหยุดงานเป็นระยะเวลานานๆ รวมทั้งส่งผลกระทบต่อภาพลักษณ์และชื่อเสียงขององค์กรได้ในที่สุด ดังนั้นการออกแบบเครื่องจักรให้ถูกต้องตามมาตรฐานความปลอดภัยสากล (International safety standard) จึงเป็นสิ่งที่ควรนำมาพิจารณา เพื่อลดอุบัติเหตุจากการทำงานและสร้างสภาพแวดล้อมการทำงานที่ปลอดภัยให้กับพนักงาน

ในกรณีศึกษาของวิทยานิพนธ์ฉบับนี้จะมุ่งเน้นไปที่เรื่องการประเมินความเสี่ยงและลดความเสี่ยงของเครื่องจักรในอุตสาหกรรมยางรถยนต์ (Tyre Industry) เพื่อเป็นกรณีตัวอย่างของการประยุกต์ใช้งานมาตรฐานความปลอดภัยสากลในการจัดการความเสี่ยงหรือลดความเสี่ยงลงให้อยู่ในระดับที่ยอมรับได้ (Reduce risk into acceptable level) โดยจะอธิบายรายละเอียดเพิ่มเติมในบทที่ 3

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาและประยุกต์ใช้มาตรฐานความปลอดภัยสากลกับเครื่องจักรในอุตสาหกรรมยางรถยนต์ในการจัดการกับความเสี่ยงหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Reduce risk into acceptable level)

2. เพื่อแสดงวิธีการประเมินความเสี่ยงและลดความเสี่ยงตามข้อกำหนดมาตรฐานความปลอดภัยสากล โดยจะประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง (Risk graph) และออกแบบระบบควบคุมความเสี่ยง SRP/CS
3. เพื่อรับรองว่าระบบควบคุมความเสี่ยง SRP/CS สามารถที่จะจัดการกับความเสี่ยงหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยพิจารณาจากค่าระดับความปลอดภัยที่ได้จากการออกแบบ (PL) กับค่าระดับความปลอดภัยที่ต้องการ (PLr)
4. เพื่อใช้เป็นแนวทางในการประเมินความเสี่ยงและลดความเสี่ยงสำหรับผู้ที่ต้องการศึกษาและนำไปประยุกต์ใช้กับเครื่องจักรในภาคอุตสาหกรรมกระบวนการผลิตอื่นๆ เพื่อช่วยส่งเสริมการลดสถิติของการเกิดอุบัติเหตุจากเครื่องจักรในประเทศไทยและสร้างสภาพแวดล้อมการทำงานที่ปลอดภัยให้กับพนักงาน

1.3 สมมุติฐานของการศึกษา

1. การประยุกต์ใช้มาตรฐานความปลอดภัยสากล EN ISO 13849-1 [1] สามารถที่จะจัดการความเสี่ยงหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
2. การประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง (Risk Graph) สามารถที่จะออกแบบระบบควบคุมความเสี่ยง SRP/CS ได้อย่างมีประสิทธิผล
3. ค่าความเสี่ยงในระดับที่ยอมรับได้ บ่งชี้ได้ว่าระบบควบคุมความเสี่ยง SRP/CS มีความน่าเชื่อถือสูง (High reliability) และมีโอกาสของการล้มเหลวของระบบน้อย (Low PFHD) สามารถที่จะรับรองความปลอดภัยให้กับพนักงานได้
4. สามารถที่จะใช้เป็นแนวทางในการประเมินความเสี่ยงและการลดความเสี่ยงให้กับเครื่องจักรในภาคอุตสาหกรรมประเภทอื่นๆ และมีส่วนทำให้สถิติของการเกิดอุบัติเหตุจากเครื่องจักรในประเทศไทยมีแนวโน้มที่ลดลง

1.4 การนำเสนอแนวคิดของวิทยานิพนธ์

ในงานวิทยานิพนธ์ฉบับนี้จะกล่าวถึงการประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง (Risk graph) โดยพารามิเตอร์สำคัญที่ใช้ในการประเมินความเสี่ยงประกอบด้วย ความรุนแรงของอันตราย (S), โอกาสในการเกิดอันตรายหรือช่วงเวลาที่อยู่ในสถานการณ์ที่อันตราย (F), และโอกาสในการหลบหลีกอันตราย (P) ซึ่งผลจากการประเมินความเสี่ยงจะทำให้รู้ถึงระดับของความเสี่ยงและค่าระดับความปลอดภัยที่ต้องการ (PLr) หลังจากนั้นจะทำการออกแบบระบบควบคุมความเสี่ยง SRP/CS เพื่อจัดการความเสี่ยงที่จะเกิดขึ้น โดยตัวแปรสำคัญที่ใช้ในการออกแบบระบบควบคุมความเสี่ยงประกอบด้วย Category, MTTFd, DCavg และ CCF หลังจากนั้นจะทำการเปรียบเทียบค่าระดับความปลอดภัยที่ได้จากการออกแบบ (PL) กับค่าระดับความปลอดภัยที่ต้องการ (PLr) ว่าเพียงพอที่จะจัดการความเสี่ยงหรือไม่ ซึ่งถ้าหากค่าระดับความปลอดภัยที่ได้จากการออกแบบ (PL) ไม่เพียงพอในการจัดการความเสี่ยง ทางทีมผู้ประเมินความเสี่ยงจะต้องพิจารณาตัวแปรที่ใช้ในการออกแบบระบบควบคุมความเสี่ยง SRP/CS ใหม่อีกครั้ง เพื่อที่จะปรับปรุงค่าระดับความปลอดภัยให้สามารถจัดการความเสี่ยงหรือลดความเสี่ยงลงให้อยู่ใน

ระดับที่ยอมรับได้ (Reduce risk into acceptable level) จึงจะสามารถรับรองความปลอดภัยให้กับพนักงานผู้ใช้งานเครื่องจักรได้

1.5 ขอบเขตของวิทยานิพนธ์

วิทยานิพนธ์ฉบับนี้ได้ทำการประเมินความเสี่ยงของเครื่องจักรในอุตสาหกรรมยางรถยนต์ (Machinery of Tyre Industry) โดยเลือกพิจารณาจากส่วนที่มีโอกาสเกิดอันตรายกับพนักงานมากที่สุด คือ ชุดขับเคลื่อน (Motor Unit) ที่บริเวณด้านหน้าของเครื่องจักรมาใช้เป็นกรณีศึกษา โดยจะประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง (Risk graph) หลังจากนั้นจะทำการออกแบบระบบควบคุมความเสี่ยง SRP/CS ให้เป็นไปตามข้อกำหนดของมาตรฐานความปลอดภัยสากล EN ISO 13849-1 [1] เพื่อใช้ในการจัดการความเสี่ยงหรือลดความเสี่ยงลงให้อยู่ในระดับที่ยอมรับได้ (Reduce risk into acceptable level) โดยข้อมูลที่นำมาใช้ในการคิด วิเคราะห์และคำนวณ จะมาจาก 2 แหล่งข้อมูลหลักๆ ได้แก่ ค่าอ้างอิงที่ระบุอยู่ในมาตรฐานความปลอดภัยสากล EN ISO 13849-1 [1] และค่าอ้างอิงจากการทดสอบอุปกรณ์ความปลอดภัยของบริษัทผู้ผลิต (Manufacturer datasheet)

ในสถานการณ์จริง เราไม่สามารถที่จะจัดการกับความเสี่ยงที่มีอยู่ทั้งหมดได้ เนื่องจากข้อจำกัดทางด้านงบประมาณเพราะว่าอุปกรณ์ป้องกันความเสี่ยงหรือการออกแบบระบบควบคุมความเสี่ยงจะต้องใช้งบประมาณในการลงทุนสูง จึงต้องมีการวางแผนในการจัดการกับความเสี่ยงที่จะเกิดขึ้น ดังนั้นความเสี่ยงที่เหลืออยู่ (Remaining of residual risk) สามารถที่จะป้องกันได้โดยการให้ข้อมูลการใช้งานเครื่องจักรที่ถูกต้องกับพนักงาน (Information for uses) ซึ่งจะอธิบายเพิ่มเติมในบทที่ 2

1.6 รายละเอียดของวิทยานิพนธ์

วิทยานิพนธ์ฉบับนี้แบ่งเนื้อหาออกเป็น 4 บท โดยมีรายละเอียดดังนี้

1. บทที่ 1 บทนำ กล่าวถึงความเป็นมาและความสำคัญของปัญหา ความมุ่งหมายและวัตถุประสงค์ของการศึกษา สมมุติฐานของการศึกษา การนำเสนอแนวคิดของวิทยานิพนธ์ ขอบเขตวิทยานิพนธ์และรายละเอียดของวิทยานิพนธ์
2. บทที่ 2 ทฤษฎีที่เกี่ยวข้องในการประเมินความเสี่ยง กล่าวถึงการออกแบบระบบควบคุมความเสี่ยง SRP/CS การหาค่าระดับความปลอดภัย การปรับปรุงค่าระดับความปลอดภัย และการรับรองค่าระดับความปลอดภัยที่ใช้ในการจัดการความเสี่ยงหรือลดความเสี่ยงลงให้อยู่ในระดับที่ยอมรับได้
3. บทที่ 3 การนำเสนองานวิจัย กล่าวถึงการประยุกต์ใช้งานมาตรฐานความปลอดภัยสากลกับเครื่องจักรในอุตสาหกรรมผลิตยางรถยนต์ในการประเมินความเสี่ยง ออกแบบระบบควบคุมความเสี่ยง SRP/CS หาระดับความปลอดภัย ปรับปรุงค่าระดับความปลอดภัยและรับรองค่าระดับความปลอดภัยที่ใช้ในการจัดการกับความเสี่ยงหรือลดความเสี่ยงลงให้อยู่ในระดับที่ยอมรับได้
4. บทที่ 4 สรุปผลการวิจัยและข้อเสนอแนะ

ในส่วนสุดท้ายของวิทยานิพนธ์เป็นส่วนของภาคผนวก

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 งานวิจัยที่เกี่ยวข้อง (Literature review)

ในปี พ.ศ. 2550 Takabumi Fukuda และคณะ [5] นำเสนองานวิจัยเรื่องการประเมินความน่าเชื่อถือของระบบควบคุมความเสี่ยง (SRP/CS) และค่าระดับความปลอดภัยของเครื่องจักร โดยแสดงการเปรียบเทียบผลของค่าระดับความปลอดภัย (PL) ที่ได้จากการประเมินโดยมาตรฐานความปลอดภัยสากล EN ISO 13849-1 [1] กับผลของค่าระดับความปลอดภัย (PL) ที่ได้จากการประเมินโดยวิธีการ ETA(Event Tree Analysis) ของวงจรทดสอบ (Tested circuit) 5 แบบซึ่งได้ผลสรุปว่าค่าระดับความปลอดภัยที่ได้จากการประเมินโดยวิธี EN ISO 13849-1 [1] กับ วิธี ETA มีค่าที่แตกต่างกันดังแสดงในตารางที่ 2.1 และพบว่าวิธี EN ISO 13849-1 [1] จะให้ค่าระดับความปลอดภัยที่ต่ำกว่าวิธี ETA และให้ความเห็นว่ามาตรฐานความปลอดภัยสากล EN ISO 13849-1 [1] ค่อนข้างยากที่จะทำความเข้าใจและนำไปประยุกต์ใช้ รวมทั้งในบางครั้งยังให้ผลลัพธ์ที่ไม่แม่นยำอีกด้วย

ตารางที่ 2.1 เปรียบเทียบค่าระดับความปลอดภัย (PL) จากวิธี EN ISO 13849-1 [1] กับวิธี ETA

Tested circuit		Circuit 1	Circuit 2	Circuit 3	Circuit 4	Circuit 5
Category classified by FMEA		1	3	4	3	4
ETA	Avg. probability of dangerous failure per hour (1/h)	6.4×10^{-3}	7.3×10^{-10}	7.5×10^{-10}	5.2×10^{-19}	7.3×10^{-10}
	PL	---	e	e	e	e
ISO 13849:1:2006	PL	b	d	---	d or e	---

ในปี พ.ศ. 2551 Patrick Lereverend[6] นำเสนองานวิจัยเรื่องมาตรฐานความปลอดภัยสากล IEC 62061 [4] และ EN ISO 13849-1 [1] ว่าเป็นมาตรฐานที่ส่งเสริมกันหรือเป็นมาตรฐานที่ขัดแย้งกัน โดยได้อธิบายรายละเอียด ประวัติความเป็นมาและหลักการของแต่ละมาตรฐาน โดยได้ให้ข้อสรุปไว้ว่า 2 มาตรฐานนี้ส่งเสริมซึ่งกันและกัน โดยที่มาตรฐาน IEC 62061 [4] จะเหมาะสำหรับการทำฟังก์ชันความปลอดภัยในระบบที่มีความซับซ้อนมากและมุ่งเน้นด้านการทำซอฟแวร์ควบคุม (Software Control) อาทิเช่น โปรแกรมอิเล็กทรอนิคส์ควบคุมระบบ (Programmable Electronic Control System) หรือการวางระบบความปลอดภัยแบบเครือข่าย (Network Safety System) ส่วนมาตรฐาน EN ISO 13849-1 [1] จะเหมาะสำหรับการทำฟังก์ชันความปลอดภัยในระบบที่มีความซับซ้อนไม่มากและมุ่งเน้นด้านการทำฮาร์ดแวร์ควบคุม (Hardware Control) อาทิเช่น การทำสัญญาณควบคุม (WiringControl Signal) แบบป้องกันการทำงานที่ผิดพลาด (Interlock System) หรือการวางระบบควบคุมแบบคู่ขนาน (Redundant Control System) เพื่อลดโอกาสของการล้มเหลวของระบบ เป็นต้น

ในปี พ.ศ. 2553 William E. Anderson [7] นำเสนองานวิจัยเรื่องการเปรียบเทียบความปลอดภัยของการออกแบบระบบระหว่างโครงสร้างแบบ Category 3 และ Category 4 เพื่อให้เกิดความเข้าใจมากยิ่งขึ้นและนำไปสู่การใช้งานที่ถูกต้องโดยได้ให้ข้อสรุปไว้ว่าโครงสร้างแบบ Category 4 ให้ความปลอดภัยสูงสุดเนื่องจากมีการพิจารณาความบกพร่องของระบบในกรณีที่ไม่สามารถตรวจจับได้ (Dangerous failure of undetected faults) จึงทำให้ระบบมีความน่าเชื่อถือสูงสุด (High Reliability) และความปลอดภัยในระดับที่รองลงมาคือโครงสร้างแบบ Category 3, Category 2, Category 1 และ Category B ตามลำดับโดยที่โครงสร้างแบบ Category B,Category 1, Category 2 ในกรณีที่เกิด Single Fault ระบบจะไม่สามารถตรวจจับความบกพร่องได้ ส่งผลให้ฟังก์ชันความปลอดภัยทำงานผิดพลาด นำไปสู่การเกิดเหตุการณ์ที่อันตรายได้ ส่วนโครงสร้างแบบ Category 3, Category 4 ในกรณีที่เกิด Single Fault ระบบสามารถที่จะตรวจจับความบกพร่องได้และสามารถที่จะป้องกันการเกิดเหตุการณ์ที่อันตรายได้ ทำให้ระบบมีความปลอดภัยและความน่าเชื่อถือที่สูงกว่า

ในปี พ.ศ. 2553 Ernesto Sorressiและคณะ [8] นำเสนองานวิจัยเรื่องการแนะนำมาตรฐานความปลอดภัยสากล EN 954-1 [3], EN ISO 13849-1 [1] และ IEC 62061 [4] โดยมีวัตถุประสงค์เพื่อให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องกับมาตรฐานเหล่านี้เกิดความเข้าใจมากยิ่งขึ้น เนื่องจากจะมีการแทนที่มาตรฐาน EN 954-1 [3] ด้วยมาตรฐาน EN ISO 13849-1 [1] และ IEC 62061 [4] อย่างสมบูรณ์และมีผลบังคับใช้ในปี พ.ศ. 2554 โดยได้ให้ข้อสรุปไว้ว่า 2 มาตรฐานที่จะมาแทนที่มาตรฐานเดิมนั้นไม่ใช่เรื่องง่ายที่จะทำความเข้าใจ เนื่องจากว่าพารามิเตอร์ที่ใช้ในการคำนวณจะมีเพิ่มมากขึ้นและส่วนใหญ่เป็นเชิงสถิติ ซึ่งแตกต่างจากมาตรฐานเดิมอย่างสิ้นเชิงทำให้เกิดความสับสนต่อผู้ใช้งานมาตรฐานเป็นอย่างมากนำไปสู่การประยุกต์ใช้งานที่ไม่ถูกต้องและส่งผลให้เกิดเหตุการณ์ที่อันตรายได้ในที่สุดโดย2 มาตรฐานนี้มีบางส่วนที่เหมือนกันและบางส่วนที่แตกต่างกันในเรื่องข้อกำหนดของการนำมาประยุกต์ใช้งานซึ่งมาตรฐาน EN ISO 13849-1 [1] จะโดดเด่นทางด้านระบบอีเลคโทรแมคคานิค (Electromechanical System) ส่วนมาตรฐาน IEC 62061 [4] จะโดดเด่นทางด้านโปรแกรมควบคุม (PLC) และระบบความปลอดภัยแบบเครือข่าย (Safety Network System) จากที่ได้กล่าวมาในเบื้องต้น ผู้ทำงานวิจัยจึงให้ความเห็นว่าองค์กรที่ทำหน้าที่ในการกำหนดมาตรฐานความปลอดภัยสากล ISO และ IEC ควรจะหาทางออกสำหรับเรื่องนี้ร่วมกันโดยการรวม 2 มาตรฐานให้เป็นมาตรฐานเดียว เพื่อไม่ให้ผู้ใช้งานเกิดความสับสน นำไปสู่การประยุกต์ใช้งานที่ไม่ถูกต้องและทำให้เกิดเหตุการณ์ที่อันตรายได้

ในปี พ.ศ. 2554 Ernesto Sorressi [9] นำเสนองานวิจัยเรื่องการนำมาตรฐาน IEC 62061 [4] มาประยุกต์ใช้กับเครื่องจักรในอุตสาหกรรมผลิตโลหะ (Machinery in Metal Industry) โดยมีวัตถุประสงค์เพื่อพิสูจน์ว่ามาตรฐาน IEC 62061 [4] สามารถใช้งานแทนมาตรฐาน EN 954-1 [3] ในการจัดการกับความเสี่ยงได้ เนื่องจากเครื่องจักรส่วนมากในอุตสาหกรรมผลิตโลหะเป็นระบบอัตโนมัติ (Automatic System) ซึ่งในแต่ละขั้นตอนของกระบวนการผลิตโลหะมีความเสี่ยงสูง ในกรณีที่พนักงานต้องเข้าไปปฏิบัติงานในพื้นที่อันตรายมีความจำเป็นที่จะต้องหยุดการทำงานของเครื่องจักรทันทีเพื่อป้องกันการเกิดเหตุการณ์ที่อันตรายซึ่งข้อกำหนดความปลอดภัยของเครื่องจักรในกระบวนการผลิตโลหะ (Safety requirement ofmachinery inmetal process) ระบุไว้ว่าเครื่องจักรจะต้องถูกออกแบบให้มีค่าระดับความปลอดภัยอย่างน้อยเท่ากับ PLd หรือโครงสร้างแบบ Category 3 โดยอ้างอิงจากมาตรฐาน CEN EN

15093 [10], CEN EN 13675 [11] และ CEN EN 15061 [12] ดังนั้นเครื่องจักรในอุตสาหกรรมผลิตโลหะจึงถูกออกแบบตั้งแต่แรกให้มีค่าระดับความปลอดภัยเท่ากับ PLd หรือโครงสร้างแบบ Category 3 ซึ่งเป็นไปตามข้อกำหนดของมาตรฐานความปลอดภัยสากล EN 954-1 [3] และ EN ISO 13849-1 [1] เพื่อที่จะสามารถป้องกันการเกิดอุบัติเหตุได้

จากงานวิจัยพบว่าในทำนองเดียวกันถ้าออกแบบเครื่องจักรด้วยมาตรฐานความปลอดภัยสากล IEC 62061 [4] จะมีค่าระดับความปลอดภัยเท่ากับ SIL 3 ซึ่งเมื่อเปรียบเทียบกับมาตรฐาน EN 954-1 [3] และ EN ISO 13849-1 [1] ดังแสดงในตารางที่ 2.2 แล้ว จะพบว่ามีค่าระดับความปลอดภัยเท่ากับ PLe จึงพิสูจน์ได้ว่ามาตรฐาน IEC 62061 [4] นำมาใช้งานแทนมาตรฐาน EN 954-1 [3] และ EN ISO 13849-1 [1] ได้และสามารถรับรองความปลอดภัยของระบบได้เช่นเดียวกัน

ตารางที่ 2.2 แสดงความสัมพันธ์ของค่าระดับความปลอดภัยระหว่าง PL กับ SIL

PL	SIL (IEC 61508-1, for information) High/continuous mode of operation
a	No correspondence
b	1
c	1
d	2
e	3

จากการศึกษางานวิจัยที่เกี่ยวข้องพบว่าในปัจจุบันตัวอย่างของการประยุกต์ใช้งานมาตรฐานความปลอดภัยสากล EN ISO 13849-1 [1] และIEC 62061 [4] ที่มาแทนมาตรฐาน EN 954-1 [3] ในการออกแบบระบบควบคุมความเสี่ยง SRP/CS ให้กับเครื่องจักรในภาคอุตสาหกรรมมีอยู่จำนวนไม่มากและไม่ครอบคลุมในทุกภาคอุตสาหกรรมกระบวนการผลิต เมื่อพิจารณาค่าสถิติของการเกิดอุบัติเหตุจากเครื่องจักรในประเทศไทยดังที่ได้กล่าวมาในตอนต้น จะพบว่ามีอุตสาหกรรมจำนวนมากที่พนักงานต้องอยู่ในสถานการณ์ที่อันตรายและมีโอกาสสูงที่จะเกิดเหตุการณ์อันตรายอีกทั้งในสถานการณ์ปัจจุบันได้มีการนำเสนอโปรแกรมที่ใช้ในการประเมินความเสี่ยงและลดความเสี่ยงจากทางบริษัทผู้ผลิตอุปกรณ์ความปลอดภัย เพื่อช่วยในการอำนวยความสะดวกให้กับผู้ออกแบบเครื่องจักร (Machine Designer) และผู้ใช้งานเครื่องจักร (Machine User) ซึ่งโปรแกรมเหล่านี้ให้ผลลัพธ์ในการคำนวณที่รวดเร็วและนำไปสู่การตัดสินใจในการเลือกซื้อผลิตภัณฑ์ส่วนมากจะมุ่งเน้นไปทางด้านการตลาด ทำให้ผู้ออกแบบเครื่องจักรและผู้ใช้งานเครื่องจักรไม่เข้าใจหลักการและวิธีการของมาตรฐานความปลอดภัยสากลอย่างแท้จริง นำไปสู่การประเมินความเสี่ยงที่ไม่ครอบคลุมและไม่สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิผลทำให้เกิดอุบัติเหตุกับพนักงานได้

ดังนั้นงานวิจัยนี้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อประยุกต์ใช้งานมาตรฐานความปลอดภัยสากล EN ISO13849-1 [1] กับเครื่องจักรในอุตสาหกรรมผลิตยางรถยนต์ (Machinery of Tyre Industry) ในการจัดการกับความเสี่ยงหรือลดความเสี่ยงลงให้อยู่ในระดับที่ยอมรับได้ และเพื่อเป็นแนวทางสำหรับผู้ที่ต้องการนำไปประยุกต์ใช้กับเครื่องจักรในภาคอุตสาหกรรมกระบวนการผลิตอื่นๆ เพื่อช่วยส่งเสริมการลด

สถิติของการเกิดอุบัติเหตุจากเครื่องจักรในประเทศไทยและสร้างสภาพแวดล้อมการทำงานที่ปลอดภัยให้กับพนักงาน

2.2 ความรู้พื้นฐานเกี่ยวกับเครื่องจักร

2.2.1 เครื่องจักรในอุตสาหกรรมกระบวนการผลิต

ในปัจจุบันเครื่องจักรที่ใช้ในอุตสาหกรรมกระบวนการผลิตมีความเสี่ยงสูงที่จะนำไปสู่การเกิดเหตุการณ์ที่อันตรายได้เนื่องมาจากสาเหตุหลักๆดังนี้

1. การออกแบบเครื่องจักรที่ไม่ถูกต้องตามมาตรฐานความปลอดภัยและไม่ได้มีการประเมินความเสี่ยงที่จะเกิดขึ้นอย่างครอบคลุม
2. การที่พนักงานไม่มีความรู้ ความเข้าใจเกี่ยวกับการใช้งานเครื่องจักรอย่างถูกต้อง

ดังนั้นผู้ที่เกี่ยวข้องกับเครื่องจักรในอุตสาหกรรมกระบวนการผลิตจำเป็นที่จะต้องมีความรู้ ความเข้าใจเกี่ยวกับมาตรฐานความปลอดภัยสากล เพื่อที่จะออกแบบเครื่องจักรให้มีความปลอดภัยและให้ความรู้ความเข้าใจที่ถูกต้องกับพนักงาน จึงจะสามารถป้องกันการเกิดเหตุการณ์ที่อันตรายได้

รูปที่ 2.1 ตัวอย่างของการทำงานร่วมกับเครื่องจักร (Working with machinery)

รูปที่ 2.2 ตัวอย่างอุบัติเหตุที่เกิดจากเครื่องจักร (Accident by machinery)

2.2.2 ข้อกำหนดของเครื่องจักรในทวีปยุโรป (European Directive)

CE Mark หรือ Conformity European Mark เป็นเครื่องหมายที่แสดงว่าสินค้าอุตสาหกรรมที่จำหน่ายในสหภาพยุโรป (European Union : EU) ทั้งสินค้านำเข้าและสินค้าที่ผลิตใน EU มีการออกแบบและการผลิตที่ได้มาตรฐานความปลอดภัยตามระเบียบข้อบังคับที่ EU กำหนด ทั้งนี้เพื่อสร้างความมั่นใจให้แก่ผู้บริโภคใน EU ถึงความปลอดภัยในการใช้สินค้าและลดผลกระทบที่อาจมีต่อสิ่งแวดล้อม รวมทั้งเพื่อสร้างมาตรฐานสินค้าของประเทศสมาชิกในกลุ่ม EU ให้เป็นมาตรฐานเดียวกัน EU เริ่มบังคับใช้เครื่องหมาย CE มาตั้งแต่ปี 2536 โดยกำหนดให้สินค้าอุตสาหกรรมทุกประเภทที่จำหน่ายใน EU ต้องติดเครื่องหมาย CE ครอบคลุมตั้งแต่ของเด็กเล่น เครื่องใช้ไฟฟ้า ผลิตภัณฑ์อิเล็กทรอนิกส์ เครื่องจักร อุปกรณ์ทางการแพทย์ ลิฟต์ อุปกรณ์ก่อสร้าง วิทยุและอุปกรณ์สื่อสาร และหม้อน้ำร้อน เป็นต้น

ขั้นตอนการขออนุญาตติดเครื่องหมาย CE บนสินค้าอุตสาหกรรม มีรายละเอียดสำคัญดังนี้

1. ตรวจสอบระเบียบข้อบังคับ (Directives) และมาตรฐานสินค้า (Harmonized Standards) เพื่อใช้เป็นแนวทางปฏิบัติ ปัจจุบันระเบียบข้อบังคับที่คณะกรรมาธิการยุโรป (European Commission) กำหนดมีกว่า 20 ฉบับ ซึ่งแต่ละฉบับจะแสดงรายละเอียดเกี่ยวกับมาตรฐานต่าง ๆ ของสินค้าอุตสาหกรรมแต่ละประเภทที่จัดทำขึ้นโดยหน่วยงานมาตรฐานสินค้าของ EU อาทิ European Committee for Standardization และ European Committee for Electro technical Standardization ผู้ผลิตสินค้าอุตสาหกรรมเพื่อส่งออกไปยัง EU จึงควรติดตามความเคลื่อนไหวของระเบียบข้อบังคับและมาตรฐานของสินค้าที่ตนผลิตอย่างใกล้ชิด เนื่องจากระเบียบและมาตรฐานดังกล่าวอาจมีการปรับปรุงและเพิ่มเติมรายละเอียดต่างๆ ให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป
2. การทดสอบผลิตภัณฑ์ เพื่อให้มีมาตรฐานความปลอดภัยตามที่ EU กำหนด ทั้งนี้ผู้ผลิตสามารถตรวจสอบและรับรองความปลอดภัยของสินค้าด้วยตนเองหากสินค้ามีความเสี่ยงน้อยในการใช้งาน แต่หากสินค้ามีความเสี่ยงสูงในการใช้งานผู้ผลิตต้องให้หน่วยงานตรวจสอบอิสระ (Notified Body) ที่ผ่านการรับรองจากคณะกรรมาธิการยุโรป (ปัจจุบันมีประมาณ 1,000 แห่งใน EU แต่ยังไม่มีในประเทศไทย) เป็นผู้ตรวจสอบและรับรองความปลอดภัยสินค้าให้
3. จัดทำแฟ้มข้อมูลด้านเทคนิค (Technical File) ผู้ผลิต ผู้นำเข้า หรือตัวแทนจำหน่ายต้องจัดทำแฟ้มข้อมูลทางเทคนิค เพื่อเป็นหลักฐานแสดงต่อคณะกรรมาธิการยุโรปเมื่อมีการเรียกตรวจสอบ ทั้งนี้ แฟ้มข้อมูลด้านเทคนิคต้องมีรายละเอียดต่างๆ ดังนี้ ชื่อและที่อยู่ของผู้ผลิต ลักษณะและประเภทของสินค้า ขั้นตอนการออกแบบ กระบวนการผลิต วิธีประเมินความเสี่ยงจากการใช้สินค้า มาตรฐานที่ใช้ในการทดสอบรายงานผลการตรวจสอบ และคู่มือการใช้งาน
4. จัดทำใบรับรอง (Declaration of Conformity) ผู้ผลิต ผู้นำเข้าหรือตัวแทนจำหน่ายต้องจัดทำใบรับรองเพื่อแสดงว่าสินค้าได้มาตรฐานความปลอดภัยตามที่ EU กำหนด โดย

ระบุรายละเอียดต่าง ๆ คือ ชื่อและที่อยู่ของผู้ผลิตหรือตัวแทนจำหน่ายใน EU ลักษณะของสินค้า ระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้องกับสินค้า มาตรฐานที่ใช้ในการตรวจสอบ ชื่อหน่วยงานตรวจสอบอิสระที่เป็นผู้ทดสอบสินค้า วันที่ออกใบรับรอง และลายมือชื่อผู้มีอำนาจของบริษัทผู้ผลิตส่วนวิเคราะห์ธุรกิจ

5. ติดเครื่องหมาย CE ผู้ผลิตจะติดเครื่องหมาย CE บนตัวสินค้าหรือบนบรรจุภัณฑ์ได้ก็ต่อเมื่อสินค้าของตนผ่านการทดสอบและมีมาตรฐานตามที่ EU กำหนด ทั้งนี้ เครื่องหมาย CE ที่ติดบนตัวสินค้าหรือบรรจุภัณฑ์ต้องมีความคงทนถาวรและมีขนาดไม่ต่ำกว่า 5 มิลลิเมตร เพื่อให้สามารถมองเห็นได้อย่างชัดเจน

แม้ว่าการติดเครื่องหมาย CE ทำให้ผู้ประกอบการไทยต้องเผชิญกับต้นทุนการผลิตที่เพิ่มขึ้น ทั้งในส่วนของค่าใช้จ่ายในการพัฒนาและปรับปรุงกระบวนการผลิต การออกแบบผลิตภัณฑ์ให้สอดคล้องกับระเบียบข้อบังคับและมาตรฐานที่ EU กำหนด ตลอดจนมีค่าใช้จ่ายในการว่าจ้างหน่วยงานตรวจสอบอิสระเพื่อทดสอบความปลอดภัยของสินค้า อย่างไรก็ตาม เครื่องหมาย CE นับเป็นใบเบิกทางสำคัญที่มีส่วนช่วยให้ผู้ประกอบการไทยสามารถลดอุปสรรคทางการค้ากับ EU และยังสามารถเคลื่อนย้ายสินค้าได้อย่างเสรีภายในกลุ่ม EU โดยที่แต่ละประเทศไม่สามารถนำมาตรฐานสินค้าของตนมากีดกันสินค้าอุตสาหกรรมส่งออกจากประเทศไทยได้

รูปที่ 2.3 กระบวนการติดเครื่องหมายรับรองความปลอดภัยให้กับเครื่องจักร (CE MarkingProcess)

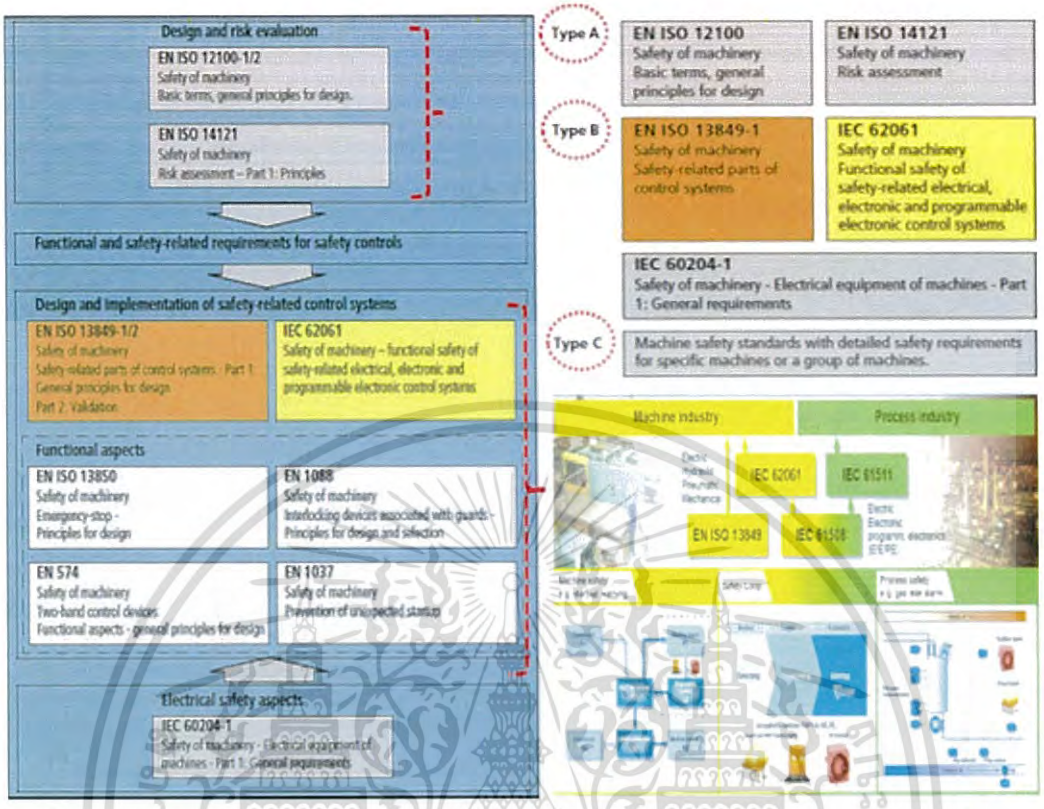
รูปที่ 2.4 ตัวอย่างการติดเครื่องหมาย CE ที่เครื่องจักร (CE Marking on Machinery)

2.2.3 มาตรฐานความปลอดภัยสากลที่ใช้กับเครื่องจักรในอุตสาหกรรมกระบวนการผลิต

2.2.3.1 มาตรฐานความปลอดภัยสากลที่เกี่ยวข้องกับการออกแบบเครื่องจักร

จากรูปที่ 2.5 มาตรฐานความปลอดภัยสากลที่เกี่ยวข้องกับการออกแบบเครื่องจักรแบ่งออกเป็น 3 ประเภท ดังนี้

1. ประเภท A เช่นมาตรฐาน EN ISO 12100 [2] และมาตรฐาน EN ISO 14121 [13] ซึ่งมาตรฐาน EN ISO 12100 [2] จะอธิบายเกี่ยวกับหลักการพื้นฐานในการออกแบบเครื่องจักรให้มีความปลอดภัยและมาตรฐาน EN ISO 14121 [13] จะอธิบายเกี่ยวกับวิธีในการประเมินความเสี่ยงของเครื่องจักร
2. ประเภท B เช่น มาตรฐาน EN ISO 13849-1 [1] ซึ่งพัฒนามาจากมาตรฐาน EN 954-1 [3] และมาตรฐานIEC 62061 [4] ซึ่งพัฒนามาจากมาตรฐาน IEC 61508 [14] โดยที่มาตรฐาน EN ISO 13849-1 [1] จะอธิบายเกี่ยวกับการออกแบบระบบควบคุมความเสี่ยงให้กับเครื่องจักรโดยจะมุ่งเน้นการออกแบบระบบทางด้านฮาร์ดแวร์ (Hardware design) เช่น ระบบอีเลคโทรแมคคานิค (Electromechanical System) และมาตรฐาน IEC 62061 [4] จะอธิบายเกี่ยวกับการออกแบบฟังก์ชันควบคุมความเสี่ยงให้กับเครื่องจักรโดยมุ่งเน้นการออกแบบระบบด้านซอฟแวร์ (Software design) เช่น ระบบควบคุม (PLC) และระบบความปลอดภัยแบบเครือข่าย (Safety NetworkSystem)
3. ประเภท C เช่น มาตรฐาน EN ISO 13850 [15], EN 1088 [16], EN 574 [17], EN 1037 [18] และ IEC 60204-1 [19] ฯลฯ ซึ่งจะอธิบายเกี่ยวกับอุปกรณ์ความปลอดภัยที่นำมาใช้ในการออกแบบระบบควบคุมความเสี่ยง เช่น มาตรฐาน EN ISO 13850 [15] จะอธิบายเกี่ยวกับการออกแบบอุปกรณ์ความปลอดภัยแบบหยุดฉุกเฉิน (Emergency stop device), มาตรฐาน EN 1088 [16] จะอธิบายเกี่ยวกับการออกแบบอุปกรณ์ความปลอดภัยสำหรับป้องกันการทำงานที่ผิดพลาด (Interlocking device), มาตรฐาน EN 574 [17] จะอธิบายเกี่ยวกับการออกแบบอุปกรณ์ความปลอดภัยสำหรับควบคุมการทำงานแบบใช้สองมือ (Two-hand control device), มาตรฐาน EN 1037 [18] จะอธิบายเกี่ยวกับการออกแบบวิธีการป้องกันอันตรายในกรณีที่เครื่องจักรเริ่มเดินโดยไม่พึงประสงค์ (Prevention of unexpected startup), มาตรฐาน IEC 60204-1 [19] จะอธิบายเกี่ยวกับการออกแบบอุปกรณ์ไฟฟ้าที่ใช้กับเครื่องจักรให้เป็นไปตามข้อกำหนดความปลอดภัย(Electrical equipment of machines for safety requirement)

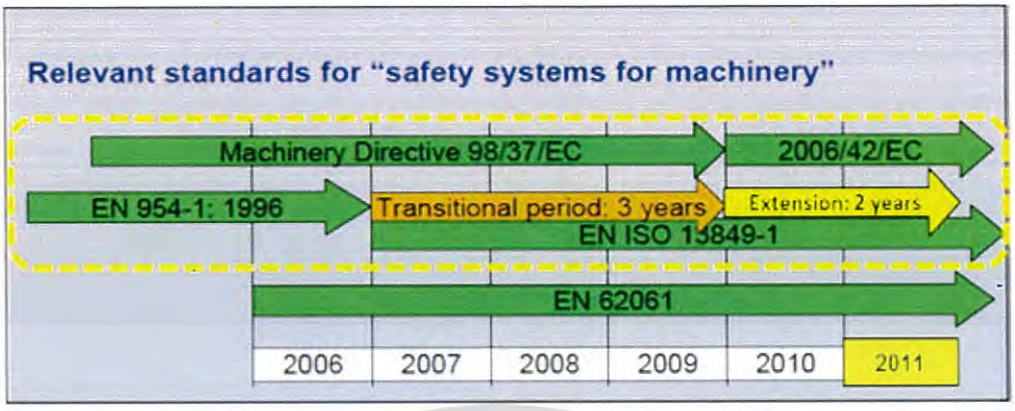


รูปที่ 2.5 มาตรฐานความปลอดภัยสากลที่ใช้กับเครื่องจักรในอุตสาหกรรมกระบวนการผลิต (Overview of International Safety Standard for Industrial Machinery)

