

ศอ.พว./CDV

ตุลาคม ๒๕๖๔

ห้ามใช้หรือยึดถือร่างนี้เป็นมาตรฐาน

ร่าง

มาตรฐาน

เครื่องตัดวงจรอัจฉริยะ - ความปลอดภัยเชิงหน้าที่

SMART CIRCUIT BREAKER - FUNCTIONAL SAFETY

สำหรับเสนอคณะกรรมการวิชาการด้านมาตรฐาน

สถาบันประเมินและรับรองเทคโนโลยีดิจิทัล

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ถนนพหลโยธิน ปทุมธานี ๑๒๑๒๐

โทรศัพท์ ๐ ๒๕๖๔ ๖๙๐๐

**คณะกรรมการวิชาการด้านมาตรฐาน
สถาบันประเมินและรับรองเทคโนโลยีดิจิทัล**

ประธานกรรมการ

ม.ร.ว.นงคราญ ชมพูนุท
นายสร้างรัฐ หัตถวงษ์

สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย

รองประธานกรรมการ

นายพงศ์พัฒน์ พันธุ์เพียร

สถาบันไฟฟ้าและอิเล็กทรอนิกส์

กรรมการ

นายสุเมธ อักษรกิตติ์

ผู้ทรงคุณวุฒิ

-

สภาอุตสาหกรรมแห่งประเทศไทย

นายมนชอล หอมกลิ่นเทียน

สถาบันมาตรวิทยาแห่งชาติ

-

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

นางสาวศรณรินทร์ แสงคะนอง

สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม

นายธีรพัฒน์ มาน้อย

นายเรืองฤทธิ์ หนีแหะ

ศูนย์ทดสอบผลิตภัณฑ์ไฟฟ้าและอิเล็กทรอนิกส์

กรรมการและเลขานุการ

นางสาวอรุณี พัคฆะญาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

นางปัญญดา พัวสกุล

นายกมล เอื้อชินกุล

คณะทำงาน

ที่ปรึกษา

นายชัย วุฒิวิวัฒน์ชัย

นายปิยวุฒิ ศรีชัยกุล

นายเฉลิมพล ชาญศรีภิญโญ

นางผกายมาต อ่ำสุริยา

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

คณะทำงาน ด้านวิชาการ

นางสุภรณ์ เหมือนหนู

นายพิทักษ์ เพิ่มประเสริฐ

นายสมเดช แสงสุรศักดิ์

นายถิรเจต พันพาไพร

นางสาวอรินี พยัคฆะญาติ

นางปัญญดา พัวสกุล

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

คณะทำงาน ด้านบรรณาธิการ

-

ในปัจจุบัน มีการนำเทคโนโลยีสมองกลฝังตัว อินเทอร์เน็ตของสรรพสิ่ง มาประยุกต์ใช้ในการออกแบบให้เครื่องตัดวงจร (circuit breaker) มีคุณสมบัติเพิ่มเติม ในการตรวจจับความผิดปกติทางไฟฟ้าเพื่อควบคุมให้อยู่ในสภาวะปลอดภัย การสื่อสารข้อมูลแบบเรียลไทม์ การวิเคราะห์สถานะ เพื่อบริหารจัดการพลังงานไฟฟ้า เป็นต้น ทำให้เครื่องตัดวงจร ทำงานได้อย่างอัตโนมัติและมีความอัจฉริยะ

การทำงานที่หลากหลายได้อย่างอัตโนมัติและมีความอัจฉริยะของเครื่องตัดวงจร ส่งผลให้มีการทำงานที่ซับซ้อนและ เชื่อมโยงกับระบบต่าง ๆ มากขึ้น ทำให้การทดสอบความปลอดภัยตามมาตรฐานที่มีอยู่เดิมจึงไม่เพียงพอ เนื่องจาก ความซับซ้อนของระบบทั้งหมดได้เพิ่มความเสี่ยงต่อความล้มเหลวในการทำงานของเครื่องตัดวงจร ส่งผลให้การ ทดสอบความปลอดภัยเชิงหน้าที่ (functional safety) มีความจำเป็นเพื่อควบคุมความเสี่ยงจากอันตรายที่อาจเกิด จากความล้มเหลวในการทำงานของเครื่องตัดวงจรอัจฉริยะ และเพื่อสร้างความมั่นใจให้กับผู้ใช้งานว่าเครื่องตัดวงจรที่มี ความอัจฉริยะ (เครื่องตัดวงจรอัจฉริยะ) จะทำงานได้อย่างปลอดภัยภายใต้สภาวะต่าง ๆ จึงกำหนดมาตรฐานเครื่องตัด วงจรอัจฉริยะ - ความปลอดภัยเชิงหน้าที่นี้ขึ้น

มาตรฐานนี้ จัดทำขึ้นโดย ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และ เทคโนโลยีแห่งชาติ ที่ตั้งอยู่ที่ ๑๑๒ อุทยานวิทยาศาสตร์ประเทศไทย ถ.พหลโยธิน ต.คลองหนึ่ง อ.คลองหลวง จ.ปทุมธานี ๑๑๑๓๐ และโทรศัพท์ ๐ ๒๕๖๔ ๖๙๐๐

มาตรฐานนี้กำหนดขึ้นโดยอาศัยข้อมูลจากผู้ทำ ผู้ใช้ และเอกสารต่อไปนี้เป็นแนวทาง

- | | |
|---------------------|---|
| มอก. 2732 เล่ม 1 | มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 1 ข้อกำหนดทั่วไป |
| มอก. 2732 เล่ม 2 | มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 2 ข้อกำหนดสำหรับระบบที่ เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ |
| มอก. 2732 เล่ม 3 | มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 3 ข้อกำหนดสำหรับซอฟต์แวร์ |
| มอก. 2732 เล่ม 3(1) | มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 3(1) ข้อกำหนดซอฟต์แวร์ - การ ใช้ซ้ำขององค์ประกอบซอฟต์แวร์ที่มีอยู่ก่อนซึ่งดำเนินการฟังก์ชันนิรภัยทั้งหมดหรือบางส่วน |

- มอก. 2732 เล่ม 4 มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 4 บทนิยามและอักษรย่อ
- มอก. 2732 เล่ม 5 มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 5 ตัวอย่างวิธีการกำหนดระดับบูรณาการความปลอดภัย
- มอก. 2732 เล่ม 6 มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 6 แนวทางการประยุกต์ใช้ มอก. 2732 เล่ม 2 และ มอก. 2732 เล่ม 3
- มอก. 2732 เล่ม 7 มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 7 ภาพรวมของเทคนิคและตัวชี้วัด

สารบัญ

หน้า

๑. ขอบข่าย.....	1
๒. เอกสารอ้างอิง.....	2
๓. นิยาม.....	4
๔. เครื่องหมาย ฉลาก และเอกสารแนะนำ.....	7
๕. ข้อกำหนดสมรรถนะด้านความปลอดภัย.....	13
๖. ข้อกำหนดด้านความปลอดภัยเชิงหน้าที่.....	14
๗. ข้อกำหนดด้านความมั่นคงปลอดภัย.....	20
๘. ข้อกำหนดด้านการคงไว้ซึ่งความปลอดภัยเชิงหน้าที่.....	21
๙. รายงานผลการทดสอบ.....	28
ภาคผนวก ก. การตรวจสอบความปลอดภัยเชิงหน้าที่ของหน้าที่ควบคุมผ่านวงจรนำร่องเมื่อเครื่องตัดวงจรทำหน้าที่ร่วมกับบริภัณฑ์อัดประจุแบบไฟฟ้ากระแสสลับสำหรับยานยนต์ไฟฟ้า.....	30
ภาคผนวก ข. หลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัย.....	30
ภาคผนวก ค. วิธีการทดสอบด้านความปลอดภัยเชิงหน้าที่.....	41
ภาคผนวก ง. แนวทางการตรวจ การทดสอบ และการบำรุงรักษาเครื่องตัดวงจร.....	57
ภาคผนวก จ. ตัวอย่างรายงานผลการทดสอบ.....	59

มาตรฐาน เครื่องตัดวงจรอัจฉริยะ - ความปลอดภัยเชิงหน้าที่

๑. ขอบข่าย

- ๑.๑ มาตรฐานนี้ให้รายละเอียดข้อกำหนดที่ต้องการ วิธีการทดสอบและเกณฑ์การตัดสินความปลอดภัยเชิงหน้าที่สำหรับเครื่องตัดวงจรอัจฉริยะที่มีการเพิ่มความสามารถเชิงหน้าที่ให้มากขึ้น และประสงค์ให้ใช้ในที่อยู่อาศัยและงานทั่วไปที่มีลักษณะคล้ายกัน ที่มีแรงดันไฟฟ้ากระแสสลับที่กำหนดไม่เกิน ๔๔๐ โวลต์ ความถี่ที่กำหนด ๕๐ เฮิรตซ์ กระแสไฟฟ้าที่กำหนดไม่เกิน ๑๒๕ แอมแปร์ ความสามารถทนกระแสไฟฟ้าลัดวงจรไม่เกิน ๒๕ ๐๐๐ แอมแปร์ เมื่อทำงานที่ความถี่ ๕๐ เฮิรตซ์

ความสามารถเชิงหน้าที่ที่เพิ่มขึ้นตามมาตรฐานนี้ หมายถึง ความสามารถในการรวบรวมข้อมูล การวิเคราะห์ข้อมูล การตัดสินใจจากข้อมูลที่ได้วิเคราะห์ไว้ และการดำเนินการต่าง ๆ ตามหน้าที่ เช่น “ตัดวงจร” เมื่อเกิดสถานการณ์กระแสเกิน กระแสเหลือ แรงดันเกิน/ตก การอาร์ก ลัดวงจร หรือสภาวะทางไฟฟ้าผิดปกติอื่น ๆ “ต่อวงจร” โดยต่อวงจรกลับตามเงื่อนไขหรือโดยอัตโนมัติ และ “เปลี่ยนค่าตั้งหรือเงื่อนไขการทำงาน” โดยสามารถเปลี่ยนได้จากระยะไกล ไม่ว่าจะจากผู้ใช้หรือจากระบบควบคุมซึ่งเป็นความสามารถของเครื่องตัดวงจร

หมายเหตุ การเพิ่มความสามารถเชิงหน้าที่ หมายรวมถึงการเพิ่มหน้าที่การทำงานใหม่ของอุปกรณ์ และการเพิ่มมอดูลหรือความสามารถโดยใช้อุปกรณ์อื่นเพื่อทำงานร่วมกันด้วย

- ๑.๒ มาตรฐานนี้ไม่ครอบคลุม ข้อกำหนดทางเทคนิค และวิธีการทดสอบ ของสมรรถนะหรือการทำงานต่าง ๆ ที่ไม่เกี่ยวข้องกับความปลอดภัยเชิงหน้าที่ ตัวอย่างเช่น

- รายละเอียดโปรโตคอลการสื่อสารที่เลือกใช้
- ขั้นตอนการกำหนดค่าพารามิเตอร์ผ่านส่วนต่อประสานกับผู้ใช้
- ตรรกะ (logic) ในการทำงานของระบบอัตโนมัติในส่วนที่ไม่เกี่ยวข้องกับการป้องกันอันตรายทางไฟฟ้า
- กลไกและค่าพารามิเตอร์สำหรับประหยัดพลังงาน

- ๑.๓ อาจมีข้อกำหนดเพิ่มเติมสำหรับ

- การใช้งานเครื่องตัดวงจรร่วมกับมอดูลเสริม หรืออุปกรณ์ต่อพ่วงอื่น ๆ เพื่อขยายขอบเขตความสามารถในการทำงาน (เช่น ระบบบริหารจัดการพลังงานขั้นสูง)

หมายเหตุ ภาคผนวก ก. ให้รายละเอียดสำหรับการตรวจสอบความปลอดภัยเชิงหน้าที่เมื่อมีการเพิ่มหน้าที่หรือมอดูลเพื่อให้เครื่องตัดวงจรทำหน้าที่ร่วมกับบริษัทที่จัดประเภทการนำไฟฟ้าสำหรับยานยนต์ไฟฟ้าชนิดไฟฟ้ากระแสสลับ โดยครอบคลุมเฉพาะหน้าที่ควบคุมผ่านวงจรนำร่อง (control pilot function)

- มาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์ทั่วไปของระบบเทคโนโลยีสารสนเทศ ความเป็นส่วนตัวของข้อมูล หรือความปลอดภัยของโครงสร้างพื้นฐานคลาวด์ ในส่วนที่ไม่เกี่ยวข้องกับความปลอดภัยเชิงหน้าที่

๒. เอกสารอ้างอิง

เอกสารอ้างอิงที่ระบุนี้ เป็นส่วนหนึ่งของข้อกำหนดในมาตรฐานนี้ สำหรับเอกสารอ้างอิงฉบับที่ระบุที่พิมพ์ ให้ใช้ฉบับที่ระบุ (รวมถึงฉบับแก้ไขเพิ่มเติม) ส่วนเอกสารอ้างอิง ที่ไม่ได้ระบุปีที่พิมพ์นั้น ให้ใช้ฉบับล่าสุด

มอก. 909	มาตรฐานผลิตภัณฑ์อุตสาหกรรม เครื่องตัดวงจรกระแสเหลือแบบมีอุปกรณ์ป้องกันกระแสเกิน สำหรับใช้ในที่อยู่อาศัยและใช้ในลักษณะที่คล้ายกัน
มอก. 1452	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ความเข้ากันได้ทางแม่เหล็กไฟฟ้า เล่ม 4 เทคนิคการทดสอบ และการวัด ส่วนที่ 2 การทดสอบภูมิคุ้มกันการปล่อยประจุไฟฟ้าสถิต
มอก. 1454	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ความเข้ากันได้ทางแม่เหล็กไฟฟ้า เล่ม 4 เทคนิคการทดสอบ และการวัดส่วนที่ 4 การทดสอบภูมิคุ้มกันภาวะชั่วคราว/เบิร์สอย่างเร็วทางไฟฟ้า
มอก. 1455	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ความเข้ากันได้ทางแม่เหล็กไฟฟ้า เล่ม 4 เทคนิคการทดสอบ และการวัด ส่วนที่ 5 การทดสอบภูมิคุ้มกันเสิร์จ
มอก. 2425	มาตรฐานผลิตภัณฑ์อุตสาหกรรม เครื่องตัดวงจรใช้กระแสเหลือแบบไม่มีอุปกรณ์ป้องกันกระแสเกิน สำหรับใช้ในที่อยู่อาศัยและใช้ในลักษณะที่คล้ายกัน เล่ม 1 หลักเกณฑ์ทั่วไป
มอก. 2732 เล่ม 1	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 1 ข้อกำหนดทั่วไป
มอก. 2732 เล่ม 2	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 2 ข้อกำหนดสำหรับระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้
มอก. 2732 เล่ม 3	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 3 ข้อกำหนดสำหรับซอฟต์แวร์

มอก. 2732 เล่ม 3(1)	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 3(1) ข้อกำหนดซอฟต์แวร์ - การใช้ซ้ำขององค์ประกอบซอฟต์แวร์ที่มีอยู่ก่อนซึ่งดำเนินการฟังก์ชันนิรภัยทั้งหมดหรือบางส่วน
มอก. 2732 เล่ม 4	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 4 บทนิยามและอักษรย่อ
มอก. 2732 เล่ม 5	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 5 ตัวอย่างวิธีการกำหนดระดับบูรณาการความปลอดภัย
มอก. 2732 เล่ม 6	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 6 แนวทางการประยุกต์ใช้ มอก. 2732 เล่ม 2 และ มอก. 2732 เล่ม 3
มอก. 2732 เล่ม 7	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ฟังก์ชันนิรภัยของระบบที่เกี่ยวข้องกับความปลอดภัยที่ใช้ไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้ เล่ม 7 ภาพรวมของเทคนิคและตัวชี้วัด
มอก. 2906	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ข้อกำหนดทั่วไปสำหรับอุปกรณ์ตรวจจับอาร์กฟอลต์
มอก. 2955	มาตรฐานผลิตภัณฑ์อุตสาหกรรม เครื่องตัดวงจรกระแสเหลือที่มีและไม่มีอุปกรณ์ป้องกันกระแสเกิน แบบ F และ แบบ B สำหรับใช้ในที่อยู่อาศัยและการใช้ในลักษณะที่คล้ายกัน
มอก. 60898 เล่ม 1	มาตรฐานผลิตภัณฑ์อุตสาหกรรม อุปกรณ์ไฟฟ้า - เครื่องตัดวงจรสำหรับป้องกันกระแสเกินสำหรับใช้ในที่อยู่อาศัยและการติดตั้งที่คล้ายกัน เล่ม 1 เครื่องตัดวงจรสำหรับไฟฟ้ากระแสสลับ
มอก. 61000 เล่ม 4(3)	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ความเข้ากันได้ทางแม่เหล็กไฟฟ้า เล่ม 4 เทคนิคการทดสอบและการวัด ส่วนที่ 3 การทดสอบภูมิคุ้มกันต่อสนามแม่เหล็กไฟฟ้าความถี่วิทยุแบบแผ่รังสี
มอก. 61000 เล่ม 4(6)	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ความเข้ากันได้ทางแม่เหล็กไฟฟ้า เล่ม 4 เทคนิคการทดสอบและการวัด ส่วนที่ 6 ภูมิคุ้มกันต่อสิ่งรบกวนที่นำกระแสความถี่วิทยุ
มอก. 61000 เล่ม 4(8)	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ความเข้ากันได้ทางแม่เหล็กไฟฟ้า เล่ม 4 เทคนิคการทดสอบและการวัด ส่วนที่ 8 ภูมิคุ้มกันต่อสนามแม่เหล็กความถี่ไฟฟ้า

มอก. 61000 เล่ม 4(11)	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ความเข้ากันได้ทางแม่เหล็กไฟฟ้า เล่ม 4 เทคนิคการทดสอบและการวัด ส่วนที่ 11 การทดสอบภูมิคุ้มกันสำหรับแรงดันไฟฟ้าดิ่งลง การขัดจังหวะช่วงสั้น และการแปรผันของแรงดันไฟฟ้า
มอก. 61851 เล่ม 1	มาตรฐานผลิตภัณฑ์อุตสาหกรรม ระบบอัดประจุแบบการนำไฟฟ้าสำหรับยานยนต์ไฟฟ้า เล่ม 1 ข้อกำหนดทั่วไป
ETSI EN 303 645	CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements
ETSI TS 103 701	Cyber Security (CYBER); Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements
IEC 61000-4-34	Electromagnetic compatibility (EMC) - Part 4-34: Testing and measurement techniques - Voltage dips, short interruptions and voltage variations immunity tests for equipment with input current more than 16 A per phase
IEC 63024	Automatic reclosing devices for circuit-breakers-RCBOs-RCCBs for household and similar uses

๓. นิยาม

ความหมายของคำที่ใช้ในมาตรฐานนี้ มีดังต่อไปนี้

- ๓.๑ ความปลอดภัยเชิงหน้าที่ (functional safety) หมายถึง ส่วนหนึ่งของความปลอดภัยโดยรวมที่เกี่ยวข้องกับอุปกรณ์ที่อยู่ภายใต้การควบคุม และระบบควบคุมอุปกรณ์ที่อยู่ภายใต้การควบคุม ซึ่งขึ้นอยู่กับการทำงานที่ถูกต้องของเครื่องตัดวงจร และมาตรการลดความเสี่ยงอื่น ๆ

หมายเหตุ ๑ อุปกรณ์ที่อยู่ภายใต้การควบคุม (Equipment Under Control; EUC) หมายถึง อุปกรณ์ เครื่องจักร เครื่องมือ หรือโรงงานที่ใช้สำหรับการผลิต กระบวนการ การขนส่ง การแพทย์ หรือกิจกรรมอื่น ๆ

หมายเหตุ ๒ ระบบควบคุมอุปกรณ์ที่อยู่ภายใต้การควบคุม (EUC control system) หมายถึง ระบบที่ตอบสนองต่อสัญญาณขาเข้าจากกระบวนการ และ/หรือ จากผู้ปฏิบัติงาน และสร้างสัญญาณขาออกเพื่อส่งผลให้อุปกรณ์ที่อยู่ภายใต้การควบคุมทำงานในลักษณะที่ต้องการ

หมายเหตุ ๓ ระบบควบคุมอุปกรณ์ที่อยู่ภายใต้การควบคุมจะแยกส่วนและแตกต่างจากตัวอุปกรณ์ที่อยู่ภายใต้การควบคุม

- ๓.๒ เครื่องตัดวงจรอัจฉริยะ (smart circuit breaker; SCB) หมายถึง เครื่องตัดวงจรสำหรับวงจรไฟฟ้าใช้ในที่อยู่อาศัยและการใช้ในลักษณะที่คล้ายกัน ที่มีความสามารถอัจฉริยะ ได้แก่ การตรวจจับ การสื่อสาร การควบคุมระยะไกล การบันทึกข้อมูล การกำหนดค่าพารามิเตอร์ การทำให้เป็นอัตโนมัติ โดยทำงานร่วมกันกับอุปกรณ์