2.2.3.2 ประวัติความเป็นมาของมาตรฐานความปลอดภัย

มาตรฐานความปลอดภัยที่ใช้ในการออกแบบระบบความปลอดภัยเครื่องจักรที่เป็นที่รู้จักอย่างแพร่หลายในอดีต คือมาตรฐาน EN 954-1 [3] เริ่มใช้งานอย่างจริงจังตั้งแต่ปี พ.ศ. 2539 ในกลุ่มประเทศแถบยุโรป เนื่องด้วยข้อกำหนดด้านการนำเข้าเครื่องจักรและผลิตเครื่องจักรในทวีปยุโรป (Machinery Directive 98/37/EC) ระบุไว้ว่าจะต้องออกแบบและผลิตเครื่องจักรให้ได้ตามมาตรฐานความปลอดภัยตามระเบียบข้อบังคับที่ EU กำหนด เพื่อสร้างความมั่นใจให้แก่ผู้ใช้งานเครื่องจักรในทวีปยุโรป

ในช่วงระหว่างปี พ.ศ. 2550 ถึง พ.ศ. 2554 ได้มีการพัฒนาและปรับปรุงมาตรฐานใหม่ขึ้นมา คือ มาตรฐาน EN ISO 13849-1 [1] ซึ่งเป็นมาตรฐานที่พัฒนามาจากแนวความคิดของมาตรฐาน EN 954-1 [3] หลังจากนั้นมีการประกาศยกเลิกใช้งานมาตรฐาน EN 954-1 [3]ในช่วงปลายปีพ.ศ. 2554 และบังคับใช้งานมาตรฐานใหม่ EN ISO 13849-1 [1] อย่างเป็นทางการ แสดงดังรูปที่ 2.6 มาตรฐานความปลอดภัยสากลที่สามารถนำมาประยุกต์ใช้กับเครื่องจักรในอุตสาหกรรมยางรถยนต์มี 3 มาตรฐานหลักๆ ดังนี้EN ISO 13849-1 [1], EN ISO 12100 [2] และEN 954-1 [3]



รูปที่ 2.6 การถ่ายโอนจากมาตรฐานเก่า EN 954-1 [3] ไปสู่มาตรฐานใหม่ EN ISO 13849-1 [1]

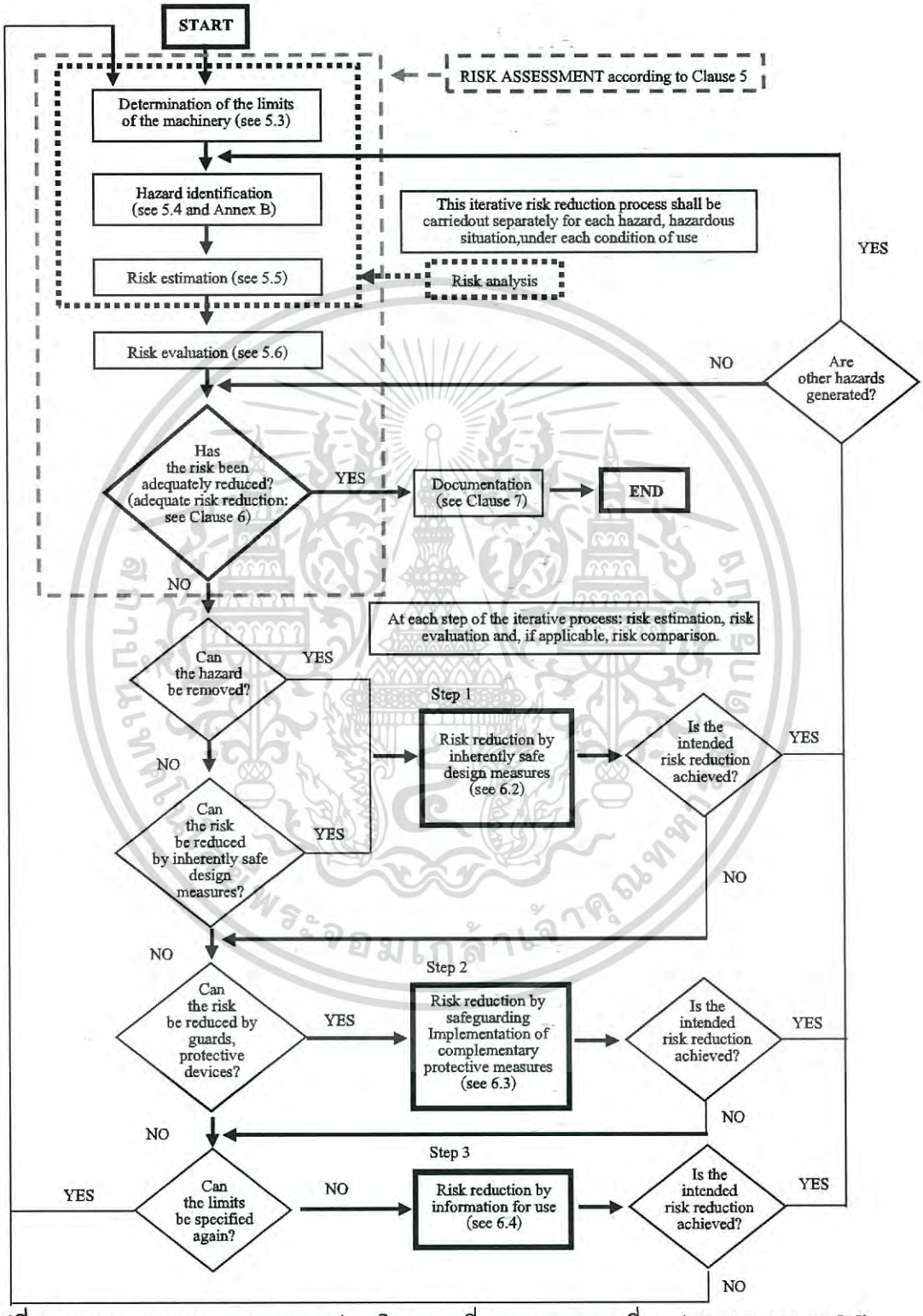
2.3 มาตรฐาน EN ISO 12100

มาตรฐาน EN ISO 12100 [2] กล่าวถึงหลักการพื้นฐานสำหรับการออกแบบเครื่องจักรให้มีความปลอดภัย โดยมุ่งเน้นในเรื่องของหลักเกณฑ์ที่ใช้ในการประเมินความเสี่ยงและลดความเสี่ยง (Risk Assessment and Risk Reduction) เพื่อเป็นแนวทางให้กับผู้ผลิตหรือผู้ออกแบบเครื่องจักรในการจัดการกับความเสี่ยงโดยมีกระบวนการดังแสดงในรูปที่ 2.7

การประเมินความเสี่ยงคือการคิด วิเคราะห์ ความเสี่ยงที่จะเกิดขึ้นด้วยหลักของเหตุและผลบนพื้นฐานของความเป็นจริงและนำไปสู่กระบวนการในการลดความเสี่ยงที่มีประสิทธิผล สามารถที่จะป้องกันการเกิดเหตุการณ์อันตรายได้ จากรูปที่ 2.7 สามารถสรุปเป็น 5 ขั้นตอนหลักๆ ได้ดังนี้

1. การพิจารณาศักยภาพ ขีดความสามารถและข้อจำกัดของเครื่องจักร (Determination of limits of machinery)
2. การระบุอันตรายหรือสถานการณ์อันตรายที่เกี่ยวข้อง (Identify the hazards and associated hazardous situations)
3. วิเคราะห์ความเสี่ยงจากอันตรายหรือสถานการณ์อันตรายที่ได้ระบุมา (Estimate the risk for each identified hazard and hazardous situation)
4. การประเมินความเสี่ยงและตัดสินใจเกี่ยวกับความเสี่ยงที่ต้องการจะลด (Evaluatethe riskand take decisions about the need for risk reduction)
5. การจัดการความเสี่ยงหรือลดความเสี่ยง (Eliminate the hazard or reduce risk)

ในกรณีที่มีความเสี่ยงเหลืออยู่ (Remaining of residual risk) กระบวนการในการประเมินความเสี่ยงและลดความเสี่ยงจะต้องมีการนำมาพิจารณาซ้ำ (Iterative process) เพื่อจัดการกับความเสี่ยงหรือลดความเสี่ยงลงให้มากที่สุดเท่าที่สามารถทำได้ โดยที่ขั้นตอนที่ 1 – 4 คือกระบวนการประเมินความเสี่ยง (Risk assessment) และขั้นตอนที่ 5 คือวิธีการลดความเสี่ยง (Risk Reduction)



รูปที่ 2.7 แผนภาพแสดงกระบวนการประเมินความเสี่ยงและลดความเสี่ยง (EN ISO 12100 [2])

2.3.1 การพิจารณาศักยภาพ ขีดความสามารถและข้อจำกัดของเครื่องจักร (Determination of limits of machinery)

1. พิจารณาข้อจำกัดด้านการใช้งานเครื่องจักร เช่น ได้มีการระบุวิธีการใช้งานเครื่องจักรหรือได้มีการคาดการณ์ล่วงหน้าของการใช้งานเครื่องจักรที่ไม่ถูกต้องไว้หรือไม่
2. พิจารณาข้อจำกัดด้านผู้ใช้งานเครื่องจักร เช่น ได้มีการระบุอายุ เพศ หรือขีดความสามารถทางด้านร่างกายของผู้ใช้งานไว้หรือไม่ (การมองเห็น, การได้ยิน, อวัยวะครบถ้วน, ความแข็งแรงของร่างกาย, โรคประจำตัว, ส่วนสูงมาตรฐาน, ฯลฯ)
3. พิจารณาข้อกำหนดการใช้งานที่เฉพาะเจาะจงของแต่ละหน่วยงาน เช่น มีการกำหนดวิธีการใช้งานเครื่องจักรสำหรับพนักงานฝ่ายผลิต, ฝ่ายซ่อมบำรุง หรือฝ่ายตรวจสอบคุณภาพผลิตภัณฑ์ไว้หรือไม่ เนื่องจากในแต่ละหน่วยงานมีวัตถุประสงค์ในการใช้งานเครื่องจักรที่ไม่เหมือนกัน ขึ้นอยู่กับหน้าที่และความรับผิดชอบของหน่วยงานนั้น
4. ข้อจำกัดด้านพื้นที่ เช่น ได้มีการระบุระยะในการเคลื่อนที่ของชิ้นส่วนที่เคลื่อนที่ได้หรือระบุระยะที่ปลอดภัยสำหรับพนักงานในการปฏิบัติงานร่วมกับเครื่องจักรไว้หรือไม่
5. ข้อจำกัดด้านเวลา เช่น ได้มีการกำหนดรอบในการเปลี่ยนชิ้นส่วนของเครื่องจักรหรือรอบในการซ่อมบำรุงเครื่องจักรไว้หรือไม่ข้อจำกัดทั่วๆไป เช่น ได้มีการระบุสภาพแวดล้อมที่เหมาะสมกับการใช้งานเครื่องจักร เช่น อุณหภูมิ, ความชื้น, ฝุ่น, ใช้งานในร่ม หรือใช้งานกลางแจ้ง รวมทั้งรอบในการทำความสะอาดเครื่องจักรไว้หรือไม่

ข้อจำกัดเหล่านี้ควรนำมาพิจารณาในขั้นตอนของการประเมินความเสี่ยง (Risk Assessment) ด้วยเพราะเป็นปัจจัยพื้นฐานที่ทำให้เกิดความเสี่ยงและนำไปสู่การเกิดเหตุการณ์ที่อันตรายได้

2.3.2 การระบุอันตรายหรือสถานการณ์อันตรายที่เกี่ยวข้อง (Identify the hazards and associatedhazardous situations)

หลังจากพิจารณาข้อจำกัดของเครื่องจักรแล้ว ขั้นตอนต่อไปคือการระบุอันตรายที่คาดการณ์ว่าจะเกิดขึ้น ซึ่งมีทั้งอันตรายที่เกิดขึ้นอย่างแน่นอน (Reasonably foreseeable hazards) และอันตรายที่อาจจะเกิดขึ้นโดยไม่ได้คาดคิด (Unexpected hazards) สิ่งที่ต้องนำมาพิจารณาในการระบุอันตรายคือ

1. ลักษณะงานที่พนักงานต้องเข้าไปทำงานร่วมกับเครื่องจักร (Human Machine Interface) เช่น การตั้งค่าเครื่องจักร (Setting Machine), การเดินเครื่องจักร (Operation Machine), การทดสอบเครื่องจักร (Testing Machine), การเริ่มเดินเครื่องจักร (Startup Machine), การหยุดเครื่องจักร (Stopping Machine), การเปลี่ยนอุปกรณ์เครื่องจักร (Tooling Change Machine), การซ่อมบำรุงเชิงป้องกัน (Preventive Maintenance), การแก้ไขปัญหาเครื่องจักรเสีย (Corrective Maintenance), การนำผลิตภัณฑ์เข้าและออกจากเครื่องจักร (Load and Unload Product), การแก้ไขปัญหาในกรณีเครื่องจักรขัดข้อง (Trouble-Shooting) เป็นต้น

2. ลักษณะการทำงานของเครื่องจักร (Machine Function) เช่น เครื่องจักรไม่ได้ทำงานตามฟังก์ชั่นที่ได้กำหนดไว้ (Malfunction) เนื่องจากอุปกรณ์ของเครื่องจักรทำงานผิดพลาด (Failure of Component), การถูกรบกวนจากปัจจัยภายนอก (External Interference) เช่นถูกรบกวนจากแรงสั่นสะเทือน (Vibration) หรือสัญญาณรบกวนทางไฟฟ้าแม่เหล็ก (Electromagnetic Interference) หรือการทำงานที่ผิดพลาดของโปรแกรม (Software Error) เป็นต้น
3. พฤติการณ์การทำงานที่ผิดพลาดของพนักงานโดยไม่ได้ตั้งใจ (Human Error) เช่นสูญเสียการควบคุมเครื่องจักร (Loss of control machine) เนื่องจากความไม่ระมัดระวังหรือไม่มีสมาธิในการทำงาน เป็นต้น

การระบุอันตรายหรือสถานการณ์อันตรายที่เกี่ยวข้องกับเครื่องจักรควรนำมาพิจารณาในขั้นตอนของการประเมินความเสี่ยง (Risk Assessment) และควรระบุไว้ในเอกสารการใช้งานของเครื่องจักรด้วยเพื่อให้ผู้ใช้งานทราบถึงอันตรายและระมัดระวังป้องกันตัวอย่างของการระบุจุดที่อันตรายแสดงดังภาคผนวก ง

2.3.3 วิเคราะห์ความเสี่ยงจากอันตรายหรือสถานการณ์อันตรายที่ได้ระบุมา (Estimate the risk foreach identified hazard and hazardous situation)

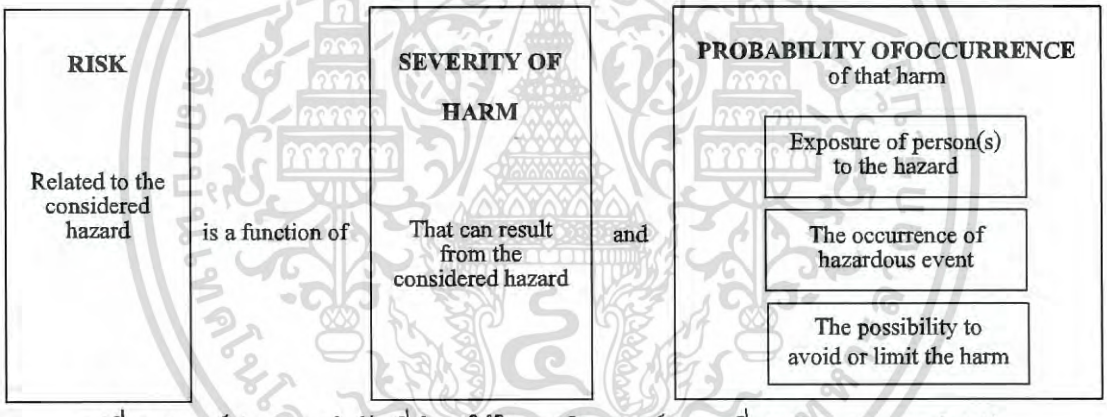
หลังจากที่ได้ระบุอันตรายหรือสถานการณ์อันตรายที่เกี่ยวข้องกับเครื่องจักรแล้ว ขั้นตอนต่อไปคือการวิเคราะห์ความเสี่ยงจากอันตรายหรือสถานการณ์อันตรายที่ได้ระบุมา โดยสิ่งต้องนำมาพิจารณาในการวิเคราะห์ความเสี่ยงประกอบด้วย

1. ความรุนแรงของอันตราย (Severity of harm) แบ่งออกเป็น 3 ระดับความรุนแรงดังนี้ ได้รับบาดเจ็บเพียงเล็กน้อย (Slight Injury), ได้รับบาดเจ็บถึงขั้นสูญเสียอวัยวะหรือพิการ (Serious Injury), ได้รับบาดเจ็บอย่างรุนแรงถึงขั้นเสียชีวิต (Death) หรือปัจจัยอื่นๆที่เกี่ยวข้องเช่นอันตรายส่งผลกระทบกับบุคคลเพียงคนเดียว (Effect to one person) หรือส่งผลกระทบกับหลายๆบุคคล (Effect to several persons) เป็นต้น
2. โอกาสในการเกิดอันตราย (Probability of occurrence of harm) แบ่งออกเป็น 3 ปัจจัยที่เกี่ยวข้องดังนี้
    2.1 พนักงานเข้าไปอยู่ในสถานการณ์ที่อันตราย (Exposure of persons to the hazard) เช่น การเข้าไปปฏิบัติแบบปกติทั่วๆไป (Normal operation), การเข้าไปแก้ไขปัญหาเครื่องจักรในสภาวะผิดปกติ (Correction of machine malfunction) หรือการเข้าไปซ่อมบำรุงเครื่องจักร (Maintenance and repair) หรือปัจจัยอื่นๆที่เกี่ยวข้อง เช่น ระยะเวลา (Time), ความถี่ (Frequency), จำนวนผู้ปฏิบัติงานที่เข้าไปอยู่สถานการณ์ที่อันตราย (Number of persons access to dangerous zone) เป็นต้น

2.2 การเกิดของเหตุการณ์ที่อันตราย (Occurrence of a hazardous event) เช่น พิจารณาจากประวัติเหตุการณ์อันตรายที่เกิดขึ้นในอดีตและผลกระทบต่อชีวิตและทรัพย์สิน

2.3 โอกาสในการหลบหลีกสถานการณ์ที่อันตรายหรือการยับยั้งอันตราย (Possibility of avoiding or limiting harm) เช่น พนักงานผู้ปฏิบัติงานได้ผ่านการอบรมหลักการความปลอดภัยพื้นฐานและการใช้งานเครื่องจักรที่ปลอดภัยหรือไม่, มีการติดป้ายหรือสัญลักษณ์แจ้งเตือนสำหรับจุดที่อันตรายและจุดที่ควรระมัดระวังไว้ที่เครื่องจักรหรือไม่, พนักงานผู้ปฏิบัติงานมีประสบการณ์ทำงานกับเครื่องจักรมาก่อนหรือไม่ หรือขนาดของพื้นที่บริเวณจุดที่อันตรายเอื้ออำนวยต่อการหลบหลีกอันตรายที่จะเกิดขึ้นหรือไม่ เป็นต้น

ยิ่งการวิเคราะห์ความเสี่ยงครอบคลุมสถานการณ์อันตรายมากเท่าไหร่ยิ่งทำให้ลดโอกาสในการเกิดอันตรายต่อผู้ใช้งานเครื่องจักรได้มากเท่านั้น องค์ประกอบสำคัญที่ใช้ในการวิเคราะห์ความเสี่ยงกล่าวโดยสรุปได้ดังรูปที่ 2.8



รูปที่ 2.8 องค์ประกอบสำคัญที่นำมาใช้ในการวิเคราะห์ความเสี่ยง (Elements of risk)

2.3.4 การประเมินความเสี่ยงและการตัดสินใจเกี่ยวกับความเสี่ยงที่ต้องการจะลด (Evaluatethe risk and take decisions about the need for risk reduction)

หลังจากที่ได้ทำการวิเคราะห์ความเสี่ยงของสถานการณ์อันตรายแล้ว ขั้นตอนต่อไปคือการประเมินความเสี่ยงและการตัดสินใจเกี่ยวกับความเสี่ยงที่ต้องการจะลด สิ่งที่ต้องนำมาพิจารณาคือ

1. เงื่อนไขการทำงานของเครื่องจักรและวิธีการปฏิบัติงานของพนักงาน
2. ความเสี่ยงที่เพิ่มขึ้น เช่น พิจารณาว่ามีการเปลี่ยนแปลงวิธีการทำของพนักงาน อุปกรณ์และฟังก์ชันการทำงานของเครื่องจักรฯลฯหรือไม่เมื่อมีการเปลี่ยนแปลงเกิดขึ้น จะต้องมีการประเมินความเสี่ยงใหม่ทุกครั้ง

3. กรณีที่มีความเสี่ยงเหลืออยู่ (Remaining of residual risk) สามารถทำให้เกิดอันตรายต่อผู้ปฏิบัติงานได้ จะต้องมีการระบุ ชี้แจงความเสี่ยงที่เหลืออยู่ให้กับพนักงานผู้ปฏิบัติงานทราบเพื่อระมัดระวังและป้องกันความเสี่ยงที่จะเกิดขึ้น
4. ความเสี่ยงจะต้องถูกจัดการให้อยู่ในระดับที่ยอมรับได้ (Reduce risk into acceptable level)

2.3.5 การจัดการความเสี่ยงหรือลดความเสี่ยง(Eliminate the hazard or reduce risk)

หลังจากที่ได้ทำการประเมินความเสี่ยงและการตัดสินใจเกี่ยวกับความต้องการที่จะลด จะนำมาสู่ขั้นตอนสุดท้ายคือการจัดการความเสี่ยงหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Eliminate or reduce risk into acceptable level) ถ้าความเสี่ยงอยู่ในระดับที่ยอมรับไม่ได้ (Non-acceptable level) วิธีการในการลดความเสี่ยงที่ควรนำมาพิจารณาได้แก่ การลดความเสี่ยงด้วยวิธีการออกแบบเครื่องจักรให้ปลอดภัยตั้งแต่แรก, การลดความเสี่ยงด้วยการติดตั้งอุปกรณ์ความปลอดภัยหรือการเพิ่มมาตรการป้องกันให้กับเครื่องจักรและการลดความเสี่ยงด้วยการให้ข้อมูลสำหรับการใช้งานเครื่องจักร

2.3.5.1 การลดความเสี่ยงด้วยวิธีการออกแบบเครื่องจักรให้ปลอดภัยตั้งแต่แรก (Risk reduction by inherently safe design measures)

1. การพิจารณาปัจจัยด้านรูปร่างลักษณะของเครื่องจักร (Geometricaland Physical factors)

1.1 รูปร่างและลักษณะของเครื่องจักร (Geometrical Aspect)ควรจะต้องถูกออกแบบให้สามารถมองเห็นพื้นที่ทำงานและพื้นที่อันตรายได้อย่างชัดเจนจากบริเวณตำแหน่งที่ทำการควบคุมเครื่องจักร (Control Position) เพื่อว่าในกรณีที่เกิดเหตุการณ์อันตรายกับพนักงานปฏิบัติงานเพื่อนร่วมงานหรือหัวหน้างานสามารถที่จะทำการหยุดการทำงานของเครื่องจักรและให้ความช่วยเหลือได้ทันที แต่ในกรณีที่ไม่สามารถหลีกเลี่ยงได้เนื่องจากพื้นที่ทำงานและพื้นที่อันตรายเป็นมุมอับ ควรจะมีการติดอุปกรณ์ช่วยสังเกตการณ์ในการป้องกันอันตราย เช่น กระจกสะท้อน กล้องวงจรปิด เป็นต้น

1.2 การออกแบบเครื่องจักร (Design Aspect) ควรจะออกแบบให้ตำแหน่งของชุดควบคุมหลัก (Main control unit) อยู่บริเวณที่ปลอดภัย เพื่อป้องกันไม่ให้พนักงานเข้าไปปฏิบัติงานในบริเวณพื้นที่ที่อันตราย ซึ่งเป็นการลดโอกาสในการเกิดเหตุการณ์ที่อันตราย

1.3 การออกแบบส่วนประกอบทางด้านแมคคานิค (Mechanical Aspect) ควรทำให้ช่องว่างของจุดที่ทำให้เกิดอันตรายมีน้อยที่สุด เช่น อันตรายจากจุดหนีบ (Crushing Point), จุดหมุน (Rotating Point) หรือจุดเฉือน (Shearing Point) เพื่อป้องกันไม่ให้ชิ้นส่วนของร่างกายสัมผัสจุดอันตรายได้

1.4 การออกแบบเครื่องจักรควรหลีกเลี่ยงส่วนที่แหลมคม (Sharp Edge) หรือส่วนที่ยื่นออกมา(Protrude Part) เพื่อป้องกันอันตรายจากการบาดเฉือนหรือดึงชิ้นส่วนของร่างกายได้

1.5 ในกรณีที่ต้องการควบคุมชุดขับเคลื่อนโดยตรง (Direct Control Actuators) ควรมีระบบที่สามารถควบคุมการทำงานได้ด้วยมือ (Manual ControlSystem) เพื่อให้พนักงานสามารถควบคุมการทำงานของชุดขับเคลื่อนได้อย่างปลอดภัย

2. การออกแบบโดยคำนึงถึงปัจจัยแวดล้อมอื่นๆที่เกี่ยวข้อง (General concerned factors)

2.1 ปัจจัยด้านการยศาสตร์ (Ergonomicfactor) เช่น การพิจารณาด้านการออกแบบวิธีการและท่าทางในการทำงานที่ถูกต้องเพื่อลดการบาดเจ็บทางด้านร่างกายเนื่องจากการบาดเจ็บทางด้านร่างกายทำให้ประสิทธิภาพในการทำงานที่ลดลง นำไปสู่การทำงานที่ผิดพลาด ซึ่งก่อให้เกิดอันตรายต่อผู้ปฏิบัติงานได้และการพิจารณาเรื่องแสงสว่างในพื้นที่ทำงาน (Illumination lighting) เนื่องจากบริเวณที่แสงสว่างไม่เพียงพอสามารถทำให้เกิดอันตรายได้

2.2 ปัจจัยด้านการเลือกใช้เทคโนโลยีที่เหมาะสม (Choice of appropriate technology) เช่น ในกระบวนการผลิตที่มีความเสี่ยงต่อการจุดระเบิด (Explosion) ควรเลือกใช้อุปกรณ์ที่ผ่านการรับรอง (Explosion Proof) เพื่อป้องกันการจุดระเบิด เป็นการลดโอกาสในการเกิดอันตรายได้

2.3 ปัจจัยด้านเงื่อนไขในการซ่อมบำรุงเครื่องจักร (Provisions for Maintenance) เช่น การพิจารณาด้านพื้นที่ในการซ่อมบำรุงเครื่องจักรควรมีความสะดวกในการถอดและเปลี่ยนอุปกรณ์เครื่องจักรซึ่งขนาดของพื้นที่ควรกว้างเพียงพอ เพื่อลดโอกาสในการเกิดอันตรายต่อพนักงานฝ่ายซ่อมบำรุง

2.4 ปัจจัยด้านอันตรายจากอุปกรณ์ของระบบไฟฟ้า (Electrical hazard) อันตรายจากอุปกรณ์ของระบบลม (Pneumatic hazard)และอันตรายจากอุปกรณ์ของระบบไฮโดรลิค(Hydraulic hazard) เนื่องจากการเลือกใช้อุปกรณ์ที่ไม่ได้ผ่านการรับรองจากมาตรฐานสากลสามารถทำให้เกิดอันตรายได้ ดังนั้นควรเลือกใช้อุปกรณ์ที่ผ่านการรับรองจากมาตรฐานสากล เพื่อลดโอกาสในการเกิดอันตรายจากความผิดพลาดของอุปกรณ์ดังกล่าว(Reduce probability of defect, failure and malfunction of equipment)

2.5 ปัจจัยที่มาจากแรงดันคงค้างในระบบ (Remain under pressure) เช่น ในกรณีที่มีการตัดพลังงานทั้งหมดออกจากเครื่องจักรแล้ว(Switch off

main power supply)แต่ยังมีพลังงานคงค้างอยู่ในอุปกรณ์ของเครื่องจักร เช่น พลังงานลมคงค้างอยู่ในกระบอกสูบ (Cylinder) หรืออุปกรณ์ที่ใช้ยกชิ้นงาน (Lifting Device) เป็นต้น สามารถทำให้เกิดอันตรายจากการเคลื่อนที่ของอุปกรณ์เนื่องมาจากพลังงานคงค้างที่มีอยู่ในอุปกรณ์เหล่านั้น ดังนั้นในกรณีที่พนักงานฝ่ายซ่อมบำรุงต้องการที่จะซ่อมบำรุงอุปกรณ์เหล่านั้นจะต้องทำการระบายแรงดันคงค้างออกจากอุปกรณ์เหล่านั้นเสียก่อน (Depressurizedout of devices) เพื่อป้องกันการเกิดอันตราย

3. การออกแบบระบบควบคุมของเครื่องจักร (Design of machinecontrol system)

การออกแบบระบบควบคุมของเครื่องจักรจะต้องเป็นไปตามมาตรฐานความปลอดภัยสากลEN ISO 13849-1 [1]โดยการออกแบบระบบควบคุมของเครื่องจักรที่ถูกต้อง จะต้องสามารถจัดการเหตุการณ์ที่อันตรายหรือลดความเสี่ยงของเหตุการณ์ที่อันตรายได้โดยพฤติการณ์ที่อันตรายของเครื่องจักร(Cause of hazardous machine behavior) มีสาเหตุมาจาก

3.1 ปัจจัยด้านการออกแบบโปรแกรมระบบควบคุมของเครื่องจักรที่ไม่ละเอียด รอบคอบหรือมีการปรับปรุงและแก้ไขโปรแกรมควบคุมเครื่องจักรอย่างไม่เหมาะสม (Unsuitable design or modification of the control logic system)

3.2 ปัจจัยด้านความบกพร่องจากอุปกรณ์ในระบบควบคุมของเครื่องจักร (Defect or failure of components in control system)

3.3 ปัจจัยด้านความบกพร่องหรือความไม่เสถียรจากระบบไฟฟ้าที่จ่ายให้กับระบบควบคุมของเครื่องจักร (Failure or variationin powersupply of control system)

3.4 ปัจจัยด้านการเลือก การออกแบบและการติดตั้งอุปกรณ์ในระบบควบคุมของเครื่องจักรที่ไม่ถูกต้อง ไม่เหมาะสม (Inappropriate selection, design andlocation of control devices)

4. ตัวอย่างผลลัพธ์ที่เกิดจากพฤติการณ์ที่อันตรายของเครื่องจักร (Example of hazardous machine behavior) มีดังนี้

4.1 การเริ่มเดินเครื่องจักรโดยที่ไม่ได้คาดการณ์ไว้ล่วงหน้า (Unexpected start-up)

4.2 การที่ไม่สามารถควบคุมความเร็วของเครื่องจักรได้ (Uncontrolled speed change)

4.3 การไม่สามารถสั่งหยุดการทำงานของเครื่องจักรได้ (Failure to stop moving part)

4.4 การที่อุปกรณ์ความปลอดภัยไม่สามารถใช้งานได้ตามฟังก์ชันที่ออกแบบไว้ (Failure of protection devices)

4.5 การที่เครื่องจักรไม่สามารถรักษาสภาวการณ์ที่ปลอดภัยไว้ได้ ทำให้ชิ้นส่วนของเครื่องจักรมีการเคลื่อนที่หรือชิ้นงานที่จับไว้ตก ล่วงลงมา (Dropping or ejection part of the machine ora workpiece clamped bymachine)

ดังนั้นการออกแบบระบบควบคุมเครื่องจักรที่ถูกต้องตามข้อกำหนดของมาตรฐานความปลอดภัยEN ISO 13849-1 [1] มีข้อแนะนำเบื้องต้น ดังนี้

- การกำหนดเงื่อนไขการใช้งานที่ชัดเจน (Clear operating provisions) เช่น เงื่อนไขการเริ่มเดินเครื่องจักร (Start-upMachine), การหยุดเครื่องจักร (Stop Machine), การรีเซทเครื่องจักรในกรณีที่หยุดการทำงานของเครื่องจักรด้วยอุปกรณ์หยุดฉุกเฉิน (Restart afterinterruption cycle by emergency stop), การนำชิ้นงานที่ค้างอยู่ออกจากเครื่องจักร (Removal of the workpiece), การเดินเครื่องจักรในกรณีที่มีอุปกรณ์บางอย่างบกพร่องอยู่ (Operation machinein case of some elements failure) เป็นต้น
- มีหน้าจอที่แสดงผลความบกพร่องของระบบอย่างชัดเจน (Clear display of the faults)
- มีการออกแบบระบบเพื่อป้องกันการทำงานที่ผิดพลาดของอุปกรณ์ (Interlocking System) เช่น ในกรณีที่เครื่องจักรหยุดและมีอุปกรณ์บางอย่างทำงานที่ผิดพลาด ถ้าหากไม่มีระบบป้องกัน อาจส่งผลให้เครื่องจักรเริ่มเดินโดยที่ไม่ได้คาดการณ์ไว้ (Unexpected start-up) ซึ่งนำไปสู่สภาวการณ์ที่อันตรายต่อผู้ปฏิบัติงานได้ เป็นต้น

2.3.5.2 การลดความเสี่ยงด้วยการติดตั้งอุปกรณ์ความปลอดภัยหรือเพิ่มมาตรการป้องกันให้กับเครื่องจักร (Risk reduction by safeguarding or implementation of complementaryprotective measures)

ในกรณีที่ไม่สามารถจัดการความเสี่ยงหรือลดความเสี่ยงได้จาก 2.3.5.1 ขั้นตอนต่อไปที่ต้องนำมาพิจารณาคือการลดความเสี่ยงด้วยการติดตั้งอุปกรณ์ความปลอดภัยหรือเพิ่มมาตรการป้องกันให้กับเครื่องจักร ตัวอย่างของอุปกรณ์ความปลอดภัย มีดังนี้

1. อุปกรณ์ป้องกันประเภทที่กั้น (Safeguarding)

1.1 ที่กั้นแบบเคลื่อนที่ไม่ได้ (Fixed Guard) คืออุปกรณ์ที่ติดตั้งเพื่อป้องกันการเข้าถึงพื้นที่อันตราย จะติดตั้งด้วยวิธีการยึดด้วยนอต (Nut & Bolt) หรือการเชื่อม (Welding) ทำให้ไม่สามารถเปิดออกหรือเคลื่อนย้ายแสดงดังรูปที่ 2.9

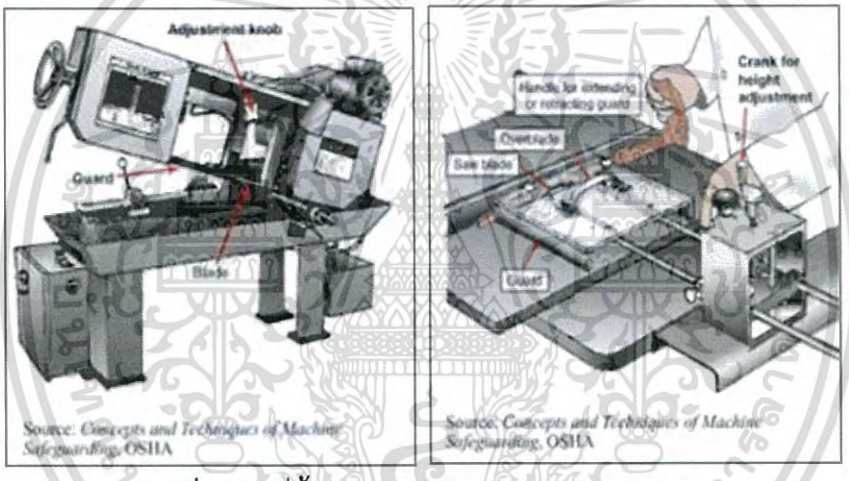
1.2 ที่กั้นแบบเคลื่อนที่ได้ (Movable Guard) คืออุปกรณ์ที่ติดตั้งเพื่อป้องกันการเข้าถึงพื้นที่อันตราย จะมีความแตกต่างจากที่กั้นแบบเคลื่อนที่ไม่ได้ คือจะออกแบบให้พนักงานสามารถเปิดออกเพื่อให้เข้าไปปฏิบัติงานในพื้นที่อันตรายได้ แสดงดังรูปที่ 2.10

1.3 ที่กั้นแบบปรับได้ (Adjustable Guard) คืออุปกรณ์ที่ติดตั้งเพื่อป้องกันการเข้าถึงพื้นที่อันตรายอาจจะเป็นที่กั้นแบบเคลื่อนที่ไม่ได้ (Fixed Guard) หรือที่กั้นแบบเคลื่อนที่ได้ (Movable Guard) มีความแตกต่างคืออาจจะมีรู (slot) หรือมือหมุน (Crank) ไว้สำหรับปรับตำแหน่งของที่กั้น (Guard) เพื่อให้ได้ตำแหน่งที่มีความเหมาะสมตามการใช้งาน แสดงดังรูปที่ 2.11

1.4 ที่กั้นแบบที่เชื่อมต่อกับระบบควบคุม (Interlocking Guard) คืออุปกรณ์ที่ติดตั้งเพื่อป้องกันการเข้าถึงพื้นที่อันตราย จะแตกต่างจากที่กั้น(Guard) ที่ได้กล่าวมาในตอนต้น คือจะต่อสัญญาณจากอุปกรณ์ (Interlock Device) เข้ากับระบบควบคุมของเครื่องจักรและสร้างฟังก์ชันในการตัดการทำงานของเครื่องจักรในบริเวณพื้นที่อันตราย เช่น ในกรณีที่เปิดที่กั้นออก (Opening Guard) ระบบควบคุมจะส่งคำสั่งหยุด (Stop Command) ไปยังชุดขับเคลื่อน (Actuator) เพื่อหยุดการทำงาน ทำให้ผู้ปฏิบัติงานสามารถเข้าไปยังพื้นที่อันตรายได้อย่างปลอดภัย ดังแสดงในรูปที่ 2.12 และรูปที่ 2.13

รูปที่ 2.9 ที่กั้นแบบเคลื่อนที่ไม่ได้ (Fixed Guard)

รูปที่ 2.10 ที่กั้นแบบเคลื่อนที่ได้ (Movable Guard)



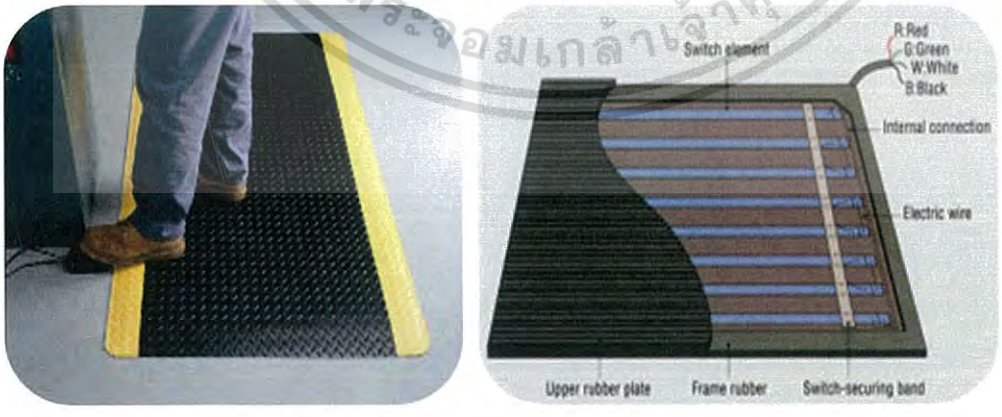
รูปที่ 2.11 ที่กั้นแบบปรับได้ (Adjustable Guard)

รูปที่ 2.12 ที่กั้นแบบที่เชื่อมต่อกับระบบควบคุม (Interlocking Guard)

รูปที่ 2.13 ตัวอย่างอุปกรณ์ Interlock Device ที่นำมาใช้งานร่วมกับ Guard

2. **อุปกรณ์ป้องกันประเภทอื่นๆ (Protective Devices)**

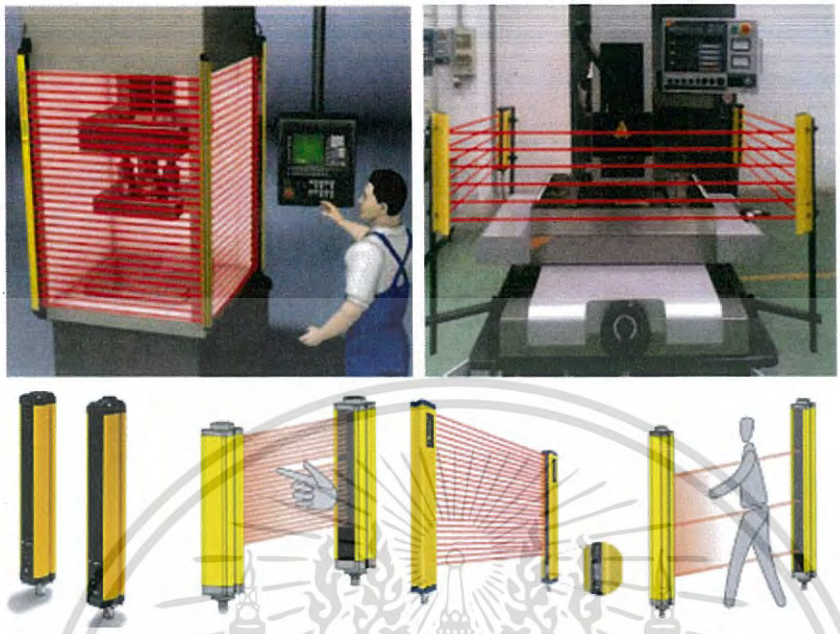
2.1 **อุปกรณ์ป้องกันประเภทเซนเซอร์ (Sensitive Protective Devices)** คืออุปกรณ์ที่ติดตั้งเพื่อป้องกันการเกิดอันตราย โดยจะต่อสัญญาณจากอุปกรณ์ป้องกันเข้ากับระบบควบคุมของเครื่องจักรและสร้างฟังก์ชันในการตัดการทำงานของเครื่องจักร เช่น ในกรณีที่ต้องเข้าไปปฏิบัติงานยังพื้นที่อันตราย อุปกรณ์ป้องกันประเภทเซนเซอร์จะทำหน้าที่ตรวจสอบว่ามีผู้ปฏิบัติงานอยู่ในพื้นที่อันตรายหรือไม่ ถ้าตรวจพบว่ามีผู้ปฏิบัติงานอยู่ในพื้นที่อันตราย จะส่งสัญญาณไปยังระบบควบคุมของเครื่องจักรและสั่งตัดการทำงานของชุดขับเคลื่อน (Actuator) ทันที ตัวอย่างของอุปกรณ์ป้องกันประเภทเซนเซอร์ เช่น อุปกรณ์ป้องกันประเภท Safety Mat และอุปกรณ์ป้องกันประเภท Safety Scanner แสดงดังรูปที่ 2.14 และรูปที่ 2.15 ตามลำดับ



รูปที่ 2.14 ตัวอย่างอุปกรณ์ป้องกันประเภท Safety Mat

รูปที่ 2.15 ตัวอย่างอุปกรณ์ป้องกันประเภท Safety Scanner

2.2 **อุปกรณ์ป้องกันประเภท AOPD(Active Optoelectronic Protective Devices)** คืออุปกรณ์ที่ติดตั้งเพื่อป้องกันการเกิดอันตราย โดยจะต่อสัญญาณจากอุปกรณ์ป้องกันประเภท AOPD เข้ากับระบบควบคุมของเครื่องจักรและสร้างฟังก์ชันในการตัดการทำงานของเครื่องจักร ลักษณะพิเศษของอุปกรณ์ป้องกันประเภท AOPD ที่แตกต่างจากอุปกรณ์ประเภทป้องกันประเภทเซนเซอร์คืออุปกรณ์ป้องกันประเภท AOPD จะประกอบด้วยชุดส่งสัญญาณ (Transmitter) และชุดรับสัญญาณ (Receiver) ซึ่งจะใช้หลักการส่งและการรับแสง เช่น ในกรณีที่ต้องเข้าไปปฏิบัติงานยังพื้นที่อันตราย เมื่อมีคน วัตถุหรือสิ่งของไปอยู่บริเวณด้านหน้าของอุปกรณ์ป้องกันประเภท AOPD จะทำให้ไปขัดขวางการส่งและการรับแสง จะส่งสัญญาณไปยังระบบควบคุมของเครื่องจักรและสั่งตัดการทำงานของชุดขับเคลื่อน (Actuator) ทันที ตัวอย่างของอุปกรณ์ป้องกันประเภท AOPD เช่น อุปกรณ์ป้องกันประเภท Safety Light Curtain และอุปกรณ์ป้องกันประเภท Safety Single Beam แสดงดังรูปที่ 2.16 และรูปที่ 2.17 ตามลำดับ

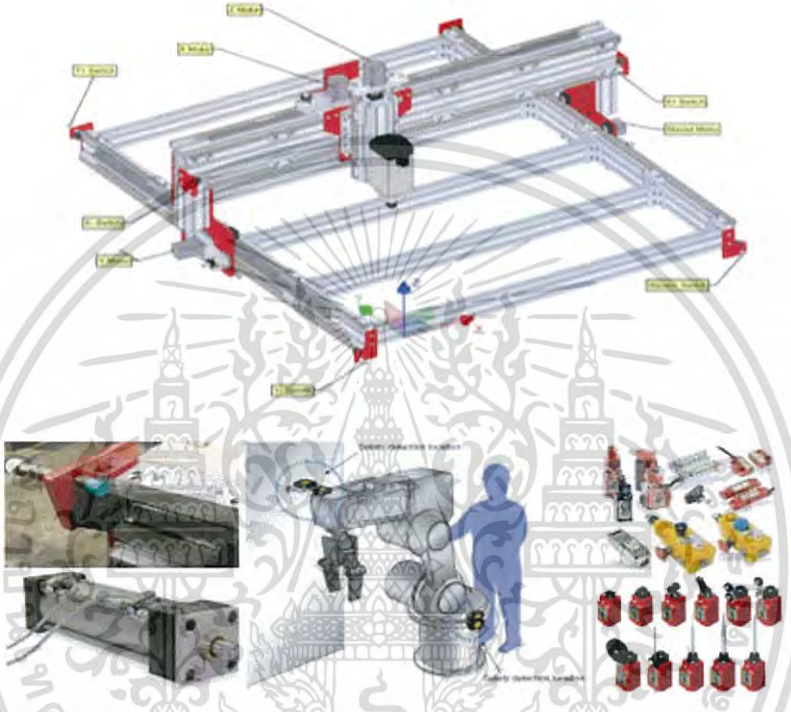


รูปที่ 2.16 ตัวอย่างอุปกรณ์ป้องกันประเภท Safety Light Curtain

รูปที่ 2.17 อุปกรณ์ป้องกันประเภท Safety Single Beam

2.3 **อุปกรณ์ป้องกันประเภทตรวจจับการทำงานเกินกำหนด (Limiting Devices)** คืออุปกรณ์ที่ติดตั้งเพื่อป้องกันการเกิดอันตรายและป้องกันอุปกรณ์ของเครื่องจักรได้รับความเสียหาย จะต่อสัญญาณจากอุปกรณ์ป้องกันประเภท Limiting Devices เข้ากับระบบควบคุมของเครื่องจักร เช่น ในกรณีที่อุปกรณ์ของเครื่องจักรเคลื่อนที่เกินตำแหน่งหรือระยะที่กำหนด อุปกรณ์ป้องกันประเภท Limiting Devices จะทำหน้าที่ตรวจจับการทำงานที่ผิดปกติ ส่งสัญญาณไปยังระบบควบคุมของเครื่องจักรและสั่งตัดการทำงานของชุดขับเคลื่อน (Actuator) ทันที

ตัวอย่างของอุปกรณ์ป้องกันประเภท Limiting Devices เช่น อุปกรณ์ป้องกันประเภท Proximity Switch, Reed Switch(Pneumatic Cylinder) และ Pressure Switch (Pneumatic System)... ฯลฯ แสดงดังรูปที่ 2.18



รูปที่ 2.18 ตัวอย่างอุปกรณ์ป้องกันประเภท Limiting Devices

2.4 **อุปกรณ์ป้องกันประเภทที่ใช้ควบคุมการทำงาน (Safety Control Devices)** คืออุปกรณ์ที่ใช้ในการควบคุมการทำงานของเครื่องจักร จะมีลักษณะพิเศษกว่าอุปกรณ์ควบคุมแบบทั่วๆไปคือจะถูกออกแบบโดยใส่ฟังก์ชันความปลอดภัยไว้ที่อุปกรณ์ด้วย เช่น

2.5 อุปกรณ์ควบคุมการทำงานแบบใช้สองมือ (Two-hand control device) เป็นอุปกรณ์ที่ออกแบบเพื่อให้ใช้สองมือสั่งการทำงานเท่านั้น ถ้าหากใช้เพียงมือเดียวในการสั่งการทำงาน อีกมือหนึ่งที่ว่างอาจจะไปอยู่ในพื้นที่อันตราย ทำให้เกิดอุบัติเหตุได้

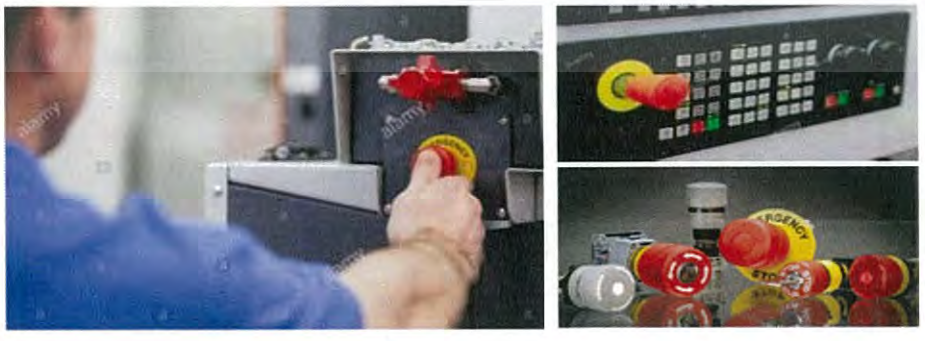
2.6 อุปกรณ์ควบคุมการทำงานแบบกดสวิตช์ค้าง (Hold-to-run control device) เป็นอุปกรณ์ที่ออกแบบเพื่อให้กดสวิตช์ค้างในการสั่งการทำงานเท่านั้น ถ้าหากมีการปล่อยสวิตช์จะหยุดทำงานทันที เพื่อป้องกันการเกิดอันตรายต่อผู้ปฏิบัติงาน

2.7 อุปกรณ์ควบคุมการทำงานแบบกดสวิตช์กด 2 จังหวะ (Enabling control device) เป็นอุปกรณ์ที่ออกแบบเพื่อให้สั่งการได้ 2 จังหวะ ดังนี้ จังหวะที่ 1 คือเมื่อกดสวิตช์ในตำแหน่งที่ 1 จะเป็นการสั่งให้ทำงาน แต่จังหวะที่ 2 คือเมื่อกดสวิตช์ในตำแหน่งที่ 2 จะเป็นการสั่งให้หยุดทำงานและเมื่อปล่อยสวิตช์จะเป็นการสั่งให้หยุดทำงานด้วยเช่นกัน ทำให้สามารถป้องกันการเกิดอันตรายได้ แสดงดังรูปที่ 2.19

Two-hand control device **Hold-to-run control device** **Enabling control device**

รูปที่ 2.19 ตัวอย่างอุปกรณ์ป้องกันประเภทที่ใช้ควบคุมการทำงาน (Safety Control Devices)

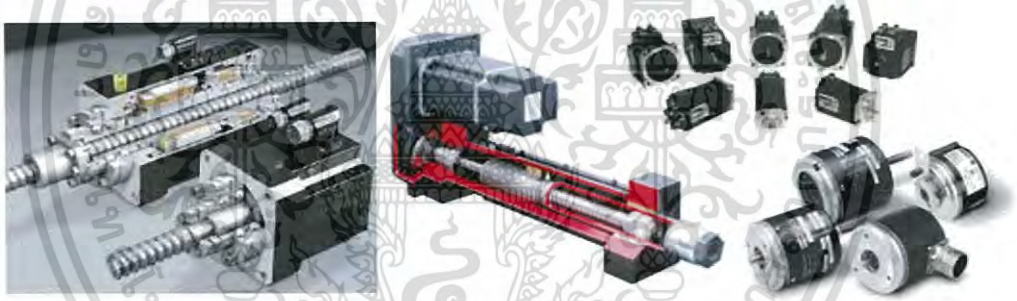
2.8 **อุปกรณ์ป้องกันประเภทหยุดฉุกเฉิน (Emergency Stop Devices)** คืออุปกรณ์ป้องกันที่ออกแบบเพื่อสั่งตัดการทำงานทั้งหมดของเครื่องจักรทันที จะติดตั้งบริเวณรอบๆเครื่องจักร เพื่อใช้สั่งตัดการทำงานในกรณีที่มีเหตุฉุกเฉิน เช่น เพื่อนร่วมงานหรือตัวพนักงานเองอยู่ในสถานการณ์ที่อันตราย สามารถป้องกันไม่ให้เกิดอันตรายได้ หรือในกรณีที่เครื่องจักรทำงานผิดปกติ สามารถป้องกันไม่ให้อุปกรณ์ของเครื่องจักรได้รับความเสียหายตัวอย่างของอุปกรณ์แสดงดังรูปที่ 2.20



รูปที่ 2.20 ตัวอย่างอุปกรณ์ป้องกันประเภทหยุดฉุกเฉิน (Emergency Stop Devices)

2.9 **อุปกรณ์ป้องกันประเภทที่ใช้กลไกควบคุมทางแมคคานิค (Mechanical Restraint Devices)** คืออุปกรณ์ป้องกันที่ออกแบบโดยใช้กลไกแมคคานิคในการควบคุมระยะเคลื่อนที่ไม่ให้เกินกำหนดและป้องกันไม่ให้อุปกรณ์ของเครื่องจักรได้รับความเสียหาย เช่น การกำหนดระยะของสกรูหมุน (Spindle Screw) หรือการติดตั้งชุดค้ำยัน (Strut) เป็นต้น แสดงดังรูปที่ 2.21

2.10 **อุปกรณ์ป้องกันประเภทที่ใช้การป้อนกลับค่าสัญญาณทางไฟฟ้า (Limited Movement Control Devices)** คืออุปกรณ์ป้องกันที่ออกแบบโดยใช้การป้อนกลับของค่าสัญญาณทางไฟฟ้าในการการควบคุมระยะการเคลื่อนที่ไม่ให้เกินกำหนดและป้องกันไม่ให้อุปกรณ์ของเครื่องจักรได้รับความเสียหาย เช่น Servo Motor หรือ AC Motor โดยใช้ชุดป้อนกลับค่าสัญญาณทางไฟฟ้า (Encoder) ในการกำหนดระยะการเคลื่อนที่ แสดงดังรูปที่ 2.21



Servo Motor & AC Motor with Spindle Screw **Servo Motor & Encoder**

รูปที่ 2.21 อุปกรณ์ประเภท Mechanical Restraint Devicesและ Limited Movement Control Devices

3. **มาตรการป้องกันอันตราย (ProtectiveMeasures)**

นอกจากอุปกรณ์ป้องกันประเภทที่กั้น (Safeguarding) และอุปกรณ์ป้องกันประเภทอื่นๆ (Protective Devices) ดังที่ได้กล่าวมาในข้างต้นแล้ว สิ่งที่สำคัญอีกอย่างในการป้องกันอันตราย คือการกำหนดมาตรการป้องกันอันตราย ซึ่งมีรายละเอียด ดังนี้

3.1 **มาตรการสำหรับหลบหลีกอันตรายและช่วยเหลือผู้ที่เผชิญกับสถานการณ์อันตราย** (Measures for the escape and rescue of trapped persons) เช่น หลังจากที่กดสวิตซ์หยุดฉุกเฉิน (Emergency Stop) ในการช่วยเหลือผู้ประสบอุบัติเหตุจะต้องมีวิธีการนำผู้ประสบ

อุบัติเหตุออกออกจากสถานที่อันตรายและจะต้องมีความพร้อมด้านอุปกรณ์ช่วยเหลือ

3.2 มาตรการสำหรับตัดแหล่งพลังงานของเครื่องจักรและกำจัดพลังงานคงค้างในเครื่องจักร (Measures for isolation and energy dissipation) เช่น ในกรณีที่ต้องเข้าไปเปลี่ยนอุปกรณ์เครื่องจักร ซ่อมบำรุงเครื่องจักร ... ฯลฯ จะต้องทำการการตัดแหล่งจ่ายพลังงานออกจากเครื่องจักร (Disconnecting all of power supplies), แยกแหล่งจ่ายพลังงานออกจากเครื่องจักร (LOTO, Lock-out Tag-out) และกำจัดพลังงานคงค้างออกจากเครื่องจักร (Release Energy) เป็นต้น เพื่อป้องกันการเคลื่อนที่ของเครื่องจักรโดยไม่คาดคิด (Unexpected Startup)

3.3 มาตรการสำหรับการเข้าไปยังพื้นที่ของเครื่องจักรอย่างปลอดภัย (Measures for safe access to machinery) เช่น ในกรณีที่เครื่องจักรมีความสูงและต้องขึ้นไปปฏิบัติงานบนเครื่องจักร ควรจะต้องออกแบบเครื่องจักรให้มีอุปกรณ์ป้องกันการตกจากที่สูง, ในกรณีที่เครื่องจักรเป็นสายพานลำเลียง (Conveyor) ควรจะต้องออกแบบเครื่องจักรให้มีบันไดหรือสะพานสำหรับข้ามสายพานลำเลียง ไม่ควรยืนอยู่บนสายพานลำเลียงเพราะอาจจะเกิดอันตรายได้ จากการเคลื่อนที่ของเครื่องจักรโดยไม่คาดคิด (Unexpected Startup) และในบริเวณพื้นที่อันตรายอื่นๆ ควรจะต้องมีการนำมาพิจารณาเช่นเดียวกัน

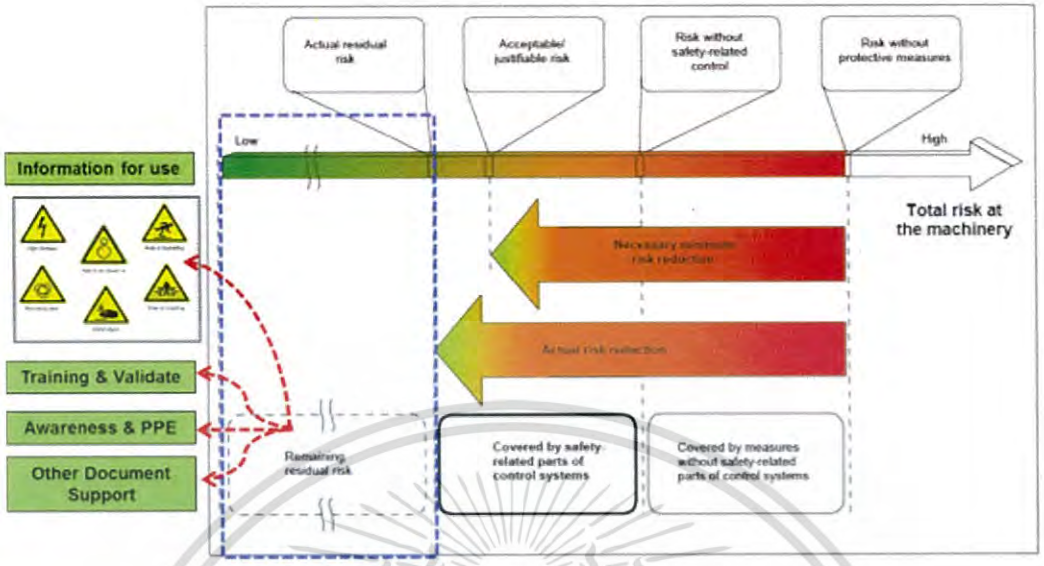
3.4 มาตรการสำหรับจับยกชิ้นงานที่มีน้ำหนักมาก (Measures for safe handling of machines and their heavy component parts) เช่น ในกรณีที่ต้องการยกชิ้นส่วนของเครื่องจักร ชิ้นงานหรือสิ่งของบริเวณเครื่องจักรที่มีน้ำหนักมาก ควรจะต้องมีอุปกรณ์ช่วยอำนวยความสะดวก เช่น รอก (Hoist), ตะขอ (Hook), สลิง(Sling) หรือรถยก (Forklift Trucks) เป็นต้น

มาตรการป้องกันอันตรายที่ได้กล่าวมาในตอนต้นเป็นเพียงข้อแนะนำเบื้องต้นเท่านั้น ในทางปฏิบัติจริงอาจจะมีมาตรการป้องกันอันตรายมากกว่านี้ ขึ้นอยู่กับประเภทของเครื่องจักรที่ใช้งานและปัจจัยแวดล้อมที่เกี่ยวข้อง

2.3.5.3 การลดความเสี่ยงด้วยการให้ข้อมูลใช้งานเครื่องจักร(Information for use)

ในกรณีที่ไม่สามารถจัดการความเสี่ยงหรือลดความเสี่ยงลงได้ด้วยวิธีการของ 2.3.5.1 และ 2.3.5.2 จะทำให้มีความเสี่ยงเหลืออยู่ (Remaining of residual risk) แสดงดังรูปที่ 2.22 ทำให้เกิดอันตรายต่อผู้ปฏิบัติงานได้ ขั้นตอนต่อไปที่จะต้องพิจารณาคือการลดความเสี่ยงด้วยการให้ข้อมูลสำหรับการใช้งานเครื่องจักร มีรายละเอียด ดังนี้

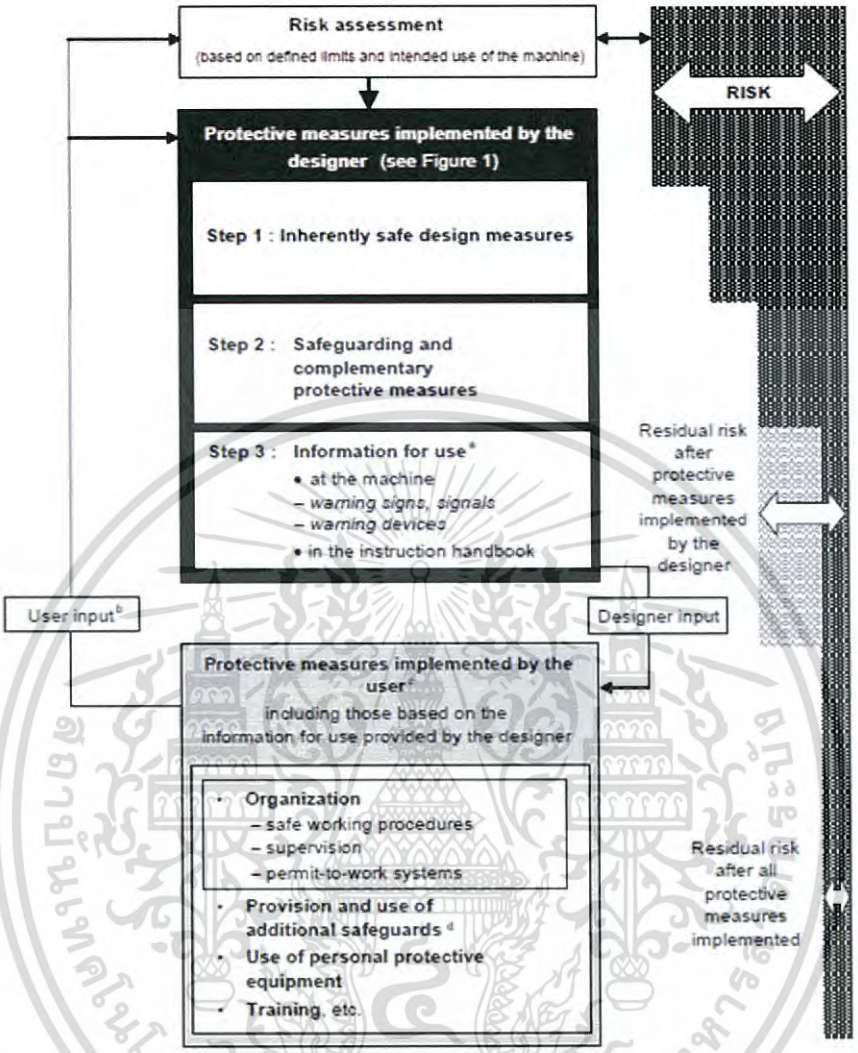
1. **เอกสารสนับสนุนที่เกี่ยวกับการใช้งานเครื่องจักร (Support document concernedwith using machinery) เช่น**เอกสารการใช้งานเครื่องจักร (Machine Operation User Manual)
   - **1.1** เอกสารการแก้ไขปัญหาเฉพาะหน้าของเครื่องจักรในกรณีที่เกิดเหตุขัดข้องระหว่างการใช้งาน (Machine Trouble-Shooting User Manual)
   - **1.2** เอกสารการซ่อมบำรุงเครื่องจักรให้อยู่ในสภาพที่พร้อมใช้งานและปลอดภัย (Machine Preventive Maintenance User Manual)
   - **1.3** เอกสารแสดงรายละเอียดของเครื่องจักร (Machine Specification) เช่น แบบไดอะแกรมของระบบไฟฟ้า, ระบบแมคคานิค, ระบบไฮดรอลิค และระบบลม (Drawing Diagram of Electrical, Mechanical, Hydraulic and Pneumatic System) รวมทั้งขนาดของเครื่องจักร (Machine Sizing), อะไหล่ของเครื่องจักร (Machine Spare Part), การติดตั้งเครื่องจักร (Machine Installation) และการรื้อถอนเครื่องจักร (Machine Dismantling) ... ฯลฯ เป็นต้น
   - **1.4** เอกสารระบุความเสี่ยงที่เหลืออยู่ (Remaining of Residual Risk) เพื่อให้พนักงานมีความระมัดระวัง
   - **1.5** เอกสารการอบรมพนักงานที่เกี่ยวข้อง (Machine Training Document) เนื่องจากพนักงานฝ่ายผลิต ฝ่ายซ่อมบำรุง และฝ่ายประกันคุณภาพ ... ฯลฯ มีวัตถุประสงค์ในการใช้งานเครื่องจักรที่ไม่เหมือนกัน ต้องมีการอบรมการใช้งานให้ถูกต้องเพื่อป้องกันการเกิดอันตราย
2. **มาตรการป้องกันความเสี่ยงที่เหลืออยู่ (Preventive Measures for Remaining of Residual Risk) เช่น**
   - **2.1** การอบรมพนักงานให้มีความรู้ความเข้าใจเกี่ยวกับความเสี่ยงที่เหลืออยู่ (Training & validating machine user for prevent remaining of residual risk) เพื่อให้พนักงานมีความระมัดระวังเพิ่มมากขึ้น
   - **2.2** การแจ้งเตือนอันตราย (Warning) ด้วยสัญลักษณ์ (Sign) รูปภาพ (Pictogram) หรือเสียงเตือน (Siren Alarm) เป็นต้น
   - **2.3** การสวมใส่อุปกรณ์ป้องกันอันตรายส่วนบุคคล PPE (Personal Protective Equipment)
   - **2.4** การกำหนดมาตรฐานการทำงานให้กับพนักงานอย่างเป็นลำดับขั้นตอน (Standard Working Procedure and Working Sequential) เพื่อป้องกันการทำงานที่ผิดพลาด



รูปที่ 2.22 ความเสี่ยงที่เหลืออยู่ (Remaining of residual risk)

วัตถุประสงค์หลักของการประเมินความเสี่ยงและลดความเสี่ยง เพื่อที่จะจัดการการจัดการกับความเสี่ยงหรือลดความเสี่ยงลงให้มากที่สุดเท่าที่สามารถทำได้ ความต้องการทางทฤษฎีคือจะต้องทำให้ไม่มีความเสี่ยง (Zero Risk) แต่ในทางปฏิบัติไม่สามารถทำได้ เนื่องมาจากอุปสรรคและข้อจำกัดต่างๆของเครื่องจักรทำให้มีความเสี่ยงเหลืออยู่ (Remaining of Residual Risk) ผู้ใช้งานเครื่องจักรจะต้องรู้และทราบถึงความเสี่ยงที่เหลืออยู่เพื่อให้เกิดการระมัดระวังอันตรายที่จะเกิดขึ้น

ดังนั้นเพื่อให้ได้ประสิทธิผลสูงสุดในการลดความเสี่ยง ผู้ออกแบบเครื่องจักร (Machine Designer) และผู้ใช้งานเครื่องจักร (Machine User) ต้องทำงานร่วมกันในขั้นตอนของการประเมินความเสี่ยงและลดความเสี่ยง เพื่อที่จะลดความเสี่ยงลงให้มากที่สุด แสดงดังรูปที่ 2.23



รูปที่ 2.23 ขั้นตอนการทำงานร่วมกันระหว่างผู้ออกแบบเครื่องจักรและผู้ใช้งานเครื่องจักร

2.4 มาตรฐาน EN 954-1

จากที่ได้กล่าวมาในหัวข้อ 2.2.3.2 มาตรฐาน EN 954-1 [3] ได้ประกาศยกเลิกการใช้ในช่วงปลายปี พ.ศ.2554 และบังคับใช้มาตรฐาน EN ISO 13849-1[1] แทน ผู้ออกแบบเครื่องจักร (Machine Designer) ผู้ผลิตเครื่องจักร (Machine Manufacturer) และผู้ใช้งานเครื่องจักร (Machine User) จะต้องเข้าใจหลักการของมาตรฐาน EN 954-1[3] เพื่อนำไปสู่การใช้งานของมาตรฐาน EN ISO 13849-1[1] ซึ่งจะอธิบายรายละเอียดในหัวข้อถัดไป

มาตรฐาน EN 954-1[3] จะเป็นวิธีเชิงกำหนด (Deterministic Approach) จะประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง (Risk Graph) และออกแบบระบบควบคุมความเสี่ยง (SRP/CS) ด้วยการกำหนดโครงสร้างของระบบ (Designated Architecture) โดยแบ่งออกเป็น 5 แบบ ดังนี้ โครงสร้างแบบ Category B, Category 1, Category 2, Category 3 และ Category 4 ซึ่งโครงสร้างของระบบในแต่ละ

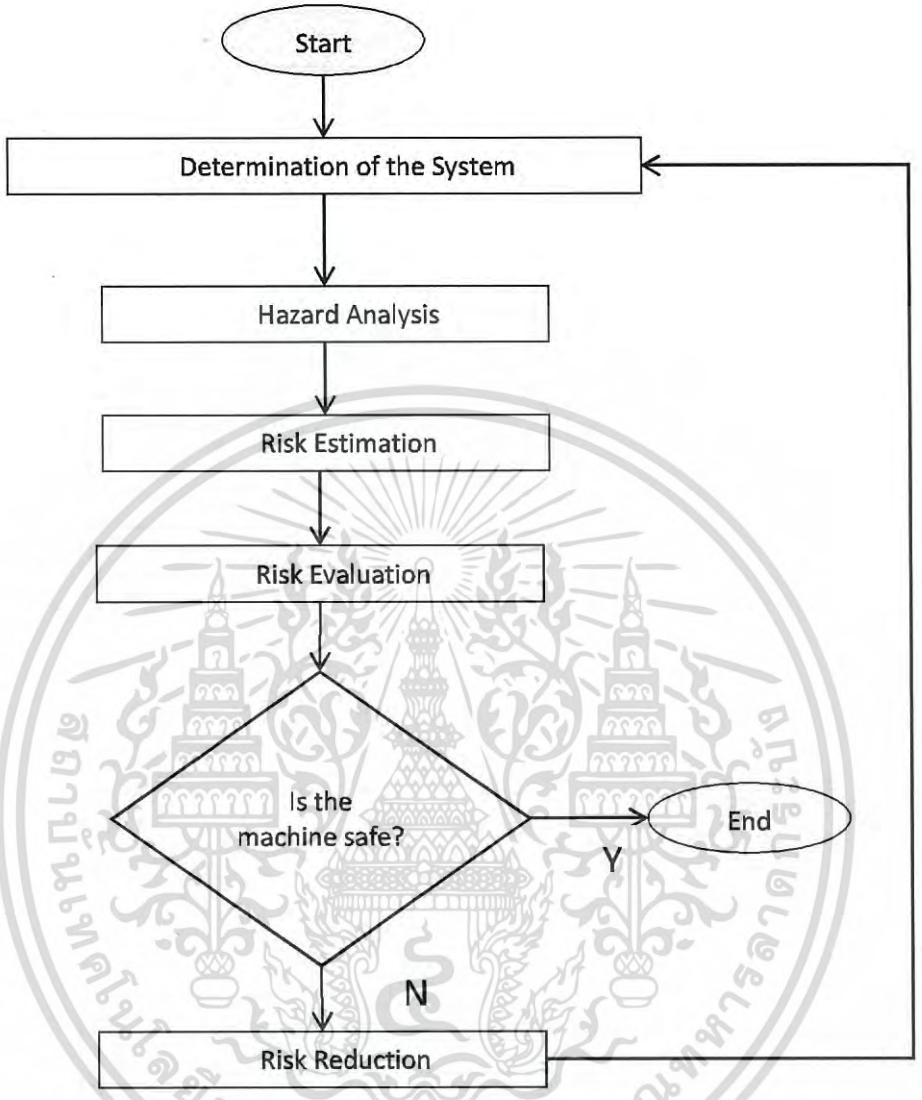
แบบจะให้ความน่าเชื่อถือของระบบ (Reliability of system) ที่แต่ต่างกัน โดยมาตรฐานนี้จะมุ่งเน้นการออกแบบด้านฮาร์ดแวร์ (Hardware design) เช่น ระบบอีเลคโทรแมคคานิค(Electromechanical System) สามารถใช้การออกแบบระบบไฟฟ้า (Electrical system) ระบบลม (Pneumatic system) และระบบไฮดรอลิค (Hydraulic system)ซึ่งวิธีการประเมินความเสี่ยงและลดความเสี่ยง (Risk Assessment and Risk Reduction) ตามข้อกำหนดของมาตรฐาน EN 954-1[3] คือ

2.4.1 กระบวนการประเมินความเสี่ยงและลดความเสี่ยงเพื่อให้บรรลุเป้าหมายความปลอดภัย (The iterative process for risk assessment and risk reduction to achieve safety level)

จากรูปที่ 2.24 แสดงกระบวนการประเมินความเสี่ยงและลดความเสี่ยงโดยพิจารณาขั้นตอนดังนี้

- การพิจารณาระบบของเครื่องจักร (Determination of the system)
- การระบุจุดที่อันตราย (Hazard Analysis)
- การประเมินความเสี่ยง (Risk Estimation)
- พิจารณาความจำเป็นในการลดความเสี่ยง(Risk Evaluation)
- การลดความเสี่ยง (Risk Reduction)

มาตรฐาน EN 954-1 [3] จะมุ่งเน้นเรื่องการลดความเสี่ยงด้วยการเลือกอุปกรณ์ป้องกันและออกแบบระบบควบคุมความเสี่ยงด้วยการกำหนดโครงสร้างของระบบแบบ Category เพื่อบรรลุเป้าหมายความปลอดภัย



รูปที่ 2.24 กระบวนการประเมินความเสี่ยงและการลดความเสี่ยงตามมาตรฐาน EN 954-1[3]
(The iterative processfor risk assessment and risk reduction to achieve safety level)

2.4.2 การพิจารณาระบบของเครื่องจักร (Determination of the system)

ดังที่ได้กล่าวมาในหัวข้อ 2.3 และหัวข้อ 2.3.1 ตามข้อกำหนดของมาตรฐาน EN ISO 12100 [1]

2.4.3 การระบุจุดที่อันตราย (Hazard Analysis)

ดังที่ได้กล่าวมาในหัวข้อ 2.3 และหัวข้อ 2.3.2 ตามข้อกำหนดของมาตรฐาน EN ISO 12100 [1] ตัวอย่างของการระบุจุดที่อันตรายแสดงดังภาคผนวก ง

2.4.4 การประเมินความเสี่ยง (Risk Estimation)

ตามข้อกำหนดของมาตรฐาน EN ISO 12100 [1] หลังจากที่ได้พิจารณาระบบของเครื่องจักรและระบุจุดที่ทำให้เกิดอันตราย จะทำการประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง (Risk graph) ดังแสดงในรูปที่ 2.25 ด้วยพารามิเตอร์ ดังนี้

2.4.4.1 ความรุนแรงของการเกิดอันตราย (S)

- S1 หมายถึงการบาดเจ็บเพียงเล็กน้อย เช่น การตัด การบาด การเฉือน ไม่ถึงขั้นสูญเสียอวัยวะ
- S2 หมายถึงการบาดเจ็บขั้นรุนแรง เช่น การสูญเสียอวัยวะจากการทำงาน หรือร้ายแรงที่สุดถึงขั้นเสียชีวิตจากการทำงาน เป็นต้น

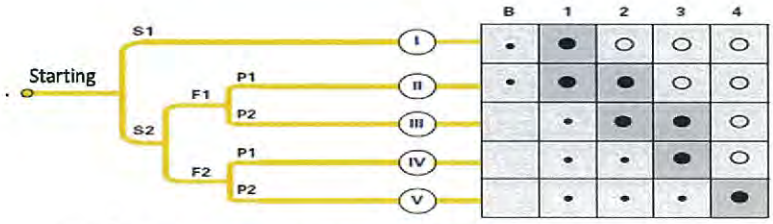
2.4.4.2 ความถี่ที่เข้าไปอยู่ในสถานที่อันตราย (F)

- F1 หมายถึงความถี่ที่เข้าไปอยู่ในสถานที่อันตรายน้อย เช่น เดือนละครั้ง (Once a month), 2 สัปดาห์ต่อครั้ง (Twice a week), สัปดาห์ละครั้ง (Once a week), วันละครั้ง (Once a day)
- F2 หมายถึงความถี่ที่เข้าไปอยู่ในสถานที่อันตรายมาก เช่น จำนวนมากกว่า 1 ครั้งต่อวัน (Many time aday) เป็นต้น

2.4.4.3 โอกาสในการหลีกเลี่ยงอันตราย (P)

- P1 หมายถึงพนักงานสามารถที่จะหลบหลีกอันตรายได้ เช่น พนักงานที่มีประสบการณ์ ผ่านการอบรมเป็นอย่างดี หรือเครื่องจักรเคลื่อนที่ด้วยความเร็วช้า มีพื้นที่กว้างเอื้อต่อการหลบหลีกอันตราย เป็นต้น
- P2 หมายถึงพนักงานไม่สามารถที่จะหลบหลีกอันตรายได้ เช่นพนักงานที่ไม่มีประสบการณ์ ไม่ผ่านการอบรม หรือเครื่องจักรเคลื่อนที่ด้วยความเร็วสูง มีพื้นที่แคบไม่เอื้อต่อการหลบหลีกอันตราย เป็นต้น คำจำกัดความของพารามิเตอร์ในการประเมินความเสี่ยงแสดงดังตารางที่ 2.3

การประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยงจะนำไปสู่การออกแบบระบบควบคุมความเสี่ยงตามโครงสร้างแบบ Category ต่างๆ ขึ้นอยู่กับว่าผลของการประเมินความเสี่ยงอยู่ในระดับที่สูงหรือระดับที่ต่ำ ยกตัวอย่างเช่น ถ้าผลของการประเมินคือ S2,F2 และ P2 หมายความคือความเสี่ยงอยู่ในระดับที่สูงสุด (The highest risk) ซึ่งนำไปสู่การออกแบบระบบควบคุมความเสี่ยงตามโครงสร้างแบบ Category 4 ซึ่งมีความน่าเชื่อถือสูงสุด (The highest reliability) เพื่อบรรลุเป้าหมายความปลอดภัย เป็นต้น



รูปที่ 2.25 การประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง (Risk graph)

ตารางที่ 2.3 คำจำกัดความของพารามิเตอร์ที่ใช้ในการประเมินความเสี่ยง EN 954-1 [3]

Legend (สัญลักษณ์)	Definition (คำจำกัดความ)
○	Starting point for risk assessment
S	Accident severity: S1 = reversible (slight) injury (i.e. small cuts, burns, light abrasions, etc.) S2 = irreversible (serious) injury or death (i.e. permanent disability, loss of limbs, breath harms, etc.)
F	Presence in the dangerous zone: F1 = from rare to quite frequent (i.e. weekly or more, to once a day) F2 = from often to continuous (i.e. from many times a day to continuous)
P	Chance to avoid the accident or to reduce its effect significantly: P1 = possible under certain conditions (i.e. possibility of the worker to realize the imminent danger) P2 = almost impossible (i.e. impossibility of the worker to realize the imminent danger)
I-V	Estimated risk level
B, 1-4	Safety categories of control systems
◐	Preferential categories foreseen for this risk level
○	Choice of a higher category
◐	Choice of a lower category