อื่นผ่านระบบเครือข่าย เพื่อควบคุมการจ่ายกระแสไฟฟ้าและตัดกระแสไฟฟ้าได้ภายใต้ภาวะวงจรปกติ รวมถึงควบคุมการจ่ายกระแสไฟฟ้าตามระยะเวลาที่กำหนด และตัดกระแสไฟฟ้าภายใต้สภาวะผิดปกติที่กำหนด เช่น ไฟฟ้าลัดวงจร กระแสเหลือ กระแสเกิน การอาร์ก โดยไม่ขึ้นกับประเภทของการตัดวงจร ซึ่งต่อไปในมาตรฐานนี้จะเรียกว่า “เครื่องตัดวงจร”

หมายเหตุ ประเภทของการตัดวงจร เช่น เทอร์โมแมกเนติก (thermal-magnetic) อิเล็กทรอนิกส์ทริป (electronic-trip) โซลิดสเตท (solid-state)

- ๓.๓ ความปลอดภัย (safety) หมายถึง สภาวะที่ปราศจากความเสี่ยงที่ไม่อาจยอมรับได้
- ๓.๔ ระดับบูรณาการความปลอดภัย (Safety Integrity Level; SIL) หมายถึง ระดับไม่ต่อเนื่อง (ระดับใดระดับหนึ่งจากสี่ระดับที่เป็นไปได้) ซึ่งสอดคล้องกับช่วงของค่าบูรณาการความปลอดภัย โดยที่ระดับบูรณาการความปลอดภัย ๔ มีระดับบูรณาการความปลอดภัยสูงสุด และระดับบูรณาการความปลอดภัย ๑ มีระดับบูรณาการความปลอดภัยต่ำสุด

หมายเหตุ ๑ มาตรการความล้มเหลวเป้าหมายสำหรับระดับบูรณาการความปลอดภัยทั้งสี่ระดับ ถูกกำหนดไว้ในตารางที่ ๒ และตารางที่ ๓ ของ มอก. 2732 เล่ม 1

หมายเหตุ ๒ ระดับบูรณาการความปลอดภัยถูกนำมาใช้สำหรับกำหนดข้อกำหนดด้านบูรณาการความปลอดภัยของหน้าที่ความปลอดภัยที่จะจัดสรรให้แก่ระบบที่เกี่ยวข้องกับความปลอดภัยประเภทไฟฟ้า/อิเล็กทรอนิกส์/อิเล็กทรอนิกส์แบบโปรแกรมได้

หมายเหตุ ๓ ระดับบูรณาการความปลอดภัยไม่ใช่คุณสมบัติของระบบ ระบบย่อย องค์ประกอบ หรือชิ้นส่วนเปลี่ยนทดแทน การตีความที่ถูกต้องของวลี “ระบบที่เกี่ยวข้องกับความปลอดภัยระดับ SIL n” (เมื่อ n คือ ๑, ๒, ๓ หรือ ๔) คือ ระบบนั้นมีขีดความสามารถในตัว (potentially capable) ที่จะรองรับหน้าที่ความปลอดภัยที่มีระดับบูรณาการความปลอดภัยได้สูงสุดถึงระดับ n

- ๓.๕ ระบบควบคุมอิเล็กทรอนิกส์แบบโปรแกรมได้ (Programmable Electronic Control System; PECS) หมายถึง ระบบหรือชุดอุปกรณ์ที่อาศัยเทคโนโลยีอิเล็กทรอนิกส์แบบโปรแกรมได้เป็นแกนหลักในการวิเคราะห์ประมวลผล ควบคุม และตัดสินใจ เพื่อการปฏิบัติงานตามหน้าที่ปกติและหน้าที่ความปลอดภัยของเครื่องตัดวงจร ซึ่งโครงสร้างการทำงาน การไหลของข้อมูล และตรรกะการประมวลผลสามารถปรับเปลี่ยนหรือตั้งค่าได้ ทั้งนี้ นิยามนี้ให้ครอบคลุมถึงระบบที่ใช้สถาปัตยกรรมแบบประมวลผลตามลำดับ (Sequential Processing) เช่น ไมโครโพรเซสเซอร์ ไมโครคอนโทรลเลอร์ ตัวประมวลผลสัญญาณดิจิทัล (Digital Signal Processor; DSP) และให้ครอบคลุมถึงระบบที่ใช้สถาปัตยกรรมลอจิกฮาร์ดแวร์แบบขนาน (Parallel Hardware Logic) เช่น อุปกรณ์ตรรกะแบบโปรแกรมได้ (Programmable Logic Device; PLD) วงจรเกตโปรแกรมได้แบบฟิลด์ (Field-Programmable Gate Array; FPGA) และวงจรรวมเฉพาะงาน (Application-Specific Integrated Circuit; ASIC)

๓.๖ **สถานะปลอดภัย (safe state)** หมายถึง สถานะของเครื่องตัวจริงและระบบไฟฟ้าที่เกี่ยวข้องซึ่งกำหนดสำหรับอันตรายหรือเหตุการณ์อันตรายแต่ละกรณี เพื่อทำให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ภายหลังเกิดความผิดพลาด ความล้มเหลว หรือสถานะอันตราย สถานะปลอดภัยอาจรวมถึงการตัดหรือแยกวงจร การคั่นหน้าที่ป้องกัน การยับยั้งการเริ่มต้นใหม่หรือการต่อกลับอัตโนมัติ หรือการดำเนินการอื่นตามที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย ทั้งนี้ การต่อกลับอัตโนมัติอาจกระทำได้เฉพาะเมื่อเงื่อนไขด้านความปลอดภัยที่กำหนดได้รับการตรวจสอบครบถ้วนแล้ว

หมายเหตุ ๑ ในการเปลี่ยนผ่านจากสถานะที่อาจเกิดอันตรายไปสู่สถานะปลอดภัยขั้นสุดท้าย อุปกรณ์ที่อยู่ภายใต้การควบคุมอาจจำเป็นต้องผ่านสถานะปลอดภัยชั้นกลางจำนวนหนึ่ง และสำหรับบางสถานการณ์ สถานะปลอดภัยจะคงอยู่ได้ก็ต่อเมื่ออุปกรณ์ที่อยู่ภายใต้การควบคุมได้รับการควบคุมอย่างต่อเนื่องเท่านั้น ซึ่งการควบคุมอย่างต่อเนื่องดังกล่าวอาจดำเนินการในช่วงระยะเวลาสั้น ๆ หรือเป็นระยะเวลาที่ไม่กำหนดแน่นอน

หมายเหตุ ๒ รูปแบบพฤติกรรมการตอบสนองเพื่อเข้าสู่สถานะปลอดภัย และกรอบเวลาความปลอดภัยของกระบวนการของแต่ละสถานะอันตราย เป็นข้อมูลที่ระบุและบันทึกไว้ในข้อกำหนดความต้องการด้านความปลอดภัย (safety requirements specification) และคู่มือความปลอดภัยประจำผลิตภัณฑ์ เพื่อใช้ประกอบการประเมินตามอนุกรม มอก. 2732

๓.๗ **ระยะเวลาทนทานต่อความผิดพลาดของเครื่องตัวจริง (Fault Tolerant Time Interval; FTTI)** หมายถึง ช่วงระยะเวลาที่สั้นที่สุดนับตั้งแต่วินาทีที่เกิดความผิดพลาดขึ้นในระบบควบคุมอิเล็กทรอนิกส์หรือซอฟต์แวร์ประมวลผล จนกระทั่งถึงจุดเวลาที่ระบบจะแปรเปลี่ยนสถานะไปสู่การเกิดอุบัติการณ์ที่เป็นอันตรายในกรณีที่เกิดจากความผิดพลาดไม่ได้ดำเนินการตอบสนอง

๓.๘ **สถาปัตยกรรม (architecture)** หมายถึง การจัดวางโครงสร้างและการเชื่อมต่อกันของหน่วยประมวลผล หรือช่องสัญญาณภายในระบบของเครื่องตัวจริง เพื่อให้บรรลุตามระดับบูรณาการความปลอดภัยที่กำหนด

๓.๙ **พารามิเตอร์ด้านความปลอดภัย (safety-related parameter)** หมายถึง ค่า ข้อมูล หรือการกำหนดค่าที่ใช้ในการกำหนดหรือมีผลต่อการทำงานของหน้าที่ความปลอดภัย รวมถึงเงื่อนไขการกระตุ้น ขอบเขตการทำงาน ระยะเวลาการตอบสนอง ลำดับความสำคัญของการทำงาน และเงื่อนไขการเข้าสู่หรือออกจากสถานะปลอดภัย ตามที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย

หมายเหตุ ตัวอย่างพารามิเตอร์ด้านความปลอดภัย เช่น ค่ากระแสหรือแรงดันที่ใช้เป็นเกณฑ์การทำงานของหน้าที่ความปลอดภัย ระยะเวลาหน่วง เงื่อนไขการต่อกลับอัตโนมัติ และค่าหรือเงื่อนไขอื่นที่กำหนดไว้ในข้อกำหนดความต้องการด้านความปลอดภัย

๓.๑๐ **ขีดความสามารถเชิงระบบ (systematic capability)** หมายถึง ระดับความมั่นใจว่าระบบควบคุมอิเล็กทรอนิกส์แบบโปรแกรมได้และซอฟต์แวร์จะทำงานได้ตามข้อกำหนดโดยปราศจากข้อผิดพลาดเชิงระบบที่สอดคล้องกับข้อกำหนดระดับบูรณาการความปลอดภัยของหน้าที่ความปลอดภัยนั้น ๆ

๔. เครื่องหมาย ฉลาก และเอกสารแนะนำ

- ๔.๑ เครื่องตั่ววงจรทุคเครื่องอย่างนัอยตั่วมีเลข อักขร เครื่องหมาย หรือข้อความ แจ้งรายละเอียดตามท่กำหนด ในข้อนี้ โดยตั่วอ่านได้ง่าย ชัดเจน และคงทนถาวร ในกรณีท่ใช้ภาษาตั่วประเทศ ตั่วมีความหมายตรงท่กับ ภาษาไทย และตั่วไม่วาเครื่องหมายหรือฉลากบนหมุดเกลียว แหวนรอน หรือชิ้นส่วนอื่่นท่ถอดออกได้
- เครื่องหมายหรือข้อความตั่วประกอบด้วยรายละเอียด ดังตั่วไปนี้

	เครื่องหมายหรือข้อความ บนเครื่องตั่ววงจร	ตั่วแหน่งของเครื่องหมายหรือข้อความ		
		มองเห็นได้ง่าย เมือตั่วตั่วเครื่อง ตั่ววงจรแล้ว	ตั่ว้นข้างหรือ ตั่ว้นหลังของ เครื่องตั่ววงจร	เอกสารแนะนำ ของผู้อั่วทำ
ก	ชื่อผู้อั่วทำ หรือเครื่องหมายการค้าท่จด ทะเบียน		X	
ข	ชื่อแบบ หมายเลขคั่วตั่วตั่วล็อก หรือ หมายเลขเครื่อง		X	
ค	แรงดันไฟฟ้าท่กำหนด	X	X	
ง ^๑	กระแสไฟฟ้าท่กำหนด	X		
จ	ความถี่ท่กำหนด - ความถี่ ๕๐ เฮิร์ตซ์ - ความถี่ท่เครื่องตั่ววงจรถูก ออกแบบให้ทำงานได้นอก เหนือจากความถี่ข้างตั่ว้น		X	X
ฉ	กระแสเหลือท่ทำงานท่กำหนด	X		
ช	การตั่วตั้งของกระแสเหลือท่ทำงาน สำหรับ เครื่องตั่ววงจรท่มีกระแสเหลือ ท่ทำงานหลายค่า	X		
ญ	ความทนกระแสไฟฟ้าลั่วตั่ววงจรท่กำหนด หน่วยเป็น แอมแปร์		X	
ฎ	อุณหภูมิสอบเทียบอั่ว้งอิง ถั่วแตกต่าง ไปจาก ๓๐ องศาเซลเซียส			X

	เครื่องหมายหรือข้อความบนเครื่องตัดวงจร	ตำแหน่งของเครื่องหมายหรือข้อความ		
		มองเห็นได้ง่ายเมื่อติดตั้งเครื่องตัดวงจรแล้ว	ด้านข้างหรือด้านหลังของเครื่องตัดวงจร	เอกสารแนะนำของผู้ทำ
ฐ ^๒	วิสัยสมารถการต่อและการตัดกระแสเหลือที่กำหนด		X	
ท	ระดับชั้นการป้องกัน (ถ้าแตกต่างไปจาก IP20 เท่านั้น)			X
ฒ	ตำแหน่งของการใช้งาน (ถ้าจำเป็น)		X	
ณ	สัญลักษณ์ S ล้อมรอบด้วยสี่เหลี่ยม  สำหรับอุปกรณ์แบบ S	X		
ด	เครื่องหมายตามประเภทวิธีการทำงาน			X
ต	ส่วนทำงานของอุปกรณ์ทดสอบ แสดงเครื่องหมายด้วยตัวอักษร T	X		
ถ ^๓	แผนผังการต่อสาย ยกเว้นจะเห็นการเชื่อมต่อได้ชัดเจน		X	
ท ^{๔ ๕}	ลักษณะเฉพาะการทำงานในกรณีของกระแสเหลือที่มีองค์ประกอบไฟฟ้ากระแสตรง	X		
ธ	ว่าง			
น	รหัส มอก. หรือ มาตรฐานผลิตภัณฑ์อ้างอิง		X	
บ	สำหรับเครื่องตัดวงจร แบบ D กระแสไฟฟ้าทริปทันทีสูงสุด (maximum instantaneous tripping current) หากมีค่ามากกว่า 20 เท่าของกระแสไฟฟ้าที่กำหนด (I_n)		X	
ป	ถ้ามีความจำเป็นต้องชี้ให้เห็นความแตกต่างระหว่างขั้วต่อสายของแหล่งจ่ายกับขั้วต่อสายของโหลด ต้องมีเครื่องหมายที่ชัดเจน (เช่น ใช้คำว่า "แหล่งจ่าย		X	

	เครื่องหมายหรือข้อความบนเครื่องตัดวงจร	ตำแหน่งของเครื่องหมายหรือข้อความ		
		มองเห็นได้ง่ายเมื่อติดตั้งเครื่องตัดวงจรแล้ว	ด้านข้างหรือด้านหลังของเครื่องตัดวงจร	เอกสารแนะนำของผู้ทำ
	(line)" และ "โหลด (load)" ติดไว้ใกล้กับขั้วต่อสายที่สอดคล้องกันหรือใช้ลูกศรชี้บอกทิศทางการไหลของกำลังไฟฟ้า)			
ผ	ขั้วต่อสายที่มีจุดประสงค์เฉพาะการต่อตัวนำนิวทรัลต้องแสดงด้วยอักษร N		X	
ผ	ขั้วต่อสายที่มีจุดประสงค์สำหรับต่อลงดินเชิงฟังก์ชัน (functional earth, FE) ต้องทำเครื่องหมายด้วยสัญลักษณ์ (IEC 60417-5018-2011-07) 		X	
พ	ระดับบูรณาการความปลอดภัยของแต่ละหน้าที่ความปลอดภัย		X	
พ ^๖	ประเภทการป้องกัน		X	
ภ	รูปแบบการเชื่อมต่อไร้สายที่รองรับ ให้แสดงด้วยสัญลักษณ์หรือเครื่องหมายที่เหมาะสม เช่น Wi-Fi หรือ Bluetooth	X		
หมายเหตุ ๑ สำหรับเครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่พื้นฐานตามข้อ ๕.๒.๑ การตัดวงจรกระแสเกิน รูปแบบการแสดงค่ากระแสไฟฟ้าที่กำหนดไม่แสดงสัญลักษณ์ "A" และใช้สัญลักษณ์ของกระแสเกินทริปทันที (B C หรือ D) นำหน้า หมายเหตุ ๒ แสดงหากแตกต่างไปจากความทนกระแสไฟฟ้าลัดวงจรที่กำหนด หมายเหตุ ๓ แผนผังการต่อสายอาจอยู่ด้านในของฝาครอบที่ถอดออกก่อนการต่อสายไฟฟ้าของแหล่งจ่าย หมายเหตุ ๔ แสดงเครื่องหมายอย่างใดอย่างหนึ่งดังต่อไปนี้ - เครื่องตัดวงจร แบบ AC ให้ใช้สัญลักษณ์  - เครื่องตัดวงจร แบบ A ให้ใช้สัญลักษณ์  - เครื่องตัดวงจร แบบ F (ป้องกันในกรณีที่มีกระแสเหลือที่เป็น กระแสลบลูปคลื่นไซน์ที่มีความถี่ที่กำหนด กระแสเหลือแบบกระแสตรงพัลส์เซดิง รวมทั้งกระแสเหลือแบบผสมที่อาจเกิดขึ้นได้ ตาม				

เครื่องหมายหรือข้อความบนเครื่องตัดวงจร	ตำแหน่งของเครื่องหมายหรือข้อความ		
	มองเห็นได้ง่ายเมื่อติดตั้งเครื่องตัดวงจรแล้ว	ด้านข้างหรือด้านหลังของเครื่องตัดวงจร	เอกสารแนะนำของผู้ทำ
มอก. 2955) ให้แสดงสัญลักษณ์  ร่วมกับสัญลักษณ์สำหรับเครื่องตัดวงจร แบบ A () เช่น    หรือแสดงด้วยสัญลักษณ์  เป็นทางเลือกได้ - เครื่องตัดวงจร แบบ B (ป้องกันในกรณีที่มีกระแสเหลือกระแสสลับรูปคลื่นไซน์ที่มีความถี่สูงถึง 1 000 Hz กระแสเหลือแบบกระแสตรงพัลส์เซตติง และกระแสเหลือแบบกระแสตรงที่เรียบ ตาม มอก. 2955) ให้แสดงสัญลักษณ์  ร่วมกับสัญลักษณ์สำหรับ แบบ F เช่น    หรือแสดงด้วยสัญลักษณ์  เป็นทางเลือกได้			
หมายเหตุ ๕	สัญลักษณ์สำหรับเครื่องตัดวงจรแบบ AC อาจไม่มองเห็นได้ง่ายเมื่อติดตั้งเครื่องตัดวงจรแล้ว โดยแสดงไว้บนเครื่องตัดวงจร		
หมายเหตุ ๖	ประเภทการป้องกันตาม ข้อ ๕.๒ ที่เครื่องตัดวงจรทำงานได้		
	- เครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่เพิ่มเติมตาม ข้อ ๕.๒.๑ และ ข้อ ๕.๒.๒ ให้แสดงเครื่องหมายด้วยตัวอักษร CB - เครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่เพิ่มเติมตาม ข้อ ๕.๒.๓ (ก) ให้แสดงเครื่องหมายด้วยตัวอักษร RCD - เครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่เพิ่มเติมตาม ข้อ ๕.๒.๓ (ข) ให้แสดงเครื่องหมายด้วยตัวอักษร Type-F - เครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่เพิ่มเติมตาม ข้อ ๕.๒.๓ (ค) ให้แสดงเครื่องหมายด้วยตัวอักษร Type-B - เครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่เพิ่มเติมตาม ข้อ ๕.๒.๔ ให้แสดงเครื่องหมายด้วยตัวอักษร AFDD - เครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่เพิ่มเติมตาม ข้อ ๕.๒.๕ ให้แสดงเครื่องหมายด้วยตัวอักษร ARD		

ความเหมาะสมสำหรับการแยกอิสระ ซึ่งเครื่องตัดวงจรทั้งหมดตามมาตรฐานนี้ อาจระบุด้วยสัญลักษณ์



(IEC 60417-6169-1) บนเครื่องตัดวงจร เมื่อทำเครื่องหมายสัญลักษณ์นี้อาจรวมอยู่ในแผนผังการ

ต่อสาย ซึ่งอาจรวมกับสัญลักษณ์ของการทำหน้าที่อื่นๆ เมื่อใช้สัญลักษณ์เพียงแบบเดียว (เช่น ไม่ใช้อยู่ในแผนผังการต่อสาย) ไม่อนุญาตให้ใช้สัญลักษณ์ของการทำงานอื่นร่วมกัน

ถ้ามีการทำเครื่องหมายระดับชั้นการป้องกันมากกว่า IP20 ตาม มอก. 513 บนเครื่องตัดวงจร ให้เป็นไปดังนั้นแล้วแต่วิธีการติดตั้ง ถ้าระดับชั้นการป้องกันที่สูงขึ้นนั้นได้มาโดยวิธีการติดตั้งเฉพาะและ/หรือการใช้อุปกรณ์เสริมเฉพาะ (เช่น ฝาครอบ ขั้วต่อ เปลือกหุ้มฯ) ให้ระบุสิ่งนี้ไว้ในเอกสารของผู้ทำ

นอกเหนือจากเครื่องตัดวงจรที่ทำงานด้วยปุ่มกด ตำแหน่งเปิดต้องแสดงด้วยสัญลักษณ์ “O” (วงกลม) IEC 60417-5008 และตำแหน่งปิดต้องแสดงด้วยสัญลักษณ์ “|” (เส้นตรงสั้นๆ ในแนวตั้ง) IEC 60417-5008