2.4.5 การตัดสินใจที่จะลดความเสี่ยง จำเป็นต้องลดความเสี่ยงหรือไม่ (Risk Evaluation)

ดังที่ได้กล่าวมาในหัวข้อ 2.3 และหัวข้อ 2.3.4 ตามข้อกำหนดของมาตรฐาน EN ISO 12100 [1]

2.4.6 การลดความเสี่ยง (Risk Reduction)

ดังที่ได้กล่าวมาในหัวข้อ 2.3 และหัวข้อ 2.3.5 ตามข้อกำหนดของมาตรฐาน EN ISO 12100 [1] ถ้าหากต้องการลดความเสี่ยงด้วยวิธีการดังหัวข้อ 2.3.5.2 "การลดความเสี่ยงด้วยการติดตั้งอุปกรณ์ความปลอดภัยหรือเพิ่มมาตรการป้องกันให้กับเครื่องจักร" จะนำมาสู่การประยุกต์ใช้งานมาตรฐาน EN 954-1 [3] และ EN ISO 13849-1 [1]

จากผลของการประเมินความเสี่ยงในหัวข้อ 2.4.4 ด้วยวิธีกราฟความเสี่ยง (Risk graph) จะทำให้สามารถระบุ Category สำหรับออกแบบโครงสร้างของระบบควบคุมความเสี่ยงได้ ซึ่งโครงสร้างของแต่ละ Category มีลักษณะที่แตกต่างกัน ดังนี้

2.4.6.1 Category B

อุปกรณ์ที่เลือกมาใช้ในการออกแบบระบบควบคุมความเสี่ยง จะต้องเป็นอุปกรณ์ที่ผ่านการทดสอบตามข้อกำหนดความปลอดภัยพื้นฐานทั่วๆไป (Basic safety

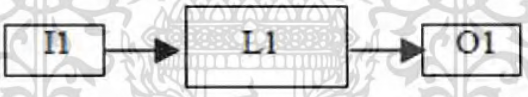
requirement) สามารถใช้งานได้ตามที่ออกแบบไว้ ลักษณะโครงสร้างแบบ Category B แสดงดังรูปที่ 2.26

ข้อเสียคือการออกแบบด้วยโครงสร้างแบบ Category B ความปลอดภัยของระบบจะขึ้นอยู่กับความน่าเชื่อถือของอุปกรณ์เพียงอย่างเดียวเท่านั้น (Reliability of equipment) ในกรณีที่อุปกรณ์ล้มเหลว (Failure of equipment) จะนำไปสู่การเกิดเหตุการณ์ที่อันตรายได้

2.4.6.2 Category 1

อุปกรณ์ที่เลือกมาใช้ในการออกแบบระบบควบคุมความเสี่ยง จะต้องเป็นอุปกรณ์ที่ผ่านการทดสอบตามข้อกำหนดความปลอดภัยพื้นฐานทั่วๆไป (Basic safety requirement) และผ่านการทดสอบในระดับที่สูงกว่า Category B(Well-tried component & Well-tried safety principles) ทำให้อุปกรณ์มีความน่าเชื่อถือสูงกว่า Category B ลักษณะโครงสร้างแบบ Category 1 แสดงดังรูปที่ 2.26

ข้อเสียคือการออกแบบด้วยโครงสร้างแบบ Category 1 ความปลอดภัยของระบบจะขึ้นอยู่กับความน่าเชื่อถือของอุปกรณ์เพียงอย่างเดียวเท่านั้น (Reliability of equipment) ในกรณีที่อุปกรณ์ล้มเหลว (Failure of equipment) จะนำไปสู่การเกิดเหตุการณ์ที่อันตรายได้

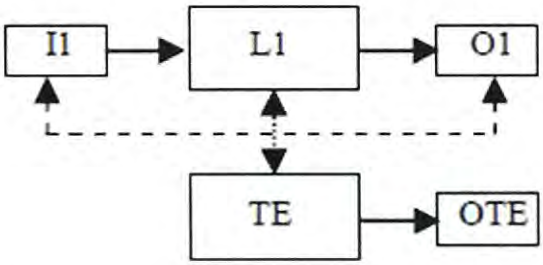


รูปที่ 2.26 การออกแบบระบบควบคุมความเสี่ยงด้วยโครงสร้างแบบ Category B และ Category 1

2.4.6.3 Category 2

ข้อกำหนดคืออุปกรณ์ที่เลือกมาใช้ในการออกแบบระบบควบคุมความเสี่ยงจะต้องเป็นไปตามข้อกำหนดของ CategoryB และ Category 1 แต่ที่ดีกว่าคือจะต้องมีการตรวจสอบฟังก์ชันความปลอดภัยว่ามีความผิดปกติหรือไม่ด้วยอุปกรณ์ TE (Testing Equipment) ทำให้ระบบมีความน่าเชื่อถือสูงกว่า Category B และ Category 1 ลักษณะโครงสร้างแบบ Category 2 แสดงดังรูปที่ 2.27

ข้อเสียคือการออกแบบด้วยโครงสร้างแบบ Category 2 ในกรณีที่อุปกรณ์ล้มเหลวระหว่างช่วงเวลาในการตรวจสอบ (Checking interval) จะนำไปสู่การเกิดเหตุการณ์ที่อันตรายได้

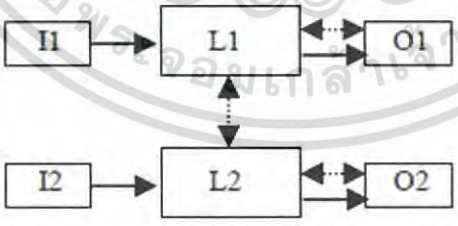


รูปที่ 2.27 การออกแบบระบบควบคุมความเสี่ยงด้วยโครงสร้างแบบ Category 2

2.4.6.4 Category 3

ข้อกำหนดคืออุปกรณ์ที่เลือกมาใช้ในการออกแบบระบบควบคุมความเสี่ยง จะต้องเป็นไปตามข้อกำหนดของ CategoryB และ Category 1 แต่ที่ดีกว่าคือโครงสร้างของระบบจะเป็นแบบคู่ขนาน (RedundantSystem) ในส่วนของชุด I (Input device) และ O (Output device) ทำให้สามารถตรวจจับความบกพร่องของอุปกรณ์ (Detected fault) ด้วยระบบมอนิเตอร์สัญญาณ (Cross Check Motoring) ดังนั้นในกรณีที่อุปกรณ์บกพร่องจะไม่ทำให้เกิดอันตราย ทำให้ระบบมีความน่าเชื่อถือสูงกว่า Category 2 ลักษณะโครงสร้างแบบ Category 3 แสดงดังรูปที่ 2.28

ข้อเสียคือการออกแบบด้วยโครงสร้างแบบ Category 3 ในกรณีที่ไม่สามารถตรวจจับความบกพร่องของอุปกรณ์ได้ (Undetected fault) เนื่องจากอุปกรณ์ชุด L (Logic device) ที่ทำหน้าที่ตรวจจับความบกพร่องของอุปกรณ์ล้มเหลว จะนำไปสู่การเกิดเหตุการณ์ที่อันตรายได้

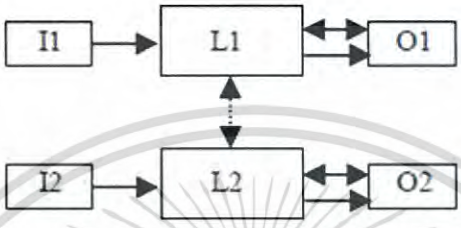


รูปที่ 2.28 การออกแบบระบบควบคุมความเสี่ยงด้วยโครงสร้างแบบ Category 3

2.4.6.5 Category 4

ข้อกำหนดคืออุปกรณ์ที่เลือกมาใช้ในการออกแบบระบบควบคุมความเสี่ยง จะต้องเป็นไปตามข้อกำหนดของ CategoryB และ Category 1 แต่ที่ดีกว่าคือโครงสร้างของระบบจะเป็นแบบคู่ขนานเต็มรูปแบบ (Fully RedundantSystem) ในส่วนของชุด I (Input device), L (Logic device) และ O (Output device) ทำให้สามารถตรวจจับ

ความบกพร่องของอุปกรณ์ได้ทั้งหมด (Detected fault& Undetected fault) ด้วยระบบมอนิเตอร์สัญญาณ (Cross Check Motoring) ดังนั้นในกรณีที่อุปกรณ์บกพร่องจะไม่ทำให้เกิดอันตราย ทำให้ระบบมีความน่าเชื่อถือสูงกว่า Category 3 ลักษณะโครงสร้างแบบ Category 4 แสดงดังรูปที่ 2.29 การออกแบบด้วยโครงสร้างแบบ Category 4 จะทำให้ระบบมีความน่าเชื่อถือสูงสุด (The highest reliability)

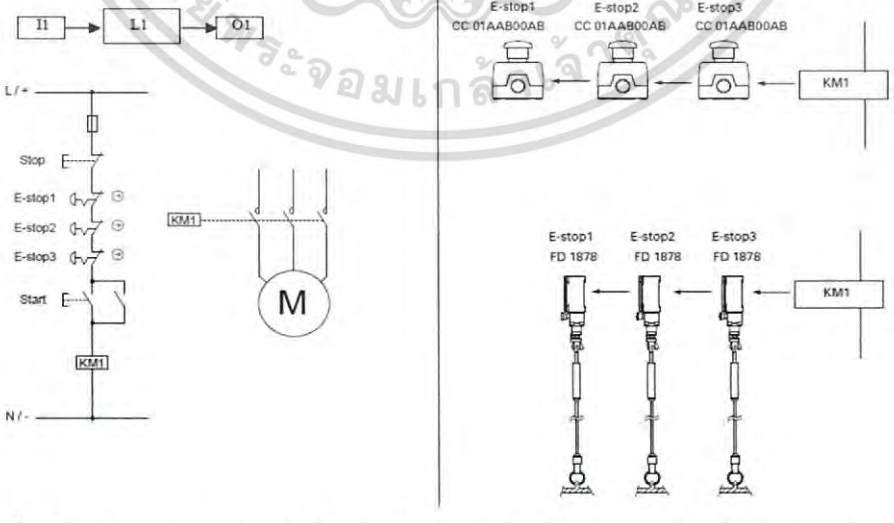


รูปที่ 2.29 การออกแบบระบบควบคุมความเสี่ยงด้วยโครงสร้างแบบ Category 4

2.4.7 ตัวอย่างการประยุกต์ใช้มาตรฐาน EN 954-1 กับระบบควบคุมเครื่องจักร

2.4.7.1 Category B & 1

ตัวอย่างการออกแบบระบบหยุดฉุกเฉิน (Emergency Stop System) ด้วยโครงสร้างแบบ Category B และ Category 1 แสดงดังรูปที่ 2.30 ความน่าเชื่อถือของระบบจะขึ้นอยู่กับอุปกรณ์เพียงอย่างเดียวเท่านั้น อุปกรณ์อินพุท (E-Stop) และอุปกรณ์เอาท์พุท (KM1) ในกรณีที่อุปกรณ์ล้มเหลว (Failure of equipment) จะทำให้ไม่สามารถตัดการทำงานของมอเตอร์ นำไปสู่การเกิดเหตุการณ์ที่อันตรายได้

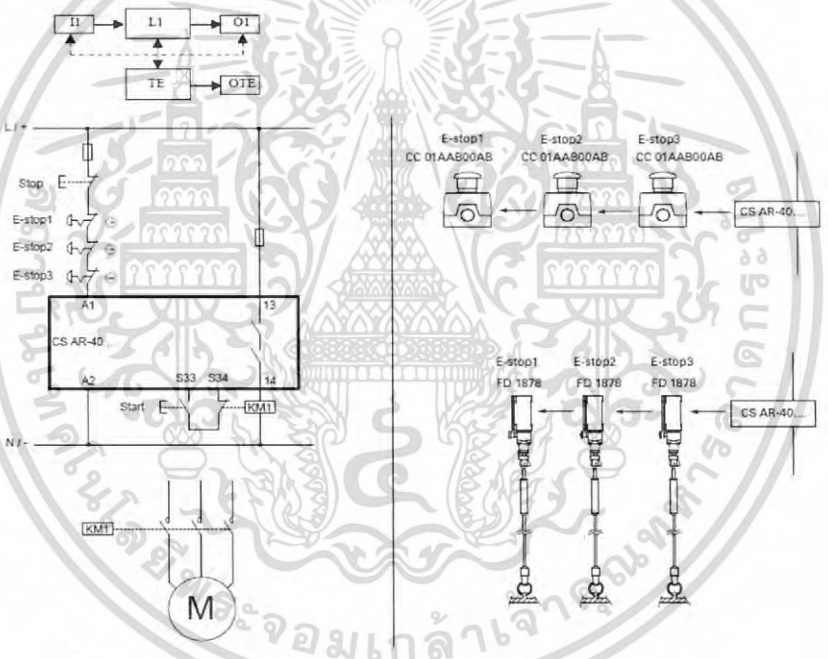


รูปที่ 2.30 ตัวอย่างการออกแบบระบบด้วยโครงสร้าง Category B และ Category 1

2.4.7.2 Category 2

ตัวอย่างการออกแบบระบบหยุดฉุกเฉิน (Emergency Stop System) ด้วยโครงสร้างแบบ Category 2 แสดงดังรูปที่ 2.31 จะมีการปรับปรุงระบบด้วยการติดตั้งอุปกรณ์ควบคุม (AR-40) ทำหน้านี้ในการตรวจสอบความผิดปกติของอุปกรณ์ด้วยฟังก์ชัน TE (Testing Equipment) ความน่าเชื่อถือของระบบสูงกว่า Category B และ Category 1 ในกรณีที่อุปกรณ์ล้มเหลว (Failure of equipment) จะตรวจพบความผิดปกติก่อนและแก้ไขได้ทัน

ข้อเสียคือถ้าหากอุปกรณ์ล้มเหลวระหว่างช่วงเวลาในการทดสอบ (Checking interval) จะทำให้ไม่สามารถตัดการทำงานของมอเตอร์ นำไปสู่การเกิดเหตุการณ์ที่อันตรายได้



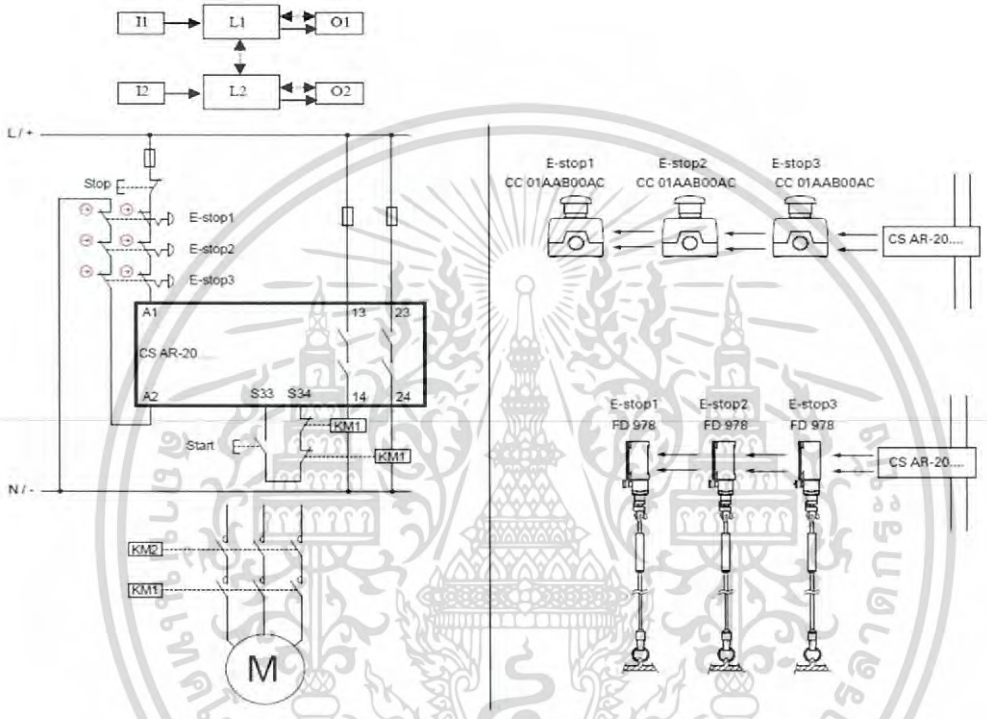
รูปที่ 2.31 ตัวอย่างการออกแบบระบบด้วยโครงสร้าง Category 2

2.4.7.3 Category 3

ตัวอย่างการออกแบบระบบหยุดฉุกเฉิน (Emergency Stop System) ด้วยโครงสร้างแบบ Category 3 แสดงดังรูปที่ 2.32 นอกจากจะมีการปรับปรุงระบบด้วยการติดตั้งอุปกรณ์ควบคุม (AR-40) ทำหน้านี้ในการตรวจสอบความผิดปกติของอุปกรณ์แล้ว โครงสร้างของระบบจะเป็นแบบคู่ขนาน (RedundantSystem) ในส่วนของชุด I (Input device) และ O (Output device) เช่น อุปกรณ์อินพุท (E-Stop) แบบ 2 Channel และอุปกรณ์เอาท์พุท (KM) 2 ชุด ความน่าเชื่อถือของระบบสูงกว่า Category 2 ในกรณีที่

อุปกรณ์ล้มเหลว ระบบควบคุมจะตรวจจับความบกพร่องของอุปกรณ์ได้ (Detected fault) จะไม่ทำให้เกิดอันตราย

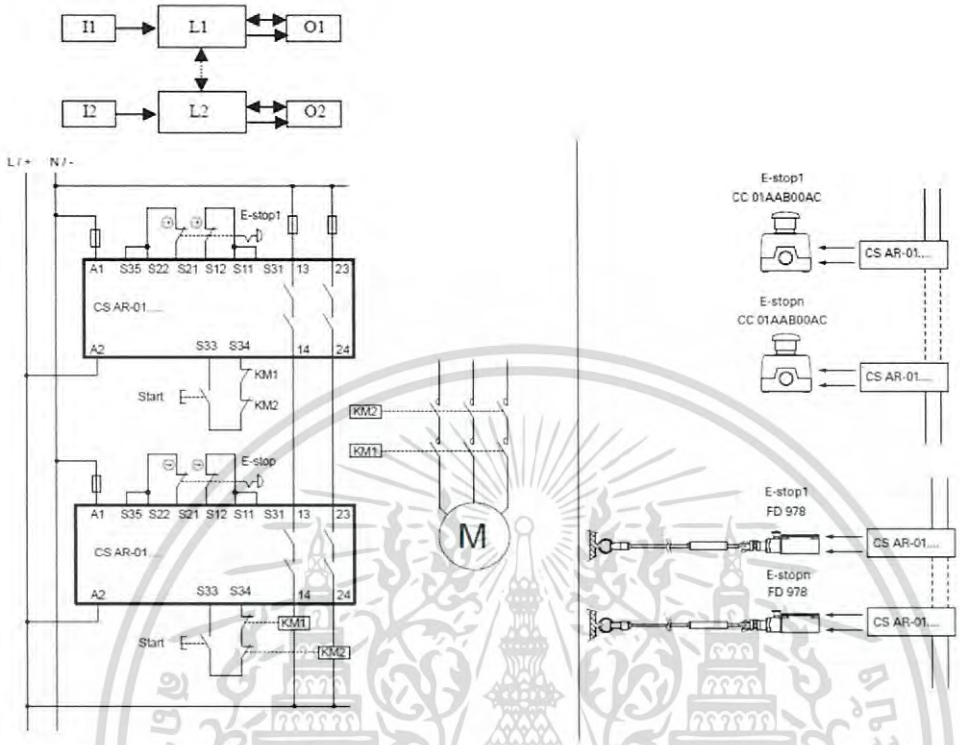
ข้อเสียคือในกรณีที่ไม่สามารถตรวจจับความบกพร่องของอุปกรณ์ได้ (Undetected fault) เนื่องจากอุปกรณ์ชุด L (Logic device) ที่ทำหน้าที่ตรวจจับความบกพร่องของอุปกรณ์ล้มเหลว จะนำไปสู่การเกิดเหตุการณ์ที่อันตรายได้



รูปที่ 2.32 ตัวอย่างการออกแบบระบบด้วยโครงสร้าง Category 3

2.4.7.4 Category 4

ตัวอย่างการออกแบบระบบหยุดฉุกเฉิน (Emergency Stop System) ด้วยโครงสร้างแบบ Category 4 แสดงดังรูปที่ 2.33 โครงสร้างของระบบจะเป็นแบบคู่ขนานเต็มรูปแบบ (Fully RedundantSystem) ในส่วนของชุด I (Input device), ชุด L (LogicDevice) และ O (Output device) เช่น อุปกรณ์อินพุท (E-Stop) แบบ 2 Channel, อุปกรณ์ควบคุม (AR-40) 2 ชุด และอุปกรณ์เอาท์พุท (KM) 2 ชุด ความน่าเชื่อถือของระบบสูงกว่า Category 3 ในกรณีที่อุปกรณ์ล้มเหลว ระบบควบคุมจะตรวจจับความบกพร่องของอุปกรณ์ทั้งหมดได้ (Detected fault& Undetected fault) จะไม่ทำให้เกิดอันตราย



รูปที่ 2.33 ตัวอย่างการออกแบบระบบด้วยโครงสร้าง Category 4

จากที่ได้กล่าวมาในตอนต้นเกี่ยวกับการออกแบบระบบด้วยโครงสร้างในแต่ละ Category สามารถสรุปได้ดังนี้

- Category B และ Category 1 ความน่าเชื่อถือของระบบจะขึ้นอยู่กับความน่าเชื่อถือของอุปกรณ์เพียงอย่างเดียวเท่านั้น ซึ่งความน่าเชื่อถือของโครงสร้างแบบ Category 1 จะสูงกว่า Category Bเนื่องจากมีการทดสอบอุปกรณ์ด้วยมาตรฐานที่สูงกว่า
- Category 2, Category 3 และ Category 4 ความน่าเชื่อถือของระบบจะไม่ได้ขึ้นอยู่กับความน่าเชื่อถือของอุปกรณ์เพียงอย่างเดียวเท่านั้น แต่จะขึ้นอยู่กับลักษณะโครงสร้างของการออกแบบระบบด้วย ซึ่งโครงสร้างแบบ Category 4 จะให้ความน่าเชื่อถือของระบบสูงที่สุด

จากลักษณะของโครงสร้างระบบทั้ง 5 แบบ โครงสร้างแบบ Category B จะให้ความน่าเชื่อถือของระบบต่ำที่สุดทำให้ระบบมีความปลอดภัยต่ำที่สุด(Lowest Reliability, Highest Risk) และโครงสร้างแบบ Category 4 จะให้ความน่าเชื่อถือของระบบจะสูงที่สุดทำให้ระบบมีความปลอดภัยสูงที่สุด (Highest Reliability, Lowest Risk) ดังนั้นการออกแบบระบบควบคุมความเสี่ยงควรเลือกโครงสร้างให้เหมาะสมและเพียงพอที่จะจัดการความเสี่ยง เพื่อให้เกิดความปลอดภัยต่อผู้ใช้งานเครื่องจักร คำอธิบายเพิ่มเติมเกี่ยวกับ Category แสดงดังภาคผนวก ง

2.5 มาตรฐาน EN ISO 13849-1

จากที่ได้กล่าวมาในหัวข้อ 2.2.3.2 ในช่วงปลายปี พ.ศ. 2554 ได้บังคับใช้มาตรฐาน EN ISO 13849-1[1] แทนมาตรฐาน EN 954-1 [3] อย่างสมบูรณ์ ข้อแตกต่างของมาตรฐานดังกล่าว มีดังนี้

มาตรฐาน EN 954-1 [3] เป็นวิธีการในเชิงกำหนด (Deterministic Approach) จะใช้ Category เป็นตัวแทนในการแสดงความน่าเชื่อถือของระบบ

EN ISO 13849-1 [1] เป็นวิธีการเชิงกำหนดผสมกับวิธีการเชิงสถิติ (Deterministic & Statistic Approach) จะใช้ PL (Performance level) เป็นตัวแทนในการแสดงค่าระดับความปลอดภัยและใช้ค่า PFHDavg(Average probability of a dangerous failure per hour (1/h)) เป็นตัวแทนแสดงความน่าเชื่อถือของระบบ

โดยที่ค่า PL สามารถพิจารณาได้จากพารามิเตอร์Category(Designated architecture from EN 954-1 [3]), MTTFd (Mean time to dangerous failure), DC(Diagnostic coverage) และ CCF(Common cause failure)หลังจากที่รู้ค่าระดับความปลอดภัยของระบบ PL(Performance level) จะทำให้รู้โอกาสในการล้มเหลวของระบบ PFHDavg (Average probability of a dangerous failure per hour (1/h)) ดังแสดงในภาคผนวก ง ซึ่งมาตรฐาน EN ISO 13849-1 [1] จะแสดงความน่าเชื่อถือของระบบในรูปแบบค่าทางสถิติ จะอธิบายวิธีการโดยละเอียด ในหัวข้อถัดไป

2.5.1 กระบวนการสำหรับการออกแบบระบบควบคุมความเสี่ยง SRP/CS ให้กับเครื่องจักร

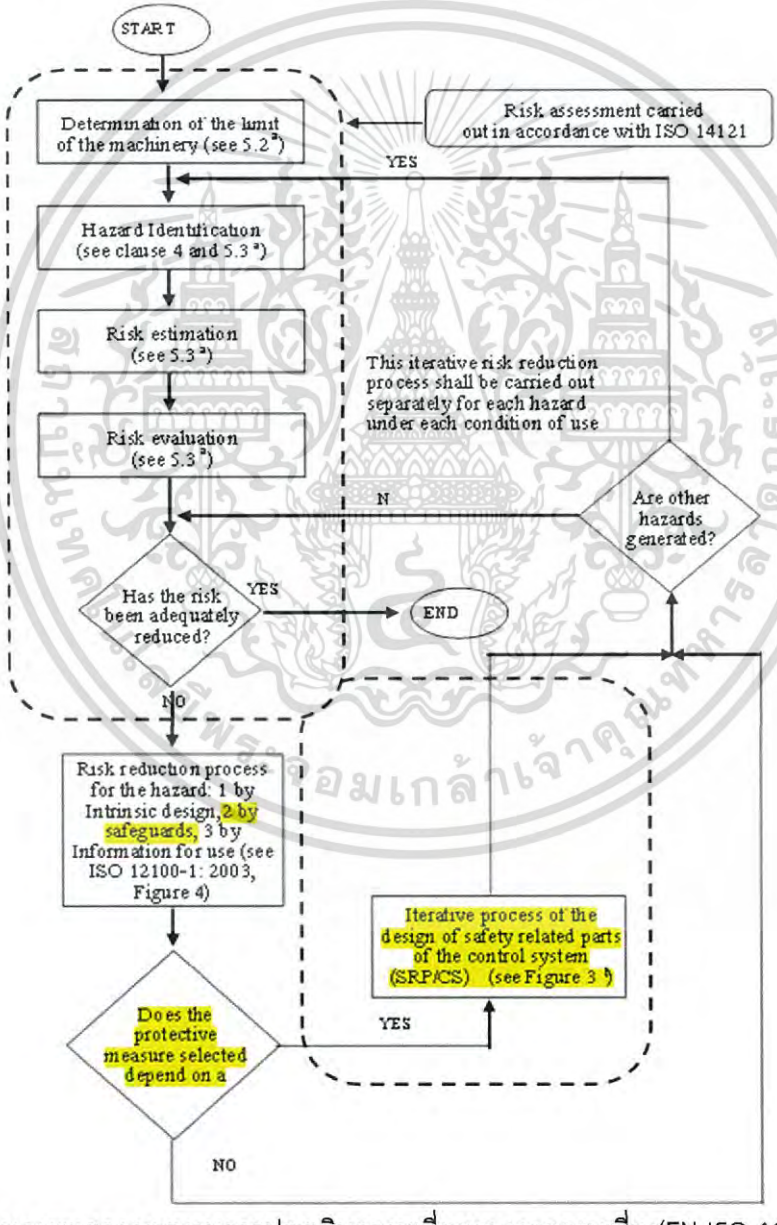
ดังที่ได้กล่าวมาในหัวข้อ 2.3 และหัวข้อ 2.3.5 ตามข้อกำหนดของมาตรฐาน EN ISO 12100 [1] ถ้าหากต้องการลดความเสี่ยงด้วยวิธีการดังหัวข้อ 2.3.5.2 “การลดความเสี่ยงด้วยการติดตั้งอุปกรณ์ความปลอดภัยหรือเพิ่มมาตรการป้องกันให้กับเครื่องจักร” จะนำมาสู่การประยุกต์ใช้งานมาตรฐาน EN 954-1 [3] และ EN ISO 13849-1 [1] ดังแสดงในรูปที่ 2.34

จากรูปที่ 2.35 หลักการของการออกแบบระบบควบคุมความเสี่ยง (SRP/CS) ให้กับเครื่องจักร เพื่อให้ค่าความเสี่ยงอยู่ในระดับที่ยอมรับได้ ตามข้อกำหนดของมาตรฐาน EN ISO 13849-1 [1] มีดังนี้

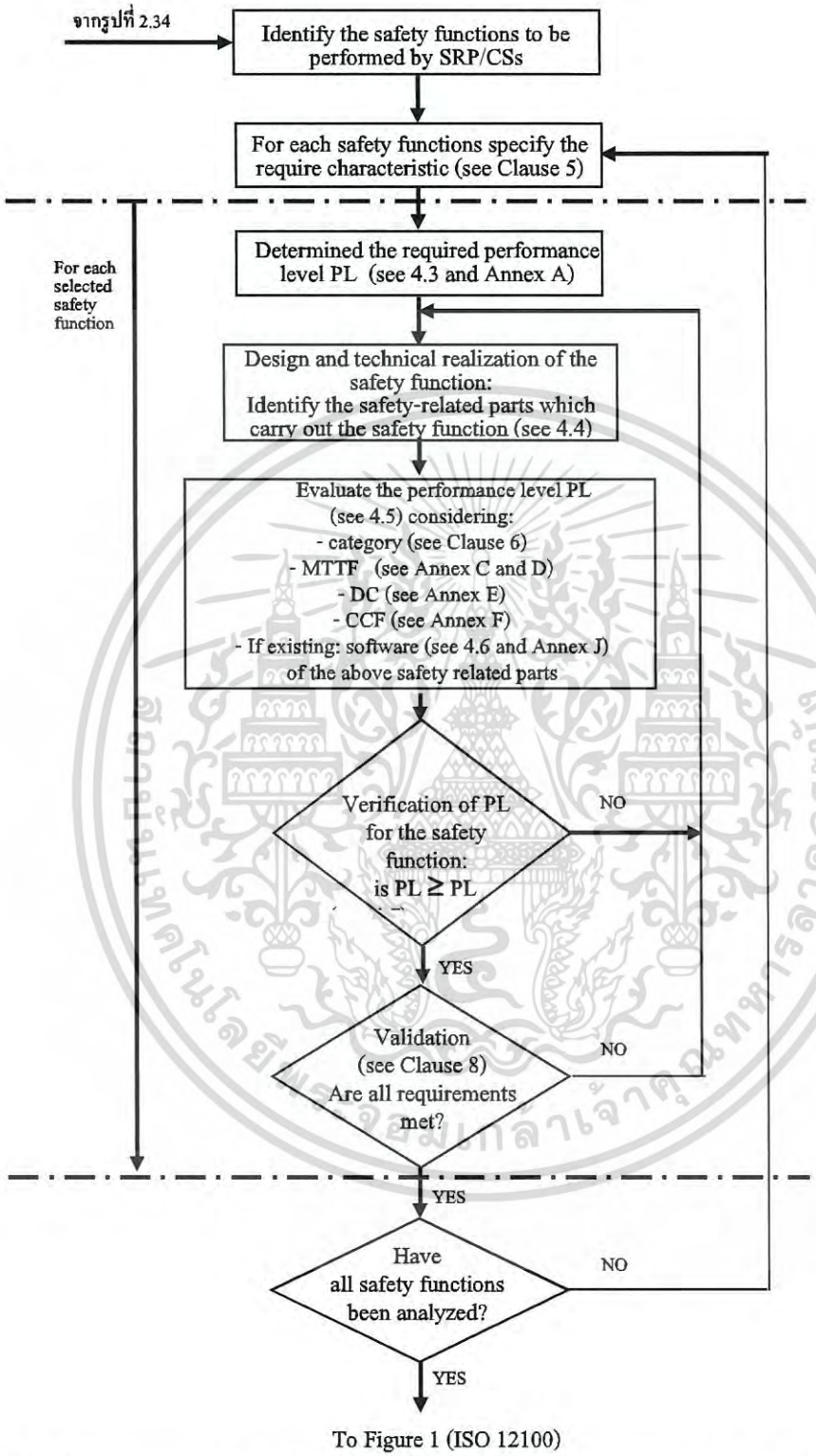
1. ระบุจุดเสี่ยงและฟังก์ชันของระบบควบคุมความเสี่ยง (Identify the safety function to be performed by SRP/CSs)
2. ประเมินความเสี่ยง เพื่อหาค่าระดับความปลอดภัยที่ต้องการในการจัดการกับความเสี่ยง (Determined the required performance level, PLr)
3. ออกแบบระบบควบคุมความเสี่ยง (SRP/CS) และกำหนดฟังก์ชันในการจัดการกับความเสี่ยง (Design and technical realization of the safety function)
4. ประเมินค่าระดับความปลอดภัยที่ได้จากการออกแบบระบบควบคุมความเสี่ยง (Evaluate performance level, PL) โดยพิจารณาจาก Category, MTTFd, DC และ CCF

5. เปรียบเทียบค่าระดับความปลอดภัยที่ได้จากการออกแบบ (PL) กับค่าระดับความปลอดภัยที่ต้องการ (PLr) ว่าเพียงพอที่จะจัดการความเสี่ยงหรือไม่ (Verification of PL for safety function, PL ≥ PLr)

หมายเหตุ: จากขั้นตอนที่ 1 – 5 ที่กล่าวมาในตอนต้น ถ้าค่าระดับความปลอดภัยที่ได้จากการออกแบบระบบควบคุมความเสี่ยงไม่เพียงพอที่จะจัดการความเสี่ยง (PL <PLr) ให้กลับไปพิจารณาทุกขั้นตอนอีกครั้ง (Iterative Process) เพื่อที่จะได้ปรับปรุงค่าระดับความปลอดภัยของระบบควบคุมความเสี่ยง (SPR/CS) ให้สามารถที่จะจัดการกับความเสี่ยงหรือลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ (Reduce risk into acceptable level)



รูปที่ 2.34 แผนภาพแสดงกระบวนการประเมินความเสี่ยงและลดความเสี่ยง(EN ISO 12100 [2])



รูปที่ 2.35 กระบวนการประเมินความเสี่ยงและลดความเสี่ยงตามมาตรฐาน EN ISO 13849-1 [1]
(The iterative processfor risk assessment and risk reduction to achieve safety)

2.5.2 ระบุจุดเสี่ยงและฟังก์ชันของระบบควบคุมความเสี่ยง (Identify the safety function to beperformed by SRP/CSs)

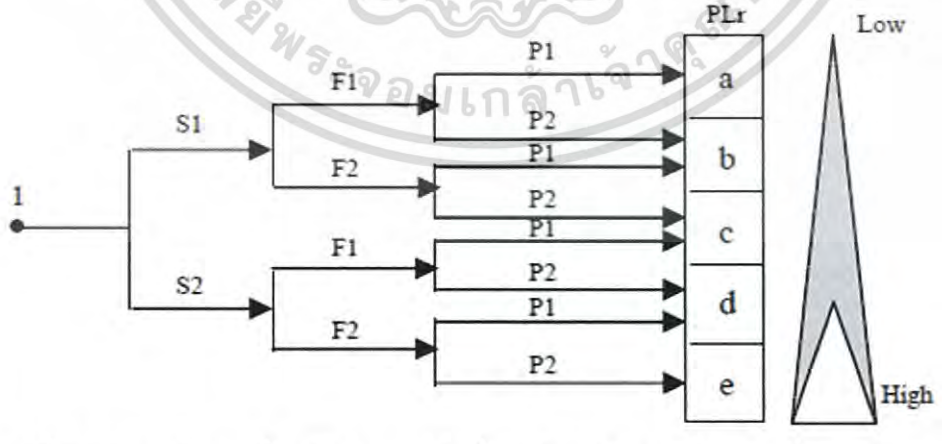
ดังที่ได้กล่าวมาในหัวข้อ 2.3 และหัวข้อ 2.3.2 ตามข้อกำหนดของมาตรฐาน EN ISO 12100 [1] ตัวอย่างของการระบุจุดที่อันตรายแสดงดังภาคผนวก ง

2.5.3 ประเมินความเสี่ยง เพื่อหาค่าระดับความปลอดภัยที่ต้องการในการจัดการกับความเสี่ยง (Determined the required performance level, PLr)

ดังที่ได้กล่าวมาในหัวข้อ 2.3 และหัวข้อ 2.3.3 ตามข้อกำหนดของมาตรฐาน EN ISO 12100 [1] หลังจากที่ได้พิจารณาระบบของเครื่องจักรและระบุจุดที่ทำให้เกิดอันตรายแล้ว จะทำการประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง (Risk graph) แสดงในรูปที่ 2.36 ซึ่งพารามิเตอร์ที่ใช้ในการประเมินความเสี่ยงมีดังนี้

- ความรุนแรงของอันตราย (S) แบ่งเป็น 2 ระดับ คือ S1 และ S2
- ความถี่ที่เข้าไปอยู่ในสถานที่อันตราย (F) แบ่งเป็น 2ระดับ คือ F1 และ F2
- โอกาสในการหลีกเลี่ยงอันตราย (P) แบ่งเป็น 2 ระดับ คือ P1 และ P2

คำจำกัดความของพารามิเตอร์S, F และ P ดังที่ได้อธิบายในหัวข้อ 2.4 และหัวข้อ 2.4.4 ตามข้อกำหนดของมาตรฐานEN 954-1 [3]แต่สิ่งที่เพิ่มขึ้นมาจากมาตรฐาน EN 954-1 [3] คือการประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง (Risk graph) จะสามารถบอกได้ว่าสถานการณ์อันตรายที่นำมาประเมินนั้นมีความเสี่ยงอยู่ในระดับที่สูง (High risk) หรือระดับที่ต่ำ (Low risk) และสามารถบอกค่าระดับความปลอดภัยที่ต้องการ PLr (Performance Level required)ในการจัดการกับความเสี่ยงหรือลดความเสี่ยงลงให้อยู่ในระดับที่ยอมรับได้ (Risk reduction into acceptable level)ซึ่งจะนำไปสู่การออกแบบระบบควบคุมความเสี่ยง (SRP/CS)ดังที่จะได้กล่าวถึงในหัวข้อถัดไป



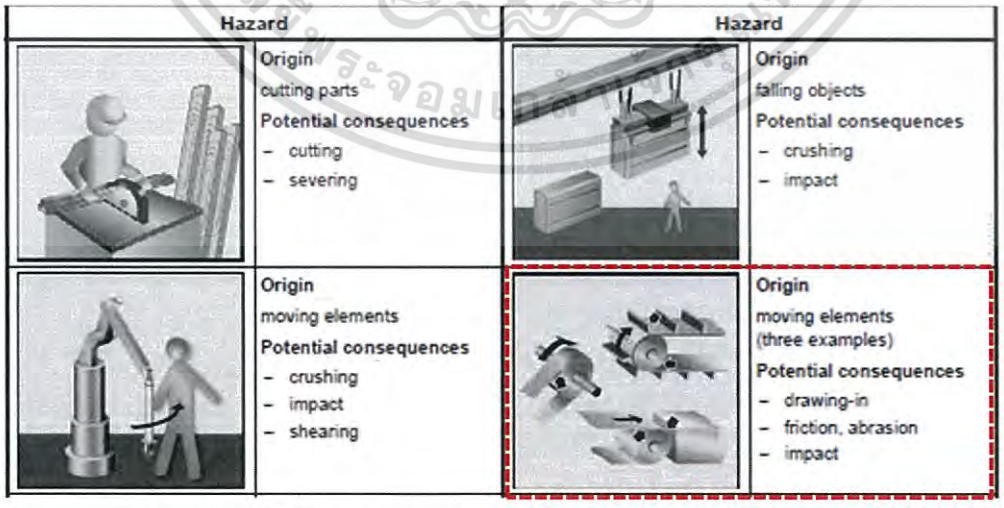
รูปที่ 2.36 กราฟความเสี่ยง (Risk graph) เพื่อหาค่าระดับความปลอดภัยที่ต้องการ (PLr)