สำหรับเครื่องตัดวงจรที่ทำงานด้วยปุ่มกด 2 ปุ่ม ปุ่มกดที่ออกแบบสำหรับการทำงานเปิดอย่างเดียวเท่านั้นต้องเป็นสีแดงและ/หรือ ทำเครื่องหมายด้วยสัญลักษณ์ “O” (IEC 60417-5008)

ห้ามใช้สีแดง สำหรับปุ่มกดอื่นๆ ของเครื่องตัดวงจร

ถ้าใช้ปุ่มกดตัวเดียวสำหรับการปิดหน้าสัมผัสและมีการระบุที่ชัดเจน ตำแหน่งที่ถูกกดลงต้องเพียงพอที่จะบอกว่าปิดอยู่

ถ้าใช้ปุ่มกดตัวเดียวสำหรับการปิดและเปิดของหน้าสัมผัสและมีการระบุที่ชัดเจน ปุ่มกดที่คงอยู่ในตำแหน่งที่ถูกกดลงต้องเพียงพอที่จะบอกว่าปิดอยู่ ในทางกลับกัน ถ้าปุ่มไม่คงอยู่ในตำแหน่งที่ถูกกดลง ต้องมีการขีดบอกเพิ่มเติม

ขั้วต่อที่มีจุดประสงค์สำหรับตัวนำป้องกัน

(ถ้ามี)

ต้องแสดงด้วยสัญลักษณ์



(IEC

60417-5019-2006-08)

หมายเหตุ

สัญลักษณ์



(IEC 60417-5017-2006-08) ที่เคยแนะนำให้ใช้ ต้องแทนด้วยสัญลักษณ์ IEC 60417-5019 ดังแสดงข้างต้น

สำหรับเครื่องตัดวงจรแบบยึดติดกับราง ต้องมีข้อมูลของรางที่เหมาะสมไว้ในเอกสารของผู้ทำ

สำหรับขั้วต่อแบบยูนิเวอร์แซล (สำหรับตัวนำเส้นเดี่ยวแข็ง ตัวนำตีเกลียวแข็งและตัวนำอ่อนตัวได้)

- ไม่ต้องทำเครื่องหมาย

สำหรับขั้วต่อแบบไม่ยูนิเวอร์แซล

- ขั้วต่อสายที่ระบุสำหรับตัวนำเส้นเดี่ยวแข็งเท่านั้น ต้องแสดงเครื่องหมายด้วยตัวอักษร “S” หรือ “sol”
- ขั้วต่อสายที่ระบุสำหรับตัวนำแข็ง (เส้นเดี่ยวหรือตีเกลียว) เท่านั้น ต้องแสดงเครื่องหมายด้วยอักษร “I”

เครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่พื้นฐานเฉพาะการตัดวงจรกระแสเกิน (ข้อ ๕.๒.๑) และการป้องกันการลัดวงจร (ข้อ ๕.๒.๒) ให้เพิ่มเติม ดังนี้

- แรงดันคงทนอิมพัลส์ที่กำหนด (rated impulse withstand voltage) ถ้ามีค่าเป็น ๒.๕ กิโลโวลต์
- วัสดุสามารถต่อการและการตัดกระแสไฟฟ้าบนขั้วป้องกัน (protected pole) แต่ละขั้วของเครื่องตัดวงจรแบบหลายขั้ว (multipole) (lcn1) ถ้าแตกต่างจากค่าความทนกระแสไฟฟ้าลัดวงจรที่กำหนด (I_{cn})

เครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่พื้นฐานในการตัดวงจรกระแสเหลือ (ข้อ ๕.๒.๓) ให้เพิ่มเติม ดังนี้

- กระแสเหลือที่เป็นไฟฟ้ากระแสสลับหรือไฟฟ้ากระแสตรงแบบพัลส์เซตติง (pulsating direct current) ผู้ทำต้องแสดงค่าเป็นปริพันธ์ของจูล I^2t และวัสดุสามารถทนกระแสไฟฟ้าคายอด I_p ของเครื่องตัดวงจร ถ้าค่าเหล่านี้ไม่ได้แสดงไว้ ให้ใช้ค่าต่ำสุดตามที่กำหนดใน มอก. 2425 ตารางที่ ๑๕

เครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่เพิ่มเติมในการตรวจจับและตัดวงจรเมื่อเกิดการอาร์ก (ข้อ ๕.๒.๔) ให้เพิ่มเติมตามที่กำหนดใน มอก. 2906 ข้อ ๖

เครื่องตัดวงจรที่มีความปลอดภัยสำหรับหน้าที่เพิ่มเติมในการต่อกลับอัตโนมัติ (ข้อ ๕.๒.๕) ให้เพิ่มเติมตามที่กำหนดใน IEC 63024 ข้อ ๖

หมายเหตุ ๑ ความสามารถในการป้องกันแต่ละประเภทอาจมีข้อกำหนดการแสดงผลและวิธีแสดงแตกต่างกัน ข้อมูลที่ซ้ำกันสามารถแสดงเพียงค่าเดียวได้ และกรณีข้อมูลชุดเดียวกันมีหลายค่า การแสดงใช้ค่าที่ให้ผลเลวร้ายที่สุด

หมายเหตุ ๒ ข้อมูลบางอย่างอนุญาตให้แสดงเป็นสัญลักษณ์ได้ หากไม่ทำให้สับสน

หมายเหตุ ๓ ข้อมูลอื่น ๆ นอกเหนือจากที่ระบุข้างต้น แต่ถูกกำหนดโดยมาตรฐานที่เกี่ยวข้อง สามารถแสดงรายละเอียดในรูปแบบของ รหัสแท่ง (barcode) รหัสแท่ง ๒ มิติ (quick response code; QR code) อาร์เอฟไอดี (radio frequency identification; RFID) หรือรูปแบบอื่น ๆ ที่สามารถใช้งานได้ในลักษณะเดียวกัน

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการตรวจพินิจเครื่องหมายหรือข้อความที่แสดงบนเครื่องตัดวงจร และทดสอบความคงทนของเครื่องหมายโดยถูด้วยผ้าฝ้ายชุบน้ำเป็นเวลา ๑๕ วินาที แล้วถูซ้ำอีก ๑๕ วินาทีด้วยผ้าฝ้ายชุบน้ำทำละลายอะซิฟาทิกเฮกเซนตาม มอก. 909 ข้อ ๙.๓ ภายหลังการทดสอบเครื่องหมายต้องอ่านได้ง่าย ต้องไม่สามารถถอดแผ่นเครื่องหมายออกโดยง่าย และแผ่นเครื่องหมายต้องไม่โค้งงอ

เครื่องหมายที่ทำเป็นรอยฝัง แบบขึ้นรูป หรือแบบแม่พิมพ์ ยกเว้นการทดสอบนี้ได้

๕. ข้อกำหนดสมรรถนะด้านความปลอดภัย

๕.๑ พิสัยสามารถในการรองรับ

เครื่องตัดวงจรต้องสามารถทำงานได้อย่างปลอดภัยตามพิสัยสามารถที่พิกัดสูงสุดที่ระบุไว้

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการทดสอบตาม มอก. 909 ข้อ ๙.๗ และข้อ ๙.๘ ที่เกี่ยวข้อง

หมายเหตุ การแสดงหลักฐานการเป็นไปตามข้อกำหนดที่เกี่ยวข้องของ มอก. 60898 เล่ม 1 หรือ มอก. 2425 หรือ มอก. 2955 หรือ มอก. 909 หรือมาตรฐานอื่นที่เทียบเท่า ถือว่าเป็นไปตามข้อกำหนดนี้

๕.๒ ความปลอดภัยสำหรับหน้าที่พื้นฐาน

เครื่องตัดวงจรต้องมีความปลอดภัยต่อผู้ใช้และผู้เกี่ยวข้อง สำหรับหน้าที่พื้นฐานทุกหน้าที่ที่สามารถทำได้ ในพิสัยที่กำหนดไว้

๕.๒.๑ การตัดวงจรกระแสเกิน

เครื่องตัดวงจรต้องทริปเพื่อตัดวงจรเมื่อมีกระแสเกินที่พิกัดสูงสุด ได้อย่างปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการทดสอบตาม มอก. 60898 เล่ม 1 ข้อ ๙.๑๐

หมายเหตุ การแสดงหลักฐานการเป็นไปตามข้อกำหนดที่เกี่ยวข้องของ มอก. 60898 เล่ม 1 หรือ มอก. 909 หรือมาตรฐานอื่นที่เทียบเท่า ถือว่าเป็นไปตามข้อกำหนดนี้

๕.๒.๒ การป้องกันการลัดวงจร

เครื่องตัดวงจรต้องทริปเพื่อตัดวงจรเมื่อมีการลัดวงจรที่พิกัดสูงสุด ได้อย่างปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการทดสอบตาม มอก. 60898 เล่ม 1 ข้อ ๙.๑๒

หมายเหตุ การแสดงหลักฐานการเป็นไปตามข้อกำหนดที่เกี่ยวข้องของ มอก. 60898 เล่ม 1 หรือ มอก. 2425 หรือ มอก. 2955 หรือ มอก. 909 หรือมาตรฐานอื่นที่เทียบเท่า ถือว่าเป็นไปตามข้อกำหนดนี้

๕.๒.๓ การตัดวงจรกระแสเหลือ

เครื่องตัดวงจรต้องทริปเพื่อตัดวงจรเมื่อมีกระแสเหลือ ตามค่าที่ตั้งไว้ในพิกัดที่กำหนด ตามประเภทของเครื่องตัดวงจร ได้อย่างปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการทดสอบตาม

- (ก) มอก. 2425 ข้อ ๙.๙.๒ และ ข้อ ๙.๙.๓ สำหรับเครื่องตัดวงจรใช้กระแสเหลือแบบไม่มีอุปกรณ์ป้องกันกระแสเกิน ประเภท RCCB

(ข) มอก. 2955 ข้อ ๙.๑.๒ ข้อ ๙.๑.๓ ข้อ ๙.๑.๖ และ ข้อ ๙.๑.๗ สำหรับเครื่องตัดวงจรกระแส
เหลือที่ไม่มีอุปกรณ์ป้องกันกระแสเกิน แบบ F และ B

(ค) มอก. 2955 ข้อ ๙.๒.๑ สำหรับเครื่องตัดวงจรกระแสเหลือที่ไม่มีอุปกรณ์ป้องกันกระแสเกิน
แบบ B

หมายเหตุ การแสดงหลักฐานการเป็นไปตามข้อกำหนดที่เกี่ยวข้องของ มอก. 2425 หรือ มอก. 909 หรือ มอก.
2955 หรือมาตรฐานอื่นที่เทียบเท่า ถือว่าเป็นไปตามข้อกำหนดนี้

๕.๒.๔ การตรวจจับและตัดวงจรเมื่อเกิดอาร์กฟอลต์

เครื่องตัดวงจรต้องสามารถตรวจจับการอาร์กและทริปตามค่าที่ตั้งไว้ในพิกัดที่กำหนด ตามประเภทของ
เครื่องตัดวงจร ได้อย่างปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการทดสอบตาม มอก. 2906 ข้อ ๙.๙.๒ และข้อ
๙.๙.๓

หมายเหตุ การแสดงหลักฐานการเป็นไปตามข้อกำหนดที่เกี่ยวข้องของ มอก. 2906 หรือมาตรฐานอื่นที่เทียบเท่า
ถือว่าเป็นไปตามข้อกำหนดนี้

๕.๒.๕ การต่อกลับอัตโนมัติ

เครื่องตัดวงจรที่มีฟังก์ชันต่อกลับอัตโนมัติ ต้องสามารถต่อวงจรกลับอัตโนมัติ เมื่อเกิดการตัดวงจรได้
ตามค่าและเงื่อนไขที่ตั้งไว้ในพิกัดที่กำหนด ได้อย่างปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการทดสอบตาม IEC 63024 ข้อ ๙.๑๘

หมายเหตุ การแสดงหลักฐานการเป็นไปตาม IEC 63024 ถือว่าเป็นไปตามข้อกำหนดนี้

๕.๓ หน้าที่อื่น ๆ

กรณีที่เครื่องตัดวงจรมีหน้าที่ความปลอดภัยอื่นที่ผู้ทำได้ออกแบบไว้ เครื่องตัดวงจรต้องสามารถทำงานได้
อย่างปลอดภัยตามหน้าที่ดังกล่าว

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการทดสอบตามมาตรฐานที่เกี่ยวข้อง

๖. ข้อกำหนดด้านความปลอดภัยเชิงหน้าที่

๖.๑ ทั่วไป

เครื่องตัดวงจรต้องมีสมรรถนะด้านความปลอดภัยเชิงหน้าที่ตามที่ระบุไว้สำหรับทุกรูปแบบผสมของการตั้ง
ค่าที่อยู่ภายในขอบเขตการใช้งานที่ผู้ทำกำหนด ผู้ทำต้องจัดให้มีหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอด

วิศวกรชีวิตด้านความปลอดภัยตามอนุกรม มอก. 2732 ที่จำเป็นและเพียงพอสำหรับแสดงความเป็นไปตามข้อกำหนดด้านความปลอดภัยเชิงหน้าที่ของเครื่องตัดวงจร หลักฐานต้องมีความครบถ้วน สอดคล้อง และสอบกลับได้ และต้องตรงกับรุ่นฮาร์ดแวร์ รุ่นซอฟต์แวร์หรือเฟิร์มแวร์ และการกำหนดค่าของเครื่องตัดวงจรที่ยื่นทดสอบ

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการพิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวิศวกรชีวิตด้านความปลอดภัยตามอนุกรม มอก. 2732

กรณีที่พบความไม่ครบถ้วน ความไม่สอดคล้อง หรือมีข้อสงสัยเกี่ยวกับความเป็นไปตามข้อกำหนด การพิจารณาให้ครอบคลุมถึงการตรวจสอบหลักฐาน รายละเอียดการกำหนดค่า ผลการทดสอบ หรือข้อมูลทางเทคนิคเพิ่มเติม รวมถึงการทดสอบเพิ่มเติมตามความจำเป็น เพื่อให้ได้ข้อมูลที่เพียงพอสำหรับการพิจารณาความเป็นไปตามข้อกำหนด

หมายเหตุ รายการหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวิศวกรชีวิตด้านความปลอดภัยตามอนุกรม มอก. 2732 ที่ใช้ประกอบการพิจารณาตามมาตรฐานนี้ แสดงไว้ในภาคผนวก ข.

๖.๒ การตรวจวินิจฉัยและการตอบสนองต่อความผิดปกติของระบบควบคุมอิเล็กทรอนิกส์แบบโปรแกรมได้

เครื่องตัดวงจรต้องสามารถตรวจพบหรือจัดการความผิดปกติของระบบควบคุมอิเล็กทรอนิกส์แบบโปรแกรมได้ที่อาจส่งผลกระทบต่อหน้าที่ความปลอดภัย โดยความผิดปกติของหน้าที่อัจฉริยะต้องไม่ทำให้สมรรถนะของหน้าที่ป้องกันพื้นฐานตามมาตรฐานผลิตภัณฑ์ที่เกี่ยวข้องลดลง

เมื่อความผิดพร่องดังกล่าวทำให้ไม่สามารถรักษาหน้าที่ความปลอดภัยได้อย่างถูกต้อง เครื่องตัดวงจรต้องเข้าสู่สภาวะปลอดภัยภายในระยะเวลาสูงสุดที่ยอมรับได้ที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย และต้องไม่เกินระยะเวลาทนทานต่อความผิดพร่องที่เกี่ยวข้อง และแสดงหรือส่งสัญญาณสถานะตามที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย

เพื่อให้เป็นไปตามข้อกำหนด เครื่องตัดวงจรต้องมีคุณลักษณะตามที่เกี่ยวข้องอย่างน้อย ดังต่อไปนี้

๖.๒.๑ การเฝ้าระวังความสมบูรณ์ของการปฏิบัติงานอย่างต่อเนื่อง

เครื่องตัดวงจรต้องมีการเฝ้าระวังหรือตรวจวินิจฉัยความสมบูรณ์ของการปฏิบัติงานของระบบควบคุมอิเล็กทรอนิกส์แบบโปรแกรมได้ในระดับและช่วงเวลาที่เพียงพอต่อหน้าที่ความปลอดภัยและระดับบูรณาการความปลอดภัยที่กำหนด เมื่อพบสภาวะผิดปกติที่อาจทำให้ไม่สามารถบรรลุหน้าที่ความปลอดภัย เครื่องตัดวงจรต้องตอบสนองตามสภาวะปลอดภัยภายในระยะเวลาสูงสุดที่ยอมรับได้ที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย โดยการตรวจพบและการตอบสนองรวมกันต้องไม่เกินระยะเวลาทนทานต่อความผิดพร่องที่เกี่ยวข้องในข้อกำหนดความต้องการด้านความปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับขอบเขตของการเฝ้าระวังหรือการตรวจวินิจฉัยอย่างต่อเนื่อง สภาวะผิดปกติที่ต้องตรวจพบ วิธีการตรวจพบ ระยะเวลาสูงสุดในการตรวจพบ การตอบสนองที่กำหนด และความสัมพันธ์กับข้อกำหนดความต้องการด้านความปลอดภัย
- ทดสอบเครื่องต้นแบบโดยกระตุ้นสภาวะผิดปกติจากภายนอกที่เกี่ยวข้องกับการเฝ้าระวังหรือการตรวจวินิจฉัย และตรวจสอบการตอบสนองของเครื่องต้นแบบตามวิธีการที่กำหนดในภาคผนวก ค.๒.๑.๑

๖.๒.๒ การตรวจวินิจฉัยความผิดปกติของอินพุตและเอาต์พุต

เครื่องต้นแบบต้องสามารถตรวจพบหรือจัดการความผิดปกติของอินพุตและเอาต์พุตที่เกี่ยวข้องกับหน้าที่ความปลอดภัย เมื่อความผิดพร่องดังกล่าวอาจทำให้ไม่สามารถบรรลุหน้าที่ความปลอดภัย เครื่องต้นแบบต้องเข้าสู่สภาวะปลอดภัยภายในระยะเวลาสูงสุดที่ยอมรับได้ตามข้อกำหนดความต้องการด้านความปลอดภัย และต้องไม่เกินระยะเวลาหนานานต่อความผิดพร่องที่เกี่ยวข้องในข้อกำหนดความต้องการด้านความปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับอินพุตและเอาต์พุตที่เกี่ยวข้องกับหน้าที่ความปลอดภัย รูปแบบความผิดพร่องที่ต้องตรวจพบหรือจัดการ วิธีการตรวจพบหรือจัดการ การตอบสนองต่อความผิดพร่อง และเวลาที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย
- ทดสอบเครื่องต้นแบบโดยสร้างหรือจำลองความผิดปกติของอินพุตและเอาต์พุตที่เกี่ยวข้องซึ่งสามารถสร้างหรือจำลองได้จากภายนอก และตรวจสอบการตอบสนองของเครื่องต้นแบบตามวิธีการที่กำหนดในภาคผนวก ค.๒.๑.๒

๖.๒.๓ การตรวจวินิจฉัยสภาวะผิดปกติของระบบแรงดันไฟเลี้ยง

เครื่องต้นแบบต้องสามารถตรวจพบหรือจัดการสภาวะผิดปกติของแรงดันไฟเลี้ยงระบบควบคุมอิเล็กทรอนิกส์แบบโปรแกรมได้ที่อาจส่งผลกระทบต่อหน้าที่ความปลอดภัย เมื่อเกิดสภาวะดังกล่าว เครื่องต้นแบบต้องคงไว้ซึ่งหน้าที่ความปลอดภัย หรือเข้าสู่สภาวะปลอดภัยภายในระยะเวลาสูงสุดที่ยอมรับได้ตามข้อกำหนดความต้องการด้านความปลอดภัย และต้องไม่เกินระยะเวลาหนานานต่อความผิดพร่องที่เกี่ยวข้อง และแสดงหรือส่งสัญญาณสถานะตามที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับขอบเขตแรงดันไฟเลี้ยงของระบบควบคุม สภาวะผิดปกติของแรงดันไฟเลี้ยงที่อาจส่งผลกระทบต่อหน้าที่ความปลอดภัย วิธีการตรวจพบหรือจัดการ การตอบสนองของเครื่องตัดวงจร และเวลาที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย
- ทดสอบเครื่องตัดวงจรโดยทำให้แรงดันไฟเลี้ยงที่สามารถเข้าถึงได้จากภายนอกเกิดสภาวะผิดปกติ และตรวจสอบการตอบสนองของเครื่องตัดวงจรตามวิธีการที่กำหนดในภาคผนวก ค.๒.๑.๓