ตารางที่ 2.4 ตารางแสดงค่าระดับความปลอดภัย (PL)

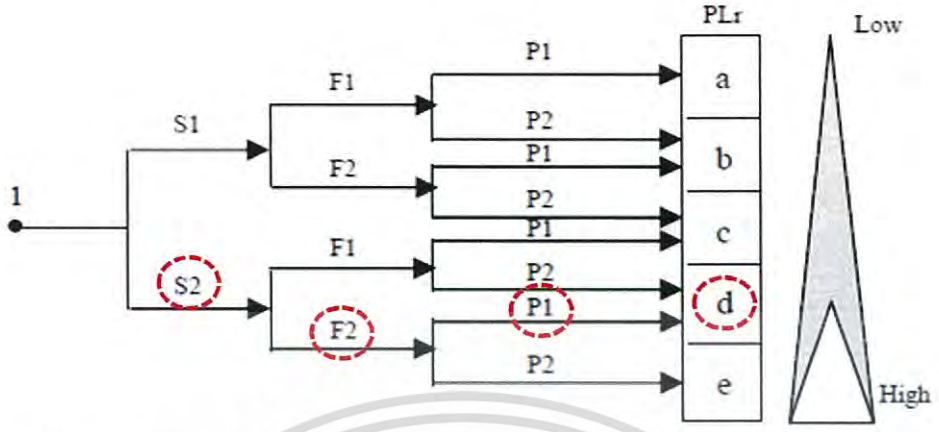
PL	Average probability of dangerous failure per hour (PFHDavg) (1/h)
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$
NOTE: Besides the average probability of dangerous failure per hour other measures are also necessary to achieve the PL	

ตัวอย่างการระบุสถานการณ์ที่อันตราย (Identify Hazard) และการประเมินความเสี่ยง (RiskAssessment)จากการถูกดึง (Drawing-in) โดยสายพานลำเรียงแสดงดังรูปที่ 2.37 จากการประเมินความเสี่ยงจะได้ว่า ความรุนแรงของอันตราย (S2) คือ ความอันตรายมีความรุนแรงถึงขั้นพิการและเสียชีวิต, ความถี่ที่เข้าไปอยู่ในสถานที่อันตราย (F2) คือ จำนวนหลายๆครั้งใน 1 วัน และโอกาสในการหลีกเลี่ยงอันตราย (P1) คือสามารถหลบหลีกได้ในกรณีที่พนักงานมีประสบการณ์และผ่านการอบรมเป็นอย่างดี แต่ถ้าเป็นพนักงานใหม่ไม่มีประสบการณ์ให้ประเมินเป็น P2 แสดงดังรูปที่ 2.38

จากผลของการประเมินความเสี่ยงจะพบว่าสถานการณ์อันตรายมีความเสี่ยงอยู่ในระดับสูง (High risk) และค่าระดับความปลอดภัยที่ต้องการในการลดความเสี่ยง (PLr) มีค่าเท่ากับ PLd ดังนั้นจะต้องออกแบบระบบควบคุมความเสี่ยง (SRP/CS) ให้มีค่าระดับความปลอดภัยอย่างน้อยเท่ากับ PLdจึงจะสามารถจัดการกับความเสี่ยงได้ ซึ่งจะแสดงตัวอย่างการออกแบบระบบควบคุมความเสี่ยง (SRP/CS) ในหัวข้อถัดไป



รูปที่ 2.37 ตัวอย่างการระบุสถานการณ์อันตราย (Hazard Identification)



รูปที่ 2.38 ตัวอย่างการประเมินความเสี่ยง(Risk Assessment) ด้วยวิธีกราฟความเสี่ยง

2.5.4 ออกแบบระบบควบคุมความเสี่ยง SRP/CSs และกำหนดฟังก์ชันในการจัดการกับความเสี่ยง(Design and technical realization of the safety function)

จากหัวข้อ 2.5.3 หลังจากที่ได้ประเมินความเสี่ยงแล้ว จะทำให้รู้ค่าระดับความปลอดภัยที่ต้องการ (PLr) นำมาสู่การเลือกอุปกรณ์ป้องกันและออกแบบระบบควบคุมความเสี่ยง (SRP/CS) ด้วยโครงสร้างแบบ Category ดังที่ได้กล่าวมาในหัวข้อ 2.4. และหัวข้อ 2.4.6 ตามข้อกำหนดของมาตรฐาน EN 954-1 [3] แต่สิ่งที่นำพิจารณาเพิ่มเติมคือโอกาสการล้มเหลวของอุปกรณ์ในระบบ (MTTFd, DC และ CCF) ที่จะกล่าวถึงในหัวข้อถัดไป

2.5.5 ประเมินค่าระดับความปลอดภัยที่ได้จากการออกแบบระบบควบคุมความเสี่ยง

จากหัวข้อ 2.5.4หลังจากที่ได้ออกแบบระบบควบคุมความเสี่ยง (SRP/CS) และกำหนดฟังก์ชันในการจัดการกับความเสี่ยงแล้ว จะทำการประเมินค่าระดับความปลอดภัย (PL) ที่ได้จากการออกแบบระบบควบคุมความเสี่ยง (SRP/CS) โดยพิจารณาจาก Category, MTTFd, DC และ CCF

2.5.5.1 Category

ระบบควบคุมความเสี่ยง (SRP/CS)ดังรูปที่ 2.39มีองค์ประกอบดังนี้

- I (Input), อุปกรณ์ส่วนอินพุท เช่น Emergency Stop,Safety Light Curtain ... ฯลฯ
- L (Logic), อุปกรณ์ส่วนควบคุมเช่น Safety Relay, PLC, Controller, Processor ... ฯลฯ
- O (Output), อุปกรณ์ส่วนเอาท์พุท เช่น Magnetic Contactor, Magnetic Relay, ... ฯลฯ
- I_{ab}, I_{bc} (Interconnect), การเชื่อมต่อสัญญาณภายใน เช่น Wiring control signal และ Wiringfeedback signal ... ฯลฯ

ลักษณะโครงสร้างของการออกแบบระบบควบคุมความเสี่ยง (SRP/CS) แบ่งออกเป็น 5 ประเภทที่แตกต่างกัน ดังนี้

1 . Category B แสดงดังรูปที่ 2.26 ตามข้อกำหนดของ EN 954-1 [3]

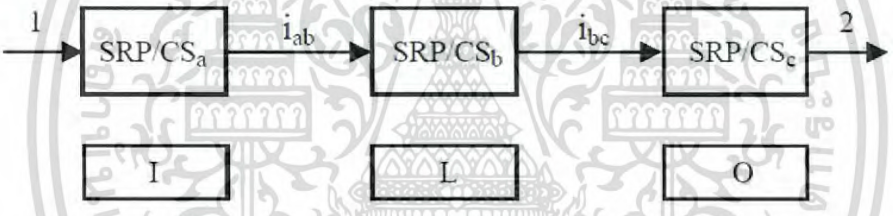
2 . Category 1 แสดงดังรูปที่ 2.26 ตามข้อกำหนดของ EN 954-1 [3]

3 . Category 2 แสดงดังรูปที่ 2.27 ตามข้อกำหนดของ EN 954-1 [3]

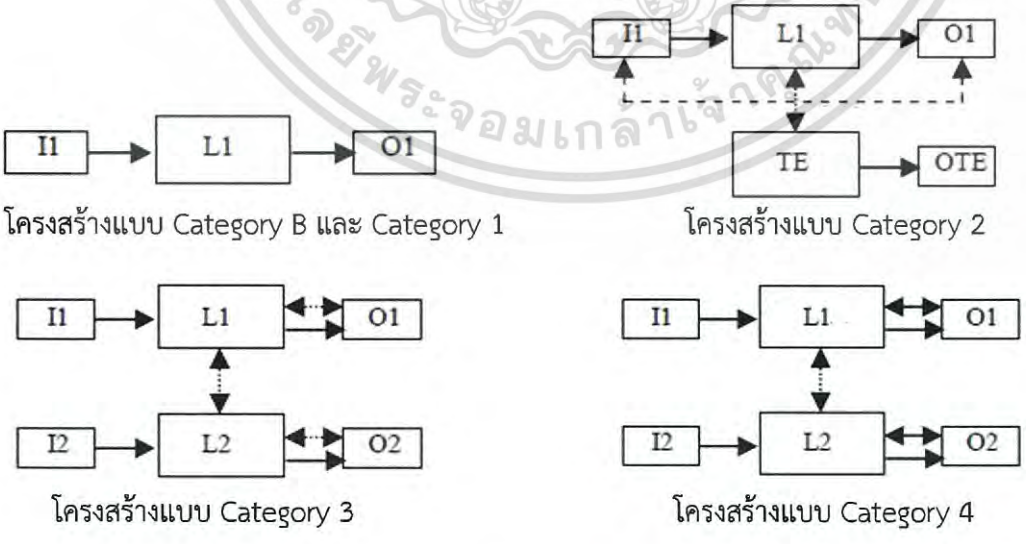
4 . Category 3 แสดงดังรูปที่ 2.28 ตามข้อกำหนดของ EN 954-1 [3]

5 . Category 4 แสดงดังรูปที่ 2.29 ตามข้อกำหนดของ EN 954-1 [3]

ดังที่ได้กล่าวมาในหัวข้อ 2.4 และหัวข้อ 2.4.6 ตามข้อกำหนดของ EN 954-1 [3] สามารถกล่าวโดยสรุปได้ดังนี้ การออกแบบระบบควบคุมความเสี่ยง(SRP/CS) ตามโครงสร้างแบบ Category 4 จะให้ความน่าเชื่อถือของระบบสูงสุด (The highest reliability) และการออกแบบระบบด้วยโครงสร้างแบบ Category B จะให้ความน่าเชื่อถือของระบบต่ำสุด (The lowest reliability) สำหรับลักษณะโครงสร้างของการออกแบบระบบควบคุมความเสี่ยง(SRP/CSs)ทั้ง 5 ประเภท แสดงโดยสรุปได้ดังรูปที่ 2.40



รูปที่ 2.39 องค์ประกอบของระบบควบคุมความเสี่ยง (SRP/CS)



โครงสร้างแบบ Category B และ Category 1

โครงสร้างแบบ Category 2

โครงสร้างแบบ Category 3

โครงสร้างแบบ Category 4

รูปที่ 2.40 ลักษณะโครงสร้างของการออกแบบระบบควบคุมความเสี่ยง (SRP/CSs) ทั้ง 5 ประเภท

2.5.5.2 MTTFd(Mean time to dangerous failure)

คือค่าที่บอกถึงอัตราการล้มเหลวของอุปกรณ์ (Failure rate of component) หรือความน่าเชื่อถือของอุปกรณ์ (Reliability of component) แบ่งออกเป็น 3 ระดับ ดังนี้

- ระดับต่ำ (Low level) คือ อัตราการล้มเหลวอุปกรณ์อยู่ในช่วงระหว่าง 3 – 10 ปี
- ระดับกลาง(Medium level) คือ อัตราการล้มเหลวอุปกรณ์อยู่ในช่วงระหว่าง 10 – 30 ปี
- ระดับสูง(High level) คืออัตราการล้มเหลวอุปกรณ์อยู่ในช่วงระหว่าง 30 – 100 ปี

กล่าวโดยสรุปได้ว่าMTTFd มีค่าต่ำแสดงว่าอุปกรณ์มีความน่าเชื่อถือต่ำ(Low reliability) ซึ่งหมายความว่าอุปกรณ์มีอัตราในการล้มเหลวมาก เช่นในช่วงระยะเวลา 3 – 10 ปี มีโอกาสที่อุปกรณ์จะทำงานผิดพลาดแต่ในทางตรงกันข้ามหากค่า MTTFd มีค่าสูง แสดงว่าอุปกรณ์มีความน่าเชื่อถือสูง(High reliability)ซึ่งหมายความว่าอุปกรณ์มีอัตราในการล้มเหลวน้อย เช่นในช่วงระยะเวลา 30 – 100 ปี มีโอกาสที่อุปกรณ์จะทำงานผิดพลาด ดังแสดงในตารางที่2.5

ตารางที่ 2.5 แสดงการแบ่งช่วงอัตราการล้มเหลวของอุปกรณ์ (MTTFd) ทั้ง 3 ระดับ

Denotation of each channel	Range of each channel
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd ≤ 100 years

<u>การหาค่า MTTFd</u>

1. วิธีการหาค่า MTTFd ของอุปกรณ์ (Calculating or Evaluating MTTFd for single components) มีดังนี้

1.1 อ้างอิงจากค่า MTTFd โดยตรง

- อ้างอิงค่า MTTFd จากมาตรฐาน EN ISO 13849-1[1] แสดงดังภาคผนวก ง
- อ้างอิงค่าMTTFdจากเอกสารที่มาจากผู้ผลิตอุปกรณ์ (Manufacturing datasheet) เนื่องจากเป็นค่าอัตราการล้มเหลวของอุปกรณ์ (Failure rate of component) ที่ผ่านการผลิตและทดสอบตามมาตรฐานความปลอดภัยสากล (Basic safety requirements and Well-tried safety principles)

1.2 คำนวณหาค่า MTTFdโดยใช้ความสัมพันธ์ของสมการที่(1) และสมการที่ (2)

- อ้างอิงค่า B10dโดยตรงจากมาตรฐาน EN ISO 13849-1[1] แสดงดังภาคผนวก ง

- อ้างอิงค่าB10dจากเอกสารที่มาจากผู้ผลิตอุปกรณ์ (Manufacturing datasheet) เนื่องจากเป็นค่าอัตราการล้มเหลวของอุปกรณ์ (Failure rate of component) ที่ผ่านการผลิตและทดสอบตามมาตรฐานความปลอดภัยสากล (Basic safety requirements and Well-tried safety principles)

$$MTTFd = \frac{B_{10d}}{0.1x(n_{op})} \quad (1)$$

$$n_{op} = \frac{(d_{op})x(h_{op})x3{,}600\,(s/h)}{t_{cycle}} \quad (2)$$

เมื่อ

B_{10d} คือ จำนวนครั้งโดยเฉลี่ยที่อุปกรณ์สามารถทำงานได้

N_{op} คือ จำนวนครั้งโดยเฉลี่ยที่อุปกรณ์ทำงานใน 1 ปี

D_{op} คือ จำนวนวันโดยเฉลี่ยที่อุปกรณ์ทำงานใน 1 ปี

h_{op} คือ จำนวนชั่วโมงโดยเฉลี่ยที่อุปกรณ์ทำงานใน 1 วัน

t_{cycle} คือ เวลาเฉลี่ยที่อุปกรณ์ทำงานใน 1 รอบ, หน่วยเป็นวินาที

โดยค่า B_{10d}สามารถหาได้จากการอ้างอิงจากมาตรฐาน EN ISO 13849-1[1] แสดงดังภาคผนวก ง และจากเอกสารที่มาจากผู้ผลิตอุปกรณ์(Manufacturing datasheet)

ตารางที่ 2.6 คำจำกัดความของพารามิเตอร์ที่ใช้ในการคำนวณ MTTFd

Symbol	Definition of abbreviate word
n_{op}	The mean number of annual operations
d_{op}	The mean operation, in days per year
h_{op}	The mean operation, in hours per day
B_{10d}	The mean number of cycles until 10% of components failure dangerously
t_{cycle}	The mean time between the beginning of two successive cycles of the component (e.g. switching of a valve) in seconds per cycle

2. วิธีการหาค่า MTTFd ของระบบ (Calculating or Evaluating MTTFd for each channel)

การหาค่า MTTFd ของระบบ สามารถหาได้จากการคำนวณMTTFd ของอุปกรณ์แต่ละตัวในระบบ ดังแสดงในสมการที่ (3)

$$\frac{1}{MTTFd} = \frac{1}{MTTFd_1} + \frac{1}{MTTFd_2} + \dots \frac{1}{MTTFd_n} \quad (3)$$

2.5.5.3 DC (Diagnostic coverage)

DC คืออัตราส่วนระหว่างค่าความผิดพลาดของอุปกรณ์ที่สามารถตรวจพบได้ (Dangerous Failure that can be detected) กับค่าความผิดพลาดที่จะเกิดขึ้นทั้งหมด (Dangerous Failure that can be detected & cannot be detected) โดยที่ประสิทธิภาพในการตรวจพบความผิดพลาดของอุปกรณ์ (The effectiveness of error detection) จะแบ่งออกเป็น 4 ระดับ ดังนี้

- None หมายถึงอัตราการตรวจพบความผิดพลาดต่ำกว่า 60%
- Low หมายถึงอัตราการตรวจพบความผิดพลาดอยู่ระหว่าง 60%- 90% (ระดับต่ำ)
- Medium หมายถึงอัตราการตรวจพบความผิดพลาดอยู่ระหว่าง 90%- 99% (ระดับปานกลาง)
- High หมายถึงอัตราการตรวจพบความผิดพลาดมากกว่า 99% (ระดับสูง)

กล่าวโดยสรุปได้ดังนี้ ค่า DC ระดับ High หมายถึงประสิทธิภาพในการตรวจพบความผิดพลาดของอุปกรณ์อยู่ในระดับสูง มีโอกาสในการเกิดอันตรายน้อยในทางตรงกันข้ามค่า DC ระดับ None และระดับ Low หมายถึงประสิทธิภาพในการตรวจพบความผิดพลาดของอุปกรณ์อยู่ในระดับต่ำ มีโอกาสในการเกิดอันตรายมากการคำนวณค่าDCavg ของทั้งระบบ สามารถคำนวณได้จากค่าDC และ MTTFd ของอุปกรณ์แต่ละตัวที่อยู่ในระบบ ดังแสดงในสมการที่ (4)ซึ่งค่า DC ของอุปกรณ์สามารถหาได้จากผลของการประมาณโดยวิธี FMEA (Failure Mode and Effect Analysis) ดังแสดงในภาคผนวก ง

$$DC_{avg} = \frac{\frac{DC_1}{MTTFd_1} + \frac{DC_2}{MTTFd_2} + \dots \frac{DC_n}{MTTFd_n}}{\frac{1}{MTTFd_1} + \frac{1}{MTTFd_2} + \dots \frac{1}{MTTFd_n}} \quad (4)$$

ตารางที่ 2.7 ตารางแสดงการแบ่งช่วงของค่า DC (Diagnostic Coverage)

Denotation	Range
None	DC < 60 %
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

2.5.5.4 CCF (Common cause failure)

CCF คือความล้มเหลวของอุปกรณ์หรือระบบควบคุมที่มาจากสาเหตุทั่วๆไปพบได้บ่อยครั้ง ดังนั้นผู้ออกแบบเครื่องจักร (Machine Designer) และผู้ใช้งานเครื่องจักร (Machine User) จำเป็นที่จะต้องนำมาพิจารณาในระหว่างกระบวนการออกแบบ โดยอ้างอิงจากรายการตรวจสอบ (Check list) ดังแสดงในภาคผนวก ง ซึ่งเกณฑ์ในการประเมินและให้คะแนนในแต่ละรายการแบ่งออกเป็น 2 ระดับ ดังนี้

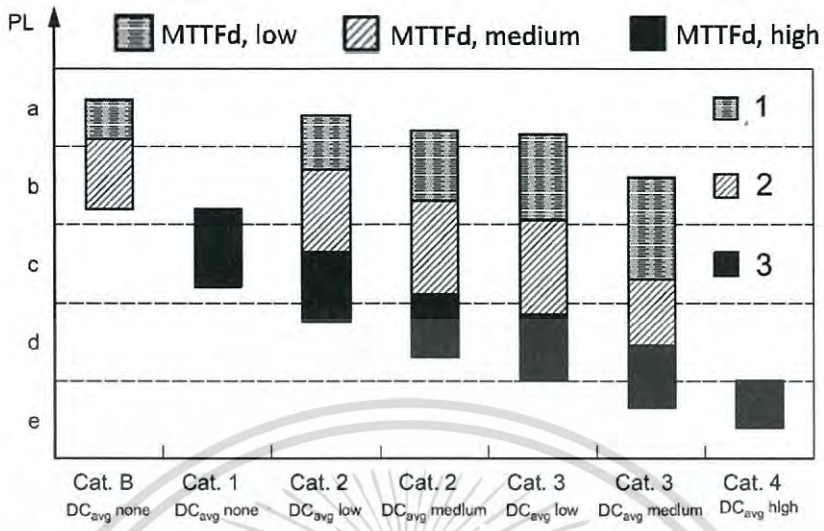
- ในกรณีที่การออกแบบระบบควบคุมเป็นไปตามเงื่อนไขที่ได้ระบุไว้ จะได้คะแนนเต็มในหัวข้อนั้น
- แต่ในทางตรงกันข้ามในกรณีที่ไม่เป็นไปตามเงื่อนไข จะไม่ได้คะแนนในหัวข้อนั้น (0 คะแนน)

ซึ่งคะแนนรวมทั้งหมดของการประเมินในทุกรายการ คือ100 คะแนน ถ้าหากผลของการประเมินได้คะแนนต่ำกว่า 65 คะแนน ทางผู้ออกแบบเครื่องจักร (Machine Designer) และผู้ใช้งานเครื่องจักร (Machine User)จะต้องพิจารณาการออกแบบระบบควบคุมความเสี่ยง(SRP/CS) ใหม่อีกครั้ง เพื่อที่จะปรับปรุงการออกแบบระบบให้มีประสิทธิภาพที่เพียงพอในการจัดการกับความเสี่ยง

2.5.5.5 เปรียบเทียบค่าระดับความปลอดภัยที่ได้จากการออกแบบ (PL) (Verification of PL for safety function, PL ≥ PLr)

จากหัวข้อ2.5.5.1 – 2.5.5.4หลังจากที่ได้พิจารณาการออกแบบระบบควบคุมความเสี่ยง(SRP/CS)จากพารามิเตอร์Category, MTTFd, DCavgและ CCFแล้วขั้นตอนต่อไปคือการหาค่าระดับความปลอดภัยที่ได้จากการออกแบบ(PL) โดยสามารถหาได้จาก 2 วิธี ดังนี้

- หา PL โดยอ้างอิงจากความสัมพันธ์ของ Category, MTTFd และ DCavg ดังรูปที่ 2.41
- หา PL โดยอ้างอิงจากความสัมพันธ์ของ Category, MTTFd และ DCavg แสดงดังตารางในภาคผนวก ง (ซึ่งตารางในภาคผนวก ง จะอธิบายได้ละเอียดกว่ารูปที่ 2.41 โดยจะอธิบายถึงค่าโอกาสในการล้มเหลวของระบบ PFHDavg)



รูปที่ 2.41 แสดงความสัมพันธ์ระหว่างค่า PL กับ Categories, DCavgและ MTTFd

หลังจากที่ได้ค่าระดับความปลอดภัย (PL) ของระบบควบคุมความเสี่ยงแล้ว จะทำการเปรียบเทียบกับค่าระดับความปลอดภัยที่ต้องการ (PLr) ที่ได้มาจากการประเมินด้วยกราฟความเสี่ยงดังนี้

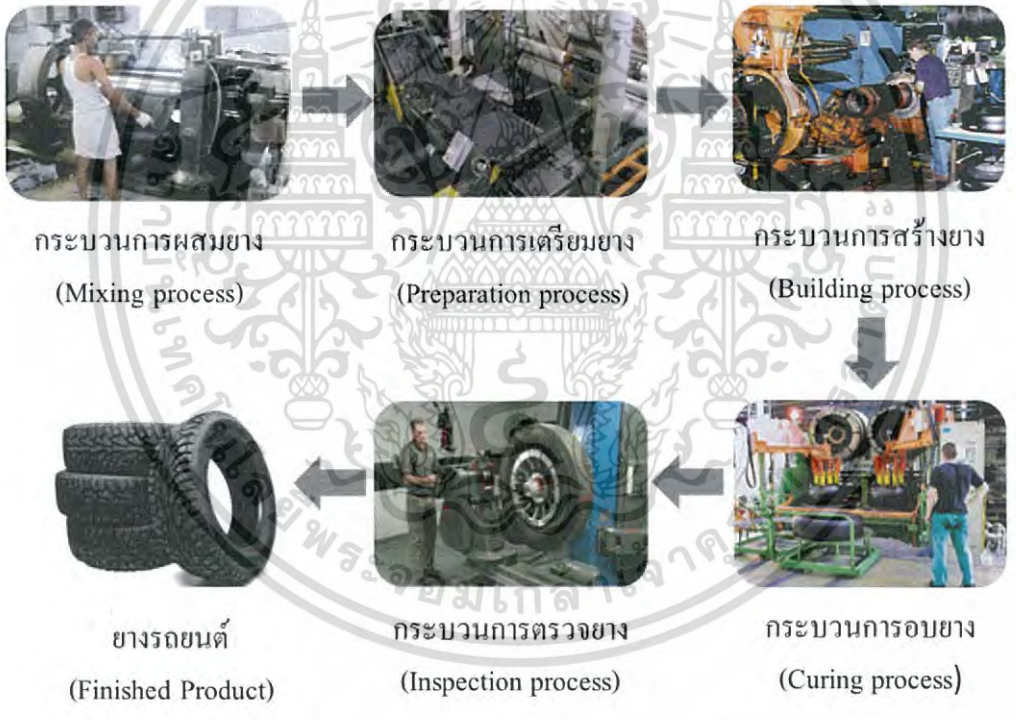
- ถ้า PL ≥ PLrแสดงว่าระบบควบคุมความเสี่ยงสามารถจัดการกับความเสี่ยงได้
- ถ้า PL <PLr แสดงว่าระบบควบคุมความเสี่ยงไม่สามารถจัดการกับความเสี่ยงได้

ในกรณีที่ PL <PLr จะต้องกลับไปพิจารณาขั้นตอนทั้งหมดอีกครั้ง (Iterative process) ดังแสดงในรูปที่ 2.34 และรูปที่ 2.35 เพื่อที่จะปรับปรุงค่าระดับความปลอดภัย (PL) ของระบบให้มีค่ามากเพียงพอที่จะจัดการกับความเสี่ยงได้

บทที่ 3
งานวิจัยที่นำเสนอ

3.1 กล่าวนำ

ในอุตสาหกรรมผลิตยางรถยนต์ ทุกขั้นตอนของกระบวนการผลิตล้วนมีความเสี่ยงที่ทำให้เกิดอันตรายต่อผู้ปฏิบัติงานได้ทั้งสิ้นกระบวนการผลิตยางรถยนต์เริ่มต้นจากกระบวนการผสมยาง (Mixing process) ส่งต่อไปยังกระบวนการเตรียมยาง (Preparation process), กระบวนการสร้างยาง (Building process), กระบวนการอบยาง (Curing process) และสิ้นสุดด้วยกระบวนการตรวจยาง (Inspection process) ตามลำดับ เพื่อให้ได้ยางรถยนต์ที่มีคุณภาพ (Finished product) และจำหน่ายให้กับลูกค้า แสดงดังรูปที่ 3.1



รูปที่ 3.1 กระบวนการผลิตยางรถยนต์ (Tyre Manufacturing Process)

จากกระบวนการผลิตยางรถยนต์ข้างต้น ผู้วิจัยได้เสนองานวิจัยโดยเลือกเครื่องจักรเก่าในกระบวนการสร้างยาง (Old Machinery of Tyre Building Process) มาเป็นกรณีศึกษาเนื่องจากว่าในสมัยก่อนข้อกำหนดด้านมาตรฐานความปลอดภัยสากลยังไม่ชัดเจนและเทคโนโลยีด้านระบบความปลอดภัยยังไม่ได้มีการพัฒนาเหมือนปัจจุบัน จึงทำให้เครื่องจักรเก่าไม่ได้ถูกผลิตตามมาตรฐานความปลอดภัยสากล อีกทั้งในกระบวนการสร้างยางเป็นกระบวนการที่ผู้ปฏิบัติงานต้องทำงานร่วมกับ

เครื่องจักรตลอดเวลาและเป็นการทำงานภายใต้สภาวการณ์ที่มีความกดดันสูงกว่ากระบวนการอื่นๆ เนื่องจากต้องสร้างผลิตภัณฑ์ในปริมาณที่มากและแข่งกับเวลาส่งผลให้ผู้ปฏิบัติงานมีความเครียดและเหนื่อยล้าจากการปฏิบัติงานที่ต่อเนื่องเป็นระยะเวลานานๆ ปัจจัยเหล่านี้ล้วนมีความเสี่ยงที่ทำให้เกิดอันตรายต่อผู้ปฏิบัติงานได้ทั้งสิ้น

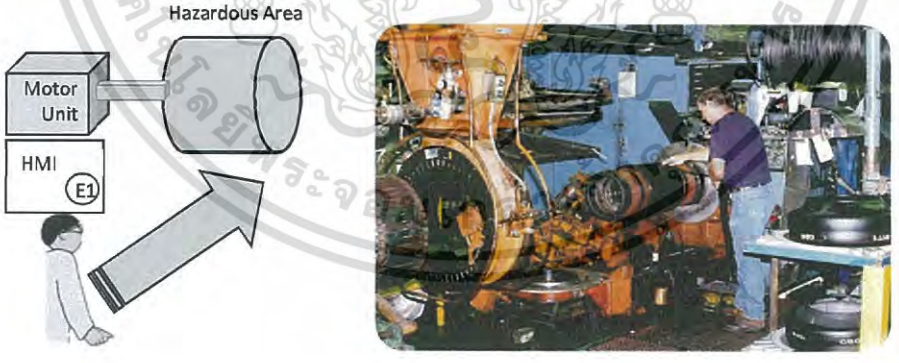
ดังนั้นงานวิจัยที่นำเสนอนี้จะแสดงการประยุกต์ใช้งานมาตรฐานความปลอดภัยสากล EN ISO 12100 [2] และ EN ISO 13849-1 [1] ในการประเมิน วิเคราะห์และจัดการกับความเสี่ยงที่จะเกิดขึ้น โดยมีขั้นตอนดังนี้

- ประเมินความเสี่ยงและหาค่าระดับความปลอดภัยที่ต้องการ PLr ด้วยวิธีกราฟความเสี่ยง
- ประเมินค่าระดับความปลอดภัยPLของระบบควบคุมความเสี่ยง (SRP/CS)
- เปรียบเทียบค่าระดับความปลอดภัยPL ของระบบควบคุมความเสี่ยง (SRP/CS) กับค่าระดับความปลอดภัยที่ต้องการ PLr
- ปรับปรุงค่าระดับความปลอดภัย PL ของระบบควบคุมความเสี่ยง (SRP/CS)

3.2 ประเมินความเสี่ยงและหาค่าระดับความปลอดภัยที่ต้องการ PLr ด้วยวิธีกราฟความเสี่ยง(Risk graph method)

จากรูปที่ 3.2 แสดงลักษณะรูปร่างของเครื่องสร้างยาง พบว่าความเสี่ยงที่สามารถเกิดขึ้นได้มาจาก 2 ส่วนหลักๆ ดังนี้

1. อันตรายที่เกิดจากการหมุน (Rotation Hazard) ของชุดขับเคลื่อน (Motor Unit)
2. อันตรายที่เกิดจากการดึงและการหนีบ (Drawing-in and Crushing Hazard) ของชุดขับเคลื่อน (Motor Unit) กับชุดเฟรมของเครื่องจักร

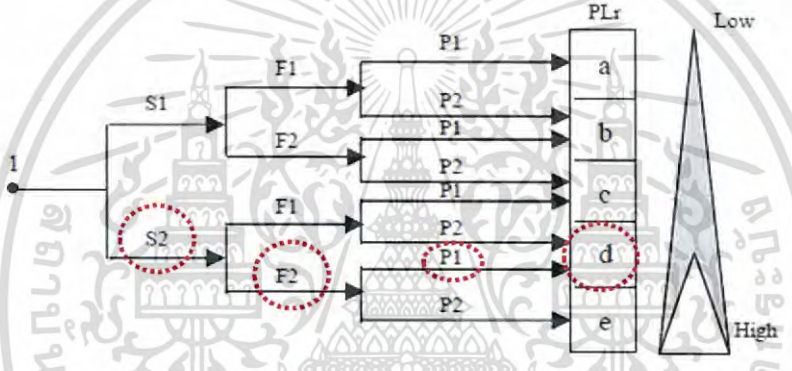


รูปที่ 3.2 ความเสี่ยงที่เกิดจากเครื่องสร้างยาง (Risk of Tyre Building Machine)

หลังจากที่ได้ระบุจุดเสี่ยงแล้ว ขั้นตอนต่อไปคือการประเมินความเสี่ยงเพื่อหาค่าระดับความปลอดภัยที่ต้องการ PLr ด้วยวิธีกราฟความเสี่ยง (Risk graph method) ซึ่งผลจากการประเมินความเสี่ยงของเครื่องสร้างยางสรุปได้ดังนี้

- ความรุนแรง (S2) เนื่องจากระดับความรุนแรงของเหตุการณ์สามารถทำให้พิการ สูญเสียอวัยวะ หรือถึงขั้นเสียชีวิตได้
- ความถี่ (F2) เนื่องจากความถี่ที่เข้าไปอยู่ในสถานการณ์ที่อันตรายอยู่ในระดับความถี่สูงเป็นจำนวนหลายครั้งในหนึ่งวัน
- โอกาสในการหลบหลีก (P1) เนื่องจากสามารถที่จะหลบหลีกอันตรายได้ ในกรณีที่พนักงานมีประสบการณ์ในการทำงานร่วมกับเครื่องจักรและผ่านการอบรมด้านการใช้งานเครื่องจักรที่ถูกต้องและปลอดภัยมาเป็นอย่างดี แต่ถ้าในกรณีที่เป็นพนักงานใหม่ที่ไม่มีประสบการณ์ทำงานร่วมกับเครื่องจักร ผลลัพธ์จากการประเมินจะเป็น (P2)

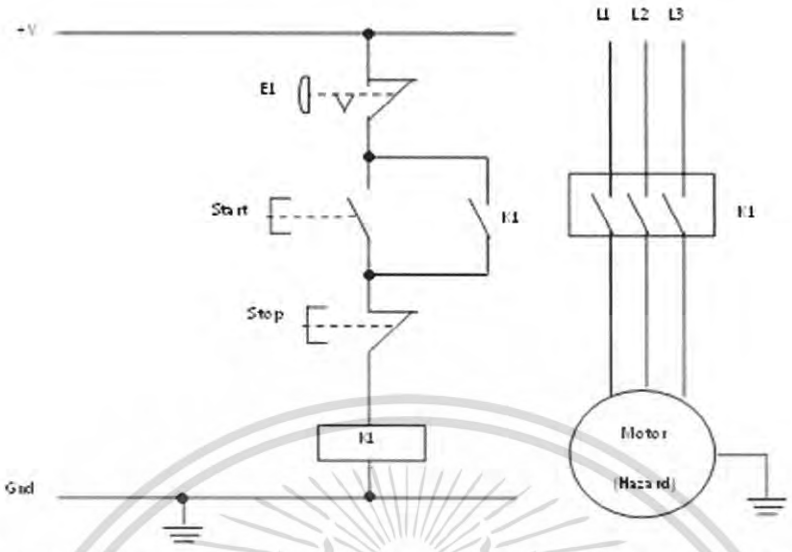
จากผลของการประเมินความเสี่ยง ทำให้ทราบว่าเครื่องจักรมีความเสี่ยงอยู่ในเกณฑ์ที่สูง (High risk) และค่าระดับความปลอดภัยที่ต้องการในการจัดการกับความเสี่ยงมีค่าเท่ากับ PLd แสดงดังรูปที่ 3.3



รูปที่ 3.3 ผลการประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง
(Result of risk assessment by risk graph method)

3.3 ประเมินค่าระดับความปลอดภัย PL ของระบบควบคุมความเสี่ยง (SRP/CS)

ระบบควบคุมความเสี่ยงดั้งเดิมของเครื่องจักรคือระบบหยุดฉุกเฉิน (Emergency Stop System) ซึ่งมีฟังก์ชันการทำงานดังนี้ เมื่อมีการกดปุ่ม Emergency Stop (E1) ระบบจะสั่งตัดการทำงานของ Magnetic Contactor (K1) ทันที ดังนั้นความเสี่ยงจะถูกจัดการโดยการตัดแหล่งจ่ายพลังงานออกจากชุดขับเคลื่อน (Motor Unit) แสดงดังรูปที่ 3.4



รูปที่ 3.4 ระบบหยุดฉุกเฉิน Emergency Stop (ก่อนปรับปรุงค่าระดับความปลอดภัย)

จากการประเมินค่าระดับความปลอดภัยจะพบว่า ระบบควบคุมความเสี่ยงออกแบบด้วยโครงสร้าง Category 1 ให้ค่าระดับความปลอดภัย PLc และโอกาสการล้มเหลวของระบบ (PFHDavg) มีค่าเท่ากับ 1.14×10^{-6} ครั้งต่อชั่วโมงแสดงดังตารางที่ 3.1 โดยมีรายละเอียดการคำนวณแสดงดังภาคผนวก ค

ข้อเสียของการออกแบบระบบด้วยโครงสร้างแบบ Category 1 คือในกรณีที่ Emergency Stop (E1) หรือ Magnetic Contactor(K1) ไม่ทำงานเนื่องจากความบกพร่องของกลไกลทางแมคคานิค จะทำให้ไม่สามารถจัดการกับความเสี่ยงได้และส่งผลให้เกิดอันตรายต่อผู้ปฏิบัติงาน

3.4 เปรียบเทียบค่าระดับความปลอดภัย PL ของระบบควบคุมความเสี่ยง (SRP/CS) กับค่าระดับความปลอดภัยที่ต้องการ PLr

จากหัวข้อ 3.2 และ 3.3 หลังจากที่ได้ค่าระดับความปลอดภัยที่ต้องการ PLr จากการประเมินด้วยวิธีกราฟความเสี่ยงมีค่าเท่ากับ PLd และค่าระดับความปลอดภัย PL จากการออกแบบระบบควบคุมความเสี่ยงของเครื่องจักร (SRP/CS) มีค่าเท่ากับ PLc แล้ว เมื่อทำการเปรียบเทียบจะพบว่าระบบควบคุมความเสี่ยงของเครื่องจักรไม่สามารถที่จะจัดการกับความเสี่ยงได้เนื่องจากไม่เป็นไปตามข้อกำหนด (PL <PLr) ดังนั้นจะต้องทำการปรับปรุงค่าระดับความปลอดภัยให้เป็นไปตามข้อกำหนด (PL ≥ PLr) กล่าวคือจะต้องปรับปรุงค่าระดับความปลอดภัยให้มีค่าเท่ากับ PLd หรือ PLe เพื่อให้สามารถจัดการกับความเสี่ยงได้

จากรูปที่ 3.4 จะเห็นว่าการออกแบบระบบด้วยโครงสร้าง Category 1 จะทำให้ระบบมีความน่าเชื่อถือต่ำ (Low Reliability) เนื่องจากความน่าเชื่อถือของระบบจะขึ้นอยู่กับความน่าเชื่อถือของอุปกรณ์เพียงอย่างเดียวเท่านั้น (Reliability of components) ในกรณีที่อุปกรณ์เกิดความบกพร่อง (Component Failure) ระบบจะไม่สามารถจัดกับการความเสี่ยงได้

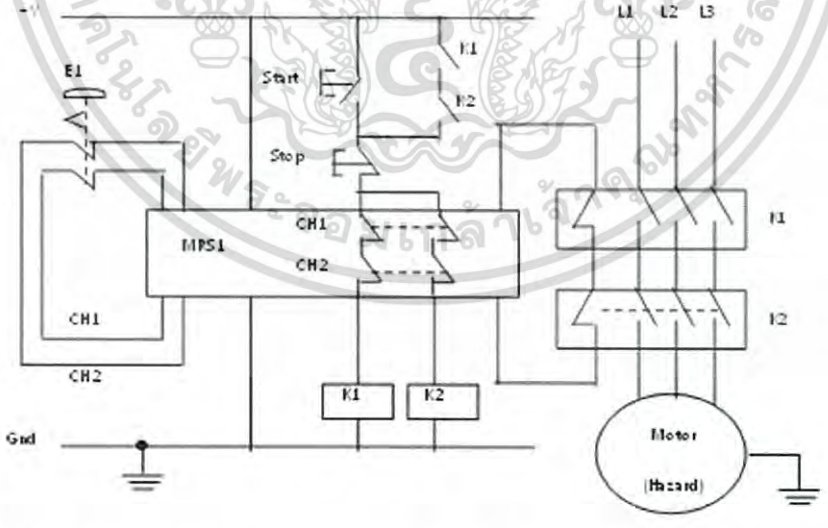
3.5 ปรับปรุงค่าระดับความปลอดภัย PL ของระบบควบคุมความเสี่ยง (SRP/CS)

งานวิจัยนี้จะแสดงการปรับปรุงค่าระดับความปลอดภัยPL ของระบบควบคุมความเสี่ยง (SRP/CS) ของเครื่องจักรด้วยวิธีการดังนี้