๖.๒.๔ วงรอบการตรวจวินิจัยตนเอง

เครื่องตัดวงจรต้องมีการตรวจวินิจัยตนเองเป็นระยะ เพื่อตรวจหาความผิดปกติที่เกี่ยวข้องกับหน้าที่ความปลอดภัยซึ่งไม่ได้รับการเฝ้าระวังอย่างต่อเนื่อง โดยช่วงเวลาระหว่างการตรวจวินิจัยแต่ละรอบรวมกับระยะเวลาในการตรวจพบและการตอบสนองต่อความผิดปกติ ต้องไม่เกินระยะเวลาสูงสุดที่ยอมรับได้ และต้องไม่เกินระยะเวลาหนานานต่อความผิดปกติที่เกี่ยวข้องตามข้อกำหนดความต้องการด้านความปลอดภัย

การตรวจวินิจัยตนเองต้องไม่ทำให้หน้าที่ความปลอดภัยหรือหน้าที่ป้องกันพื้นฐานตามมาตรฐานผลิตภัณฑ์ที่เกี่ยวข้องหยุดชะงักหรือมีสมรรถนะลดลง

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับความผิดปกติที่อยู่ในขอบเขตของการตรวจวินิจัยตนเอง วงรอบการตรวจวินิจัย ระยะเวลาสูงสุดในการตรวจพบความผิดปกติ ระยะเวลาการตอบสนอง และความสัมพันธ์กับเวลาที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย
- ทดสอบเครื่องตัดวงจรเพื่อตรวจสอบว่าในระหว่างการตรวจวินิจัยตนเอง เครื่องตัดวงจรยังคงสามารถปฏิบัติหน้าที่ความปลอดภัยและหน้าที่ป้องกันพื้นฐานได้ตามที่กำหนด ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๑.๔

๖.๓ การตรวจสอบความผิดปกติระดับซอฟต์แวร์และการประมวลผลเชิงตรรกะ

๖.๓.๑ การตรวจวินิจัยความผิดปกติในการคำนวณและการจัดการข้อมูลตัวแปร

เครื่องตัดวงจรต้องสามารถป้องกัน ตรวจพบ หรือจัดการความผิดปกติในการคำนวณและการจัดการข้อมูลที่อาจส่งผลกระทบต่อหน้าที่ความปลอดภัย เมื่อความผิดปกติดังกล่าวทำให้ไม่สามารถดำเนินหน้าที่ความปลอดภัยได้อย่างถูกต้อง เครื่องตัดวงจรต้องเข้าสู่สภาวะปลอดภัยภายในระยะเวลาสูงสุดที่ยอมรับได้ตามข้อกำหนดความต้องการด้านความปลอดภัย และต้องไม่เกินระยะเวลาหนานานต่อความผิดปกติที่เกี่ยวข้อง และแสดงหรือส่งสัญญาณสถานะตามที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับข้อกำหนดความต้องการด้านความปลอดภัย สถาปัตยกรรมความปลอดภัย การวิเคราะห์ความล้มเหลว และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องตัววงจรโดยป้อนค่าพารามิเตอร์ทางไฟฟ้าจากภายนอกที่ค่าขอบเขต ค่านอกขอบเขต และลำดับค่าที่กำหนดเพื่อทำการคำนวณและการจัดการข้อมูล ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๑.๕

๖.๓.๒ การตรวจวินิจฉัยความผิดปกติของในตรรกะการควบคุมและรักษาพฤติกรรมการทำงาน

เครื่องตัววงจรต้องมีพฤติกรรมการทำงานที่คงที่เมื่อค่าพารามิเตอร์ทางไฟฟ้าเปลี่ยนแปลงหรือผันผวนบริเวณขอบเขตการเปลี่ยนสถานะของตรรกะการควบคุม และต้องไม่เกิดการเปิดและปิดวงจรสลับกันโดยไม่ตั้งใจ เมื่อเกิดความผิดปกติของตรรกะการควบคุมที่ทำให้ไม่สามารถรักษาหน้าที่ความปลอดภัยได้ เครื่องตัววงจรต้องเข้าสู่สภาวะปลอดภัยภายในระยะเวลาสูงสุดที่ยอมรับได้ตามข้อกำหนดความต้องการด้านความปลอดภัย และต้องไม่เกินระยะเวลาทนทานต่อความผิดปกติที่เกี่ยวข้อง และแสดงหรือส่งสัญญาณสถานะตามที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับข้อกำหนดความต้องการด้านความปลอดภัย สถาปัตยกรรมความปลอดภัย การวิเคราะห์ความล้มเหลว และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องตัววงจรโดยทำให้ค่าพารามิเตอร์ทางไฟฟ้าผันผวนซ้ำรอบค่าขอบเขตการทำงานตามวิธีการที่กำหนดในภาคผนวก ค.๒.๑.๖

๖.๓.๓ การตรวจวินิจฉัยความผิดปกติของในลำดับการดำเนินงานและการเปลี่ยนสถานะเชิงตรรกะ

เครื่องตัววงจรต้องสามารถตรวจพบหรือจัดการความผิดปกติของลำดับการดำเนินงานและการเปลี่ยนสถานะที่อาจส่งผลกระทบต่อหน้าที่ความปลอดภัย ต้องไม่ยอมรับลำดับคำสั่งหรือสถานะที่ไม่สอดคล้องกับเงื่อนไขด้านความปลอดภัย และเมื่อไม่สามารถยืนยันสถานะการทำงานที่ปลอดภัยได้ เครื่องตัววงจรต้องเข้าสู่สภาวะปลอดภัยภายในระยะเวลาสูงสุดที่ยอมรับได้ตามข้อกำหนดความต้องการด้านความปลอดภัย และต้องไม่เกินระยะเวลาทนทานต่อความผิดปกติที่เกี่ยวข้อง และแสดงหรือส่งสัญญาณสถานะตามที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับข้อกำหนดความต้องการด้านความปลอดภัย สถาปัตยกรรมความปลอดภัย การวิเคราะห์ความล้มเหลว และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องตัดวงจรโดยส่งคำสั่งหรือเหตุการณ์ผ่านส่วนต่อประสานภายนอกทั้งในลำดับปกติ ลำดับผิดปกติ และกรณีขัดจังหวะระหว่างการเปลี่ยนสถานะ ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๑.๗

๖.๓.๔ การจัดการคำสั่งที่ขัดแย้งกับหน้าที่ความปลอดภัย

เครื่องตัดวงจรต้องจัดการคำสั่งหรือการเปลี่ยนแปลงค่าที่อาจขัดแย้งกับหน้าที่ความปลอดภัยตามลำดับความสำคัญด้านความปลอดภัยที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย โดยหน้าที่ความปลอดภัยต้องยังคงบรรลุผลการตอบสนองภายในระยะเวลาสูงสุดที่ยอมรับได้ และไม่เกินระยะเวลาทนทานต่อความผิดพลาดที่เกี่ยวข้อง

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับข้อกำหนดความต้องการด้านความปลอดภัย ลำดับความสำคัญของคำสั่งและหน้าที่ การออกแบบตรรกะการควบคุม และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องตัดวงจรโดยกระตุ้นหน้าที่ความปลอดภัย แล้วส่งคำสั่งหรือกำหนดค่าผ่านส่วนต่อประสานที่ผลิตภัณฑ์รองรับซึ่งอาจขัดแย้งกับหน้าที่ดังกล่าว ตามวิธีการที่กำหนดในภาคผนวก ค. ๒.๑.๘

๖.๔ การทดสอบความทนทานต่อสภาวะแวดล้อม

๖.๔.๑ ความทนทานต่อสัญญาณรบกวนทางแม่เหล็กไฟฟ้า

เครื่องตัดวงจรต้องมีความทนทานต่อสัญญาณรบกวนทางแม่เหล็กไฟฟ้า โดยต้องรักษาสมรรถนะและความปลอดภัยเชิงหน้าที่ภายใต้สภาวะการถูกรบกวนเชิงแม่เหล็กไฟฟ้าที่ครอบคลุมปรากฏการณ์ต่าง ๆ ตามมาตรฐานพื้นฐาน ซึ่งกำหนดระดับการทดสอบขั้นต่ำ ดังต่อไปนี้

- (๑) ภูมิคุ้มกันต่อการปล่อยประจุไฟฟ้าสถิต ตาม มอก. 1452 ที่ระดับการทดสอบอย่างน้อยระดับ ๒
- (๒) ภูมิคุ้มกันต่อภาวะชั่วคราวอย่างเร็วทางไฟฟ้า ตาม มอก. 1454 ที่ระดับการทดสอบอย่างน้อยระดับ ๒ รวมถึงการทดสอบภูมิคุ้มกันที่พอร์ตสื่อสาร
- (๓) ภูมิคุ้มกันต่อเสิร์จ ตาม มอก. 1455 ที่ระดับการทดสอบอย่างน้อยระดับ ๓
- (๔) ภูมิคุ้มกันต่อสนามแม่เหล็กไฟฟ้าความถี่วิทยุแบบแผ่รังสี ตาม มอก. 61000 เล่ม 4(3) ที่ระดับการทดสอบอย่างน้อยระดับ ๓

- (๕) ภูมิคุ้มกันต่อสิ่งรบกวนที่นำกระแสความถี่วิทยุ ตาม มอก. 61000 เล่ม 4(6) ที่ระดับการทดสอบอย่างน้อยระดับ ๓
- (๖) ภูมิคุ้มกันต่อสนามแม่เหล็กความถี่ไฟฟ้า ตาม มอก. 61000 เล่ม 4(8) ที่ระดับการทดสอบอย่างน้อยระดับ ๔
- (๗) ภูมิคุ้มกันต่อแรงดันไฟฟ้าดิ่งลง การขัดจังหวะช่วงสั้น และการแปรผันของแรงดันไฟฟ้า สำหรับเครื่องตัดวงจรที่มีพิกัดกระแสไฟฟ้าใช้งานไม่เกิน ๑๖ แอมแปร์ต่อเฟส ให้ทดสอบตาม มอก. 61000 เล่ม 4(11) กรณีเครื่องตัดวงจรมีพิกัดกระแสไฟฟ้าใช้งานเกิน ๑๖ แอมแปร์ ถึง ๑๒๕ แอมแปร์ต่อเฟส ให้ทดสอบตาม IEC 61000-4-34

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการพิจารณาหลักฐานผลการทดสอบที่ผู้จัดทำให้มี โดยผู้ทำต้องดำเนินการทดสอบตามเกณฑ์และระดับการทดสอบของปรากฏการณ์สัญญาณรบกวนทางแม่เหล็กไฟฟ้าที่ระบุไว้ใน (๑) ถึง (๗) และจัดส่งหลักฐานที่แสดงว่าในระหว่างและภายหลังการทดสอบเครื่องตัดวงจรยังคงรักษาหน้าที่ความปลอดภัยและหน้าที่ป้องกันพื้นฐานได้ตามข้อกำหนด และไม่เกิดการสั่งการ การเปลี่ยนสถานะ การต่อวงจร หรือการเริ่มระบบใหม่โดยไม่ตั้งใจ

๖.๔.๒ ความทนทานต่อสภาวะอากาศและความชื้น

เครื่องตัดวงจรต้องมีความทนทานต่อสภาวะอากาศร้อนชื้นในระดับวิกฤต โดยต้องรักษาสมรรถนะและความปลอดภัยเชิงหน้าที่ภายใต้สภาวะอากาศร้อนชื้นในระดับวิกฤตตามข้อกำหนดที่ระบุไว้ใน มอก. 909 ข้อ ๙.๗.๑

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการพิจารณาหลักฐานผลการทดสอบที่ผู้จัดทำให้มี โดยผู้ทำต้องดำเนินการทดสอบตาม มอก. 909 ข้อ ๙.๗.๑ และจัดส่งหลักฐานแสดงว่า ในระหว่างและภายหลังการทดสอบภายใต้สภาวะอากาศร้อนชื้น เครื่องตัดวงจรยังคงรักษาหน้าที่ความปลอดภัยและหน้าที่ป้องกันพื้นฐานได้ตามข้อกำหนดที่เกี่ยวข้อง และไม่เกิดการสั่งการ การเปลี่ยนสถานะ การต่อวงจร หรือการเริ่มระบบใหม่โดยไม่ตั้งใจ

๗. ข้อกำหนดด้านความมั่นคงปลอดภัย

๗.๑ ความมั่นคงปลอดภัยทางไซเบอร์

เครื่องตัดวงจรต้องเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์ตาม ETSI EN 303 645, ข้อ ๕ ตามเงื่อนไขการใช้ของข้อกำหนดแต่ละข้อที่เกี่ยวข้องกับคุณลักษณะและความสามารถของเครื่องตัดวงจร

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการประเมินความสอดคล้องตาม ETSI TS 103 701

๘. ข้อกำหนดด้านการคงไว้ซึ่งความปลอดภัยเชิงหน้าที่

๘.๑ ทัวไป

เครื่องตัวจริงต้องมีการกำหนดค่าฐานอ้างอิงเริ่มต้น (initial reference configuration) ของฮาร์ดแวร์ ซอฟต์แวร์ เฟิร์มแวร์ และพารามิเตอร์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัย และต้องมีข้อมูลที่สามารถใช้สอบกลับการเปลี่ยนแปลงจากการกำหนดค่าฐานอ้างอิงเริ่มต้นดังกล่าวได้ตลอดวัฏจักรชีวิตด้านความปลอดภัยของเครื่องตัวจริง

ผู้ทำต้องระบุอายุการใช้งานที่ออกแบบไว้ของฮาร์ดแวร์ และระยะเวลาการสนับสนุนซอฟต์แวร์และเฟิร์มแวร์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัยแยกจากกันในเอกสารแนะนำของผู้ทำ โดยระยะเวลาการสนับสนุนซอฟต์แวร์และเฟิร์มแวร์ต้องไม่น้อยกว่า ๔ ปี

ผู้ทำต้องกำหนดมาตรการเมื่อสิ้นสุดระยะเวลาการสนับสนุนซอฟต์แวร์หรือเฟิร์มแวร์ไว้ล่วงหน้าและระบุไว้ในเอกสารแนะนำของผู้ทำ โดยมาตรการดังกล่าวต้องทำให้เครื่องตัวจริงยังคงไว้ซึ่งหน้าที่ความปลอดภัยตามข้อกำหนดของมาตรฐานนี้ หรือเข้าสู่สภาวะปลอดภัยตามที่กำหนด

ภายหลังการเปลี่ยนแปลงการกำหนดค่า ซอฟต์แวร์ หรือเฟิร์มแวร์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัยหรือตรรกะการควบคุม เครื่องตัวจริงต้องคงไว้ซึ่งสมรรถนะด้านความปลอดภัยเชิงหน้าที่ตามข้อกำหนดของมาตรฐานนี้

ผู้ทำต้องประเมินผลกระทบของการเปลี่ยนแปลงดังกล่าวต่อหน้าที่ความปลอดภัย และต้องดำเนินการทวนสอบซ้ำในส่วนที่ได้รับผลกระทบก่อนนำการเปลี่ยนแปลงไปใช้

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดยการพิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับอายุการใช้งานที่ออกแบบไว้ของฮาร์ดแวร์ การกำหนดค่าฐานอ้างอิงเริ่มต้น การสอบกลับการเปลี่ยนแปลง ระยะเวลาการสนับสนุนซอฟต์แวร์และเฟิร์มแวร์ มาตรการเมื่อสิ้นสุดระยะเวลาการสนับสนุน การประเมินผลกระทบจากการเปลี่ยนแปลง และผลการทวนสอบของผู้ทำตามภาคผนวก ข.

หมายเหตุ การกำหนดค่าฐานอ้างอิงเริ่มต้น หมายถึง ชุดข้อมูลที่ระบุสถานะของฮาร์ดแวร์ ซอฟต์แวร์ เฟิร์มแวร์ พารามิเตอร์ และการกำหนดค่าที่เกี่ยวข้องกับหน้าที่ความปลอดภัย ณ จุดเริ่มต้นที่กำหนดไว้ เพื่อใช้เป็นฐานสำหรับการระบุ การเปรียบเทียบ และการสอบกลับการเปลี่ยนแปลงในภายหลัง ทั้งนี้ ไม่ได้หมายถึงค่าปริยาย (default value) ของเครื่องตัวจริง

๘.๒ ความถูกต้องสมบูรณ์ของข้อมูลและการบันทึกเหตุการณ์

เครื่องตัวจริงต้องรักษาความถูกต้องสมบูรณ์ของข้อมูลที่เกี่ยวข้องกับหน้าที่ความปลอดภัย รวมถึงคำสั่ง ค่าพารามิเตอร์ ซอฟต์แวร์ เฟิร์มแวร์ และข้อมูลบันทึกที่ใช้ประกอบการตัดสินใจด้านความปลอดภัย ตามความสำคัญและความเสี่ยงของข้อมูลนั้น อย่างน้อยดังต่อไปนี้

๘.๒.๑ เครื่องตัวจริงต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัย การวินิจฉัย และการสอบกลับอย่างน้อย ดังต่อไปนี้

- (ก) การทำงานของหน้าที่ป้องกันหรือหน้าที่ความปลอดภัย รวมถึงการทริป การตัดวงจร และการต่อกลับอัตโนมัติ
- (ข) การตรวจพบความผิดปกติหรือสภาวะผิดปกติที่อาจส่งผลกระทบต่อหน้าที่ความปลอดภัย
- (ค) การเปลี่ยนแปลงพารามิเตอร์ด้านความปลอดภัย การกำหนดค่า ซอฟต์แวร์ หรือเฟิร์มแวร์ที่อาจส่งผลกระทบต่อหน้าที่ความปลอดภัย
- (ง) การเข้าสู่สภาวะปลอดภัย และการออกจากสภาวะปลอดภัย
- (จ) การดำเนินการบำรุงรักษา การตรวจสอบหรือทวนสอบตามวาระ การเปลี่ยนชิ้นส่วนหรือมอดูล หรือการเข้าสู่โหมดบำรุงรักษา ที่เครื่องตัวจริงสามารถตรวจจับหรือรับข้อมูลได้และอาจส่งผลกระทบต่อหน้าที่ความปลอดภัย

บันทึกเหตุการณ์แต่ละรายการต้องมีข้อมูลอย่างน้อย ดังต่อไปนี้

- (ก) วันและเวลาที่เกิดเหตุการณ์
- (ข) ชนิดหรือรหัสเหตุการณ์
- (ค) สถานะการทำงานของเครื่องตัวจริงที่เกี่ยวข้องกับเหตุการณ์นั้น

สำหรับเหตุการณ์ที่เกี่ยวข้องกับการเปลี่ยนแปลงพารามิเตอร์ด้านความปลอดภัย การกำหนดค่า ซอฟต์แวร์ หรือเฟิร์มแวร์ หรือกิจกรรมตาม (จ) บันทึกเหตุการณ์ต้องสามารถระบุพารามิเตอร์ การกำหนดค่า รุ่นซอฟต์แวร์หรือเฟิร์มแวร์ หรือกิจกรรมที่เกี่ยวข้องได้ ตามที่เครื่องตัวจริงสามารถตรวจจับหรือรับข้อมูลดังกล่าวได้

เครื่องตัวจริงต้องสามารถเก็บรักษาและเรียกคืนบันทึกเหตุการณ์ย้อนหลังได้เป็นระยะเวลาไม่น้อยกว่า ๑ ปีนับจากเวลาที่เกิดเหตุการณ์ ข้อมูลที่บันทึกต้องถูกต้อง ครบถ้วน และคงอยู่ได้เมื่อแหล่งจ่ายไฟฟ้าขาดหาย

เมื่อความจุของพื้นที่จัดเก็บถึงขีดจำกัด เครื่องตัดวงจรต้องจัดการข้อมูลโดยไม่ทำให้บันทึกเหตุการณ์ที่ยังอยู่ภายในระยะเวลาเก็บรักษาที่กำหนดสูญหาย ถูกเขียนทับ หรือไม่สามารถเรียกคืนได้

กรณีที่ใช้ระบบเครือข่ายหรือระบบประมวลผลภายนอกสำหรับการเก็บรักษาข้อมูล เครื่องตัดวงจรต้องสามารถเก็บรักษาข้อมูลที่ยังส่งไปยังระบบดังกล่าวไม่สำเร็จในระหว่างที่การเชื่อมต่อไม่พร้อมใช้งาน และต้องสามารถส่งต่อข้อมูลดังกล่าวเมื่อการเชื่อมต่อกลับคืนตามเงื่อนไขที่กำหนด

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับข้อกำหนดและการออกแบบสำหรับการบันทึกเหตุการณ์ การเก็บรักษาและเรียกคืนบันทึก การจัดการข้อมูลเมื่อความจุของพื้นที่จัดเก็บถึงขีดจำกัด การเก็บรักษาและส่งต่อข้อมูลเมื่อการเชื่อมต่อไม่พร้อมใช้งาน และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องตัดวงจรโดยสร้างเหตุการณ์ที่กำหนดให้ต้องบันทึก ตรวจสอบข้อมูลที่บันทึก การเก็บรักษา การเรียกคืน การคงอยู่เมื่อแหล่งจ่ายไฟฟ้าขาดหาย การจัดการเมื่อพื้นที่จัดเก็บถึงขีดจำกัด และการสอบกลับ รวมทั้งกรณีการเชื่อมต่อกับระบบภายนอกไม่พร้อมใช้งาน ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๓.๒ และ ค.๒.๔

๘.๒.๒ เครื่องตัดวงจรต้องทวนสอบความถูกต้องสมบูรณ์ของข้อมูลพารามิเตอร์ด้านความปลอดภัยและซอฟต์แวร์หรือเฟิร์มแวร์ที่ใช้ในการดำเนินหน้าที่ความปลอดภัยในช่วงเวลาที่เพียงพอต่อความเสี่ยงและข้อกำหนดความต้องการด้านความปลอดภัย เมื่อพบว่าข้อมูลดังกล่าวไม่ถูกต้องหรือไม่สมบูรณ์ เครื่องตัดวงจรต้องปฏิเสธการนำข้อมูลนั้นไปใช้ และต้องคงไว้ซึ่งหน้าที่ความปลอดภัยหรือเข้าสู่สภาวะปลอดภัยตามที่กำหนด

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับข้อมูลพารามิเตอร์ด้านความปลอดภัย ซอฟต์แวร์หรือเฟิร์มแวร์ กลไกการทวนสอบความถูกต้องสมบูรณ์ การตอบสนองเมื่อข้อมูลไม่ถูกต้องหรือไม่สมบูรณ์ และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องตัดวงจรโดยป้อน ส่งผ่าน หรือเปลี่ยนแปลงข้อมูลที่เกี่ยวข้องจากภายนอกให้ครอบคลุมข้อมูลที่ถูกต้องและสมบูรณ์ ข้อมูลที่ถูกเปลี่ยนแปลง และข้อมูลที่ไม่ครบถ้วน แล้วตรวจสอบการตอบสนองของเครื่องตัดวงจร ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๓.๑

๘.๒.๓ เครื่องตัดวงจรต้องบันทึกและส่งมอบข้อมูลบันทึกที่รูปคลื่นสัญญาณ หรือข้อมูลโปรไฟล์พารามิเตอร์ทางไฟฟ้าเชิงเวลาของแรงดันไฟฟ้าและกระแสไฟฟ้า พร้อมข้อมูลอ้างอิงเวลาและกรอบเวลาที่สัมพันธ์กับเหตุการณ์ โดยต้องครอบคลุมช่วงก่อนเกิดเหตุการณ์ตามช่วงเวลาที่ผู้ทำระบุ และชุดข้อมูลดังกล่าวต้องมี

ความละเอียด ความถูกต้อง และความครบถ้วนเพียงพอที่จะนำกลับมาประมวลผลเพื่อจำลองรูปคลื่นสัญญาณย้อนหลังหรือแสดงเส้นแนวโน้มพฤติกรรมทางไฟฟ้าได้อย่างถูกต้อง

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับการบันทึกรูปคลื่นสัญญาณหรือข้อมูลโปรไฟล์พารามิเตอร์ทางไฟฟ้าเชิงเวลา ข้อมูลอ้างอิงเวลากรอบเวลาที่สัมพันธ์กับเหตุการณ์ ช่วงเวลาการบันทึก ความละเอียด ความถูกต้อง ความครบถ้วน และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องตัวจริงโดยสร้างเหตุการณ์ที่ทำให้เกิดการบันทึกข้อมูล ตรวจสอบข้อมูลที่บันทึกและส่งมอบ รวมทั้งความสามารถในการนำข้อมูลกลับมาประมวลผลเพื่อจำลองรูปคลื่นสัญญาณย้อนหลังหรือแสดงเส้นแนวโน้มพฤติกรรมทางไฟฟ้า ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๔

หมายเหตุ วิธีการจัดการข้อมูลเมื่อความจุของพื้นที่จัดเก็บถึงขีดจำกัด เช่น การเขียนทับข้อมูลที่พ้นระยะเวลาเก็บรักษาที่กำหนด การถ่ายโอนข้อมูลไปยังระบบจัดเก็บภายนอก หรือการแจ้งสถานะเมื่อพื้นที่จัดเก็บใกล้ถึงขีดจำกัด

๘.๓ การจำกัดการปรับตั้งค่าที่ไม่ปลอดภัย

เครื่องตัวจริงต้องมีกลไกทวนสอบค่าพารามิเตอร์ด้านความปลอดภัยก่อนนำไปบันทึกหรือบังคับใช้ โดยค่าพารามิเตอร์ที่นำไปบันทึกหรือบังคับใช้ต้องอยู่ภายในขอบเขตความปลอดภัยเชิงหน้าที่และพิกัดขีดความสามารถทางกายภาพของเครื่องตัวจริง

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับข้อกำหนดขอบเขตพารามิเตอร์ด้านความปลอดภัย พิกัดและข้อจำกัดของผลิตภัณฑ์ การออกแบบกลไกทวนสอบและจำกัดค่าปรับตั้งให้อยู่ภายในขอบเขตที่กำหนด และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องตัวจริงโดยกำหนดค่าพารามิเตอร์ด้านความปลอดภัยที่ค่าขอบเขต ค่านอกขอบเขต และค่าที่ขัดกับพิกัดของเครื่องตัวจริงผ่านส่วนต่อประสานที่ผู้ทำอนุญาต ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๕

๘.๔ ความเป็นอิสระในการปฏิบัติงานของเครื่องตัวจริง

เครื่องตัวจริงต้องสามารถรักษาหน้าที่ความปลอดภัยที่จำเป็นได้โดยไม่พึ่งพาบริการหรือการประมวลผลภายนอกที่ไม่มีการรับประกันความพร้อมใช้งานตามข้อกำหนดความต้องการด้านความปลอดภัย และต้องรักษาสมรรถนะของหน้าที่ความปลอดภัยให้อยู่ภายในเกณฑ์ที่กำหนดในระหว่างการทำงานของหน้าที่สื่อสารหน้าที่อัจฉริยะ หรือหน้าที่อื่นที่ไม่เกี่ยวข้องกับความปลอดภัย

เครื่องตัดวงจรต้องรักษาขีดความสามารถและเวลาตอบสนองของหน้าที่ป้องกันพื้นฐานและการทริปปลดวงจรทางไฟฟ้าให้เป็นไปตามเกณฑ์ที่กำหนดในทุกสภาวะการควบคุมและการบริหารจัดการด้านความปลอดภัยเชิงหน้าที่

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับสถาปัตยกรรมและการจัดสรรหน้าที่ความปลอดภัย การแยกส่วนหน้าที่ความปลอดภัยจากหน้าที่อื่น การวิเคราะห์การพึ่งพาระบบหรือบริการภายนอก การวิเคราะห์ความล้มเหลว และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องตัดวงจรโดยใช้งานหน้าที่สื่อสาร หน้าที่อัจฉริยะ หรือหน้าที่อื่นที่ไม่เกี่ยวข้องกับความปลอดภัยซึ่งอาจมีผลต่อหน้าที่ความปลอดภัย แล้วทำให้การเชื่อมต่อสื่อสารภายนอก บริการ หรือระบบประมวลผลภายนอกที่เกี่ยวข้องไม่พร้อมใช้งานและคืนสู่สภาวะพร้อมใช้งาน พร้อมกระตุ้นหน้าที่ความปลอดภัยที่เกี่ยวข้อง ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๖

๘.๕ การปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์

เครื่องตัดวงจรที่รองรับการปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ ต้องมีคุณลักษณะ ดังต่อไปนี้

- (๑) เครื่องตัดวงจรต้องทวนสอบความถูกต้องสมบูรณ์และความแท้จริงของซอฟต์แวร์หรือเฟิร์มแวร์ก่อนการติดตั้ง
- (๒) ในระหว่างกระบวนการดาวน์โหลด การติดตั้ง การปรับปรุง หรือการกู้คืนซอฟต์แวร์หรือเฟิร์มแวร์ เครื่องตัดวงจรต้องรักษาหน้าที่ความปลอดภัยไว้ตามข้อกำหนดความต้องการด้านความปลอดภัย หากไม่สามารถรักษาหน้าที่ความปลอดภัยได้ เครื่องตัดวงจรต้องเข้าสู่สภาวะปลอดภัยและยับยั้งการจ่ายพลังงานหรือการต่อกลับที่ไม่ปลอดภัยจนกว่ากระบวนการดังกล่าวจะเสร็จสมบูรณ์และผ่านการทวนสอบ
- (๓) เมื่อกระบวนการติดตั้งหรือการปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ขัดข้องหรือล้มเหลว เครื่องตัดวงจรต้องสามารถกู้คืนไปยังซอฟต์แวร์ เฟิร์มแวร์ หรือการกำหนดค่าที่ผ่านการทวนสอบและมีผลใช้งานอยู่ก่อนเริ่มการปรับปรุง หรือเข้าสู่สภาวะปลอดภัยภายในเวลาที่กำหนดตามข้อกำหนดความต้องการด้านความปลอดภัย
- (๔) ภายหลังการปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ ข้อมูลพารามิเตอร์ด้านความปลอดภัยที่ต้องคงไว้ต้องมี ความถูกต้องสมบูรณ์ และค่าพารามิเตอร์ที่นำไปใช้ต้องผ่านการทวนสอบตามข้อกำหนด

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับกลไกการปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ การพิสูจน์ความแท้จริง ความถูกต้องสมบูรณ์ การกู้คืน การรักษาหน้าที่ความปลอดภัย และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องต้นวงจรโดยดำเนินการปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ รวมถึงกรณีการปรับปรุงสำเร็จ กรณีใช้ชุดซอฟต์แวร์หรือเฟิร์มแวร์ที่ไม่ผ่านการพิสูจน์ความแท้จริงหรือการตรวจสอบความถูกต้องสมบูรณ์ กรณีขัดจังหวะการปรับปรุง และการกู้คืน ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๒

๘.๖ การเปลี่ยนชิ้นส่วนหรือมอดูล

๘.๖.๑ ภายหลังการสับเปลี่ยนหรือทดแทนชิ้นส่วนหรือมอดูล เครื่องต้นวงจรต้องยังคงสามารถปฏิบัติหน้าที่ความปลอดภัยและเป็นไปตามเกณฑ์สมรรถนะในส่วนที่ได้รับผลกระทบจากการเปลี่ยนแปลงนั้น

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับชิ้นส่วนหรือมอดูลทดแทน การประเมินผลกระทบ หน้าที่ความปลอดภัยและเกณฑ์สมรรถนะที่ได้รับผลกระทบ และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องต้นวงจรภายหลังการเปลี่ยนชิ้นส่วนหรือมอดูลที่ผู้ทำอนุญาต โดยทวนสอบเฉพาะหน้าที่ความปลอดภัยและเกณฑ์สมรรถนะในส่วนที่ได้รับผลกระทบจากการเปลี่ยนแปลง ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๘

๘.๖.๒ สำหรับมอดูลควบคุมทดแทนที่มีซอฟต์แวร์หรือเฟิร์มแวร์ติดตั้งอยู่ภายใน เครื่องต้นวงจรต้องสามารถทวนสอบความเข้ากันได้ของมอดูลและรุ่นซอฟต์แวร์หรือเฟิร์มแวร์ก่อนการเปิดใช้งาน และต้องอนุญาตให้เปิดใช้งานเฉพาะเมื่อผลการทวนสอบเป็นไปตามเงื่อนไขความเข้ากันได้ที่กำหนด

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับมอดูลควบคุมทดแทน เงื่อนไขความเข้ากันได้ของมอดูลและรุ่นซอฟต์แวร์หรือเฟิร์มแวร์ และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องต้นวงจรโดยเปลี่ยนมอดูลควบคุมที่ผู้ทำอนุญาต และทดสอบกรณีมอดูลหรือรุ่นซอฟต์แวร์หรือเฟิร์มแวร์ที่ไม่เข้ากันตามที่สามารถดำเนินการได้จากภายนอก แล้วตรวจสอบการทวนสอบความเข้ากันได้ก่อนการเปิดใช้งาน ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๘

๘.๗ การตรวจสอบ การทวนสอบ และการบำรุงรักษา

สำหรับการตรวจสอบ การทวนสอบ หรือการบำรุงรักษาที่เครื่องต้นวงจรรองรับให้ดำเนินการในขณะติดตั้งใช้งาน เครื่องต้นวงจรต้องรักษาหน้าที่ความปลอดภัยที่จำเป็นไว้ หรือเข้าสู่สภาวะปลอดภัยตามที่กำหนด

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับวิธีการตรวจสอบ การทวนสอบ หรือการบำรุงรักษาที่เครื่องตัดวงจรรองรับให้ดำเนินการในขณะติดตั้งใช้งาน ผลกระทบต่อหน้าที่ความปลอดภัย และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบเครื่องตัดวงจรโดยดำเนินวิธีตรวจสอบ ทวนสอบ หรือบำรุงรักษาที่ผู้ทำกำหนดและเครื่องตัดวงจรรองรับให้ดำเนินการในขณะติดตั้งใช้งาน พร้อมกระตุ้นหน้าที่ความปลอดภัยที่อาจได้รับผลกระทบตามวิธีการที่กำหนดในภาคผนวก ค.๒.๗

๘.๘ ส่วนต่อประสานและเครื่องมือซ่อมบำรุง

- ๘.๘.๑ เครื่องตัดวงจรที่รองรับการเชื่อมต่อกับเครื่องมือ อุปกรณ์ทดสอบ หรือซอฟต์แวร์ประยุกต์ภายนอก เพื่อปรับตั้งหรือเปลี่ยนแปลงพารามิเตอร์ การกำหนดค่า ซอฟต์แวร์ หรือเฟิร์มแวร์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัย ต้องมีการควบคุมการเข้าถึงและการพิสูจน์สิทธิ์ก่อนอนุญาตให้ดำเนินการดังกล่าว โดยการควบคุมการเข้าถึงและการพิสูจน์สิทธิ์ต้องเป็นไปตามข้อ ๗.๑

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับการควบคุมการเข้าถึง การพิสูจน์สิทธิ์ การกำหนดสิทธิ์สำหรับเครื่องมือซ่อมบำรุง และผลการทวนสอบของผู้ทำตามภาคผนวก ข. โดยการควบคุมการเข้าถึงและการพิสูจน์สิทธิ์ให้พิจารณาร่วมกับข้อ ๗.๑
- ทดสอบเครื่องตัดวงจรโดยเชื่อมต่อเครื่องมือซ่อมบำรุงตามที่ยูทำกำหนด แล้วทดสอบการเข้าถึงด้วยสิทธิ์ที่ถูกต้องและการพยายามเข้าถึงหรือเปลี่ยนแปลงโดยไม่มีสิทธิ์ ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๑๐ (ก) และ (ข)

- ๘.๘.๒ เมื่อการสื่อสารกับเครื่องมือซ่อมบำรุงขัดข้องหรือขาดหายในระหว่างการปรับตั้งหรือเปลี่ยนแปลงพารามิเตอร์หรือการกำหนดค่าที่เกี่ยวข้องกับหน้าที่ความปลอดภัย เครื่องตัดวงจรต้องคงการทำงานตามค่าพารามิเตอร์และการกำหนดค่าที่ผ่านการทวนสอบและมีผลใช้งานอยู่ก่อนเริ่มการเปลี่ยนแปลงนั้น หรือเข้าสู่สภาวะปลอดภัยตามที่กำหนด

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับการสื่อสารกับเครื่องมือซ่อมบำรุง การจัดการกรณีการสื่อสารขัดข้องหรือขาดหาย ค่าพารามิเตอร์และการกำหนดค่าที่ผ่านการทวนสอบและมีผลใช้งานอยู่ และผลการทวนสอบของผู้ทำตามภาคผนวก ข.

- ทดสอบเครื่องตัดวงจรโดยขัดจังหวะการสื่อสารกับเครื่องมือซ่อมบำรุงระหว่างการเปลี่ยนพารามิเตอร์หรือการกำหนดค่า แล้วตรวจสอบการตอบสนองของเครื่องตัดวงจร ตามวิธีการที่กำหนดในภาคผนวก ค.๒.๑๐ (ค)

หมายเหตุ แนวทางการตรวจ การทดสอบ และการบำรุงรักษาเครื่องตัดวงจร รวมถึงการจัดการการเปลี่ยนแปลง การบันทึกหลักฐาน และการใช้เครื่องมือซ่อมบำรุง แสดงไว้ในภาคผนวก ง.

๙. รายงานผลการทดสอบ

การรายงานผลการทดสอบ ต้องมีรายละเอียดอย่างน้อย ดังนี้

- (๑) ชื่อและที่อยู่ของห้องปฏิบัติการทดสอบหรือหน่วยงานทดสอบ
- (๒) รายละเอียดของเครื่องตัดวงจร ได้แก่ ชื่อตราสินค้า รุ่น หมายเลขประจำตัวเครื่อง
- (๓) ระดับคุณภาพความปลอดภัยที่กำหนดสำหรับหน้าที่ความปลอดภัยที่เกี่ยวข้อง (ถ้ามี)
- (๔) ข้อมูลรุ่น ได้แก่ รุ่นของฮาร์ดแวร์ รุ่นของซอฟต์แวร์หรือเฟิร์มแวร์ และค่าตรวจสอบความถูกต้องสมบูรณ์ของซอฟต์แวร์หรือเฟิร์มแวร์
- (๕) รายการส่วนประกอบวิกฤตที่มีผลต่อหน้าที่ความปลอดภัย ได้แก่ หน่วยประมวลผลหลัก อุปกรณ์ตรวจวัดกลไกการทริป
- (๖) พารามิเตอร์การทดสอบและการกำหนดค่าของตัวอย่างทดสอบ รวมถึงพารามิเตอร์ด้านความปลอดภัยและการกำหนดค่าอื่นที่มีผลต่อผลการทดสอบ
- (๗) วันที่ดำเนินการทดสอบ
- (๘) ชื่อผู้ทดสอบ
- (๙) สภาพแวดล้อมและสิ่งอำนวยความสะดวกที่ใช้ในการทดสอบ
- (๑๐) รายงานผลการทดสอบตามหัวข้อ ดังนี้
 - (๑๐.๑) ข้อกำหนดสมรรถนะด้านความปลอดภัย ตามข้อกำหนดข้อที่ ๕
 - (๑๐.๒) ข้อกำหนดด้านความปลอดภัยเชิงหน้าที่ ตามข้อกำหนดข้อที่ ๖
 - (๑๐.๓) ข้อกำหนดด้านความมั่นคงปลอดภัย ตามข้อกำหนดข้อที่ ๗
 - (๑๐.๔) ข้อกำหนดด้านการคงไว้ซึ่งความปลอดภัยเชิงหน้าที่ ตามข้อกำหนดข้อที่ ๘

การรายงานผลตามข้อ (๑๐.๒) ถึงข้อ (๑๐.๔) ให้รายงานถึงระดับข้อย่อที่เกี่ยวข้อง โดยแยกผลการพิจารณาหลักฐาน ผลการทดสอบเครื่องตัดวงจรเมื่อข้อกำหนดกำหนดให้มีการทดสอบ และผลการประเมินความเป็นไปตามข้อกำหนดให้สามารถสอบกลับได้

ผลการทดสอบแต่ละกรณีตามภาคผนวก ค. ต้องระบุกรณีทดสอบ วิธีการทดสอบ การกำหนดค่าของตัวอย่าง สภาวะทดสอบ ผลที่ได้ เกณฑ์การยอมรับ และผลผ่านหรือไม่ผ่าน โดยต้องสามารถสอบกลับไปยังข้อกำหนดที่ประเมินได้

กรณีที่มีการดำเนินการเพิ่มเติมตามข้อ ข.๔ หรือการทดสอบเพิ่มเติมตามข้อ ค.๓ ให้ระบุเหตุผล วิธีดำเนินการ และผลที่ได้ไว้ในรายงานผลการทดสอบ

หมายเหตุ ตัวอย่างรายงานผลการทดสอบให้ไว้ในภาคผนวก จ.

ภาคผนวก ก.

การตรวจสอบความปลอดภัยเชิงหน้าที่ของหน้าที่ควบคุมผ่านวงจรนำร่องเมื่อเครื่องตัดวงจรทำ
หน้าที่ร่วมกับบริภัณฑ์อัดประจุแบบไฟฟ้ากระแสสลับสำหรับยานยนต์ไฟฟ้า

(ข้อกำหนด)

(ข้อ ๑.๓)

ก.๑ ทัวไป

เครื่องตัดวงจรที่มีหน้าที่ควบคุมผ่านวงจรนำร่อง (control pilot function) หรือมีการติดตั้งมอดูลเสริมเพื่อ
เพิ่มหน้าที่ดังกล่าวสำหรับการอัดประจุยานยนต์ไฟฟ้า ให้เป็นไปตามข้อกำหนดของภาคผนวกนี้

ก.๒ หน้าที่ควบคุมผ่านวงจรนำร่อง

ผู้ทำต้องประเมินผลกระทบของหน้าที่ควบคุมผ่านวงจรนำร่องหรือมอดูลที่เกี่ยวข้องต่อหน้าที่ความปลอดภัย
เดิมของเครื่องตัดวงจร และต้องแสดงว่าการเพิ่มหน้าที่หรือมอดูลดังกล่าวไม่ทำให้หน้าที่ความปลอดภัยหรือ
หน้าที่ป้องกันพื้นฐานของเครื่องตัดวงจรลดลง

หน้าที่ควบคุมผ่านวงจรนำร่องของเครื่องตัดวงจร หรือของมอดูลเสริมที่ติดตั้งร่วม ต้องเป็นไปตาม มอก.
61851 เล่ม 1 ภาคผนวก ก.