3.5.1 ปรับปรุงค่าระดับความปลอดภัยของระบบหยุดฉุกเฉิน Emergency Stop

จากรูปที่ 3.4 จะเห็นได้ว่าระบบหยุดฉุกเฉิน Emergency Stop ออกแบบด้วยโครงสร้าง Category 1 ความน่าเชื่อถือของระบบขึ้นอยู่กับความน่าเชื่อถือของอุปกรณ์เพียงอย่างเดียวเท่านั้น (Reliability of components) ทำให้ระบบมีความน่าเชื่อถือต่ำ (Low Reliability) และไม่สามารถที่จะจัดการความเสี่ยงได้ จึงต้องออกแบบระบบให้มี Category ที่สูงขึ้น เพื่อที่จะปรับปรุงค่าระดับความปลอดภัยให้อยู่ในระดับที่ยอมรับได้ ซึ่งในงานวิจัยนี้จะทำการออกแบบระบบด้วยโครงสร้างแบบ Category 3 โดยมีรายละเอียด ดังนี้

- ติดตั้งอุปกรณ์ควบคุม (Processing Unit) เพื่อทำหน้านี้ในการตรวจสอบความผิดปกติของอุปกรณ์ในกรณีที่เกิดความบกพร่อง (Detect component failure) เช่น Master Control Relay (MRS1) เพื่อให้ระบบมีความน่าเชื่อถือสูงขึ้น ดังรูปที่ 3.5
- ปรับปรุงโครงสร้างในส่วนของชุดอินพุท (Input device) ให้เป็นแบบคู่ขนาน (Redundant System) เช่น ปรับปรุงอุปกรณ์ Emergency Stop จาก 1 Channel เป็น 2 Channel เพื่อให้ระบบมีความน่าเชื่อถือสูงขึ้น ดังรูปที่ 3.5
- ปรับปรุงโครงสร้างในส่วนของชุดเอาท์พุท (Output device) ให้เป็นแบบคู่ขนาน (Redundant System) เช่น ปรับปรุงอุปกรณ์ Magnetic Contactor จาก 1 ชุด เป็น 2 ชุด เพื่อให้ระบบมีความน่าเชื่อถือสูงขึ้นดังรูปที่ 3.5



รูปที่ 3.5 ระบบหยุดฉุกเฉิน Emergency Stop (หลังปรับปรุงค่าระดับความปลอดภัย)

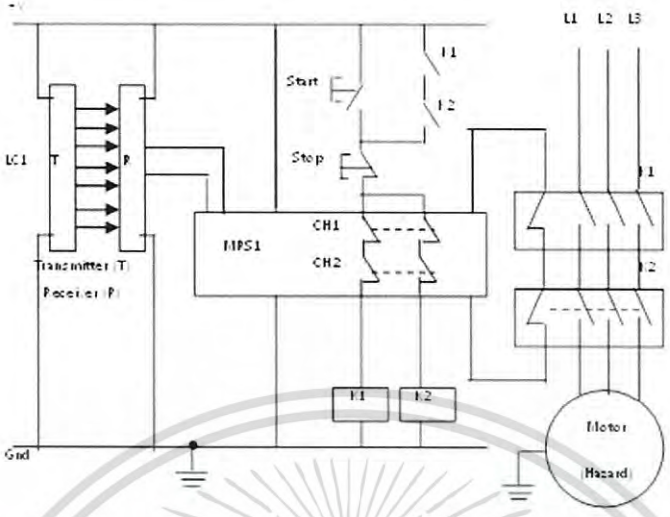
ฟังก์ชันการทำงานของระบบหยุดฉุกเฉิน Emergency Stop หลังจากปรับปรุงค่าระดับความปลอดภัย มีดังนี้ เมื่อมีการกดปุ่ม Emergency Stop (E1) ระบบจะสั่งตัดการทำงานของ Magnetic Contactor K1 และ K2 ทันที ดังนั้นความเสี่ยงจะถูกจัดการโดยการตัดแหล่งจ่ายพลังงานออกจากชุดขับเคลื่อน (Motor Unit) ในกรณีที่อุปกรณ์ในระบบเกิดความบกพร่อง (Component Failure) ไม่ว่าจะเป็นในส่วนของอินพุท (Emergency Stop) หรือเอาท์พุท (Magnetic Contactor) ชุดควบคุม (Processing Unit, MRS1) จะตรวจพบและสั่งหยุดการทำงานก่อนที่จะเกิดเหตุการณ์อันตราย ทำให้ผู้ปฏิบัติงานมีความปลอดภัยในการทำงาน

จากการประเมินค่าระดับความปลอดภัยของระบบหยุดฉุกเฉิน Emergency Stop หลังจากที่ได้ทำการปรับปรุงระบบ พบว่าระบบควบคุมความเสี่ยงของเครื่องจักร (SRP/CS) ที่ออกแบบด้วยโครงสร้าง Category 3 ให้ค่าระดับความปลอดภัย PLe และมีค่าโอกาสการล้มเหลวของระบบ (PFHDavg) เท่ากับ 4.73×10^{-8} ครั้งต่อชั่วโมงแสดงดังตารางที่ 3.1 โดยมีรายละเอียดการคำนวณแสดงดังภาคผนวก ค

3.5.2 ปรับปรุงระดับความปลอดภัยด้วยการติดตั้งระบบม่านแสงนิรภัย Safety Light Curtain

จาก 3.5.1 การปรับปรุงค่าระดับความปลอดภัยของระบบหยุดฉุกเฉิน Emergency Stop เพียงอย่างเดียวไม่เพียงพอที่จะจัดการกับความเสี่ยงที่เกิดขึ้นได้ เนื่องจากในกรณีที่ผู้ปฏิบัติงานไม่สามารถที่จะกดปุ่มหยุดฉุกเฉินได้ทันเวลา สามารถทำให้เกิดเหตุการณ์อันตรายต่อผู้ปฏิบัติงานได้ ดังนั้นการติดตั้งระบบม่านแสงนิรภัยจึงเป็นหนึ่งทางเลือกของการนำเทคโนโลยีด้านความปลอดภัยที่มีอยู่ในปัจจุบันมาใช้กับเครื่องจักรเก่าในกระบวนการสร้างยาง (Old Machinery of Tyre Building Process) เพื่อวัตถุประสงค์ในการจัดการกับความเสี่ยง ซึ่งในงานวิจัยนี้จะนำเสนอการติดตั้งระบบม่านแสงนิรภัยด้วยโครงสร้างแบบ Category 3 โดยมีรายละเอียด ดังนี้

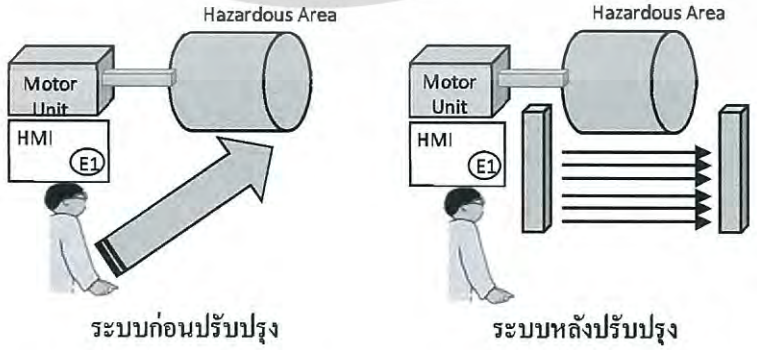
- ติดตั้งอุปกรณ์ควบคุม (Processing Unit) เพื่อทำหน้านี้ในการตรวจสอบความผิดปกติของอุปกรณ์ในกรณีที่เกิดความบกพร่อง (Detect component failure) เช่น Master Control Relay (MRS1) เพื่อให้ระบบมีความน่าเชื่อถือสูงขึ้น ดังรูปที่ 3.6
- ติดตั้งอุปกรณ์ม่านแสงนิรภัย Safety Light Curtain (LC1) เพื่อให้ระบบมีความน่าเชื่อถือสูงขึ้นดังรูปที่ 3.6
- ปรับปรุงโครงสร้างในส่วนของชุดเอาท์พุท (Output device) ให้เป็นแบบคู่ขนาน (Redundant System) เช่น ปรับปรุงอุปกรณ์ Magnetic Contactor จาก 1 ชุด เป็น 2 ชุด เพื่อให้ระบบมีความน่าเชื่อถือสูงขึ้นดังรูปที่ 3.6



รูปที่ 3.6 ระบบม่านแสงนิรภัย Safety Light Curtain (หลังปรับปรุงค่าระดับความปลอดภัย)

ฟังก์ชันการทำงานของระบบม่านแสงนิรภัย Safety Light Curtain หลังจากปรับปรุงค่าระดับความปลอดภัย มีดังนี้ เมื่อผู้ปฏิบัติงานเข้าไปยังพื้นที่อันตรายโดยผ่านระบบม่านแสงนิรภัย ระบบจะสั่งตัดการทำงานของ Magnetic Contactor K1 และ K2 ทันที ดังนั้นความเสี่ยงจะถูกจัดการโดยการตัดแหล่งจ่ายพลังงานออกจากชุดขับเคลื่อน (Motor Unit) ในกรณีที่อุปกรณ์ในระบบเกิดความบกพร่อง (Component Failure) ไม่ว่าจะเป็นในส่วนของอินพุท (Emergency Stop) หรือเอาท์พุท (Magnetic Contactor) ชุดควบคุม (Processing Unit, MRS1) จะตรวจพบและสั่งหยุดการทำงานก่อนที่จะเกิดอันตราย ทำให้ผู้ปฏิบัติงานมีความปลอดภัยในการทำงาน

จากการประเมินค่าระดับความปลอดภัยของระบบม่านแสงนิรภัย Safety Light Curtain หลังจากที่ได้ปรับปรุงระบบ จะพบว่าระบบควบคุมความเสี่ยงของเครื่องจักร (SRP/CS) ที่ออกแบบด้วยโครงสร้าง Category 3 ให้ค่าระดับความปลอดภัย PLe และมีค่าโอกาสการล้มเหลวของระบบ (PFHDavg) เท่ากับ 5.52×10^{-8} ครั้งต่อชั่วโมงแสดงดังตารางที่ 3.1 โดยมีรายละเอียดการคำนวณแสดงดังภาคผนวก ค



รูปที่ 3.7 ระบบก่อนปรับปรุงกับระบบหลังปรับปรุงค่าระดับความปลอดภัย

ตารางที่ 3.1 ระดับความปลอดภัยของระบบควบคุมความเสี่ยงดังรูปที่ 3.4, 3.5 และ 3.6 (โดยรายละเอียดการคำนวณแสดงดังภาคผนวก ค)

System	SRP/ CS	Cat.	B10d (cycles)	Working Day (days/year)	Activated of SRP/CS (cycle/day)	n_{op} (cycle/ year)	MTTFd (years)	MTTFd (avg.)	DC (%)	DC_{avg} (%)	CCF (points)	PL	PFHD (1/h)	$PFHD_{avg}$ (1/h)	*
รูปที่ 3.4	E1	Cat.1	100,000	365	3	1095	913	830	N/A	N/A	N/A	PLc	$1.14x10^{-6}$	$1.14x10^{-6}$	(1)
	K1	Cat.1	2,000,000	365	6	2190	9132		N/A		N/A				(1)
รูปที่ 3.5	E1	Cat.3	100,000	365	3	1095	913	761	90	90	85	PLe	$4.29x10^{-8}$	$4.73x10^{-8}$	(1)
	K1	Cat.3	2,000,000	365	6	2190	9132		90						(1)
	K2	Cat.3	2,000,000	365	6	2190	9132		90						(1)
	MRS1	Cat.4	N/A	N/A	N/A	N/A	355	355	N/A	N/A		PLe	$4.35x10^{-9}$		(2)
รูปที่ 3.6	LC1	Cat.4	N/A	N/A	N/A	N/A	20	20	N/A	N/A	85	PLe	$7.93x10^{-9}$	$5.52x10^{-8}$	(2)
	MRS1	Cat.4	N/A	N/A	N/A	N/A	355	355	N/A	N/A		PLe	$4.35x10^{-9}$		(2)
	K1	Cat.3	2,000,000	365	6	2190	9132	4566	90	90		PLe	$4.29x10^{-8}$		(1)
	K2	Cat.3	2,000,000	365	6	2190	9132		90						(1)

* Note:

(1) Means data of B10d refer from EN ISO 13849-1 [1] (Page 50, Table C.1) and calculation data of nop, MTTFd, DC, CCF and PFHD refer from method of standard EN ISO 13849-1 [1],

(2) Means that data of MTTFd, PL and PFHD refer from manufacturer datasheet.

บทที่ 4
บทสรุป

4.1 สรุปผลการดำเนินงาน

จากกรณีศึกษาเรื่องการประยุกต์ใช้งานมาตรฐานความปลอดภัยสากล EN ISO 12100 [2] และ EN ISO 13849-1 [1] ในการประเมินความเสี่ยงและลดความเสี่ยงของเครื่องจักรเก่าในกระบวนการสร้างยาง (Old Machinery of Tyre Building Process) โดยจุดเสี่ยงเลือกมาพิจารณาเป็นจุดที่มีความรุนแรงและความถี่ในการเกิดอันตรายสูงสุด ซึ่งอันตรายเกิดจากการหมุน การหนีบและการดึงของชุดขับเคลื่อนที่บริเวณชุดสร้างยาง ผลจากการประเมินความเสี่ยงด้วยวิธีกราฟความเสี่ยง (Risk graph method) พบว่าความเสี่ยงอยู่ในระดับที่สูง (High risk) และค่าระดับความปลอดภัยที่ต้องการในการจัดการกับความเสี่ยงมีค่า PLd หลังจากนั้นทำการประเมินค่าระดับความปลอดภัยของระบบควบคุมความเสี่ยง (SRP/CS) ของเครื่องจักร คือระบบหยุดฉุกเฉิน Emergency Stop ที่ออกแบบด้วยโครงสร้าง Category 1 พบว่ามีค่าระดับความปลอดภัย PLc และค่าโอกาสของการล้มเหลวของระบบ (PFHDavg) มีค่าเท่ากับ 1.14×10^{-6} ครั้งต่อชั่วโมงซึ่งการออกแบบระบบด้วยโครงสร้าง Category 1 จะทำให้ระบบมีความน่าเชื่อถือต่ำ (Low Reliability) เนื่องจากความน่าเชื่อถือของระบบจะขึ้นอยู่กับความน่าเชื่อถือของอุปกรณ์เพียงอย่างเดียวเท่านั้น (Reliability of components) ในกรณีที่อุปกรณ์เกิดความบกพร่อง (Component Failure) ระบบจะไม่สามารถจัดกับการความเสี่ยงได้

ดังนั้นทางทีมผู้ประเมินความเสี่ยงมีความเห็นตรงกันว่าต้องทำการปรับปรุงค่าระดับความปลอดภัยของระบบให้สูงขึ้น เพื่อให้ระบบมีความน่าเชื่อถือสูงขึ้น (High Reliability) โดยทำการปรับปรุงระบบหยุดฉุกเฉิน Emergency Stop ให้มีโครงสร้างแบบ Category 3 ผลจากการประเมินพบว่าระบบมีค่าระดับความปลอดภัยที่สูงขึ้น มีค่าเท่ากับ PLe และค่าโอกาสของการล้มเหลวของระบบ (PFHDavg) มีค่าเท่ากับ 4.73×10^{-8} ครั้งต่อชั่วโมงแต่การปรับปรุงระบบหยุดฉุกเฉิน Emergency Stop เพียงอย่างเดียวไม่เพียงพอที่จะจัดการกับความเสี่ยงได้จึงได้นำเทคโนโลยีปัจจุบันคือระบบม่านแสงนิรภัย (Safety Light Curtain) ที่มีโครงสร้างแบบ Category 3 มาติดตั้งเพื่อป้องกันการเกิดอันตรายในกรณีที่พนักงานต้องเข้าปฏิบัติงานยังพื้นที่เสี่ยงผลจากการประเมินพบว่าระบบมีค่าระดับความปลอดภัยที่สูงขึ้น PLe และค่าโอกาสของการล้มเหลวของระบบ (PFHDavg) มีค่าเท่ากับ 5.52×10^{-8} ครั้งต่อชั่วโมง

จากผลของการปรับปรุงค่าระดับความปลอดภัยของระบบด้วยการปรับปรุงระบบหยุดฉุกเฉิน Emergency Stop และการติดตั้งระบบม่านแสงนิรภัย (Safety Light Curtain) พบว่าค่าระดับความปลอดภัยรวมของระบบมีค่าเท่ากับPLe ซึ่งมีค่ามากกว่าค่าระดับความปลอดภัยที่ต้องการ PLd และค่าโอกาสของการล้มเหลวของระบบ (PFHDavg) อยู่ในระดับที่ยอมรับได้ (Acceptable level) จึงสรุปได้ว่าระบบสามารถที่จะจัดการกับความเสี่ยงที่เกิดขึ้นได้และสร้างสภาพแวดล้อมการทำงานที่ปลอดภัยให้กับพนักงาน

4.2 ข้อเสนอแนะ

ในปัจจุบันตัวอย่างการประยุกต์ใช้มาตรฐานความปลอดภัยสากลกับเครื่องจักรในอุตสาหกรรมยังมีอยู่ไม่มากและไม่ครอบคลุมในทุกอุตสาหกรรม อีกทั้งเนื้อหาและภาษาที่ใช้ในมาตรฐานความปลอดภัยสากลค่อนข้างยากที่จะทำความเข้าใจ ทางผู้วิจัยหวังเป็นอย่างยิ่งว่าในอนาคตทางองค์กรที่เกี่ยวข้องกับการกำหนดมาตรฐานควรจะมีการแสดงตัวอย่างของการนำมาประยุกต์ใช้ให้มากขึ้นหรือมีการจัดอบรม ให้ผู้ใช้งานมีความเข้าใจที่ถูกต้อง เพื่อเป็นการป้องกันไม่ให้เกิดความสับสนหรือการตีความหมายที่ผิดไปจากที่มาตรฐานกำหนด ซึ่งสิ่งเหล่านี้สามารถนำไปสู่การเกิดสถานการณ์ที่อันตรายต่อผู้ปฏิบัติงานได้

ในขณะที่มาตรฐานยังมีความคลุมเครือ ความรู้และประสบการณ์ของผู้เข้าร่วมประเมินจึงเป็นหนึ่งในตัวแปรสำคัญที่จะทำให้กระบวนการประเมินความเสี่ยงและลดความเสี่ยงของเครื่องจักรในทุกอุตสาหกรรมประสบความสำเร็จได้ โดยทีมผู้เข้าร่วมประเมินควรจะต้องประกอบด้วยพนักงานที่เกี่ยวข้องในทุกๆฝ่าย เช่น พนักงานฝ่ายผลิต ฝ่ายซ่อมบำรุง ฝ่ายประกันคุณภาพ ฝ่ายความปลอดภัย รวมทั้งผู้ออกแบบและผู้ผลิตเครื่องจักร เป็นต้น และต้องเป็นพนักงานที่มีความรู้ ความเข้าใจ และมีประสบการณ์เกี่ยวกับเครื่องจักรเป็นอย่างดี จึงจะสามารถประเมินความเสี่ยงได้อย่างครอบคลุมและเสนอมาตรการในการจัดการความเสี่ยงได้อย่างสมเหตุสมผลบนพื้นฐานของข้อเท็จจริง

อีกตัวแปรหนึ่งที่สำคัญในการออกแบบระบบควบคุมความเสี่ยง คือเรื่องของต้นทุน (Cost) ซึ่งเป็นตัวแปรสำคัญที่ควรนำมาพิจาณาด้วย ยิ่งออกแบบระบบให้มีความปลอดภัยมากเท่าไหร่ ยิ่งต้องใช้เงินในการลงทุนที่สูงมากขึ้นเท่านั้น จึงควรมีการพิจารณาหาจุดที่เหมาะสมในการลงทุนสำหรับการจัดการความเสี่ยงหรือลดความเสี่ยงลงให้อยู่ในระดับที่ยอมรับได้ (Eliminate/Reduce risk into acceptable level with optimized cost)

เอกสารอ้างอิง

[1] European Standard. "Safety of machinery –Safety-related parts of control systems – Part 1: General principles for design" **EN ISO 13849-1,** 2006.

[2] International Standard. "Safety of machinery – General principles for design – Risk assessment and risk reduction" **EN ISO 12100,** 2010.

[3] European Standard. "Safety of machinery – Safety related parts of control systems – General principles for design" **EN 954-1,** 1996.

[4] International Electrotechnical Commission. "Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems" **IEC 62061,** 2005.

[5] Takabumi Fukuda, Makoto Hirayama, Naoya Kasai, and Kazuyoshi Sekine. **"Evaluation of Operative Reliability of Safety-Related Part of Control System of Machine and Safety Level"** SICE Annual Conference, Kagawa University, Japan, September 2007.

[6] Patrick Lerévérend. **"Inside the Standardization Jungle: IEC 62061 and ISO 13849-1, Complementary or Competing ?"** Pepperl+Fuchs GmbH, Königsberger-Allee 85, Mannheim, Germany 2008.

[7] William E. Anderson. **"Risk Category 3 or 4 ?"** IEEE Transactions on Industry Applications, Vol. 46, No. 1, February 2010.

[8] Ernesto Soressi. **"Introduction in Safety Rules EN954-1, EN13849 and EN62061"** 5th IET International System Safety Conference, 18-20, Manchester, UK, October, 2010.

[9] Ernesto Soressi. **"Introduction of Safety Rule IEC EN62061 in Metal Industry"** IEEE International Conference on Automation Science and Engineering, Trieste, Italy - August, 2011.

[10] European Standard. "Safety requirements for hot flat rolling mills", **CEN EN 15093,** 2008.

[11] European Standard. "Safety requirement for tube forming and rolling mills and their finishing line equipment", **CEN EN 13675,** 2004.

[12] European Standard. "Safety requirements for strip processing line machinery and equipment", **CEN EN 15061,** 2007.

[13] International Standard. "Safety of machinery – Risk assessment – Part 1: Principles" **EN ISO 14121-1,** 2007.

[14] International Electrotechnical Commission. "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems" **IEC 61508,** 2001.

[15] International Standard. "Safety of machinery – Emergency stop function – Principles for design" **EN ISO 13850,** 2015.

[16] International Standard. "Safety of machinery – Interlocking devices associated with guards – Principles for design and selection" **EN 1088**, 2008.

[17] International Standard. "Safety of machinery – Two-hand control devices – Functional aspects. Principles for design" **EN 574**, 2008.

[18] International Standard. "Safety of machinery – Prevention of unexpected start-up" **EN 1037**, 2008.

[19] International Standard. "Safety of machinery – Electrical equipment of machines" **EN 60204**, 2005.

[20] N. Wongpiriyayothar, and S. Chitwong, "Implementation of International Safety Standard EN ISO 13849 into Machinery of Tyre Industry," **Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2017, 15-17 March, 2017, Hong Kong, pp632-637**

ภาคผนวก

ภาคผนวก ก บทความวิจัยที่ได้รับการตีพิมพ์
ภาคผนวก ข รายงานข้อมูลการเกิดอุบัติเหตุทางสถิติตั้งแต่ปี พ.ศ. 2551 ถึง พ.ศ. 2558
ภาคผนวก ค แสดงตัวอย่างการคำนวณ PL, PLr ของงานวิจัยที่นำเสนอ
ภาคผนวก ง ข้อมูลสนับสนุนการทำวิจัยอ้างอิงจากมาตรฐานสากล

ภาคผนวก ก

บทความวิจัยที่ได้รับการตีพิมพ์

บทความวิจัยที่ได้รับการตีพิมพ์ในวารสารทางวิชาการระดับนานาชาติในวิทยานิพนธ์นี้มี รายละเอียดดังต่อไปนี้

N. Wongpiriyayothar, and S. Chitwong, "Implementation of International Safety Standard EN ISO 13849 into Machinery of Tyre Industry," **Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2017, 15-17 March, 2017, Hong Kong, pp632-637**

Lecture Notes in Engineering and Computer Science

IMECS 2017

International MultiConference of Engineers and Computer Scientists 2017

Volume II

S. I. Ao
Oscar Castillo
Craig Douglas
David Dagan Feng
A. M. Korsunsky (Eds.)

Hong Kong
15-17 March, 2017

IA ENG
International Association of Engineers

ISBN: 978-988-14047-7-0
ISSN: 2078-0958

Implementation of International Safety Standard EN ISO 13849 into Machinery of Tyre Industry

N. Wongpiriyayothar, S. Chitwong

Abstract— **This paper presents application of international safety standard in risk assessment and risk reduction following by machinery directive. Many industries using machinery for manufacturing products have tendency to take risk from poor-quality of machinery design which may not be produced according to international safety standard. This can lead dangerous situation to machine user. The new standard EN ISO 13849-1 [1] which replaced the old standard EN 954-1 [2] definitely in December 2011 made machine designer not be familiar with the new concept and feel confused due to most of concerned parameters shown in term of statistic value that there are difficulty in interpretation and understanding. In the present, there is still lack of examples of implementation this standard into machinery of specific industry, especially in tyre industry. Therefore the objective of this paper is made for implementation this safety standard into machinery of tyre industry in order to build a safe situation for machine user.**

Keywords— **Safety-Related Parts of Control System (SRP/CS), Performance Level (PL), Mean Time to Dangerous Failure (MTTFd), Common Cause Failure (CCF), Diagnostic Coverage (DC).**

I. Introduction

TYRE industry machinery processes starting from mixing process of raw material, preparing process of material, tyre building process, tyre curing process and final inspection process respectively which all processes caused unsafe situation to machine user, especially in tyre building process that most of unsafe situations came from pinch point and rotation point of automatic building unit in front of machine.

Most of machineries in tyre industry are automation machine using safety control circuits in order to prevent entering to moving part of machine and/or to prevent unexpected starting up of machine by generating stop function to hold machine in safe stage. The well-known safety rule explained about procedure of risk assessment and risk reduction is EN ISO 12100 [3] following five-step method, i.e. (1) determination of the limits of the machinery , (2) hazard identification, (3) risk estimation, (4) risk evaluation, and (5) risk reduction. In the risk reduction process consisting of three-step method which all suitable protective measures must be followed, i.e. first step, inherently safe design measures, second step, safeguarding and/or complementary protective measures, the last step, information for uses.

Manuscript received December 22, 2016; revised January 12, 2017. N. Wongpiriyayothar and S. Chitwong are with the department of Instrumentation and Control Engineering, King Mongkut's Institute of Technology Ladkrabang, Ladkrabang, Bangkok 10520 THAILAND. (e-mail : engineer_napat1@hotmail.com, sakreya.ch@kmitl.ac.th)

Therefore, the machine designer must eliminate hazard and/or reduce risks as much as possible by following three-step method of risk reduction process respectively in order to let machine perform safety function effectively and to provide safe situation for machine user.

This paper mainly focuses on the second step of risk reduction process that this part was regarded as belonging to standard EN ISO 13849 [1]. Thus, the purpose of this paper is to review and verify design of safety function of old machinery in tyre industry by comparing PLr (Performance level required) to PL (Performance level designed). If PL is greater than or equal to PLr (PL $\geq$ PLr), it means that machine can guarantee to perform the safe stage and meet requirement with design principles of international safety standard, on the other hand, if the verification result does not meet with requirement. What does machine designer need to do to eliminate hazard. These will be more explained in this paper.

II. Background of Machinery Safety Standard

A. EN 954-1

In the past, the well-known machinery safety standard EN 954-1 [2] was introduced in 1996 which this version is familiar to most of machine designers and is used in many automation industrials broadly, especially in European region. This standard defined Safety Categories to manage fault under foreseeable condition to prevent loss of safety function. These categories are divided into five levels, termed Categories B, 1, 2, 3 and 4 which Cat-4 can provide the highest safety level with redundant configuration. The procedure of this standard is quite simple and easy to understand for machine designer due to most of concerned criteria that are presented in term of deterministic approach following these steps, i.e. firstly identify safety function required to eliminate hazard, secondly consider whether fault condition can lead to loss of safety function or not and finally select safety category to manage fault condition.

B. EN ISO 13849-1

Standard EN ISO 13849-1 [4] was introduced first time in 1999 (original version), then was revised in 2006 (second version, [1]). The purpose of this standard is to replace the old standard EN 954-1 [2] which is going to be retired in December 2011. The concept of this standard is not only focusing on the deterministic approach (Category), but also statistic approach (PL, MTTFd, CCF and DC). Moreover, there is determining the designated architectures of category to perform a safety function which may be implemented by one or more SRP/CS. Combination of SRP/CS to perform a safety function (see Figure 1) consisting of input (SRP/CS_a),

logic/processing (SRP/CS_b), output/power control elements (SRP/CS_c) and interconnecting means (i_{ab}, i_{bc}). However, this standard is quite difficult to understand for machine designers due to most of concerned criteria and calculated parameters presented in term of both deterministic and statistic approach leading most of them to use some kind of commercial computerization program to provide the quick result without understanding the basic principle in calculation and source of those formulas having an effect on poor quality in risk reduction process. Thus, these will be introduced in the next part of this paper to be the guideline and overview for general principles of this standard.

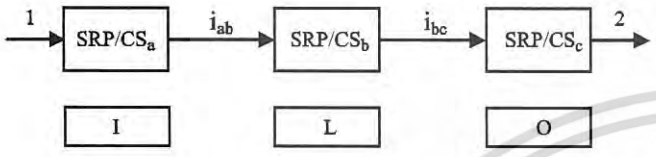


Figure 1 — Diagrammatic presentation of combination of safety-related parts of control systems for processing typical safety function

III. General Principles of EN ISO 13849-1

A. Overview

The purpose of this international safety standard is to provide machine designers, machine developers and machine manufacturers with an overall scope and guideline for design safety-related parts of control system (SRP/CS). The ability of safety-related parts of control systems is to perform a safety function under foreseeable conditions classified into five levels, called performance levels (PL) in term of PL a, b, c, d and e. These performance levels are defined in terms of probability of dangerous failure per hour (PFHD), (see Table I). The probability of dangerous failure of the safety function depends on several factors, consisting of designated architecture of SRP/CS (Category), reliability of components (MTTFd, CCF), fault detection of mechanisms (DC), design process, operating stress, environmental conditions and operation procedures. In order to achieve PL, the concept of this standard based on the categorization of structures following specific design criteria and specific behaviors under fault conditions. These categories are classified into five levels, termed Categories B, 1, 2, 3 and 4. For example of SRS/CS (input elements: interlocking devices, electro-sensitive protective devices, pressure sensitive devices...etc.), (logic elements: Program Logic Controller devices (PLC), Monitoring System, Data Processing Unit...etc.), and (output elements: Contactors, Relays, Valves...etc.).

TABLE I — CLASSIFICATION OF PERFORMANCE LEVELS (PL)

PL	Average probability of dangerous failure per hour (PFHD) (1/h)
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

NOTE Besides the average probability of dangerous failure per hour other measures are also necessary to achieve the PL

This standard is developed to provide a clear cut concept in application of SRP/CS on machinery which can be assessed and audited by third party to certify whether safety function was designed correctly according to machinery directive or not.

B. Concept of EN ISO 13849-1

After we completed in risk assessment and risk reduction following EN ISO 12100 [3] if the result of risk reduction is required to implement protective measures on machinery in order to eliminate hazard and/or reduce risk. This will lead to part of EN ISO 13849-1 [1] which concerns with general principles for design of SRP/CS. Then, the iterative process for design of SRP/CS shall be followed according to EN ISO 13849-1 [1] (Page 13, Figure 3) following these steps, i.e. (1) identify the safety functions to be performed by SRP/CSs, (2) determined the required performance level (PLr), (3) design safety function and identify SRP/CS to carry out safety function, (4) evaluate PL by considering Category, MTTFd, DC and CCF, (5) verify PL of safety function (PL $\geq$ PLr or not), (6) validate (meet with all requirements or not) sequentially. In step (5) and (6), if verification and validation step did not meet with requirement, this iterative process should be reconsidered.

Determination of PLr by Risk Graph Method

Risk Graph Method is part of standard EN ISO 13849-1 [1], using in determining PLr for each safety function to be carried out by SRP/CS (see Figure 2). There are concerned parameters using in estimation of risk following these, i.e. Severity of injury represented by S "(S1, slight injury), (S2, serious injury)", Frequency/Exposure of hazard represented by F "(F1, seldom happened/exposure time is short), (F2, continuously happened/exposure time is long)", Possibility of avoiding hazard/limiting harm represented by P "(P1, possible under specific condition), (P2, impossible)", and point number 1 is starting point of this method. Thus, the result of this method will let us know the level of risk (low, medium or high) and required PLr in selection each SRP/CS to perform safety function. This method given here is to provide as the guideline concept to machine designer in estimation of risk.

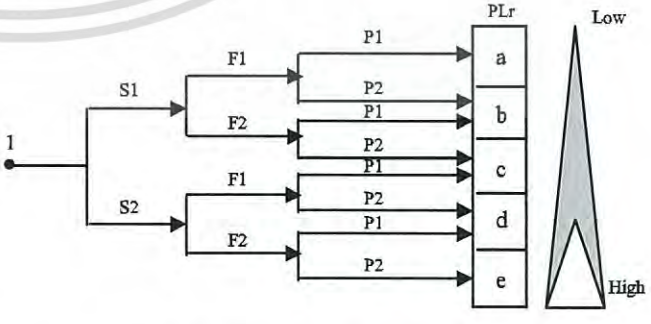


Figure 2 — Risk Graph for determining required PLr for safety function

C. Evaluation of PL by Category, MTTFd, DC and CCF

The ability of SRP/CS to perform safety function shall be expressed through PL and determined by estimation following these aspects: *(1) Category, (2) MTTFd, (3) DC and (4) CCF.*

(1) Category

System requirement and system behavior to withstand fault condition are explained in term of Categories. SRP/CS shall be met with requirement of one of the five categories, termed Categories B, 1, 2, 3 and 4 (see Figure 3, 4, 5 and 6).

Category B is the basic category in which occurrence of fault can lead to the loss of safety function. This category provides the lowest safety level.

Category 1 is developed from Cat-B in which the occurrence of a fault can lead to the loss of safety function, but the ability to withstand fault is higher than Cat-B by using the concept of selection and implementation of well-tried components and well-tried safety principles.

Category 2 is required to apply Cat-B and Cat-1. In addition, the safety function shall be checked by machine control system periodically in which the occurrence of a fault can lead to the loss of safety function during checking period and the loss of safety function can be detected by the check.

Category 3 is required to apply Cat-B and Cat-1. In addition, safety-related parts shall be designed to ensure that single fault cannot lead the loss of safety function and single fault will be detected properly in case of reasonable practice in which the occurrence of the accumulated fault can lead to the loss of safety function.

Category 4 is required to apply Cat-B and Cat-1. In addition, safety-related parts shall be designed to ensure that single fault and accumulated fault cannot lead to the loss of safety function and the fault will be detected in time to prevent the loss of safety function. This category provides the highest safety level. For more explain in detail of categories are provided in EN ISO 13849-1 [1] (Page 38, Table 10 – summary of requirements for categories).

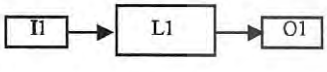


Figure 3

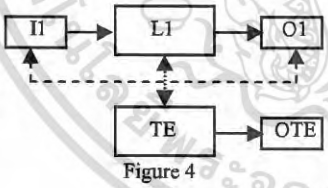


Figure 4

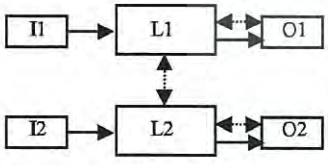


Figure 5

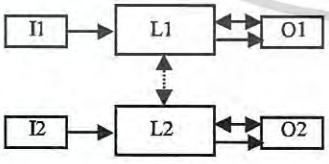


Figure 6

Figure 3 — Designated architecture for category B and category 1
Figure 4 — Designated architecture for category 2
Figure 5 — Designated architecture for category 3
Figure 6 — Designated architecture for category 4

(2) MTTFd (Mean time to dangerous failure)

MTTFd is classified into three levels (low, medium and high). This value describes the failure rate of component (reliability of component) in unit of years. The lowest MTTFd is 3 years and the highest MTTFd is 100 years to be taken into account (see Table II).

TABLE II — MEAN TIME TO DANGEROUS FAILURE OF EACH CHANNEL (MTTFd)

Denotation of each channel	Range of each channel
Low	3 years ≤ MTTFd < 10 years
Medium	10 years ≤ MTTFd < 30 years
High	30 years ≤ MTTFd ≤ 100 years

Calculating or Evaluating MTTFd for single components

To evaluate the statistic value of MTTFd for each component, these value can be referred from standard value of components which are manufactured according to basic and well-tried safety principles as shown in EN ISO 13849-1 [1] (Page 50–56, Table C.1-C.7) or can be calculated from B_{10d}, this is another statistic parameter provided by suppliers that they need to evaluate and declare into manufacturer data sheet. For terminology (see Table III).

Calculation of MTTFd from B_{10d} can be referred from these formulas; "(1)" and "(2)".

$$MTTFd = \frac{B_{10d}}{0.1x(n_{op})} \quad (1)$$

$$n_{op} = \frac{(d_{op})x(h_{op})x3{,}600\,(s/h)}{t_{cycle}} \quad (2)$$

TABLE III - TERMINOLOGY

Symbol	Definition of abbreviate word
n_{op}	The mean number of annual operations.
d_{op}	The mean operation, in days per year.
h_{op}	The mean operation, in hours per day.
B_{10d}	The mean number of cycles until 10% of components failure dangerously.
t_{cycle}	The mean time between the beginning of two successive cycles of the component. (e.g. switching of a valve) in seconds per cycle.

Calculating or Evaluating MTTFd for each channel

The MTTFd values of all single components which are part of the channel can be calculated by formula "(3)".

$$\frac{1}{MTTFd} = \frac{1}{MTTFd_{\,1}} + \frac{1}{MTTFd_{\,2}} + \ldots \frac{1}{MTTFd_{\,n}} \quad (3)$$

(3) DC (Diagnostic coverage)

The diagnostic coverage is ratio between failure rate of dangerous failure that can be detected and failure rate of total dangerous failure (total dangerous failure consists of dangerous failure which can be detected and cannot be detected). The DC is presented in term of statistic value to measure effectiveness of diagnostics, classified into four levels (see Table IV). DC can be estimated from EN ISO 13849-1 [1] (Page 59–61, Table E.1).

TABLE IV — DIAGNOSTIC COVERAGE (DC)

Denotation	Range
None	DC < 60 %
Low	60% ≤ DC < 90%
Medium	90% ≤ DC < 99%
High	99% ≤ DC

For SRP/CS consisting of several parts, DC can be estimated by an average value of DC, so-called DC_{avg} and can be calculated by formula "(4)".

$$DC_{avg} = \frac{\frac{DC_1}{MTTFd_1} + \frac{DC_2}{MTTFd_2} + \dots \frac{DC_n}{MTTFd_n}}{\frac{1}{MTTFd_1} + \frac{1}{MTTFd_2} + \dots \frac{1}{MTTFd_n}} \quad (4)$$

(4) CCF (Common cause failure)

CCF concept is to provide a checklist to let machine designer take into account to evaluate whether common problem had already been solved or not following check list in EN13849-1 [1] (Page 63, Table F.1). Maximum of evaluation score is 100 points. If evaluation score is less than 65 points, means that does not meet with requirement. Thus, machine designer should select appropriate measures to improve this factor to get score higher than 65 points.

Evaluation of PL

After completed in considering of Category, MTTFd, DC and CCF, then machine designer can evaluate PL of SRP/CS by following EN ISO 13849-1 [1] (Page 81-82, Table K.1). To meet with requirement, machine designer has to verify that PL is greater than or equal to PLr. In case of PL is less than PLr, the iterative process should be reconsidered.

IV. EXAMPLE OF IMPLEMENTATION

Life time to review and verify risk assessment of old machinery in tyre industry will be conducted every 5 years periodically in order to ensure whether safety function work properly according to concept of international safety standard or not by using *Risk Graph Method* to determine PLr and compare with PL. If PL is greater than or equal to PLr (PL $\geq$ PLr), this can guarantee that safety function meet with requirement but if PL is less than PLr (PL < PLr), then safety function and design feature of machinery must be reconsidered.

The old tyre building machine was reviewed following period of 5 years. For the required participants to verify risk assessment consist of machine designer, machine user (e.g. maintenance member, operation member, tooling change member and quality assurance member) and site safety officer to brainstorm any ideas in risk assessment and risk reduction to eliminate hazardous situation and/or reduce risk as much as possible.