การตรวจสอบการเป็นไปตามข้อกำหนด ให้ทำโดย

- พิจารณาหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องกับ
หน้าที่ควบคุมผ่านวงจรนำร่อง ผลกระทบต่อหน้าที่ความปลอดภัยและหน้าที่ป้องกันพื้นฐานของเครื่อง
ตัดวงจร และผลการทวนสอบของผู้ทำตามภาคผนวก ข.
- ทดสอบหน้าที่ควบคุมผ่านวงจรนำร่องตาม มอก. 61851 เล่ม 1 ภาคผนวก ก.

หมายเหตุ การแสดงหลักฐานการเป็นไปตาม มอก. 61851 เล่ม 1 ภาคผนวก ก. ถือว่าเป็นไปตามข้อกำหนดการทดสอบ
หน้าที่ควบคุมผ่านวงจรนำร่องตามข้อนี้

ภาคผนวก ข.

หลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัย

(ข้อกำหนด)

(ข้อ ๖, ข้อ ๗, ข้อ ๘ และภาคผนวก ก.)

ข.๑ ทัวไป

ผู้ทำต้องจัดส่งหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัยที่เกี่ยวข้องตาม อนุกรม มอก. 2732

กรณีเครื่องตัดวงจรอยู่ในขอบข่ายภาคผนวก ก. หลักฐานตามภาคผนวกนี้ต้องครอบคลุมหน้าที่ควบคุมผ่าน วงจรนำร่องหรือมอดูลที่เกี่ยวข้อง และผลกระทบต่อหน้าที่ความปลอดภัยและหน้าที่ป้องกันพื้นฐานของเครื่อง ตัดวงจร ตามที่เกี่ยวข้อง

หลักฐานแต่ละรายการต้องระบุฉบับแก้ไข สถานะการอนุมัติ และความสัมพันธ์กับรุ่นฮาร์ดแวร์ รุ่นซอฟต์แวร์ หรือเฟิร์มแวร์ และการกำหนดค่าของผลิตภัณฑ์ที่ยื่นทดสอบ

กรณีที่หลักฐานรายการหนึ่งครอบคลุมรายละเอียดที่กำหนดไว้มากกว่าหนึ่งรายการ ผู้ทำไม่จำเป็นต้องจัดทำ เอกสารแยกต่างหาก หากสามารถแสดงความครบถ้วน ความสอดคล้อง และการสอบกลับของรายละเอียดที่กำหนดได้

ข.๒ รายการและสาระของหลักฐานด้านความปลอดภัยเชิงหน้าที่ตลอดวัฏจักรชีวิตด้านความปลอดภัย

หลักฐานที่ผู้ทำจัดส่ง อย่างน้อยต้องประกอบด้วยหลักฐานตามข้อ ข.๒.๑ ถึง ข.๒.๖ ที่เกี่ยวข้องกับเครื่องตัด วงจร โดยแต่ละรายการต้องมีรายละเอียดตามที่กำหนดอย่างน้อย ดังต่อไปนี้

ข.๒.๑ หลักฐานด้านการวางแผนและการจัดการวัฏจักรชีวิตด้านความปลอดภัย

หลักฐานในหมวดนี้ อย่างน้อยต้องประกอบด้วยรายการและรายละเอียดตามที่กำหนด ดังต่อไปนี้

- (ก) แผนการจัดการความปลอดภัยเชิงหน้าที่และขอบเขตวัฏจักรชีวิตด้านความปลอดภัย ต้องระบุ ขอบเขตกิจกรรม ระยะหรือขั้นตอนของวัฏจักรชีวิต กิจกรรมด้านความปลอดภัยที่ต้องดำเนินการ ผลลัพธ์หรือหลักฐานที่ต้องจัดทำ จุดทบทวนหรืออนุมัติ และความสัมพันธ์ระหว่างกิจกรรมที่เกี่ยวข้อง
- (ข) การกำหนดขอบเขตผลิตภัณฑ์ การใช้งานที่ตั้งใจไว้ และข้อจำกัดการใช้งาน ต้องระบุขอบเขต ของเครื่องตัดวงจร หน้าที่และส่วนต่อประสานที่เกี่ยวข้อง สภาวะใช้งานและสภาวะแวดล้อมที่กำหนด สมมติฐานในการใช้งาน และข้อจำกัดที่มีผลต่อความปลอดภัยเชิงหน้าที่

- (ค) การกำหนดบทบาท ความรับผิดชอบ อำนาจหน้าที่ และความเป็นอิสระของกิจกรรมที่เกี่ยวข้อง ต้องระบุผู้รับผิดชอบกิจกรรมด้านความปลอดภัยเชิงหน้าที่ การทวนสอบ การตรวจสอบความใช้ได้ การทบทวน และการอนุมัติ รวมถึงความเป็นอิสระตามที่กำหนดสำหรับกิจกรรมนั้น
- (ง) หลักฐานความสามารถของบุคลากร ต้องแสดงความรู้ ทักษะ ประสบการณ์ การฝึกอบรม หรือคุณสมบัติที่เกี่ยวข้องกับกิจกรรมที่ได้รับมอบหมาย และระดับบูรณาการความปลอดภัยที่เกี่ยวข้อง
- (จ) แผนการทวนสอบและแผนการตรวจสอบความใช้ได้ ต้องระบุขอบเขตและข้อกำหนดที่จะตรวจวิธีดำเนินการ เกณฑ์การยอมรับ ผู้รับผิดชอบ สถานะและการกำหนดค่าที่ใช้ และหลักฐานผลลัพธ์ที่ต้องจัดทำ
- (ฉ) การจัดการเอกสาร การจัดการการกำหนดค่า และการควบคุมรุ่น ต้องระบุรายการที่อยู่ภายใต้การควบคุม วิธีระบุรุ่นหรือฉบับแก้ไข สถานะการอนุมัติ ความสัมพันธ์ระหว่างฮาร์ดแวร์ ซอฟต์แวร์ เฟิร์มแวร์ พารามิเตอร์ และเอกสาร รวมถึงวิธีป้องกันการใช้รายการที่ไม่ถูกต้องหรือไม่เป็นปัจจุบัน
- (ช) การจัดการความผิดปกติ ข้อบกพร่อง และการดำเนินการแก้ไข ต้องระบุวิธีบันทึก จำแนก ประเมินผลกระทบ ติดตาม แก้ไข ทวนสอบผลการแก้ไข และปิดรายการที่อาจมีผลต่อหน้าที่ความปลอดภัย
- (ซ) การควบคุมผู้ส่งมอบและองค์ประกอบที่จัดหาจากภายนอก ต้องระบุข้อกำหนดที่ใช้กับผู้ส่งมอบหรือองค์ประกอบ หลักฐานที่ต้องได้รับ วิธีประเมินความเหมาะสมในการนำไปใช้ และการควบคุมการเปลี่ยนแปลงที่อาจมีผลต่อหน้าที่ความปลอดภัย
- (ฌ) การจัดการการเปลี่ยนแปลงและการวิเคราะห์ผลกระทบ ต้องระบุรายการที่เปลี่ยนแปลง เหตุผล ขอบเขตและผลกระทบต่อหน้าที่ความปลอดภัย ระดับบูรณาการความปลอดภัย การกำหนดค่า เอกสาร และการทวนสอบหรือการตรวจสอบความใช้ได้ที่ต้องดำเนินการซ้ำ
- (ญ) แผนการประเมินความปลอดภัยเชิงหน้าที่ ต้องระบุขอบเขต เกณฑ์ วิธีดำเนินการ ผู้รับผิดชอบ หรือผู้ประเมิน ระดับความเป็นอิสระที่กำหนด ช่วงเวลาหรือจุดที่ต้องดำเนินการ และหลักฐานผลลัพธ์ที่ต้องจัดทำ ตามที่เกี่ยวข้อง

ข.๒.๒ หลักฐานระดับองค์ประกอบ

สำหรับองค์ประกอบที่เกี่ยวข้องกับหน้าที่ความปลอดภัย หลักฐานในหมวดนี้ อย่างน้อยต้องประกอบด้วยรายการและรายละเอียดตามที่กำหนด ดังต่อไปนี้

- (ก) ข้อมูลระบุองค์ประกอบ ต้องระบุชนิด ผู้ทำอุปกรณ์ หมายเลขชิ้นส่วน รุ่น ฉบับแก้ไข และข้อมูลอื่นที่จำเป็นต่อการสอบกลับองค์ประกอบที่นำมาใช้จริง
- (ข) ข้อกำหนดหรือข้อมูลจำเพาะขององค์ประกอบ ต้องระบุหน้าที่ที่เกี่ยวข้องกับความปลอดภัย คุณลักษณะทางไฟฟ้า เชิงตรรกะ หรือเชิงกลที่เกี่ยวข้อง และส่วนต่อประสานที่มีผลต่อการนำไปใช้
- (ค) พิกัด สภาวะแวดล้อม ข้อจำกัด เงื่อนไข และสมมติฐานในการใช้งาน ต้องระบุขอบเขตที่องค์ประกอบสามารถใช้งานได้และเงื่อนไขที่ต้องปฏิบัติเพื่อคงคุณลักษณะด้านความปลอดภัย
- (ง) ข้อมูลความล้มเหลว ต้องระบุรูปแบบความล้มเหลว ผลกระทบ ข้อมูลอัตราความล้มเหลวหรือข้อมูลที่ใช้ในการวิเคราะห์เชิงปริมาณ แหล่งที่มาของข้อมูล และเงื่อนไขการใช้ข้อมูลตามที่เกี่ยวข้อง
- (จ) กลไกตรวจวินิจฉัย ต้องระบุความผิดปกติที่ครอบคลุม วิธีการตรวจพบ ระยะเวลาหรือวงจรการตรวจ การตอบสนองเมื่อพบความผิดปกติ และข้อจำกัดของกลไกดังกล่าว
- (ฉ) ข้อผิดพลาดหรือข้อบกพร่องที่ทราบ ต้องระบุรายการที่มีผลต่อการนำองค์ประกอบไปใช้ ข้อจำกัด วิธีหลีกเลี่ยงหรือมาตรการชดเชย และสถานะการแก้ไขตามที่เกี่ยวข้อง
- (ช) คู่มือความปลอดภัยหรือเอกสารเทียบเท่า หากมี ต้องระบุข้อกำหนด เงื่อนไข สมมติฐาน ข้อจำกัด และวิธีการบูรณาการหรือใช้งานที่จำเป็นต่อการรักษาคุณลักษณะด้านความปลอดภัยขององค์ประกอบ
- (ซ) หลักฐานการทวนสอบหรือการตรวจสอบความใช้ได้ขององค์ประกอบ ต้องระบุข้อกำหนดที่ตรวจ วิธีดำเนินการ เกณฑ์การยอมรับ การกำหนดค่าที่ใช้ ผลที่ได้ และข้อสรุป
- (ฌ) หลักฐานการรับรองหรือการประเมินตามอนุกรม มอก. 2732 หากนำมาใช้ประกอบการพิจารณา ต้องระบุขอบข่าย รุ่นหรือฉบับแก้ไข ระดับบูรณาการความปลอดภัยหรือขีดความสามารถเชิงระบบ เงื่อนไข สมมติฐาน และข้อจำกัดที่เกี่ยวข้อง

กรณีที่ผู้ทำเครื่องต้นดวงจริงไม่ได้เป็นผู้ทำองค์ประกอบ ผู้ทำอาจใช้หลักฐานจากผู้ทำองค์ประกอบประกอบการพิจารณาความเป็นไปตามข้อกำหนดได้ เฉพาะส่วนที่อยู่ภายในขอบข่ายของหลักฐานการประเมินหรือการรับรองนั้น และต้องแสดงว่าองค์ประกอบ รุ่น ฉบับแก้ไข เงื่อนไข สมมติฐาน ข้อจำกัด และการนำไปใช้จริงในเครื่องต้นดวงจริงสอดคล้องกับขอบข่ายดังกล่าว

ข.๒.๓ หลักฐานระดับการออกแบบและการบูรณาการ

หลักฐานในหมวดนี้ อย่างน้อยต้องประกอบด้วยรายการและรายละเอียดตามที่กำหนด ดังต่อไปนี้

- (ก) การวิเคราะห์อันตรายและความเสี่ยง ต้องระบุขอบเขตการวิเคราะห์ อันตรายและเหตุการณ์อันตราย สาเหตุและผลที่อาจเกิดขึ้น สภาพะการดำเนินงานที่พิจารณา วิธีและเกณฑ์การประเมินความเสี่ยง มาตรการลดความเสี่ยง และความสัมพันธ์กับหน้าที่ความปลอดภัยที่กำหนด
- (ข) การกำหนดหน้าที่ความปลอดภัยและระดับบูรณาการความปลอดภัย ต้องระบุหน้าที่ความปลอดภัยแต่ละหน้าที่ เหตุการณ์หรือเงื่อนไขที่ทำให้หน้าที่ต้องทำงาน ผลการตอบสนองที่ต้องการ ระดับบูรณาการความปลอดภัยที่กำหนด และเหตุผลหรือผลการวิเคราะห์ที่ใช้กำหนดระดับดังกล่าว
- (ค) ข้อกำหนดความต้องการด้านความปลอดภัย ต้องระบุข้อกำหนดสำหรับแต่ละหน้าที่ความปลอดภัย อย่างน้อยให้ครอบคลุมเงื่อนไขหรือเหตุการณ์ที่ต้องตอบสนอง พฤติกรรมและผลการตอบสนองที่ต้องการ พารามิเตอร์และขอบเขตการทำงานที่เกี่ยวข้อง การแสดงหรือส่งสัญญาณสถานะ การตอบสนองต่อความผิดปกติ ข้อกำหนดด้านเวลาที่เกี่ยวข้อง และข้อกำหนดด้านบูรณาการความปลอดภัยที่เกี่ยวข้อง
- (ง) การกำหนดสถานะปลอดภัยและระยะเวลาที่เกี่ยวข้องกับความปลอดภัย ต้องระบุสถานะปลอดภัยสำหรับอันตรายหรือเหตุการณ์อันตรายที่เกี่ยวข้อง เงื่อนไขการเข้าสู่และออกจากสภาวะดังกล่าว ระยะเวลาที่เกี่ยวข้องกับความปลอดภัย ระยะเวลาสูงสุดที่ยอมรับได้ในการเข้าสู่สภาวะปลอดภัย และระยะเวลาทนทานต่อความผิดปกติตามที่เกี่ยวข้อง พร้อมเอกสารอธิบายเหตุผลหรือผลการคำนวณทางฟิสิกส์ที่อ้างอิงจากขีดจำกัดความทนทานของเครื่องตัดวงจรหรือสายไฟฟ้าที่ได้รับการป้องกัน แสดงความสมเหตุสมผลของเกณฑ์เวลาที่กำหนด และแสดงความสัมพันธ์กับข้อกำหนดความต้องการด้านความปลอดภัย
- (จ) สถาปัตยกรรมระบบ ฮาร์ดแวร์ ซอฟต์แวร์ และการจัดสรรหน้าที่ความปลอดภัย ต้องแสดงองค์ประกอบและองค์ประกอบย่อยที่เกี่ยวข้อง เส้นทางสัญญาณและข้อมูล ส่วนประมวลผล ส่วนตรวจวัด ส่วนตัดต่อวงจรหลัก กลไกตรวจวินิจฉัย ความซ้ำซ้อนหรือความเป็นอิสระตามที่มี และการจัดสรรหน้าที่ความปลอดภัยไปยังส่วนต่าง ๆ
- (ฉ) ข้อกำหนดส่วนต่อประสานและการบูรณาการระหว่างองค์ประกอบ ต้องระบุชนิดและทิศทางของสัญญาณหรือข้อมูล รูปแบบและช่วงค่าที่อนุญาต พฤติกรรมเมื่อข้อมูลขาดหายหรือผิดปกติ ลำดับการทำงาน และเงื่อนไขที่มีผลต่อหน้าที่ความปลอดภัย
- (ช) การวิเคราะห์ความล้มเหลว ต้องระบุขอบเขตและวิธีการวิเคราะห์ องค์ประกอบหรือหน้าที่ที่วิเคราะห์ รูปแบบความล้มเหลว สาเหตุ ผลกระทบต่อหน้าที่ความปลอดภัย วิธีตรวจพบหรือควบคุมความล้มเหลว และผลที่ใช้ประกอบการออกแบบหรือกำหนดมาตรการด้านความปลอดภัย โดยอาจใช้การวิเคราะห์รูปแบบความล้มเหลวและผลกระทบ การวิเคราะห์รูปแบบ

ความล้มเหลว ผลกระทบ และการตรวจวินิจฉัย การวิเคราะห์แผนภูมิต้นไม้ความขัดข้อง หรือวิธีอื่นที่เหมาะสม

- (ซ) การวิเคราะห์ความล้มเหลวจากสาเหตุร่วมและความเป็นอิสระ ต้องระบุส่วนที่อาจได้รับผลจากสาเหตุร่วม การพึ่งพาระหว่างส่วนหรือหน้าที่ มาตรการแยกหรือป้องกัน และผลต่อความสามารถในการบรรลุหน้าที่ความปลอดภัย ตามที่เกี่ยวข้อง
- (ฌ) การวิเคราะห์เวลาและการตอบสนองต่อความผิดปกติ ต้องแสดงลำดับเวลาและระยะเวลาสูงสุดในการตรวจพบความผิดปกติ การประมวลผลหรือการตัดสินใจ การตอบสนอง และการเข้าสู่สภาวะปลอดภัย รวมทั้งระยะเวลารวมตั้งแต่เกิดความผิดปกติจนถึงการเข้าสู่สภาวะปลอดภัย โดยต้องแสดงว่าระยะเวลารวมไม่เกินระยะเวลาสูงสุดที่ยอมรับได้และระยะเวลาดำเนินการต่อความผิดปกติที่กำหนดตามข้อ (ง)
- (ญ) การวิเคราะห์แหล่งจ่าย การเริ่มระบบใหม่ และการคืนสภาพ ต้องระบุสภาวะแรงดันไฟฟ้าเลี้ยงที่เกี่ยวข้อง พฏิกิริยาเมื่อแหล่งจ่ายผิดปกติหรือขาดหาย การเริ่มระบบ การเริ่มระบบใหม่ การคืนสภาพ การคงอยู่ของพารามิเตอร์ด้านความปลอดภัย และผลต่อหน้าที่ความปลอดภัย
- (ฎ) การแยกส่วนหน้าที่ความปลอดภัยจากหน้าที่อื่น ต้องระบุการพึ่งพาทรัพยากร ข้อมูล การสื่อสาร ซอฟต์แวร์หรือบริการร่วม มาตรการป้องกันการรบกวน และผลการวิเคราะห์ว่าหน้าที่อื่นไม่ทำให้หน้าที่ความปลอดภัยลดลงต่ำกว่าข้อกำหนด
- (ฏ) การวิเคราะห์ผลกระทบของความมั่นคงปลอดภัยทางไซเบอร์และความถูกต้องสมบูรณ์ของข้อมูล ต้องระบุส่วนต่อประสานและทรัพย์สินที่เกี่ยวข้อง ภัยคุกคามหรือการเข้าถึงที่อาจมีผลต่อหน้าที่ความปลอดภัย มาตรการควบคุม การพิสูจน์ความแท้จริง การพิสูจน์สิทธิ์ การรักษาความถูกต้องสมบูรณ์ การบันทึกเหตุการณ์ และผลกระทบเมื่อมาตรการดังกล่าวล้มเหลว ตามที่เกี่ยวข้อง
- (ฐ) การวิเคราะห์ผลกระทบจากการเปลี่ยนแปลง ต้องระบุรายการและเหตุผลของการเปลี่ยนแปลง ส่วนของการออกแบบหรือหน้าที่ความปลอดภัยที่ได้รับผลกระทบ ผลต่อระดับบูรณาการความปลอดภัย การกำหนดค่าและเอกสาร และขอบเขตการทวนสอบหรือการตรวจสอบความใช้ได้ซ้ำที่กำหนด

ข.๒.๔ หลักฐานการทวนสอบและการตรวจสอบความใช้ได้ของผู้ทำ

ผู้ทำต้องจัดส่งแผนและผลการทวนสอบและการตรวจสอบความใช้ได้ที่เกี่ยวข้องกับข้อกำหนดด้านความปลอดภัยเชิงหน้าที่ โดยหลักฐานต้องครอบคลุมระดับองค์ประกอบ การออกแบบและการบูรณาการ และเครื่องตัดวงจรประกอบสำเร็จตามที่เกี่ยวข้อง และต้องสามารถสอบกลับไปยังข้อกำหนดที่ตรวจได้