V. RESULT OF RISK ASSESSMENT AND RISK REDUCTION

Risk of tyre building machine concerned with *Pinch Point* and *Rotation Point* of automatic building unit in front of machine (see Figure 7). The result of risk assessment following risk graph method which was evaluated by concerned participants is S2, F2, and P1. Thus, PLd is required for eliminating hazardous situation.

After completed in risk assessment process of old tyre building machine, we found 2 points of SRP/CS must be improved following second step of risk reduction process by implementing of safeguarding and complementary protective measures that consist of First point, upgrading system of emergency stop is needed due to the original design of this system was designed by category-1 (see Figure 9) which provided only PLc (not meet requirement with PLd), and Second point, implementing system of safety light curtain is needed due to the original design of this system was designed without protective measures in front of automatic building unit that can lead to unsafe situation when maintenance member access to dangerous zone to repair machine or operator access to verify specification of product or quality assurance member access to verify quality of product or tooling change member access to change equipment for producing the new size of tyre following daily production planning …etc. All of these behaviors have a chance to take risk from unexpected start-up of machine function and cause of serious injury eventually.

Therefore, these 2 points must be improved in order to eliminate hazardous situation and/or reduce risk.

VI. VERIFICATION PL OF SAFETY FUNCTION

A. Original design of emergency stop system (see Figure 9)

Safety function explanation:

- When emergency stop device E1 was activated, control voltage of contactor K1 will be interrupted and de-energized power out of movement part (Motor). Then, hazardous situation of will be eliminated.
- This was designed by category-1 that cannot maintain all component failures. Safety function depends on reliability of components only. There is no implementing of fault detection that can lead to the loss of the safety function.
- The stopping function of emergency stop device is implementing of complementary protective measure to hazardous area.

Design feature:

- Meet requirement with category-B, implement of well-tried components and well-tried safety principles.
- Design of the closed-circuit current and earth connection regard to well-tried safety principles concept.
- Selection of emergency stop device E1 regards to well-tried components concept in according with IEC 60947-5-1 [5].
- Selection of contactor K1 regards to well-tried components concept in according with table D.4 of EN ISO 13849-2 [6].
- Wiring control signal to contactor in according with stop category type 0 of EN 60204-1 [7].

Result of PFHD and PL:

- MTTFd was calculated by emergency stop E1 is standard emergency stop device according to table C.1 of EN ISO 13849-1 [1], the life time of switching operation (B_{10d}) is 100,000 cycles and to be activated 3 times per day before starting each shift following standard operation procedure for testing safety device (3 shifts/day, 365 working day/year), Therefore n_{op} is 1,095 cycles/year and MTTFd is 913 years.
- MTTFd was calculated by contactor K1 according to table C.1 of EN ISO 13849-1 [1], B_{10d} is 2,000,000 cycles and start/stop to be activated 6 times/day before starting/stopping of each shift (3 shifts/day , 365

working days/year), Therefore n_{op} is 2,190 cycles/year and MTTFd is 9,132 years.
- PL was defined by using $MTTFd_{avg}$ between E1 and K1 which is 830 years (consider at maximum value 100 years, high) and designated architecture which is category-1 according to Table K.1 of EN ISO 13849-1 [1], therefore the PFHD of this system is $1.14x10^{-6}$ per hour. *This corresponds to PLc.*

B. Upgrading design of emergency stop system (see Figure 10)

Safety function explanation:
- When emergency stop device E1 was activated, control voltage of contactor K1 and K2 will be interrupted and de-energized power out of movement part (Motor). Then, hazardous situation will be eliminated.
- This was designed by category-3 that both feedback signal of emergency stop E1 and feedback signal of redundant contactors K1, K2 were monitored by the monitoring safety relay (MSR1). But this cannot maintain an accumulation of undetected faults that can lead to the loss of the safety function.
- The stopping function of emergency stop device is implementing of complementary protective measure to hazardous area.

Design feature:
- Meet requirement with category-B, implement of well-tried components and well-tried safety principles.
- Design of the closed-circuit current and earth connection regard to well-tried safety principles concept.
- Selection of emergency stop device E1 regards to well-tried components concept in according with IEC 60947-5-1 [5].
- Selection of contactor K1, K2 regards to well-tried components concept in according with table D.4 of EN ISO 13849-2 [6].
- The monitoring safety relay (MSR1) meet requirement with category-4, PLe, MTTFd is $4.35x10^{-9}$ per hour according to manufacturer datasheet.

Result of PFHD and PL:
- MTTFd calculated by emergency stop E1, is 913 years (Same concept as previous mentioned).
- MTTFd calculated by contactor K1, is 9,132 years. (Same concept as previous mentioned).
- MTTFd calculated by contactor K2, is 9,132 years. (Same concept as previous mentioned).
- DC_{avg} and CCF are relevant in category-3, Therefore DC_{avg} of E1 and K1, K2 are 90% according to table E.1 of EN ISO13849-1 [1] and CCF of this system are 85 according to table F.1 of EN ISO 13849-1 [1].
- PL was defined by using $MTTFd_{avg}$ between E1 and K1, K2 which is 761 years (consider at maximum value 100 years, high) and designated architecture which is category-3 and DC_{avg} is 90% (medium) according to Table K.1 of EN ISO 13849-1 [1], PFHD is $4.29x10^{-8}$ per hour. Following additional of subsystem MSR1that PFHD is $4.35x10^{-9}$ per hour. Therefore the average PFHD of this system is $4.73x10^{-8}$ per hour. *This corresponds to PLe.*

C. Implementing of protective measure by safety light curtain system (see Figure 11)

Safety function explanation:
- When safety light curtain device (LC1) was activated, control voltage of contactor K1 and K2 will be interrupted and de-energized power out of movement part (Motor). Then, hazardous situation will be eliminated.
- This was designed by category-3 that both feedback signal of safety light curtain device (LC1) and feedback signal of redundant contactors K1, K2 were monitored by MSR1. But this cannot maintain an accumulation of undetected faults that can lead to the loss of the safety function.
- The stopping function of safety light curtain device (LC1) is implementing of complementary protective measure to hazardous area.

Design feature:
- Meet requirement with category-B, implement of well-tried components and well-tried safety principles.
- Design of the closed-circuit current and earth connection regard to well-tried safety principles concept.
- Selection of contactor K1, K2 regards to well-tried components concept in according with table D.4 of EN ISO 13849-2 [6].
- The monitoring safety relay (MSR1) meet requirement with category-4, PLe, MTTFd is $4.35x10^{-9}$ per hour according to manufacturer datasheet.
- The safety light curtain device (LC1) meet requirement with category-4, PLe, MTTFd is $7.93x10^{-9}$ per hour according to manufacturer datasheet.

Result of PFHD and PL:
- MTTFd calculated by contactor K1, is 9,132 years. (Same concept as previous mentioned).
- MTTFd calculated by contactor K2, is 9,132 years. (Same concept as previous mentioned).
- DC_{avg} and CCF are relevant in category-3, Therefore K1 and K2 are 90% according to table E.1 of EN ISO13849-1 [1] and CCF of this system are 85 according to table F.1 of EN ISO 13849-1 [1].
- PL was defined by using $MTTFd_{avg}$ between K1 and K2 which is 4,566 years (consider at maximum value 100 years, high) and designated architecture which is category-3 and DC_{avg} is 90% (medium) according to Table K.1 of EN ISO 13849-1 [1], PFHD is $4.29x10^{-8}$ per hour. Following additional of subsystem MSR1that PFHD is $4.35x10^{-9}$ per hour and LC1 that PFHD is $7.93x10^{-9}$ per hour. Therefore the average PFHD of this system is $5.52x10^{-8}$ per hour. *This corresponds to PLe.*

VII. SUMMARY AND CONCLUSION

From the result of risk assessment of the old tyre building machine, the result showed that PLd is required to eliminate hazardous situation and/or reduce risk. However, not only the original design of emergency stop system (see Figure 9) that provide PLc is not enough to reduce risk, but also there are lacking of protective measure in front of hazardous area that can lead unsafe situation to machine user. Therefore the

purpose of this paper is want to implement SRP/CS by upgrading design of emergency stop system (see Figure 10) and implementing of protective measure by safety light curtain system (see Figure 11) following international safety standard requirement. Both of these systems provide PLe (see Table V) which is more than enough to reduce risk and can ensure that machine will be able to perform safe stage and build safe situation for machine user (see Figure 8).

By the writer's opinions and experiences, all processes of risk assessment and risk reduction are not easy to achieve and get more effective result. The important parameters which need to be taken into account are experience and knowledge of participants who involved in this activity. If they are lack all of these, they cannot identify "where are the risk points which need to be eliminated" and cannot offer any improvement idea "how to develop SRP/CS to eliminate hazardous situation". Therefore, in order to get more effective result the chairman and/or project leader should require concerned participants who have an experience related with machinery up to 5 years in different domains to do this activity. Machine designer is not only the person in charge of this activity, but other domains also are essential to exchange any different point of view in eliminating risk and optimization of investment cost should be considered also.

REFERENCES

[1] ISO 13849-1:2006, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design.
[2] CEN EN 954-1:1996, Safety-related parts of control systems.
[3] ISO 12100:2010, Safety of machinery — General principles for design — Risk assessment and risk reduction.
[4] ISO 13849-1:1999, Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design.
[5] IEC 60947-5-1:2003, Low-voltage switchgear and controlgear – Part 5: Control circuit devices and switching elements – Section 1: Electromechanical control circuit devices.
[6] EN ISO 13849-2:2010, Safety of machinery - Safety-related parts of control systems - Part 2: Validation
[7] EN 60204-1:2009, Safety of machinery – Electrical equipment of machines – Part 1: General requirements
[8] BGIA Report 2:2008, Functional safety of machine controls – Application of EN ISO 13849.

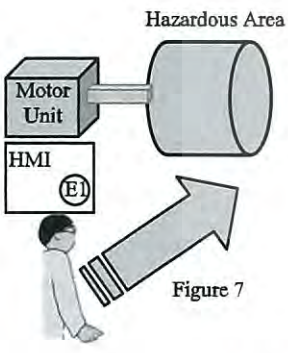


Figure 7

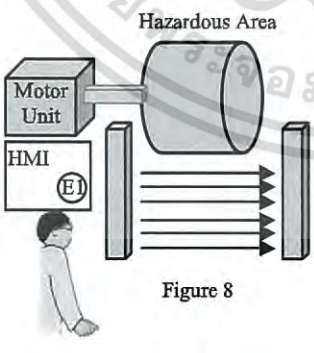


Figure 8

Figure 7 — Hazardous situation from pinch and rotation point
Figure 8 — Implemented of SRP/CS to eliminate hazardous situation

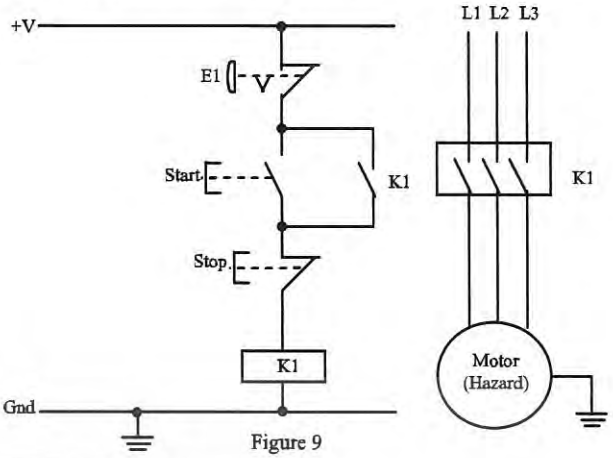


Figure 9

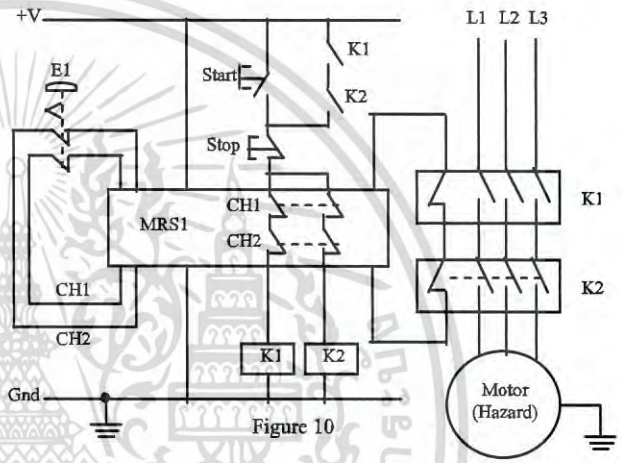


Figure 10

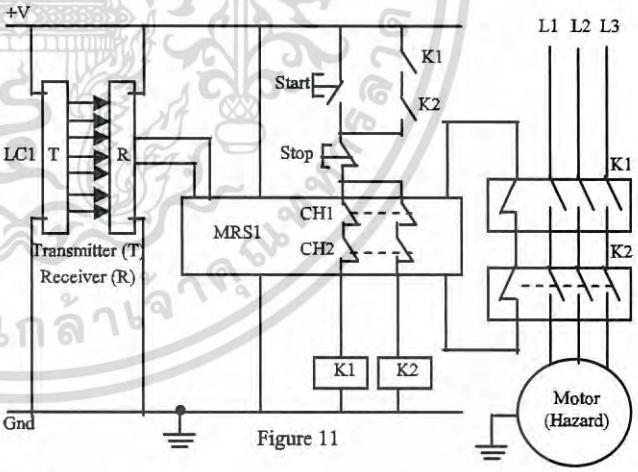


Figure 11

Figure 9 — Original design of emergency stop system
Figure 10 — Upgrading design of emergency stop system
Figure 11 — Implementing of protective measure by safety light curtain

TABLE V — EVALUATION RESULT OF PL AND $PFHD_{avg}$ OF EACH SYSTEM BY CATEGORY, MTTFd, DC AND CCF

System	SRP/CS	Cat.	B10d (cycles)	Working Day (days/year)	Activated of SRP/CS (cycle/day)	n_{op} (cycle/year)	MTTFd (years)	MTTFd (avg.)	DC (%)	DC_{avg} (%)	CCF (points)	PL	PFHD (1/h)	$PFHD_{avg}$ (1/h)	*
Figure 9	E1	Cat.1	100,000	365	3	1095	913	830	N/A	N/A	N/A	PLc	$1.14x10^{-6}$	$1.14x10^{-6}$	(1)
	K1	Cat.1	2,000,000	365	6	2190	9132		N/A		N/A				(1)
Figure 10	E1	Cat.3	100,000	365	3	1095	913	761	90	90	85	Ple	$4.29x10^{-8}$	$4.73x10^{-8}$	(1)
	K1	Cat.3	2,000,000	365	6	2190	9132		90						(1)
	K2	Cat.3	2,000,000	365	6	2190	9132		90						(1)
	MRS1	Cat.4	N/A	N/A	N/A	N/A	355	355	N/A	N/A		Ple	$4.35x10^{-9}$		(2)
Figure 11	LC1	Cat.4	N/A	N/A	N/A	N/A	20	20	N/A	N/A	85	Ple	$7.93x10^{-9}$	$5.52x10^{-8}$	(2)
	MRS1	Cat.4	N/A	N/A	N/A	N/A	355	355	N/A	N/A		Ple	$4.35x10^{-9}$		(2)
	K1	Cat.3	2,000,000	365	6	2190	9132	4566	90	90		Ple	$4.29x10^{-8}$		(1)
	K2	Cat.3	2,000,000	365	6	2190	9132		90						(1)

* **Note:** (1) Means that data of B10d refer from EN ISO 13849-1 [1] (Page 50, Table C.1) and calculation data of nop, MTTFd, DC, CCF and PFHD refer from method of standard EN ISO 13849-1 [1], (2) Means that data of MTTFd, PL and PFHD refer from manufacturer datasheet.

ภาคผนวก ข

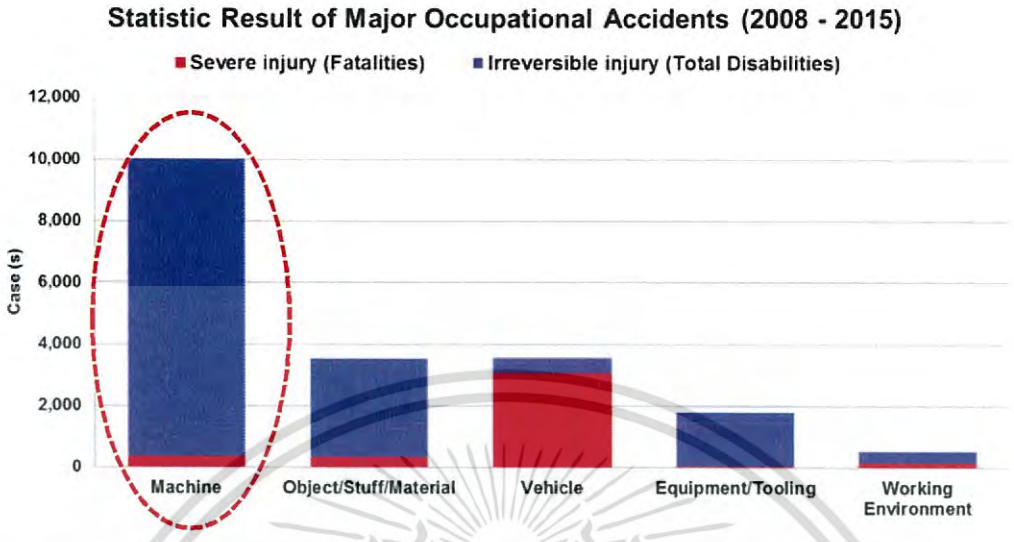
รายงานข้อมูลการเกิดอุบัติเหตุทางสถิติตั้งแต่ปี พ.ศ. 2551 ถึง พ.ศ. 2558

จากค่าสถิติการเกิดอุบัติเหตุที่มาจาก 5 สาเหตุหลักๆ ในประเทศไทยตั้งแต่ปี พ.ศ. 2551 ถึง พ.ศ. 2558 แสดงดังตารางที่ ข1 พบว่าสาเหตุหลักๆที่ทำให้พนักงานได้รับอันตรายมาจากเครื่องจักร วัตถุ/สิ่งของ ยานพาหนะ เครื่องมือและสิ่งแวดล้อมเกี่ยวกับการทำงาน ซึ่งสาเหตุที่ทำให้ได้รับบาดเจ็บ สูญเสียอวัยวะและถึงขั้นเสียชีวิตมาจากเครื่องจักรเป็นส่วนใหญ่ เมื่อพิจารณาค่าทางสถิติ ดังแสดงในรูป ข1 – ข3 พบว่าอัตราการเกิดอุบัติเหตุเนื่องจากเครื่องจักรไม่ได้มีแนวโน้มที่ลดลง

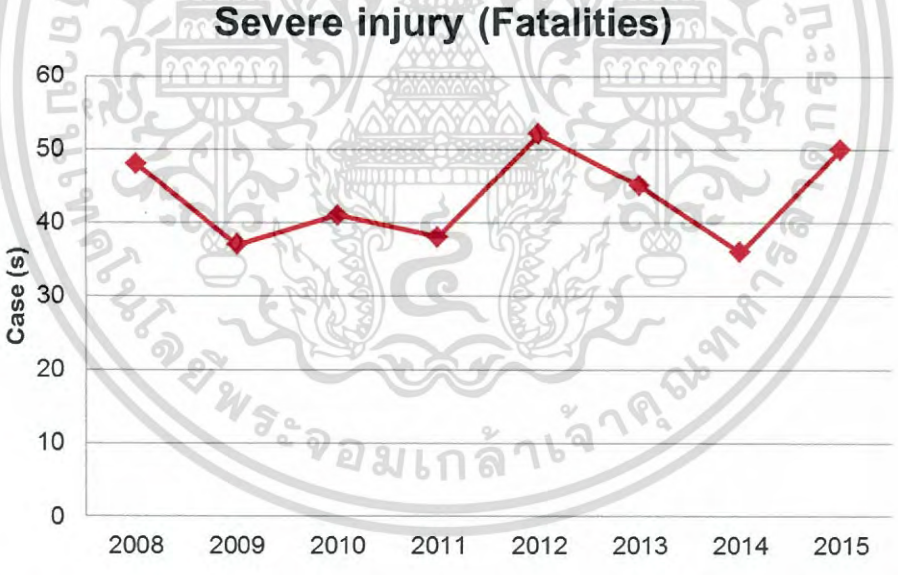
ดังนั้นงานวิจัยนี้จัดทำขึ้นเพื่อที่จะศึกษามาตรฐานความปลอดภัยสากลในการประเมินความเสี่ยงและลดความเสี่ยง เพื่อเป็นตัวอย่างของการประยุกต์ใช้กับเครื่องจักรในภาคอุตสาหกรรมอื่นๆ โดยหวังว่าในอนาคตสถิติของการเกิดอุบัติเหตุจากเครื่องจักรจะมีแนวโน้มที่ลดลง

ตารางที่ ข1 ค่าสถิติการเกิดอุบัติเหตุที่มาจาก 5 สาเหตุหลักๆ ในประเทศไทยตั้งแต่ปี พ.ศ. 2551 ถึง พ.ศ. 2558 (อ้างอิงจาก: สำนักงานกองทุนเงินทดแทน สำนักงานประกันสังคมกระทรวงแรงงานประไทย)

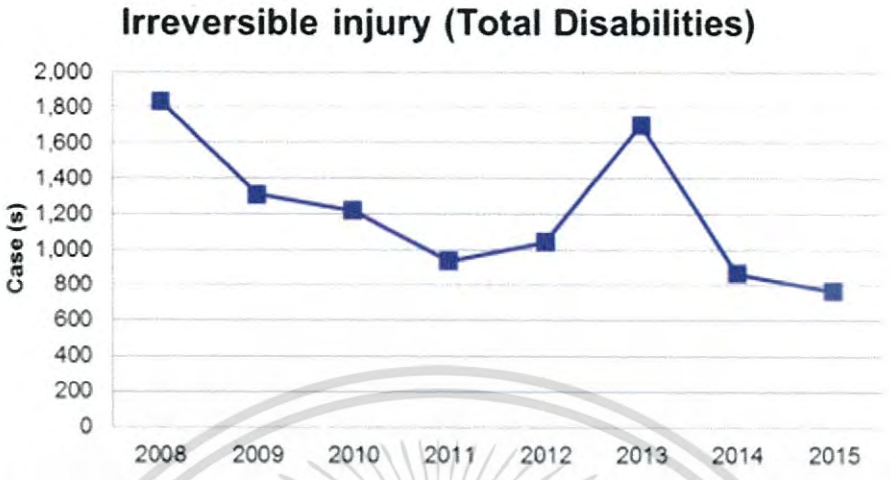
พ.ศ.	สิ่งที่ทำให้ประสบอันตราย	ตาย (คน)	ทุพพลภาพ (คน)	สูญเสียอวัยวะ (คน)	หยุดงานเกิน 3 วัน (คน)	หยุดงานไม่เกิน 3 วัน (คน)
2551	เครื่องจักร	48	2	1835	10011	11531
	วัตถุหรือสิ่งของ	30	0	670	16593	64775
	ยานพาหนะ	314	5	79	3850	4607
	เครื่องมือ	3	0	337	6311	15598
	สิ่งแวดล้อมเกี่ยวกับการทำงาน	8	2	65	3143	10230
2552	เครื่องจักร	37	1	1311	8091	9171
	วัตถุหรือสิ่งของ	34	1	558	14469	53163
	ยานพาหนะ	304	2	62	3547	4378
	เครื่องมือ	1	0	263	5547	13044
	สิ่งแวดล้อมเกี่ยวกับการทำงาน	13	0	70	2930	8828
2553	เครื่องจักร	41	2	1220	8408	9364
	วัตถุหรือสิ่งของ	49	2	488	14885	51924
	ยานพาหนะ	297	3	66	3452	3964
	เครื่องมือ	6	0	227	5331	12577
	สิ่งแวดล้อมเกี่ยวกับการทำงาน	27	1	50	2941	8300
2554	เครื่องจักร	38	1	938	7612	8357
	วัตถุหรือสิ่งของ	39	0	377	13468	45442
	ยานพาหนะ	303	1	46	3063	3482
	เครื่องมือ	3	0	190	4809	11589
	สิ่งแวดล้อมเกี่ยวกับการทำงาน	12	0	28	2655	7649
2555	เครื่องจักร	52	4	1044	7677	8778
	วัตถุหรือสิ่งของ	55	4	438	13453	46570
	ยานพาหนะ	932	6	62	3196	3496
	เครื่องมือ	1	0	186	4257	10607
	สิ่งแวดล้อมเกี่ยวกับการทำงาน	22	0	28	2814	7516
2556	เครื่องจักร	45	2	1705	6069	7193
	วัตถุหรือสิ่งของ	57	2	713	11741	38294
	ยานพาหนะ	323	7	108	2926	2828
	เครื่องมือ	2	0	331	3945	9512
	สิ่งแวดล้อมเกี่ยวกับการทำงาน	20	0	82	2533	6245
2557	เครื่องจักร	36	2	868	5951	6542
	วัตถุหรือสิ่งของ	37	0	334	10528	33217
	ยานพาหนะ	303	3	40	2665	2732
	เครื่องมือ	3	0	136	3659	9237
	สิ่งแวดล้อมเกี่ยวกับการทำงาน	15	0	33	2281	5446
2558	เครื่องจักร	50	1	769	5656	6383
	วัตถุหรือสิ่งของ	43	1	311	9861	30885
	ยานพาหนะ	267	0	51	2511	2550
	เครื่องมือ	2	0	119	3532	9102
	สิ่งแวดล้อมเกี่ยวกับการทำงาน	25	0	28	2346	5561



รูปที่ ข1 ข้อมูลทางสถิติการเกิดอุบัติเหตุ (สำนักงานประกันสังคมกระทรวงแรงงานประเทศไทย พ.ศ. 2551 ถึง พ.ศ. 2558)



รูปที่ ข2 ข้อมูลทางสถิติของการเสียชีวิตเนื่องจากเครื่องจักร (พ.ศ. 2551 ถึง พ.ศ. 2558)



รูปที่ ข3 ข้อมูลทางสถิติของการบาดเจ็บ สูญเสียอวัยวะเนื่องจากเครื่องจักร (พ.ศ. 2551 ถึง พ.ศ. 2558)

ภาคผนวก ค

แสดงตัวอย่างการคำนวณ PL, PLr ของงานวิจัยที่นำเสนอ

ขั้นตอนในการประเมินค่า PLr และ PL ของงานวิจัยที่นำเสนอแบ่งเป็น 4 ขั้นตอน ดังต่อไปนี้

ขั้นตอนที่ 1 แสดงตัวอย่างการประเมินค่า PLr ของเครื่องจักรในอุตสาหกรรมยางรถยนต์

1.1 ระบุจุดเสี่ยงของเครื่องจักร (Identify Hazardous Situation) จากรูป ค1 สามารถวิเคราะห์ความเสี่ยงได้ดังนี้

1) แหล่งกำหนดของอันตราย (Origin Hazard) คือชุดหมุน (Rotating Element)
2) อันตรายและผลกระทบที่จะเกิดขึ้น (Potential Consequences) มีดังนี้
   - อันตรายจากการหมุน (Rotating Hazard), ดึงชิ้นส่วนของร่างกายเข้าไปในเครื่องจักร
   - อันตรายจากการดึง (Drawing-in Hazard), ดึงชิ้นส่วนของร่างกายเข้าไปในเครื่องจักร
   - อันตรายจากการถูกหนีบ (Crushing Hazard), หนีบชิ้นส่วนของร่างกายกับเฟรม เครื่องจักร

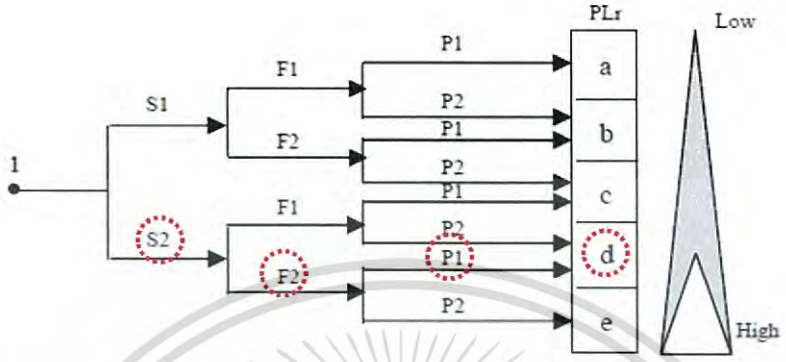
วิธีการในการระบุจุดเสี่ยงของเครื่องจักรอ้างอิงจากภาคผนวก ง

รูปที่ ค1 ตัวอย่างความเสี่ยงของเครื่องจักรในอุตสาหกรรมยางรถยนต์

1.2 ประเมินความเสี่ยงและหาค่าระดับความปลอดภัยที่ต้องการ (PLr) ด้วยวิธีกราฟความเสี่ยง ดังรูปที่ ค 2 ผลจากการประเมินความเสี่ยงร่วมกันระหว่างผู้เข้าร่วมประเมินที่เกี่ยวข้อง สรุปได้ดังนี้

- ความรุนแรง (S2) เนื่องจากระดับความรุนแรงของเหตุการณ์สามารถทำให้พิการ สูญเสีย อวัยวะ หรือถึงขั้นเสียชีวิตได้
- ความถี่ (F2) เนื่องจากความถี่ที่เข้าไปอยู่ในสถานการณ์ที่อันตรายอยู่ในระดับความถี่สูง เป็นจำนวนหลายครั้งในหนึ่งวัน
- โอกาสในการหลบหลีก (P1) เนื่องจากสามารถที่จะหลบหลีกอันตรายได้ ในกรณีที่พนักงานมีประสบการณ์ในการทำงานร่วมกับเครื่องจักรและผ่านการอบรมด้านการใช้งานเครื่องจักรที่ถูกต้องและปลอดภัยมาเป็นอย่างดี แต่ถ้าในกรณีที่เป็นพนักงานใหม่ที่ไม่มีประสบการณ์ทำงานร่วมกับเครื่องจักร ผลลัพธ์จากการประเมินจะเป็น (P2)

จากผลของการประเมินความเสี่ยง ทำให้ทราบว่าเครื่องจักรมีความเสี่ยงอยู่ในเกณฑ์ที่สูง (High risk) และค่าระดับความปลอดภัยที่ต้องการในการจัดการกับความเสี่ยงมีค่าเท่ากับ PLd แสดงดังรูปที่ **ค2**

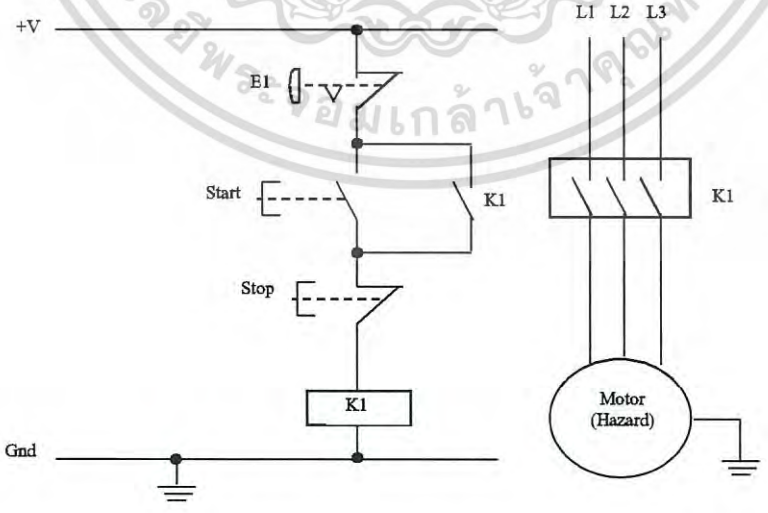


รูปที่ ค2 ตัวอย่างการประเมินความเสี่ยงของเครื่องจักรในอุตสาหกรรมยางรถยนต์

ขั้นตอนที่ 2 แสดงตัวอย่างการคำนวณค่า PL ของระบบ E-Stop (ก่อนปรับปรุง)

2.1 พิจารณา Category

โครงสร้างของระบบควบคุมความเสี่ยง SRP/CS ของเครื่องจักร (ระบบหยุดฉุกเฉิน) ดังรูปที่ ค3 เมื่อทำการเปรียบเทียบกับโครงสร้างมาตรฐาน ดังรูปที่ ค4 จะพบว่าระบบถูกออกแบบด้วยโครงสร้างแบบ Category B และ Category 1 ทำให้ระบบมีความน่าเชื่อถือต่ำ (Low Reliability) เนื่องจากความน่าเชื่อถือของระบบจะขึ้นอยู่กับความน่าเชื่อถือของอุปกรณ์เพียงอย่างเดียวเท่านั้น (Reliability of components) ในกรณีที่อุปกรณ์เกิดความบกพร่อง (Component Failure) ระบบจะไม่สามารถจัดกับการความเสี่ยงได้



รูปที่ ค3 ระบบหยุดฉุกเฉินของเครื่องจักร (ก่อนปรับปรุงค่า PL)

รูปที่ ค4 การออกแบบระบบควบคุมความเสี่ยงด้วยโครงสร้างแบบ Category B และ Category 1

2.2 พิจารณา MTTFd(avg.) ของระบบควบคุมความเสี่ยง SRP/CS จากอุปกรณ์ในระบบ
พิจารณาอุปกรณ์ส่วนอินพุทในระบบ (Input device: Emergency Stop) จะพบว่า Emergency Stop (E1) มีค่า B10d มีค่าเท่ากับ 100,000 cycle อ้างอิงจากตารางที่ ง5 ในภาคผนวก ง เงื่อนไขการทำงานของ Emergency Stop (E1) มีดังนี้

- ทำงาน 3 ครั้ง/วัน ตามข้อกำหนดการทดสอบอุปกรณ์ความปลอดภัยก่อนเข้ากะ
- ทำงาน 365 วัน (คิดที่ Maximum กรณีที่เครื่องจักรทำงานต่อเนื่อง 24 ชั่วโมง/3 กะ)
- แทนค่าในสมการ (1) และ (2) จะได้ค่า MTTFd (E1) มีค่าเท่ากับ 913 ปี

$$MTTFd = \frac{B_{10d}}{0.1x(n_{op})} \quad (1)$$

$$n_{op} = \frac{(d_{op})x(h_{op})x3,600(s/h)}{t_{cycle}} \quad (2)$$

พิจารณาอุปกรณ์ส่วนควบคุมในระบบ (Logic device: ระบบไม่มีอุปกรณ์ส่วนควบคุม)
พิจารณาอุปกรณ์ส่วนเอาท์พุทในระบบ (Output device: Magnetic Contactor)
จะพบว่า Magnetic Contactor (K1) มีค่า B10d มีค่าเท่ากับ 2,000,000 cycle อ้างอิงจากตารางที่ ง5 ในภาคผนวก ง เงื่อนไขการทำงานของ Magnetic Contactor (K1) มีดังนี้

- ทำงาน 6 ครั้ง/วัน ตามข้อกำหนดการทดสอบอุปกรณ์ความปลอดภัยก่อนเข้ากะ
- ทำงาน 365 วัน (คิดที่ Maximum กรณีที่เครื่องจักรทำงานต่อเนื่อง 24 ชั่วโมง/3 กะ)
- แทนค่าในสมการ (1) และ (2) จะได้ค่า MTTFd (K1) มีค่าเท่ากับ 9132 ปี

$$\frac{1}{MTTFd} = \frac{1}{MTTFd_{\ 1}} + \frac{1}{MTTFd_{\ 2}} + \ldots \frac{1}{MTTFd_{\ n}} \quad (3)$$

- แทนค่า MTTFd (E1) และ MTTFd (K1) ในสมการ (3) จะได้ค่า MTTFd(avg.) ของระบบมีค่าเท่ากับ 830ปี (ในกรณีที่ MTTFd มีค่ามากกว่า 100 ปี จะถือว่าค่า MTTFd อยู่ในระดับสูง, MTTFd มีค่าเท่ากับ high)

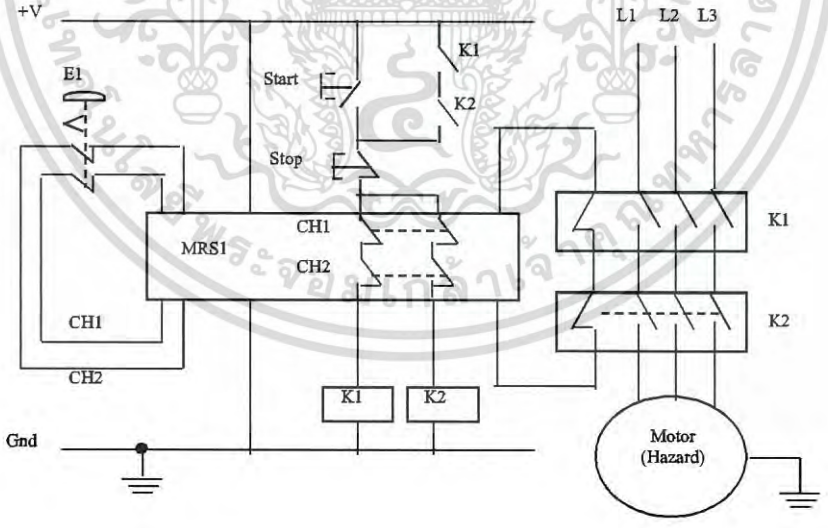
2.3 พิจารณา DC(avg.) (ในกรณีที่ระบบออกแบบด้วย Category B & 1, จะไม่มีการพิจารณาค่า DC)
2.4 พิจารณา CCF (ในกรณีที่ระบบออกแบบด้วย Category B & 1, จะไม่มีการพิจารณาค่า CCF)
2.5 พิจารณา PL จาก Category, MTTFd(avg.) และ DC(avg.)

จาก 2.1 ถึง 2.3 สรุปได้ดังนี้ Category ของระบบคือ Category B & 1, MTTFd(avg.) ของระบบมีค่า High และ DC(avg.) (ในกรณีที่ระบบออกแบบด้วย Category B & 1, จะไม่มีการพิจารณาค่า DC) จะพบว่าระบบควบคุมความเสี่ยง SRP/CS มีค่าระดับความปลอดภัยเท่ากับ PLc และค่า PFHD(avg.) เท่ากับ 1.14×10^{-6} ครั้งต่อชั่วโมง อ้างอิงจากตารางที่ ง8 แสดงดังภาคผนวก ง

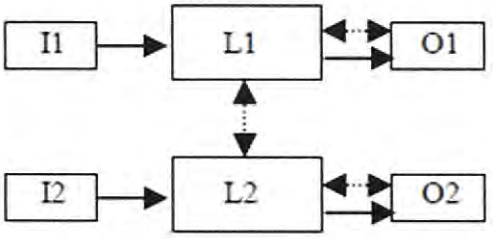
ขั้นตอนที่ 3 แสดงตัวอย่างการคำนวณค่า PL ของระบบ E-Stop (หลังปรับปรุง)

3.1 พิจารณา Category

โครงสร้างของระบบควบคุมความเสี่ยง SRP/CS ของเครื่องจักร (ระบบหยุดฉุกเฉิน หลังปรับปรุง) ดังรูปที่ ค5 เมื่อทำการเปรียบเทียบกับโครงสร้างมาตรฐาน ดังรูปที่ ค6 จะพบว่าระบบถูกออกแบบด้วยโครงสร้างแบบ Category 3 ทำให้ระบบมีความน่าเชื่อถือสูง (High Reliability) เนื่องจากความน่าเชื่อถือของระบบไม่ได้ขึ้นอยู่กับความน่าเชื่อถือของอุปกรณ์เพียงอย่างเดียวเท่านั้น (Reliability of components) แต่ยังขึ้นอยู่กับโครงสร้างของการออกแบบ(Designated Architecture) ด้วย ในกรณีที่อุปกรณ์เกิดความบกพร่อง (Component Failure) อุปกรณ์ชุดควบคุม MRS1 จะตรวจพบความบกพร่องที่เกิดขึ้นและสั่งหยุดการทำงานของชุดขับเคลื่อนทันที ทำให้สามารถจัดการกับการความเสี่ยงได้



รูปที่ ค5 ระบบหยุดฉุกเฉินของเครื่องจักร (หลังปรับปรุงค่า PL)



รูปที่ ค6 การออกแบบระบบควบคุมความเสี่ยงด้วยโครงสร้างแบบ Category 3

3.2 พิจารณา MTTFd(avg.) ของระบบควบคุมความเสี่ยง SRP/CS จากอุปกรณ์ในระบบ
วิธีการหาค่า MTTFd(avg.) เหมือนกับหัวข้อ 2.2 ซึ่งสามารถสรุปผลได้ดังนี้
- Emergency Stop (E1), MTTFd มีค่าเท่ากับ 913 ปี
- Magnetic Contactor (K1), MTTFd มีค่าเท่ากับ 9132 ปี
- Magnetic Contactor (K2), MTTFd มีค่าเท่ากับ 9132 ปี

ดังนั้น MTTFd(avg.) มีค่าเท่ากับ 761 ปี (ในกรณีที่ MTTFd มีค่ามากกว่า 100 ปี จะถือว่าค่า MTTFd อยู่ในระดับสูง, MTTFd มีค่าเท่ากับ high)

3.3 พิจารณา DC(avg.) (ในกรณีที่ระบบออกแบบด้วย Category 2 ขึ้นไป, จะมีการพิจารณาค่า DC)
วิธีการหาค่า DC สามารถหาได้จากตารางที่ ง6 ในภาคผนวก ง ซึ่งสามารถสรุปผลได้ดังนี้
- Emergency Stop (E1), DC มีค่าเท่ากับ 90 %
- Magnetic Contactor (K1), DC มีค่าเท่ากับ 90 %
- Magnetic Contactor (K2), DC มีค่าเท่ากับ 90 %

ดังนั้น DC(avg.) มีค่าเท่ากับ 90 % (ในกรณีที่ DC มีค่าอยู่ในช่วง 90% ถึง 99% จะถือว่าค่า DC อยู่ในระดับปานกลาง, DC(avg.) มีค่าเท่ากับ medium)

3.4 พิจารณา CCF (ในกรณีที่ระบบออกแบบด้วย Category 2 ขึ้นไป, จะมีการพิจารณาค่า CCF)
วิธีการหาค่า CCF สามารถหาได้จากตารางที่ ง7 ในภาคผนวก ง ซึ่งสามารถสรุปผลได้ดังนี้
- เมื่อพิจารณาจากโครงสร้างของการออกแบบควบคุมความเสี่ยง SRP/CS ดังรูปที่ ค6 จะพบว่า CCF มีค่าเท่ากับ 85 คะแนน (ในกรณี CCF มีค่าต่ำกว่า 65 คะแนน จะต้องพิจารณาการออกแบบระบบควบคุมความเสี่ยงใหม่อีกครั้ง เพื่อปรับปรุงการออกแบบให้ได้ค่า CCF ตามที่มาตรฐานกำหนด

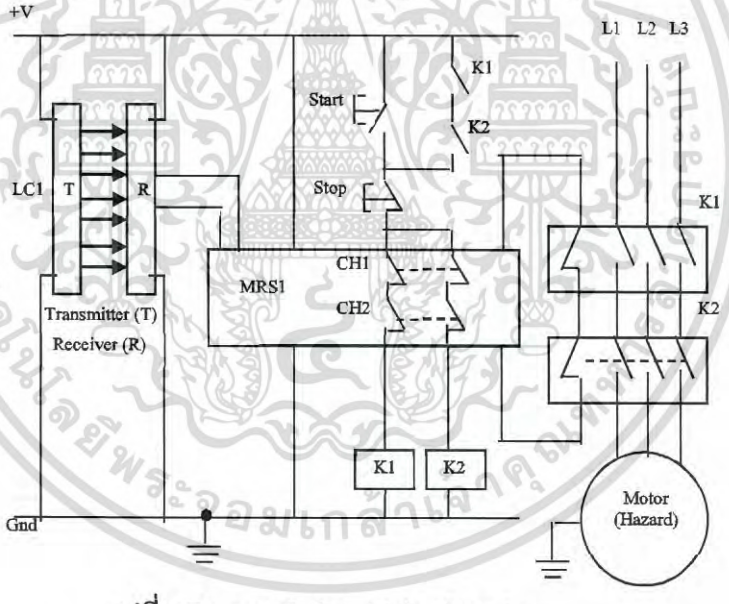
3.5 พิจารณา PL จาก Category, MTTFd(avg.) และ DC(avg.)
- จาก 3.1 ถึง 3.3 สรุปได้ดังนี้ Category ของระบบคือ Category 3, MTTFd(avg.) ของระบบมีค่า High และ DC(avg.) มีค่าเท่ากับ medium ค่าระดับความปลอดภัยของอุปกรณ์ส่วนอินพุท (E1) และส่วนเอาท์พุท (K1, K2) มีค่าเท่ากับ PLe และค่า PFHD(avg.) เท่ากับ 4.29×10^{-8} ครั้งต่อชั่วโมง อ้างอิงจากตารางที่ ง8 แสดงดังภาคผนวก ง
- ค่าระดับความปลอดภัยของอุปกรณ์ส่วนควบคุม (MRS1) มีค่าเท่ากับ PLe และค่า PFHD(avg.) เท่ากับ 4.35×10^{-9} ครั้งต่อชั่วโมง อ้างอิงจากข้อมูลของบริษัทผู้ผลิต (Manufacturer Datasheet)

ดังนั้นค่าระดับความปลอดภัยของอุปกรณ์ทั้งระบบคือ PLe และค่า PFHD (avg.) ของทั้งระบบมีค่าเท่ากับ 4.73×10^{-8} ครั้งต่อชั่วโมง

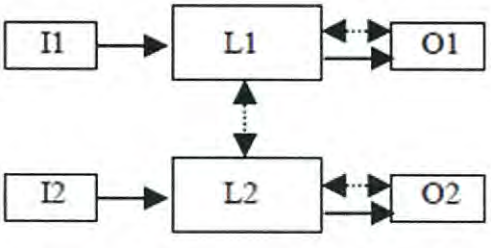
ขั้นตอนที่ 4 แสดงตัวอย่างการคำนวณค่า PL ของระบบ Safety Light Curtain

4.1 พิจารณา Category

โครงสร้างของระบบควบคุมความเสี่ยง SRP/CS ของเครื่องจักร (ระบบม่านแสงนิรภัย หลังปรับปรุง) ดังรูปที่ ค7 เมื่อทำการเปรียบเทียบกับโครงสร้างมาตรฐาน ดังรูปที่ ค8 จะพบว่าระบบถูกออกแบบด้วยโครงสร้างแบบ Category 3 ทำให้ระบบมีความน่าเชื่อถือสูง (High Reliability) เนื่องจากความน่าเชื่อถือของระบบไม่ได้ขึ้นอยู่กับความน่าเชื่อถือของอุปกรณ์เพียงอย่างเดียวเท่านั้น (Reliability of components) แต่ยังขึ้นอยู่กับโครงสร้างของการออกแบบ(Designated Architecture) ด้วย ในกรณีที่อุปกรณ์เกิดความบกพร่อง (Component Failure) อุปกรณ์ชุดควบคุม MRS1 จะตรวจพบความบกพร่องที่เกิดขึ้นและสั่งหยุดการทำงานของชุดขับเคลื่อนทันที ทำให้สามารถจัดการกับการความเสี่ยงได้



รูปที่ ค7 ระบบ Safety Light Curtain



รูปที่ ค8 การออกแบบระบบควบคุมความเสี่ยงด้วยโครงสร้างแบบ Category 3

4.2 พิจารณา MTTFd(avg.) ของระบบควบคุมความเสี่ยง SRP/CS จากอุปกรณ์ในระบบ
วิธีการหาค่า MTTFd(avg.) เหมือนกับหัวข้อ 2.2 ซึ่งสามารถสรุปผลได้ดังนี้

- Magnetic Contactor (K1), MTTFd มีค่าเท่ากับ 9132 ปี
- Magnetic Contactor (K2), MTTFd มีค่าเท่ากับ 9132 ปี

ดังนั้น MTTFd(avg.) มีค่าเท่ากับ 4566 ปี (ในกรณีที่ MTTFd มีค่ามากกว่า 100 ปี จะถือว่าค่า MTTFd อยู่ในระดับสูง, MTTFd มีค่าเท่ากับ high)

4.3 พิจารณา DC(avg.) (ในกรณีที่ระบบออกแบบด้วย Category 2 ขึ้นไป, จะมีการพิจารณาค่า DC)
วิธีการหาค่า DC สามารถหาได้จากตารางที่ ง6 ในภาคผนวก ง ซึ่งสามารถสรุปผลได้ดังนี้

- Magnetic Contactor (K1), DC มีค่าเท่ากับ 90 %
- Magnetic Contactor (K2), DC มีค่าเท่ากับ 90 %

ดังนั้น DC(avg.) มีค่าเท่ากับ 90 % (ในกรณีที่ DC มีค่าอยู่ในช่วง 90% ถึง 99% จะถือว่าค่า DC อยู่ในระดับปานกลาง, DC(avg.) มีค่าเท่ากับ medium)

4.4 พิจารณา CCF (ในกรณีที่ระบบออกแบบด้วย Category 2 ขึ้นไป, จะมีการพิจารณาค่า CCF)
วิธีการหาค่า CCF สามารถหาได้จากตารางที่ ง7 ในภาคผนวก ง ซึ่งสามารถสรุปผลได้ดังนี้

- เมื่อพิจารณาจากโครงสร้างของการออกแบบควบคุมความเสี่ยง SRP/CS ดังรูปที่ ค7 จะพบว่า CCF มีค่าเท่ากับ 85 คะแนน (ในกรณี CCF มีค่าต่ำกว่า 65 คะแนน จะต้องพิจารณาการออกแบบระบบควบคุมความเสี่ยงใหม่อีกครั้ง เพื่อปรับปรุงการออกแบบให้ได้ค่า CCF ตามที่มาตรฐานกำหนด)

4.5 พิจารณา PL จาก Category, MTTFd(avg.) และ DC(avg.)

- จาก 4.1 ถึง 4.3 สรุปได้ดังนี้ Category ของระบบคือ Category 3, MTTFd(avg.) ของระบบมีค่า High และ DC(avg.) มีค่าเท่ากับ medium ค่าระดับความปลอดภัยของอุปกรณ์ส่วนเอาท์พุท K1, K2 มีค่าเท่ากับ PLe และค่า PFHD(avg.) เท่ากับ 4.29×10^{-8} ครั้งต่อชั่วโมง อ้างอิงจากตารางที่ ง8 แสดงดังภาคผนวก ง
- ค่าระดับความปลอดภัยของอุปกรณ์ส่วนควบคุม MRS1 มีค่าเท่ากับ PLe และค่า PFHD(avg.) เท่ากับ 4.35×10^{-9} ครั้งต่อชั่วโมง อ้างอิงจากข้อมูลของบริษัทผู้ผลิต (Manufacturer Datasheet)
- ค่าระดับความปลอดภัยของอุปกรณ์ส่วนอินพุท LC1 มีค่าเท่ากับ PLe และค่า PFHD(avg.) เท่ากับ 7.93×10^{-9} ครั้งต่อชั่วโมง อ้างอิงจากข้อมูลของบริษัทผู้ผลิต (Manufacturer Datasheet)

ดังนั้นค่าระดับความปลอดภัยของอุปกรณ์ทั้งระบบคือ PLe และค่า PFHD (avg.) ของทั้งระบบมีค่าเท่ากับ 5.52×10^{-8} ครั้งต่อชั่วโมง

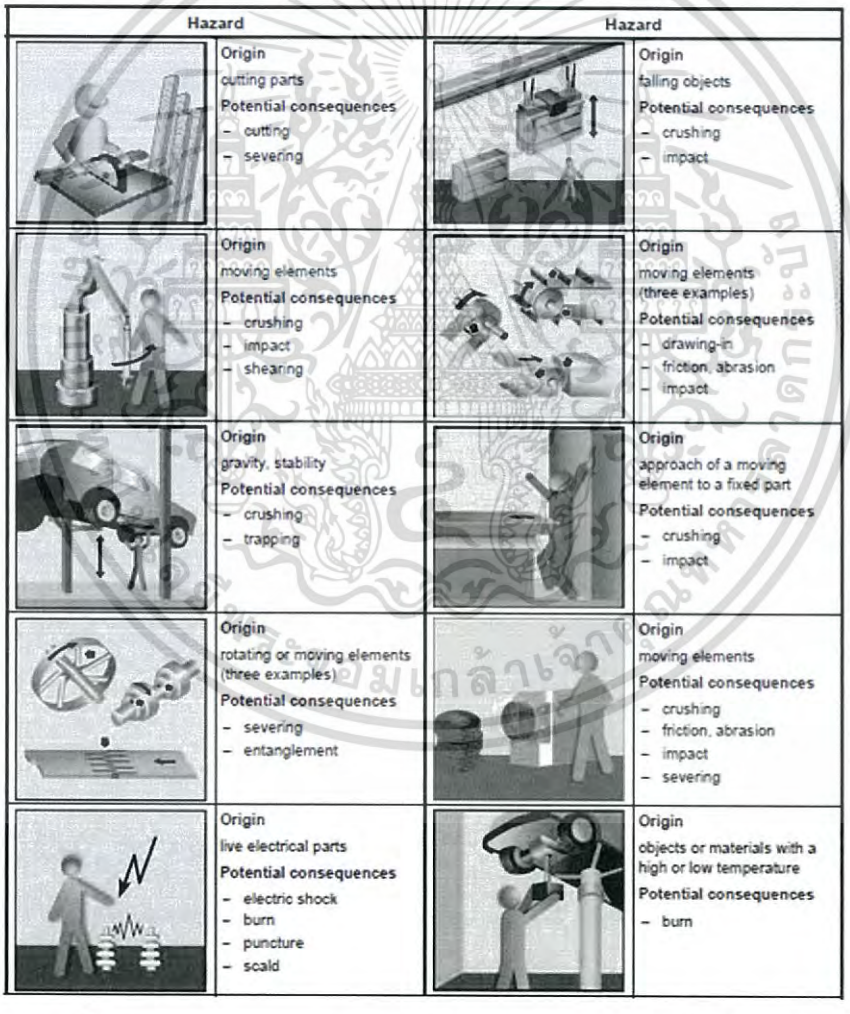
ภาคผนวก ง

ข้อมูลสนับสนุนการทำวิจัยอ้างอิงจากมาตรฐานสากล

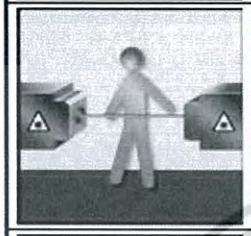
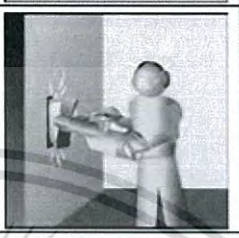
การระบุอันตราย (Hazard Identification)

ตัวอย่างของการระบุอันตราย (Hazard Identification) เพื่อนำไปใช้ในการประเมินความเสี่ยง แสดงดังรูปที่ ง1 และรูปที่ ง2 โดยสิ่งที่จำเป็นจะต้องระบุ มีดังนี้

1. จุดกำเนิดของอันตราย (Origin) เช่น อันตรายจากการตัด (Cutting), การเคลื่อนที่ (Moving), การหมุน (Rotation), กระแสไฟฟ้า (Electric), การตกหล่น (Falling) ... ฯลฯ เป็นต้น
2. อันตรายและผลกระทบที่จะเกิดขึ้น (Potential Consequences) เช่น การตัด (Cutting), การหนีบ(Crushing), การถูกดึง (Drawing-in), การเฉือน (Shearing), การถูกไฟฟ้าดูด (Electric Shock) ... ฯลฯ เป็นต้น



รูปที่ ง1 ตัวอย่างการระบุอันตรายหรือสถานการณ์อันตรายที่เกี่ยวข้อง
(Identify the hazards and associated hazardous situations)

Hazard		Hazard	
	**Origin** vibrating equipment **Potential consequences** – osteo-articular disorder – vascular disorder		**Origin** noisy manufacturing process **Potential consequences** – fatigue – hearing impairment – loss of awareness – stress
	**Origin** laser beam **Potential consequences** – burn – damage to eyes and skin		**Origin** dust (emissions) **Potential consequences** – breathing difficulties – explosion – loss of sight
	**Origin** posture **Potential consequences** – discomfort – fatigue – musculoskeletal disorder		**Origin** fumes **Potential consequences** – breathing difficulties – irritation – poisoning
	**Origin** location of control devices **Potential consequences** – any as a consequence of human error – stress		**Origin** gravity (bulk material solidified) **Potential consequences** – collapse, falling – crushing – slumping/sagging – suffocation – wedging/jamming

รูปที่ ง2 ตัวอย่างการระบุอันตรายหรือสถานการณ์อันตรายที่เกี่ยวข้อง
(Identify the hazards and associated hazardous situations)

ตารางที่ ง1 แสดงตัวอย่างของการระบุจุดกำเนิดอันตรายและผลกระทบที่จะเกิดขึ้น

No	Type or group	Examples of hazards	
		Origin[a]	Potential consequences[b]
1	Mechanical hazards	- acceleration, deceleration; - angular parts; - approach of a moving element to a fixed part; - cutting parts; - elastic elements; - falling objects; - gravity; - height from the ground; - high pressure; - instability; - kinetic energy; - machinery mobility; - moving elements; - rotating elements; - rough, slippery surface; - sharp edges; - stored energy; - vacuum.	- being run over; - being thrown; - crushing; - cutting or severing; - drawing-in or trapping; - entanglement; - friction or abrasion; - impact; - injection; - shearing; - slipping, tripping and falling; - stabbing or puncture; - suffocation.
2	Electrical hazards	- arc; - electromagnetic phenomena; - electrostatic phenomena; - live parts; - not enough distance to live parts under high voltage; - overload; - parts which have become live under fault conditions; - short-circuit; - thermal radiation.	- burn; - chemical effects; - effects on medical implants; - electrocution; - falling, being thrown; - fire; - projection of molten particles; - shock.
3	Thermal hazards	- explosion; - flame; - objects or materials with a high or low temperature; - radiation from heat	- burn; - dehydration; - discomfort; - frostbite; - injuries by the radiation of heat sources;

No	Type or group	Examples of hazards	
		Origin[a]	Potential consequences[b]
		sources.	- scald.
4	Noise hazards	- cavitation phenomena; - exhausting system; - gas leaking at high speed; - manufacturing process (stamping, cutting, etc.); - moving parts; - scraping surfaces; - unbalanced rotating parts; - whistling pneumatics; - worn parts.	- discomfort; - loss of awareness; - loss of balance; - permanent hearing loss; - stress; - tinnitus; - tiredness; - any other (for example, mechanical, electrical) as a consequence of an interference with speech communication or with acoustic signals.
5	Vibration hazards	- cavitation phenomena; - misalignment of moving parts; - mobile equipment; - scraping surfaces; - unbalanced rotating parts; - vibrating equipment;	- discomfort; - low-back morbidity; - neurological disorder; - osteo-articular disorder; - trauma of the spine; - vascular disorder.
6	Radiation hazards	- ionizing radiation source; - low frequency electromagnetic - optical radiation (infrared, visible and ultraviolet), including laser; radio frequency electromagnetic radiation.	- burn; - damage to eyes and skin; - effects on reproductive capability; - mutation; - headache, insomnia, etc.
7	Material/substance Hazards	- aerosol; - biological and microbiological (viral or bacterial) agent; - combustible; - dust; - explosive; - fiber; - flammable; - fluid; - fume, mist; - gas;	- breathing difficulties, - suffocation; - cancer; - corrosion; - effects on reproductive - capability; - explosion; - fire; - infection; - mutation; - poisoning; - sensitization.

No	Type or group	Examples of hazards	
		Origin[a]	Potential consequences[b]
		- oxidizer.	
8	Ergonomic hazards	- access; - design or location of indicators and visual displays units; - design, location or identification of control devices; - effort; - flicker, dazzling, shadow, - stroboscopic effect; - local lighting;	- discomfort; - fatigue; - musculoskeletal disorder; - stress; - any other (for example, mechanical, electrical) as a consequence of a human error.
9	Hazards associated with the environment in which the machine is used	- dust and fog; - electromagnetic disturbance; - lightning; - moisture; - pollution; - snow; - temperature; - water; - wind; - lack of oxygen.	- burn; - slight disease; - slipping, falling; - suffocation; - any other as a consequence of the effect caused by the sources of the hazards on the machine or parts of the machine.
10	Combination of hazards	- for example, repetitive activity + effort + high environmental temperature	- for example, dehydration, loss of awareness, heat stroke
a	A single origin of a hazard can have several potential consequences.		
b	For each type of hazard or group of hazards, some potential consequences can be related to several origins of hazard.		

ตารางที่ ง2 แสดงตัวอย่างของการระบุสถานการณ์ที่อันตราย (Identify Hazardous Situation)

Phases of machine life cycle	**Examples of tasks**
Transport	– Lifting – Loading – Packing – Transportation – Unloading – Unpacking
Assembly and installation Commissioning	– Adjustments of the machine and its components – Assembly of the machine – Connecting to disposal system (for example, exhaust system, waste water installation) – Connecting to power supply (for example, electric power supply, compressed air) – Demonstration – Feeding, filling, loading of ancillary fluids (for example, lubricant, grease, glue) – Fencing – Fixing, anchoring – Preparations for the installation (for example, foundations, vibration isolators) – Running the machine without load – Testing – Trials with load or maximum load
Setting Teaching/programming and/or process changeover	– Adjustment and setting of protective devices and other components – Adjustment and setting or verification of functional parameters of the machine (for example, speed, pressure, force, travelling limits) – Clamping/fastening the workpiece – Feeding, filling, loading of raw material – Functional test, trials – Mounting or changing tools, tool-setting – Programming verification – Verification of the final product
Operation	– Clamping/fastening the workpiece – Control/inspection – Driving the machine – Feeding, filling, loading of raw material – Manual loading/unloading – Minor adjustments and setting of functional parameters of the machine (for example, speed, pressure, force, travel limits)

Phases of machine life cycle	Examples of tasks
	– Minor interventions during operation (for example, removing waste material, eliminating jams, local cleaning) – Operating manual controls – Restarting the machine after stopping/interruption – Supervision
Cleaning Maintenance	– Adjustments – Cleaning, disinfection – Dismantling/removal of parts, components, devices of the machine – Housekeeping – Isolation and energy dissipation – Lubrication – Replacement of tools – Replacement of worn parts – Resetting – Restoring fluid levels – Verification of parts, components, devices of the machine
Fault-finding/ Troubleshooting	– Adjustments – Dismantling/removal of parts, components, devices of the machine – Fault-finding – Isolation and energy dissipation – Recovering from control and protective devices failure – Recovering from jam – Repairing – Replacement of parts, components, devices of the machine – Rescue of trapped persons – Resetting – Verification of parts, components, devices of the machine
Dismantling Disabling	– Disconnection and energy dissipation – Dismantling – Lifting – Loading – Packing – Transportation – Unloading
NOTE These tasks can be applied to the machine or parts of it.	

ตารางที่ ง3 แสดงตัวอย่างของการระบุเหตุการณ์ที่อันตราย (Identify Hazardous Event)

Origin related to...	Hazardous event
Shape and/or superficial finishing of accessible parts of the machine	– Contact with rough surfaces – Contact with sharp edges and corners, protruding parts
Moving parts of the machine	– Contact with moving parts – Contact with rotating open ends
Kinetic energy and/or potential energy (gravity) of the machine, parts of the machine, tools and materials used, processed, handled	– Falling or ejection of objects
Stability of the machine and/or parts of the machine	– Loss of stability
Mechanical strength of parts of the machine, tools, etc.	– Break-up during operation
Pneumatic, hydraulic equipment	– Displacement of moving elements – Projection of high pressure fluids – Uncontrolled movements
Electrical equipment	– Direct contact – Disruptive discharge – Electric arc – Fire – Indirect contact – Short-circuit
Control system	– Dropping or ejection of a moving part of the machine or of a workpiece clamped by the machine – Failure to stop moving parts – Machine action resulting from inhibition (defeating

Origin related to...	Hazardous event
	or failure) of protective devices – Uncontrolled movements (including speed change) – Unintended/unexpected start-up – Other hazardous events due to failure(s) or poor design of the control system
Materials and substances or physical factors (temperature, noise, vibration, radiation and environment)	– Contact with objects with high or low temperature – Emission of a substance that can be hazardous – Emission of a level of noise that can be hazardous – Emission of a level of noise that can interfere with a speech communication or with acoustic signals – Emission of a level of vibration that can be hazardous – Emission of radiation fields that can be hazardous – Harsh environmental conditions
Workstation and/or work process design	– Excessive effort – Human errors/misbehavior (unintentional and/or deliberately induced by the design) – Loss of direct visibility of the working area – Painful and tiring postures

ตารางที่ ง4 คำจำกัดความของ Category ตามข้อกำหนด EN 954-1 และ EN ISO 13849-1

Category	Summary of requirements	System behavior	Principle used to achieve safety	$MTTF_d$ of each channel	DC_{avg}	CCF
B (see 6.2.3)	SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used	The occurrence of a fault can lead to the loss of the safety function.	Mainly characterized by selection of components	Low to medium	None	Not relevant
1 (see 6.2.4)	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for category B.	Mainly characterized by selection of components	High	None	Not relevant

Category	Summary of requirements	System behavior	Principle used to achieve safety	$MTTF_d$ of each channel	DC_{avg}	CCF
2 (see 6.2.5)	Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system.	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of safety function is detected by the check.	Mainly characterized by structure	Low to high	Low to medium	See Annex F
3 (see 6.2.6)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that a single fault in any of these parts does not lead to the loss of the safety function, and Whenever reasonably practicable, the single fault is detected.	When a single fault occurs, the safety function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to the loss of the safety function.	Mainly characterized by structure	Low to high	Low to medium	See Annex F

Category	Summary of requirements	System behavior	Principle used to achieve safety	$MTTF_d$ of each channel	DC_{avg}	CCF
4 (see 6.2.7)	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that a single fault in any of these parts does not lead to a loss of the safety function, and The single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.	Mainly characterized by structure	High	High including accumulation of faults	See Annex F
NOTE	For full requirements, see Clause 6.					

ตารางที่ ง5 อุปกรณ์ที่ผ่านทดสอบตามมาตรฐาน (Basic and well-tried safety principles)

	Basic and well-tried safety principles according to ISO 13849-2:2003	Other relevant standards	Typical values: MTTFd (years) B10d (cycles)
Mechanical components	Tables A.1 and A.2	-	$MTTF_d$ = 150
Hydraulic components	Tables C.1 and C.2	EN 982	$MTTF_d$ = 150
Pneumatic components	Tables B.1 and B.2	EN 983	B_{10d} = 20 000 000
Relays and contactor relays with small load (mechanical load)	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 20 000 000
Relays and contactor relays with maximum load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10d} = 400 000
Proximity switches with small load (mechanical load)	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Proximity switches with maximum load	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 400 000
Contactors with small load (mechanical load)	Tables D.1 and D.2	IEC 60947	B_{10d} = 20 000 000
Contactors with nominal load	Tables D.1 and D.2	IEC 60947	B_{10d} = 2 000 000
Position switches independent of load [a]	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 20 000 000
Position switches (with separate actuator, guard locking) independent of load [a]	Tables D.1 and D.2	IEC 60947 EN 1088	B_{10d} = 2 000 000
Emergency stop devices independent of the load a	Tables D.1 and D.2	IEC 60947 ISO 13850	B_{10d} = 100 000

	Basic and well-tried safety principles according to ISO 13849-2:2003	Other relevant standards	Typical values: MTTFd (years) B10d (cycles)
Emergency stop devices with maximum operational demands a	Tables D.1 and D.2	IEC 60947 ISO 13850	B_{10d} = 6 050
Push buttons (e.g. enabling switches) independent of the load [a]	Tables D.1 and D.2	IEC 60947	B_{10d} = 100 000
For the definition and use of B_{10d}, see C.4. NOTE 1 B_{10d} is estimated as two times B_{10} (50 % dangerous failure). NOTE 2 "Small load" means, for example, 20 % of the rated value (for more information, see EN 13849-2).			
[a] If fault exclusion for direct opening action is possible.			

ตารางที่ ง6 ตารางประเมินค่า DC (Diagnostic Coverage) ตาม EN ISO 13849-1

Measure	Diagnostic coverage (DC)
Input device	
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e!
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %
Logic	
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application

Measure	Diagnostic coverage (DC)
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Simple temporal time monitoring of the logic (e.g. timer as watchdog, where trigger points are within the program of the logic)	60 %
Temporal and logical monitoring of the logic by the watchdog, where the test equipment does plausibility checks of the behavior of the logic	90 %
Start-up self-tests to detect latent faults in parts of the logic (e.g. program and data memories, input/output ports, interfaces)	90 % (depending on the testing technique)
Checking the monitoring device reaction capability (e.g. Watchdog) by the main channel at start-up or whenever the safety function is demanded or whenever an external signal demand it, through an input facility	90 %
Dynamic principle (all components of the logic are required to change the state ON-OFF-ON when the safety function is demanded), e.g. interlocking circuit implemented by relays	99 %
Invariable memory: signature of one word (8 bit)	90 %
Invariable memory: signature of double word (16 bit)	99 %
Variable memory: RAM-test by use of redundant data e.g. flags, markers, constants, timer, cross comparison of these data	60 %
Variable memory: check for readability and write ability of used data memory cells	60 %

Measure	Diagnostic coverage (DC)
Variable memory: RAM monitoring with modified Hamming code or RAM self-test (e.g. "galpat" or "Abraham")	99 %
Processing unit: self-test by software	60 % to 90 %
Processing unit: coded processing	90 % to 99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level "e"!
Output device	
Monitoring of outputs by one channel without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of outputs without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90 %
Cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Redundant shut-off path with no monitoring of the actuator	0 %
Redundant shut-off path with monitoring of one of the actuators either by logic or by test equipment	90 %
Redundant shut-off path with monitoring of the actuators bylogic and test equipment	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application

Measure	Diagnostic coverage (DC)
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level “e”!
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
NOTE 1 For additional estimations for DC, see, e.g., IEC 61508-2:2000, Tables A.2 to A.15. NOTE 2 If medium or high DC is claimed for the logic, at least one measure for variable memory, invariable memory and processing unit with each DC at least 60 % has to be applied. There may also be measures that used other than those listed in this table.	

ตารางที่ ง7 ตารางประเมินค่า CCF (Common Cause Failure) ตาม EN ISO 13849-1

No.	Measure against CCF	Score
1	**Separation/ Segregation**	
	Physical separation between signal paths: separation in wiring/piping, sufficient clearances and creep age distances on printed-circuit boards.	15
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, Measuring of distance and pressure, digital and analog. Components of different manufactures.	20
3	**Design/application/experience**	
3.1	Protection against over-voltage, over-pressure, over-current, etc.	15
3.2	Components used are well-tried.	5
4	**Assessment/analysis**	
	Are the results of a failure mode and effect analysis taken into account to avoid common-cause-failures in design.	5
5	**Competence/training**	
	Have designers/ maintainers been trained to understand the causes and consequences of common cause failures?	5
6	**Environmental**	
6.1	Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. - Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. - Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electric systems, both aspects should be considered.	25
6.2	Other influences Have the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards) bee considered?	10

No.	Measure against CCF	Score
	Total	[max. achievable 100]

Total score	Measures for avoiding CCF[a]
65 or better	Meets the requirements
Less than 65	Process failed ⇒choose additional measures

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

ตารางที่ ง8 ความสัมพันธ์ระหว่างตัวแปร Category, MTTFd, DCavg, PLและ PFHDavg

	Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)						
MTTFd for each channel years	Cat. B PL DCavg = none	Cat. 1 PL DCavg = none	Cat. 2 PL DCavg = low	Cat. 2 PL DCavg = medium	Cat. 3 PL DCavg = low	Cat. 3 PL DCavg = medium	Cat. 4 PL DCavg = high
3	3.80×10^{-5} a		2.58×10^{-5} a	1.99×10^{-5} a	1.26×10^{-5} a	6.09×10^{-6} b	
3.3	3.46×10^{-5} a		2.33×10^{-5} a	1.79×10^{-5} a	1.13×10^{-5} a	5.41×10^{-6} b	
3.6	3.17×10^{-5} a		2.13×10^{-5} a	1.62×10^{-5} a	1.03×10^{-5} a	4.86×10^{-6} b	
3.9	2.93×10^{-5} a		1.95×10^{-5} a	1.48×10^{-5} a	9.37×10^{-6} b	4.40×10^{-6} b	
4.3	2.65×10^{-5} a		1.76×10^{-5} a	1.33×10^{-5} a	8.39×10^{-6} b	3.89×10^{-6} b	
4.7	2.43×10^{-5} a		1.60×10^{-5} a	1.20×10^{-5} a	7.58×10^{-6} b	3.48×10^{-6} b	
5.1	2.24×10^{-5} a		1.47×10^{-5} a	1.10×10^{-5} a	6.91×10^{-6} b	3.15×10^{-6} b	
5.6	2.04×10^{-5} a		1.33×10^{-5} a	9.87×10^{-6} b	6.21×10^{-6} b	2.80×10^{-6} c	
6.2	1.84×10^{-5} a		1.19×10^{-5} a	8.80×10^{-6} b	5.53×10^{-6} b	2.47×10^{-6} c	
6.8	1.68×10^{-5} a		1.08×10^{-5} a	7.93×10^{-6} b	4.98×10^{-6} b	2.20×10^{-6} c	
7.5	1.52×10^{-5} a		9.75×10^{-6} b	7.10×10^{-6} b	4.45×10^{-6} b	1.95×10^{-6} c	
8.2	1.39×10^{-5} a		8.87×10^{-6} b	6.43×10^{-6} b	4.02×10^{-6} b	1.74×10^{-6} c	
9.1	1.25×10^{-5} a		7.94×10^{-6} b	5.71×10^{-6} b	3.57×10^{-6} b	1.53×10^{-6} c	
10	1.14×10^{-5} a		7.18×10^{-6} b	5.14×10^{-6} b	3.21×10^{-6} b	1.36×10^{-6} c	
11	1.04×10^{-5} a		6.44×10^{-6} b	4.53×10^{-6} b	2.81×10^{-6} c	1.18×10^{-6} c	
12	9.51×10^{-6} b		5.84×10^{-6} b	4.04×10^{-6} b	2.49×10^{-6} c	1.04×10^{-6} c	

	Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)						
MTTFd for each channel years	Cat. B PL DCavg = none	Cat. 1 PL DCavg = none	Cat. 2 PL DCavg = low	Cat. 2 PL DCavg = medium	Cat. 3 PL DCavg = low	Cat. 3 PL DCavg = medium	Cat. 4 PL DCavg = high
	8.78×10^{-6} b		5.33×10^{-6} b	3.64×10^{-6} b	2.23×10^{-6} c	9.21×10^{-7} d	
15	7.61×10^{-6} b		3.17×10^{-6} b	3.01×10^{-6} b	1.82×10^{-6} c	7.44×10^{-7} d	
16	7.13×10^{-6} b		4.21×10^{-6} b	2.77×10^{-6} c	1.67×10^{-6} c	6.76×10^{-7} d	
18	6.34×10^{-6} b		3.68×10^{-6} b	2.37×10^{-6} c	1.41×10^{-6} c	5.67×10^{-7} d	
20	5.71×10^{-6} b		3.26×10^{-6} b	2.06×10^{-6} c	1.22×10^{-6} c	4.85×10^{-7} d	
22	5.19×10^{-6} b		2.93×10^{-6} c	1.82×10^{-6} c	1.07×10^{-6} c	4.21×10^{-7} d	
24	4.76×10^{-6} b		2.65×10^{-6} c	1.62×10^{-6} c	9.47×10^{-7} d	3.70×10^{-7} d	
27	4.23×10^{-6} b		2.32×10^{-6} c	1.39×10^{-6} c	8.04×10^{-7} d	3.10×10^{-7} d	
30		3.80×10^{-6} b	2.06×10^{-6} c	1.21×10^{-6} c	6.94×10^{-7} d	2.65×10^{-7} d	9.54×10^{-8} e
33		3.46×10^{-6} b	1.85×10^{-6} c	1.06×10^{-6} c	5.94×10^{-7} d	2.30×10^{-7} d	8.57×10^{-8} e
36		3.17×10^{-6} b	1.67×10^{-6} c	9.39×10^{-7} d	5.16×10^{-7} d	2.01×10^{-7} d	7.77×10^{-8} e
39		2.93×10^{-6} c	1.53×10^{-6} c	8.40×10^{-7} d	4.53×10^{-7} d	1.78×10^{-7} d	7.11×10^{-8} e
43		2.65×10^{-6} c	1.37×10^{-6} c	7.34×10^{-7} d	3.87×10^{-7} d	1.54×10^{-7} d	6.37×10^{-8} e
47		2.43×10^{-6} c	1.24×10^{-6} c	6.49×10^{-7} d	3.35×10^{-7} d	1.34×10^{-7} d	5.76×10^{-8} e
51		2.24×10^{-6} c	1.13×10^{-6} c	5.80×10^{-7} d	2.93×10^{-7} d	1.19×10^{-7} d	5.26×10^{-8} e
56		2.04×10^{-6} c	1.02×10^{-6} c	5.10×10^{-7} d	2.52×10^{-7} d	1.03×10^{-7} d	4.73×10^{-8} e
62		1.84×10^{-6} c	9.06×10^{-7} d	4.43×10^{-7} d	2.13×10^{-7} d	8.84×10^{-8} e	4.22×10^{-8} e

	Average probability of a dangerous failure per hour (1/h) and corresponding performance level (PL)						
MTTFd for each channel years	Cat. B PL DCavg = none	Cat. 1 PL DCavg = none	Cat. 2 PL DCavg = low	Cat. 2 PL DCavg = medium	Cat. 3 PL DCavg = low	Cat. 3 PL DCavg = medium	Cat. 4 PL DCavg = high
68		1.68×10^{-6} c	8.17×10^{-7} d	3.90×10^{-7} d	1.84×10^{-7} d	7.68×10^{-8} e	3.80×10^{-8} e
75		1.52×10^{-6} c	7.31×10^{-7} d	3.40×10^{-7} d	1.57×10^{-7} d	6.62×10^{-8} e	3.41×10^{-8} e
82		1.39×10^{-6} c	6.61×10^{-7} d	3.01×10^{-7} d	1.35×10^{-7} d	5.79×10^{-8} e	3.08×10^{-8} e
91		1.25×10^{-6} c	5.88×10^{-7} d	2.61×10^{-7} d	1.14×10^{-7} d	4.49×10^{-8} e	2.74×10^{-8} e
100		1.14×10^{-6} c	5.28×10^{-7} d	2.29×10^{-7} d	1.01×10^{-7} d	4.29×10^{-8} e	2.47×10^{-8} e

ประวัติผู้เขียน

ชื่อ-นามสกุล นายณภัทร วงศ์พิริยโยธา

วัน เดือน ปีเกิด 07 ธันวาคม 2531

สถานที่เกิด อำเภอเมือง จังหวัดขอนแก่น

ที่อยู่ 939/66 ม.19 ต.ศิลา อ.เมือง จ.ขอนแก่น 40000

ประวัติการศึกษา

สำเร็จการศึกษาระดับปริญญาตรีหลักสูตรวิศวกรรมศาสตรบัณฑิต
สาขาวิศวกรรมไฟฟ้า จากคณะวิศวกรรมศาสตร์ มหาวิทยาลัยขอนแก่น ปีการศึกษา 2554

ความชำนาญเฉพาะด้าน

1. การประเมินความเสี่ยงและการลดความเสี่ยงของเครื่องจักรในอุตสาหกรรม (Risk assessment and risk reduction for industrial machinery)
2. การออกแบบโปรแกรมควบคุมระบบอัตโนมัติที่ใช้กับเครื่องจักรในอุตสาหกรรม (Design programmable logic control of automation system for industrial machinery)
3. การซ่อมบำรุงเครื่องจักรในอุตสาหกรรมกระบวนการผลิตและเครื่องจักรโรงจักรต้นกำลังเพื่อป้องกันปัญหาการหยุดของกระบวนการผลิต (Maintenance industrial machinery and utility machinery to prevent stopping of manufacturing process)

ประสบการณ์การทำงาน

- พ.ศ.2554-2556 ตำแหน่งวิศวกรฝ่ายซ่อมบำรุง บริษัท ยางสยาม (พระประแดง) จำกัด
- พ.ศ.2556-2559 ตำแหน่งวิศวกรอาวุโสฝ่ายวิศวกรรมระบบอัตโนมัติ บริษัท สยามมิชลิน จำกัด
- พ.ศ.2559-2560 ตำแหน่งวิศวกรอาวุโสฝ่ายวิศวกรรมโรงจักรต้นกำลัง บริษัท โตโยต้า มอเตอร์ เอเชีย แปซิฟิค เอ็นจิเนียริ่ง แอนด์ แมนูแฟคเจอริ่ง จำกัด (TMAP-EM)

ปัจจุบัน ตำแหน่งวิศวกรอาวุโสฝ่ายวิศวกรรมโรงจักรต้นกำลัง บริษัท โตโยต้า ไดฮัทสุ เอ็นจิเนียริ่ง แอนด์ แมนูแฟคเจอริ่ง จำกัด (TDEM)