หลักฐานอย่างน้อยต้องระบุข้อกำหนดที่ตรวจ วัตถุประสงค์และขอบเขต วิธีการทวนสอบหรือการตรวจสอบความใช้ได้ เกณฑ์การยอมรับ กรณีทดสอบ การกำหนดค่าตัวอย่าง รุ่นฮาร์ดแวร์ รุ่นซอฟต์แวร์หรือเฟิร์มแวร์ ค่าตรวจสอบความถูกต้องสมบูรณ์ (integrity verification value) ของซอฟต์แวร์หรือเฟิร์มแวร์ พารามิเตอร์ด้านความปลอดภัย เครื่องมือและการต่อวงจร สภาพทดสอบ วิธีการสร้างความผิดปกติหรือสถานะผิดปกติที่ใช้ในการทดสอบ ผลที่คาดหวัง ผลที่ได้ ผลผ่านหรือไม่ผ่าน ความผิดปกติหรือข้อเบี่ยงเบนที่พบ การดำเนินการแก้ไข ผลการทวนสอบหรือการทดสอบซ้ำ ผู้ดำเนินการ ผู้ทบทวน และวันที่ดำเนินการ รวมทั้งผลการประเมินความปลอดภัยเชิงหน้าที่ ซึ่งต้องระบุขอบเขต เกณฑ์ที่ใช้ ผลการพิจารณา รายการความไม่เป็นไปตามข้อกำหนดหรือรายการที่ต้องดำเนินการแก้ไข และสถานะการดำเนินการ ตามที่เกี่ยวข้อง

หากการกำหนดค่าที่ใช้ในการทวนสอบหรือการตรวจสอบความใช้ได้แตกต่างจากการกำหนดค่าของผลิตภัณฑ์สำหรับจำหน่าย ผู้ทำต้องระบุความแตกต่างและแสดงว่าผลที่ได้สามารถใช้กับการกำหนดค่าของผลิตภัณฑ์สำหรับจำหน่ายได้

สำหรับข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์ที่มีผลต่อหน้าที่ความปลอดภัย หลักฐานต้องระบุ ขอบข่าย รุ่นและการกำหนดค่าที่ทดสอบ ส่วนต่อประสานหรือช่องทางที่ครอบคลุม สถานการณ์ภัยคุกคามหรือการเข้าถึงที่พิจารณา วิธีและเครื่องมือทดสอบ ผลที่พบ การจัดการข้อบกพร่อง และผลการทดสอบซ้ำภายหลังการแก้ไข ตามที่เกี่ยวข้อง

หมายเหตุ หลักฐานการทดสอบด้านความมั่นคงปลอดภัยทางไซเบอร์อาจได้จากการทดสอบเจาะระบบ (penetration testing) การทดสอบด้วยข้อมูลนำเข้าที่ไม่ถูกต้อง ผิดรูปแบบ หรือไม่คาดหมาย (fuzz testing) การทดสอบการควบคุมการเข้าถึงและการพิสูจน์สิทธิ์ (access control and authentication testing) การทดสอบความถูกต้องสมบูรณ์และความแท้จริงของข้อมูลหรือซอฟต์แวร์ (integrity and authenticity testing) หรือการทดสอบด้านความมั่นคงปลอดภัยอื่นที่เหมาะสมกับ ความเสี่ยงและลักษณะของผลิตภัณฑ์

ข.๒.๕ หลักฐานระดับเครื่องต้นวงจรประกอบสำเร็จ

หลักฐานในหมวดนี้ อย่างน้อยต้องประกอบด้วยรายการและรายละเอียดตามที่กำหนด ดังต่อไปนี้

- (ก) ข้อมูลระบุผลิตภัณฑ์ ต้องระบุชื่อตราสินค้า รุ่น หมายเลขประจำตัว และการกำหนดค่าของผลิตภัณฑ์สำหรับจำหน่ายที่ใช้เป็นฐานในการประเมิน
- (ข) ข้อมูลรุ่นของฮาร์ดแวร์ ซอฟต์แวร์หรือเฟิร์มแวร์ ต้องระบุรุ่น ฉบับแก้ไข และค่าตรวจสอบความถูกต้องสมบูรณ์ของซอฟต์แวร์หรือเฟิร์มแวร์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัย
- (ค) การกำหนดค่าพารามิเตอร์ด้านความปลอดภัย ต้องระบุพารามิเตอร์ ค่า ช่วงที่อนุญาต ค่าเริ่มต้น และข้อจำกัดที่เกี่ยวข้องกับการกำหนดค่าที่ประเมิน

- (ง) รายงานการตรวจสอบความใช้ได้ของผู้ทำ ต้องระบุหน้าที่ความปลอดภัยที่ตรวจ สภาวะและการกำหนดค่าที่ใช้ เกณฑ์การยอมรับ ผลที่ได้ และข้อสรุปว่าผลิตภัณฑ์ประกอบสำเร็จเป็นไปตามข้อกำหนดความต้องการด้านความปลอดภัยที่เกี่ยวข้อง
- (จ) รายงานการทดสอบเครื่องตัดวงจรประกอบสำเร็จของผู้ทำ ต้องระบุวิธีและสภาวะทดสอบ การกำหนดค่าที่ใช้ ผลที่ได้ และข้อสรุป โดยครอบคลุมข้อต่อ ส่วนควบคุม ส่วนต่อประสาน ช่องทางสื่อสาร แหล่งจ่าย หรือสภาวะแวดล้อมที่เกี่ยวข้องกับหน้าที่ความปลอดภัย
- (ฉ) รายงานการทดสอบสมรรถนะและสภาวะแวดล้อม ต้องระบุมาตรฐานหรือวิธีทดสอบ ระดับหรือสภาวะที่ใช้ การกำหนดค่าของตัวอย่าง ผลการทดสอบ และความสัมพันธ์กับหน้าที่ความปลอดภัยที่เกี่ยวข้อง
- (ช) หลักฐานความสอดคล้องของการบูรณาการ ต้องแสดงว่าหน้าที่ องค์ประกอบและองค์ประกอบย่อย รุ่น การกำหนดค่า และผลการทวนสอบที่นำมาใช้ตรงกับผลิตภัณฑ์สำหรับจำหน่ายที่ยื่นทดสอบ
- (ซ) ข้อจำกัดและเงื่อนไขการติดตั้ง การใช้งาน การเดินเครื่อง และการบำรุงรักษา ต้องระบุเงื่อนไขที่ผู้ติดตั้ง ผู้ใช้ หรือผู้บำรุงรักษาต้องปฏิบัติเพื่อรักษาหน้าที่ความปลอดภัยและระดับบูรณาภาพความปลอดภัยที่กำหนด
- (ณ) หลักฐานการจัดการรุ่นและการเปลี่ยนแปลงของผลิตภัณฑ์สำเร็จ ต้องแสดงประวัติรุ่นหรือการเปลี่ยนแปลงที่เกี่ยวข้อง ผลการวิเคราะห์ผลกระทบ และสถานะการทวนสอบหรือการตรวจสอบความใช้ได้ของรุ่นที่ยื่นทดสอบ

ข.๒.๖ หลักฐานด้านการใช้งาน การบำรุงรักษา และการจัดการการเปลี่ยนแปลง

หลักฐานในหมวดนี้ อย่างน้อยต้องประกอบด้วยรายการและรายละเอียดตามที่กำหนด ดังต่อไปนี้

สำหรับการจัดการการเปลี่ยนแปลง หลักฐานต้องระบุการกำหนดค่าฐานอ้างอิงเริ่มต้นของฮาร์ดแวร์ ซอฟต์แวร์ เฟิร์มแวร์ และพารามิเตอร์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัย รวมถึงข้อมูลที่สามารถใช้สอบกลับการเปลี่ยนแปลงจากการกำหนดค่าฐานอ้างอิงเริ่มต้นดังกล่าวได้

- (ก) วิธีการและช่วงเวลาสำหรับการตรวจสอบ การทดสอบ หรือการทวนสอบตามวาระ ต้องระบุส่วนหรือหน้าที่ที่ตรวจ วิธีดำเนินการ ช่วงเวลา เกณฑ์การยอมรับ การตอบสนองเมื่อพบความบกพร่อง และเหตุผลหรือหลักฐานที่ใช้กำหนดช่วงเวลาดังกล่าว
- (ข) เกณฑ์และวิธีการบำรุงรักษา ต้องระบุส่วนที่ต้องบำรุงรักษา วิธีดำเนินการ เกณฑ์ที่ใช้ตัดสินการบำรุงรักษาหรือเปลี่ยนทดแทน และวิธีทวนสอบหน้าที่ความปลอดภัยภายหลังการดำเนินการ

- (ค) ข้อกำหนดสำหรับชิ้นส่วนหรือมอดูลทดแทน ต้องระบุรายการที่อนุญาต เจาะไขและข้อจำกัดในการทดแทน ความเข้ากันได้ของฮาร์ดแวร์ ซอฟต์แวร์หรือเฟิร์มแวร์ และการทวนสอบที่ต้องดำเนินการภายหลังการเปลี่ยน
- (ง) ข้อกำหนดสำหรับเครื่องมือ อุปกรณ์ทดสอบ หรือซอฟต์แวร์ประยุกต์ภายนอก ต้องระบุเครื่องมือและรุ่นที่อนุญาต ขอบเขตการใช้งาน สิทธิการเข้าถึง การเชื่อมต่อ การป้องกันการเปลี่ยนแปลงค่าที่ไม่ปลอดภัย พฤติกรรมของเครื่องตัดวงจรเมื่อการสื่อสารขัดข้องหรือขาดหาย ในระหว่างการเปลี่ยนพารามิเตอร์หรือการกำหนดค่า และข้อจำกัดที่เกี่ยวข้อง
- (จ) ข้อมูลและบันทึกสำหรับการสอบกลับ ต้องระบุข้อมูลที่ต้องบันทึกสำหรับกิจกรรมการบำรุงรักษา การปรับตั้ง การเปลี่ยนแปลง และการทวนสอบภายหลังการดำเนินการ รวมถึงวันเวลา ผู้ดำเนินการ รุ่นหรือการกำหนดค่าที่เกี่ยวข้อง ผลการดำเนินการ และระยะเวลาการเก็บรักษาตามที่จำเป็น
- (ฉ) การวิเคราะห์ผลกระทบจากการเปลี่ยนแปลง ต้องระบุการเปลี่ยนแปลงองค์ประกอบ ฮาร์ดแวร์ ซอฟต์แวร์ เฟิร์มแวร์ พารามิเตอร์ เครื่องมือพัฒนา หรือการกำหนดค่าที่อาจกระทบหน้าที่ความปลอดภัย ผลกระทบที่ประเมิน และขอบเขตการทวนสอบ การตรวจสอบความใช้ได้ หรือการทดสอบซ้ำที่กำหนด
- (ช) ผลการทวนสอบ การตรวจสอบความใช้ได้ หรือการทดสอบซ้ำภายหลังการบำรุงรักษาหรือการเปลี่ยนแปลง ต้องระบุข้อกำหนดหรือหน้าที่ที่ตรวจ วิธีดำเนินการ การกำหนดค่าที่ใช้ ผลที่ได้ และข้อสรุป ตามที่เกี่ยวข้อง
- (ซ) หลักฐานการสนับสนุนซอฟต์แวร์และเฟิร์มแวร์ ต้องระบุอายุการใช้งานที่ออกแบบไว้ของฮาร์ดแวร์แยกจากระยะเวลาการสนับสนุนซอฟต์แวร์และเฟิร์มแวร์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัย ซึ่งต้องไม่น้อยกว่า ๔ ปี รวมถึงจุดเริ่มต้นและเงื่อนไขของระยะเวลาการสนับสนุน วิธีหรือช่องทางการสนับสนุน มาตรการและเงื่อนไขการดำเนินการเมื่อสิ้นสุดระยะเวลาการสนับสนุน และหลักฐานแสดงว่าเมื่อสิ้นสุดระยะเวลาดังกล่าว เครื่องตัดวงจรยังคงไว้ซึ่งหน้าที่ความปลอดภัยตามข้อกำหนดหรือเข้าสู่สภาวะปลอดภัยตามที่กำหนด
- (ฌ) หลักฐานการปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ ต้องระบุกลไกและเงื่อนไขการปรับปรุง การพิสูจน์ความแท้จริงและความถูกต้องสมบูรณ์ของชุดซอฟต์แวร์หรือเฟิร์มแวร์ พฤติกรรมระหว่างการดาวน์โหลด การติดตั้ง การปรับปรุงและการกู้คืน วิธีการกู้คืนเมื่อกระบวนการขัดข้องหรือล้มเหลว การคงไว้หรือการทวนสอบพารามิเตอร์ด้านความปลอดภัยภายหลังการปรับปรุง และผลการทวนสอบที่เกี่ยวข้อง

(ญ) หลักฐานการบันทึกเหตุการณ์และการเก็บรักษาข้อมูล ต้องระบุประเภทเหตุการณ์ที่บันทึกข้อมูลที่บันทึกสำหรับแต่ละเหตุการณ์ ระยะเวลาการเก็บรักษา ความสามารถในการคงอยู่และเรียกคืนข้อมูลเมื่อแหล่งจ่ายไฟฟ้าขาดหาย หลักเกณฑ์การจัดการเมื่อพื้นที่จัดเก็บถึงขีดจำกัด และกรณีใช้ระบบจัดเก็บภายนอก ให้ระบุพฤติกรรมเมื่อการเชื่อมต่อไม่พร้อมใช้งานและการส่งต่อข้อมูลเมื่อการเชื่อมต่อกลับคืน รวมทั้งข้อกำหนดของข้อมูลบันทึกที่กลุ่มคลื่นสัญญาณหรือข้อมูลโปรไฟล์พารามิเตอร์ทางไฟฟ้าเชิงเวลาตามที่เกี่ยวข้อง

ข.๓ การพิจารณาหลักฐาน การสอบกลับ และการประเมินความเพียงพอ

ผู้ทำต้องจัดให้มีการสอบกลับอย่างน้อยจากอันตรายและเหตุการณ์อันตราย ไปยังหน้าที่ความปลอดภัย ระดับคุณภาพความปลอดภัย ข้อกำหนดความต้องการด้านความปลอดภัย การออกแบบและองค์ประกอบที่เกี่ยวข้อง มาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์และความถูกต้องสมบูรณ์ของข้อมูลที่มีผลต่อหน้าที่ความปลอดภัย การทวนสอบของผู้ทำ การตรวจสอบความใช้ได้ การจัดการการเปลี่ยนแปลง และผลการทดสอบของเครื่องตัวจริงประกอบสำเร็จ ตามที่เกี่ยวข้อง

ในการพิจารณาหลักฐาน ต้องดำเนินการอย่างน้อยดังต่อไปนี้

- (ก) ตรวจสอบว่ามีหลักฐานที่จำเป็นตามข้อ ข.๒ ครบถ้วนตามที่เกี่ยวข้องกับข้อกำหนดที่ประเมิน และมีสาระตามที่กำหนดสำหรับหลักฐานแต่ละรายการ
- (ข) ตรวจสอบว่าหลักฐานตรงกับรุ่นฮาร์ดแวร์ รุ่นซอฟต์แวร์หรือเฟิร์มแวร์ และการกำหนดค่าของเครื่องตัวจริงที่ยื่นทดสอบ
- (ค) ตรวจสอบความสอดคล้องระหว่างข้อกำหนดความต้องการด้านความปลอดภัย การวิเคราะห์อันตรายและความเสี่ยง การออกแบบ การวิเคราะห์ความล้มเหลว ผลการทวนสอบ และผลการตรวจสอบความใช้ได้ ตามที่เกี่ยวข้อง
- (ง) ตรวจสอบการสอบกลับจากข้อกำหนดที่ประเมินไปยังหน้าที่ความปลอดภัย ข้อกำหนดความต้องการด้านความปลอดภัย การออกแบบหรือมาตรการที่ใช้ และผลการทวนสอบที่เกี่ยวข้อง
- (จ) ตรวจสอบว่าผลการทวนสอบหรือการทดสอบของผู้ทำมีวิธีการ สภาวะทดสอบ เกณฑ์การยอมรับ การกำหนดค่าที่ทดสอบ และผลที่เพียงพอสำหรับยืนยันข้อกำหนดที่ประเมิน
- (ฉ) เปรียบเทียบสาระของหลักฐานกับผลการทดสอบตามภาคผนวก ค. ในกรณีที่ข้อกำหนดนั้นกำหนดให้มีการทดสอบ
- (ช) สำหรับเครื่องตัวจริงที่อยู่ในขอบข่ายภาคผนวก ก. ให้ตรวจสอบว่าหลักฐานที่เกี่ยวข้องตามข้อ ข.๒ ครอบคลุมหน้าที่ควบคุมผ่านวงจรนำร่องหรือมอดูลที่เกี่ยวข้อง และผลกระทบต่อหน้าที่ความปลอดภัยและหน้าที่ป้องกันพื้นฐานของเครื่องตัวจริง

ให้ถือว่าหลักฐานเพียงพอเมื่อหลักฐานมีความครบถ้วน ถูกต้อง สอดคล้อง สอบกลับได้ ตรงกับแบบและการกำหนดค่าของเครื่องตัดวงจรที่ยื่นทดสอบ และมีข้อมูลเพียงพอสำหรับแสดงความเป็นไปตามข้อกำหนดที่ประเมิน

ข.๔ การตรวจสอบเพิ่มเติมกรณีหลักฐานไม่เพียงพอ

กรณีที่พบความไม่ครบถ้วน ความไม่สอดคล้อง ความไม่ชัดเจน หรือหลักฐานไม่เพียงพอสำหรับการพิจารณาความเป็นไปตามข้อกำหนด ให้พิจารณาการกำหนดค่า รายละเอียดทางเทคนิค หลักฐาน หรือผลการทวนสอบเพิ่มเติมตามความจำเป็น เพื่อให้ได้ข้อมูลที่เพียงพอสำหรับการพิจารณาความเป็นไปตามข้อกำหนด หากจำเป็นต้องดำเนินการทดสอบเพิ่มเติม ให้ดำเนินการตามภาคผนวก ค.๓ และให้บันทึกเหตุผลและผลการดำเนินการไว้ในรายงานผลการทดสอบ

ภาคผนวก ค.
วิธีการทดสอบด้านความปลอดภัยเชิงหน้าที่
(ข้อกำหนด)
(ข้อ ๖ และข้อ ๘)

ค.๑ ข้อกำหนดทั่วไปสำหรับการทดสอบ

ค.๑.๑ ทัวไป

การทดสอบตามภาคผนวกนี้ให้ดำเนินการกับเครื่องต้นวงจรที่ประกอบสำเร็จในสภาพพร้อมจำหน่ายและมีการกำหนดค่าตามที่ผู้ทำกำหนดสำหรับการใช้งาน เว้นแต่วิธีการทดสอบเฉพาะจะกำหนดไว้เป็นอย่างอื่น วิธีการทดสอบให้เลือกระหว่างการดำเนินการตามหน้าที่ คุณลักษณะ ช่องสัญญาณ ช่องทางสื่อสาร ช่องทางการเข้าถึง และการเชื่อมต่อที่มีในเครื่องต้นวงจรและเกี่ยวข้องกับข้อกำหนดที่ประเมิน

ก่อนดำเนินการทดสอบตามข้อ ค.๒ และข้อ ค.๓ ต้องกำหนดกรณีทดสอบที่จำเป็นสำหรับการประเมินความเป็นไปตามข้อกำหนดที่เกี่ยวข้อง โดยพิจารณาจากหน้าที่ คุณลักษณะ ส่วนต่อประสาน การกำหนดค่า สภาพการทำงาน สภาพผิดปกติ ความผิดปกติ และเหตุการณ์ที่กำหนดไว้ในข้อกำหนด และวิธีการทดสอบที่เกี่ยวข้องกับเครื่องต้นวงจร

กรณีทดสอบแต่ละกรณีต้องสามารถสอบกลับไปยังข้อกำหนดที่ประเมินและวิธีการทดสอบที่เกี่ยวข้องได้

กรณีทดสอบแต่ละกรณีต้องประกอบด้วย รหัสกรณีทดสอบ ข้อกำหนดที่ประเมิน วิธีการทดสอบที่ใช้ วัตถุประสงค์ของกรณีทดสอบ ตัวอย่างและการกำหนดค่าที่ใช้ สภาพเริ่มต้น สภาพทดสอบหรือการกระทำ ผลที่คาดหวัง เงื่อนไขการยอมรับ ข้อมูลที่ต้องบันทึก และการคืนสภาพเมื่อจำเป็น เมื่อดำเนินการทดสอบแล้ว ต้องบันทึกผลที่ได้ ผลการตัดสินใจ และหลักฐานอ้างอิงให้สามารถเชื่อมโยงกับกรณีทดสอบนั้นได้

กรณีที่หน้าที่ คุณลักษณะ ส่วนต่อประสาน การกำหนดค่า สภาพ หรือเหตุการณ์หลายรายการมีหลักการทำงาน วิธีการประมวลผล วิธีการตรวจพบหรือจัดการ และการตอบสนองที่เกี่ยวข้องกับการทดสอบในลักษณะเดียวกัน อาจเลือกกรณีที่เป็นตัวแทนสำหรับการทดสอบได้ โดยต้องไม่มีความแตกต่างที่อาจมีผลต่อผลการทดสอบ และต้องบันทึกเหตุผลในการเลือกและขอบเขตที่กรณีดังกล่าวใช้เป็นตัวแทน

ค.๑.๒ ตัวอย่างทดสอบและการกำหนดค่า

ก่อนทดสอบต้องบันทึกรุ่น หมายเลขประจำตัว รุ่นฮาร์ดแวร์ รุ่นซอฟต์แวร์หรือเฟิร์มแวร์ ค่าตรวจสอบความถูกต้องสมบูรณ์ของซอฟต์แวร์หรือเฟิร์มแวร์ พารามิเตอร์ด้านความปลอดภัย การตั้งค่าการต่อกลับอัตโนมัติ การกำหนดค่าการสื่อสาร โมดูลหรืออุปกรณ์เสริมที่ใช้ และข้อมูลอื่นที่มีผลต่อผลการทดสอบ

การกำหนดค่าต้องเป็นการกำหนดค่าของผลิตภัณฑ์สำหรับจำหน่าย เว้นแต่ข้อกำหนดเฉพาะระบุเป็นอย่างอื่น

กรณีที่ใช้ตัวอย่างมากกว่าหนึ่งตัวอย่าง ให้ระบุการจัดสรรตัวอย่างสำหรับแต่ละวิธีทดสอบและแสดงว่าการกำหนดค่าของตัวอย่างแต่ละตัวสอดคล้องกับขอบข่ายที่ประเมิน

กรณีที่มีการใช้การกำหนดค่ามากกว่าหนึ่งแบบในการทดสอบ ต้องสามารถระบุได้ว่าการกำหนดค่าแต่ละแบบใช้กับกรณีทดสอบใด และต้องแสดงว่าการกำหนดค่าที่ใช้ครอบคลุมขอบข่ายที่ประเมิน

ค.๑.๓ สภาวะและเครื่องมือทดสอบ

ให้จัดเตรียมแหล่งจ่าย โหลด เครื่องมือวัด ระบบสื่อสาร และสภาวะแวดล้อมตามที่กำหนดในข้อทดสอบที่เกี่ยวข้อง เครื่องมือวัดต้องมีพิสัย ความละเอียด และความไม่แน่นอนของการวัดเหมาะสมกับเกณฑ์การยอมรับ ต้องบันทึกแผนผังการต่อวงจรและการกำหนดค่าเครื่องมือที่มีผลต่อผลการทดสอบ

ค.๑.๔ การดำเนินการทดสอบ

การทดสอบตามข้อ ค.๒ และข้อ ค.๓ ให้ดำเนินการตามวิธีการทดสอบที่เกี่ยวข้องและกรณีทดสอบที่กำหนดไว้ตามข้อ ค.๑.๑ โดยในแต่ละกรณีทดสอบต้องกำหนดสภาวะเริ่มต้น สร้างสภาวะทดสอบหรือดำเนินการตามวิธีการทดสอบกำหนด สังเกตผลการทำงานของเครื่องตัวจริง และคืนสภาพเมื่อวิธีการทดสอบกำหนด

ต้องบันทึกผลการสังเกตและข้อมูลที่เป็นต่อการประเมินผลของแต่ละกรณีทดสอบ รวมทั้งสถานะการติดต่อของวงจรหลัก การแสดงหรือส่งสัญญาณสถานะ ข้อมูลเหตุการณ์ เวลาตอบสนอง และพารามิเตอร์ด้านความปลอดภัยที่กำหนดให้เป็นส่วนหนึ่งของผลที่ต้องประเมินในกรณีทดสอบนั้น

กรณีที่วิธีการทดสอบกำหนดให้ใช้ค่าขอบเขตหรือค่านอกขอบเขต ให้ใช้ค่าขอบเขตที่ผู้ทำกำหนดสำหรับเครื่องตัวจริงที่ประเมิน และกำหนดค่านอกขอบเขต ดังต่อไปนี้

- (ก) กรณีที่ค่าที่ป้อนหรือกำหนดในการทดสอบมีความละเอียดในการปรับค่าที่กำหนด ให้ใช้ค่าที่อยู่นอกขอบเขตและใกล้ขอบเขตนั้นมากที่สุดตามความละเอียดดังกล่าว โดยต้องสามารถยืนยันได้ว่าอยู่นอกขอบเขต หากค่าดังกล่าวยังไม่สามารถยืนยันได้ว่าอยู่นอกขอบเขต ให้ใช้ค่าถัดออกไปจนสามารถยืนยันได้
- (ข) กรณีที่ค่าที่ป้อนหรือกำหนดในการทดสอบสามารถเปลี่ยนแปลงได้อย่างต่อเนื่อง ให้กำหนดค่านอกขอบเขตโดยคำนึงถึงความไม่แน่นอนของการสร้างและการวัดค่า โดยช่วงค่าที่ครอบคลุมความไม่แน่นอนดังกล่าวต้องอยู่นอกขอบเขตทั้งหมด

- (ค) กรณีที่ค่านอกขอบเขตเป็นปริมาณทางไฟฟ้า สัญญาณ หรือสภาวะทางกายภาพที่บ่อนให้เครื่องตัดวงจร ค่าดังกล่าวต้องไม่เกินพิกัดความปลอดภัยของเครื่องตัดวงจรหรือส่วนของเครื่องตัดวงจรที่รับปริมาณ สัญญาณ หรือสภาวะดังกล่าว

กรณีที่ความผิดพลาดที่ต้องประเมินไม่สามารถสร้างขึ้นได้โดยตรง อาจใช้วิธีการสร้างหรือจำลองความผิดพลาดที่เหมาะสมกับการออกแบบของเครื่องตัดวงจร โดยวิธีการดังกล่าวต้องสามารถทำให้เกิดผลต่อส่วนหรือหน้าที่ที่ประเมินในลักษณะที่เป็นตัวแทนของความผิดพลาดนั้นได้

กรณีที่สภาวะทดสอบหรือความผิดพลาดตามวิธีการทดสอบไม่สามารถสร้างหรือจำลองจากภายนอกได้ โดยวิธีที่เครื่องตัดวงจรรองรับ และการดำเนินการดังกล่าวจำเป็นต้องดัดแปลงหรือเข้าถึงส่วนภายในในลักษณะที่อาจเปลี่ยนสภาพของตัวอย่าง ผู้ทำต้องระบุสภาวะหรือความผิดพลาดดังกล่าว พร้อมเหตุผลทางเทคนิคและหลักฐานสนับสนุน และให้พิจารณาความเป็นไปตามข้อกำหนดจากหลักฐานที่เกี่ยวข้องตามภาคผนวก ข.

กรณีที่สภาวะทดสอบอาจทำให้เครื่องตัดวงจรหรือส่วนที่เกี่ยวข้องเกิดความเสียหายถาวร หรือทำให้เกิดการพิกัดหรือขีดจำกัดด้านความปลอดภัย ไม่ต้องดำเนินการทดสอบในสภาวะดังกล่าว โดยผู้ทำต้องระบุสภาวะที่ไม่สามารถทดสอบได้ พร้อมเหตุผลทางเทคนิคและหลักฐานสนับสนุน และให้พิจารณาความเป็นไปตามข้อกำหนดจากหลักฐานที่เกี่ยวข้องตามภาคผนวก ข.

ค.๑.๕ เกณฑ์การยอมรับทั่วไป

ระหว่างและภายหลังการทดสอบ เครื่องตัดวงจรต้องไม่เกิดการจ่ายพลังงานหรือการต่อวงจรโดยไม่ตั้งใจ หน้าที่ความปลอดภัยต้องไม่ถูกระงับหรือหน่วงรั้งจนทำให้ระยะเวลารวมในการตอบสนองเกินระยะเวลาสูงสุดที่ยอมรับได้หรือระยะเวลาทนทานต่อความผิดพลาดที่เกี่ยวข้อง หากไม่สามารถรักษาหน้าที่ความปลอดภัยได้ต้องเข้าสู่สภาวะปลอดภัยตามที่กำหนด และต้องรักษาความถูกต้องสมบูรณ์ของพารามิเตอร์ด้านความปลอดภัยและบันทึกเหตุการณ์ตามข้อกำหนดที่เกี่ยวข้อง ทั้งนี้ ต้องเป็นไปตามเกณฑ์การยอมรับเฉพาะที่กำหนดในวิธีการทดสอบแต่ละข้อด้วย

ผลที่คาดหวังของแต่ละกรณีทดสอบต้องสอดคล้องกับข้อกำหนดที่ประเมินและเกณฑ์การยอมรับที่ใช้กับวิธีการทดสอบนั้น และให้เปรียบเทียบผลที่ได้กับผลที่คาดหวังและเกณฑ์การยอมรับเพื่อพิจารณาผลผ่านหรือไม่ผ่าน

ผลการทดสอบแต่ละกรณีต้องสามารถสลับไปยังกรณีทดสอบ วิธีการทดสอบ ข้อกำหนดที่ประเมิน การกำหนดค่าของตัวอย่าง สภาวะทดสอบ และผลการพิจารณาหลักฐานตามภาคผนวก ข. ที่ใช้ประกอบการประเมิน

ค.๒ วิธีการทดสอบเฉพาะ

ค.๒.๑ การทดสอบการตอบสนองต่อความผิดพลาด

ให้จัดเครื่องตัวจริงในสถานะใช้งานปกติและการกำหนดค่าที่เกี่ยวข้องกับหน้าที่ความปลอดภัยที่จะทดสอบ แล้วสร้างความผิดพลาดหรือสถานะผิดปกติตามวิธีการที่กำหนดในข้อ ค.๒.๑.๑ ถึง ค.๒.๑.๘

ให้ตรวจสอบเส้นทางการตอบสนองตั้งแต่การสร้างความปลอดภัยหรือสถานะผิดปกติ การตรวจพบหรือการจัดการ การตอบสนองของเครื่องตัวจริง จนถึงการคงไว้ซึ่งหน้าที่ความปลอดภัยหรือการเข้าสู่สถานะปลอดภัยตามที่กำหนด และเมื่อข้อกำหนดความต้องการด้านความปลอดภัยกำหนดระยะเวลาการตอบสนอง ต้องตรวจสอบว่าการตอบสนองเป็นไปตามระยะเวลาดังกล่าว

ให้ตรวจสอบสถานะการติดต่อของวงจรหลัก หน้าที่ความปลอดภัย หน้าที่ป้องกันพื้นฐาน การแสดงหรือส่งสัญญาณสถานะ และข้อมูลที่กำหนดในกรณีทดสอบ ภายหลังการสร้างความปลอดภัยหรือสถานะผิดปกติที่อาจมีผลต่อหน้าที่ป้องกันพื้นฐาน ให้กระตุ้นหน้าที่ป้องกันพื้นฐานตามข้อ ๕ และตรวจสอบว่าหน้าที่ดังกล่าวยังคงตอบสนองได้ตามข้อกำหนด

เครื่องตัวจริงต้องคงไว้ซึ่งหน้าที่ความปลอดภัย กรณีที่ไม่สามารถคงไว้ได้ ต้องเข้าสู่สถานะปลอดภัยตามข้อกำหนดความต้องการด้านความปลอดภัย และต้องไม่ทำให้หน้าที่ป้องกันพื้นฐานลดลง

หมายเหตุ การทดสอบตามข้อนี้ใช้ทดสอบพฤติกรรมและเส้นทางการตอบสนองต่อความผิดพลาดหรือสถานะผิดปกติที่สามารถสร้างหรือจำลองได้ ส่วนการวิเคราะห์ความล้มเหลวและการประเมินความครอบคลุมของการตรวจวินิจฉัยพิจารณาจากหลักฐานตามภาคผนวก ข.

ค.๒.๑.๑ การทดสอบการเฝ้าระวังความสมบูรณ์ของการปฏิบัติงานอย่างต่อเนื่อง

ค.๒.๑.๑.๑ การจัดสภาพตัวอย่าง

ให้เครื่องตัวจริงทำงานในสถานะใช้งานปกติ โดยเปิดใช้งานหน้าที่ความปลอดภัยและช่องทางการรับส่งสัญญาณหรือข้อมูลที่ใช้กับหน้าที่ที่ทดสอบตามการกำหนดค่าของเครื่องตัวจริงสำหรับจำหน่าย

ให้ดำเนินการทดสอบตลอดช่วงเวลาที่ครอบคลุมการเฝ้าระวังหรือการตรวจวินิจฉัยที่ผู้ทำกำหนดสำหรับหน้าที่ที่ทดสอบ

ค.๒.๑.๑.๒ การทดสอบสัญญาณหรือข้อมูล

การทดสอบสัญญาณหรือข้อมูลแต่ละชนิดที่ผู้ทำกำหนดให้อยู่ภายใต้การเฝ้าระวังหรือการตรวจวินิจฉัยอย่างต่อเนื่องและสามารถสร้างสภาวะผิดปกติจากภายนอกได้ ต้องครอบคลุมสภาวะผิดปกติที่ผู้ทำกำหนดให้กลไกดังกล่าวตรวจพบหรือจัดการ

ให้สร้างสภาวะผิดปกติแต่ละสภาวะและคงไว้จนสามารถตรวจสอบการตรวจพบ การจัดการ และการตอบสนองของเครื่องตัวจริงได้ครบถ้วน และเมื่อข้อกำหนดความต้องการด้านความปลอดภัยกำหนดระยะเวลาการตอบสนอง ต้องตรวจสอบว่าการตอบสนองเป็นไปตามระยะเวลาดังกล่าว

ค.๒.๑.๑.๓ การทดสอบการสื่อสาร

การทดสอบช่องทางสื่อสารแต่ละช่องทางที่ผู้ทำกำหนดให้อยู่ภายใต้การเฝ้าระวังหรือการตรวจวินิจฉัยอย่างต่อเนื่องและเกี่ยวข้องกับหน้าที่ความปลอดภัย ต้องครอบคลุมอย่างน้อยดังต่อไปนี้

- (ก) การสื่อสารขาดหาย
- (ข) การสื่อสารถูกขัดจังหวะระหว่างการรับส่งข้อมูล
- (ค) ข้อมูลที่รับไม่ครบถ้วน
- (ง) ข้อมูลที่ไม่เป็นไปตามรูปแบบที่ช่องทางสื่อสารนั้นรองรับ

ให้คงแต่ละสภาวะจนสามารถตรวจสอบการตรวจพบ การจัดการ และการตอบสนองของเครื่องตัวจริงได้ครบถ้วน

ค.๒.๑.๑.๔ การคืนสภาพ

ภายหลังแต่ละกรณีทดสอบ ให้คืนสัญญาณ ข้อมูล หรือการสื่อสารสู่สภาวะปกติ และตรวจสอบว่าไม่เกิดการต่อวงจร การเปลี่ยนสถานะ หรือการเริ่มทำงานที่ไม่ปลอดภัยโดยไม่ตั้งใจ

ผลการตรวจพบ การจัดการ และการตอบสนองตามข้อ ค.๒.๑.๑ ต้องเป็นไปตามข้อกำหนดความต้องการด้านความปลอดภัย และต้องไม่ทำให้หน้าที่ป้องกันพื้นฐานของเครื่องตัวจริงลดลง

ค.๒.๑.๒ การทดสอบความผิดพลาดของอินพุตและเอาต์พุต

การทดสอบความผิดพลาดของอินพุตและเอาต์พุต ต้องดำเนินการกับอินพุตและเอาต์พุตแต่ละชนิดที่เกี่ยวข้องกับหน้าที่ความปลอดภัยและสามารถสร้างหรือจำลองความผิดพลาดจากภายนอกได้

โดยใช้รูปแบบความผิดพลาดที่ผู้ทำกำหนดจากการออกแบบหรือการวิเคราะห์ความล้มเหลวของเครื่องตัววงจร

การทดสอบอินพุตต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) การขาดหายของสัญญาณหรือข้อมูล
- (ข) กรณีที่อินพุตมีช่วงค่าการทำงานที่กำหนด ให้ทดสอบค่าที่ขอบเขตต่ำ ค่าต่ำกว่าขอบเขตต่ำ ค่าที่ขอบเขตสูง และค่าสูงกว่าขอบเขตสูง
- (ค) กรณีที่อินพุตมีสถานะที่กำหนด ให้ทดสอบสถานะที่ไม่เป็นไปตามเงื่อนไขที่กำหนด
- (ง) ค่าหรือสถานะที่ไม่สมเหตุผลตามรูปแบบสัญญาณหรือข้อมูลที่อินพุตนั้นรองรับ
- (จ) ความผิดพลาดอื่นที่ผู้ทำกำหนดให้ต้องตรวจพบหรือจัดการจากการออกแบบหรือการวิเคราะห์ความล้มเหลว

เอาต์พุตแต่ละชนิดที่เกี่ยวข้องกับหน้าที่ความปลอดภัย ต้องทดสอบความผิดพลาดของเอาต์พุตที่สามารถสร้างหรือจำลองได้จากภายนอกตามรูปแบบความผิดพลาดที่กำหนดจากการออกแบบหรือการวิเคราะห์ความล้มเหลวของเครื่องตัววงจร

ให้ตรวจสอบการตรวจพบหรือการจัดการความผิดพลาด การตอบสนองของเครื่องตัววงจร การคงไว้ซึ่งหน้าที่ป้องกันพื้นฐาน การเข้าสู่สภาวะปลอดภัยเมื่อกำหนด และการแสดงหรือส่งสัญญาณสถานะ

ค.๒.๑.๓ การทดสอบสภาวะผิดปกติของแรงดันไฟเลี้ยงระบบควบคุม

การทดสอบสภาวะผิดปกติของแรงดันไฟเลี้ยงระบบควบคุม ให้ดำเนินการกับแรงดันไฟเลี้ยงที่สามารถเข้าถึงจากภายนอก หรือสภาวะที่สามารถสร้างหรือจำลองจากภายนอกได้ตามข้อ ค.๑.๔ โดยต้องครอบคลุมอย่างน้อยสภาวะต่อไปนี้ที่สามารถดำเนินการได้ตามข้อ ค.๑.๔

- (ก) แรงดันไฟเลี้ยงปกติ
- (ข) ขอบเขตต่ำสุดที่ผู้ทำกำหนด
- (ค) ค่าต่ำกว่าขอบเขตต่ำสุด
- (ง) ขอบเขตสูงสุดที่ผู้ทำกำหนด
- (จ) ค่าสูงกว่าขอบเขตสูงสุด
- (ฉ) การขาดหายของแรงดันไฟเลี้ยง

(ซ) การคืนแรงดันไฟเลี้ยงจากสภาวะขาดหายหรือค่านอกขอบเขตกลับสู่สภาวะปกติ

ค่านอกขอบเขตให้กำหนดตามข้อ ค.๑.๔ ให้คงแต่ละสภาวะจนสามารถตรวจสอบพฤติกรรมและการตอบสนองของเครื่องตัดวงจรได้ครบถ้วน

ในระหว่างการทดสอบและภายหลังการคืนแรงดันไฟเลี้ยงสู่สภาวะปกติ ให้ตรวจสอบว่าไม่เกิดการต่อวงจร การเปลี่ยนสถานะ หรือการเริ่มระบบใหม่โดยไม่ตั้งใจ พารามิเตอร์ด้านความปลอดภัยยังคงถูกต้อง และหน้าที่ความปลอดภัยยังคงทำงานหรือเครื่องตัดวงจรเข้าสู่สภาวะปลอดภัยตามที่กำหนด

ค.๒.๑.๔ การทดสอบวงจรการตรวจวินิจฉัยตนเอง

การทดสอบวงจรการตรวจวินิจฉัยตนเอง ต้องดำเนินการโดยให้เครื่องตัดวงจรทำงานตลอดช่วงเวลาที่ยาวที่สุดที่ผู้ทำกำหนด

กรณีที่สมารถระบุช่วงเวลาที่เกิดการตรวจวินิจฉัยตนเองทำงานได้ ให้กระตุ้นหน้าที่ความปลอดภัยอย่างน้อยหนึ่งครั้งในช่วงเวลาที่กลไกการตรวจวินิจฉัยกำลังทำงาน

ตรวจสอบว่าระหว่างการตรวจวินิจฉัยตนเอง เครื่องตัดวงจรยังคงสามารถปฏิบัติหน้าที่ความปลอดภัยและหน้าที่ป้องกันพื้นฐานได้ตามข้อกำหนด และไม่เกิดการหยุดชะงัก การยับยั้ง หรือการหน่วงรั้งหน้าที่ดังกล่าวเกินระยะเวลาที่กำหนด

ให้บันทึกวงจรการตรวจวินิจฉัยที่ผู้ทำกำหนด ช่วงเวลาที่ดำเนินการทดสอบ และผลการตอบสนองของเครื่องตัดวงจร

ค.๒.๑.๕ การทดสอบการคำนวณและการจัดการข้อมูล

การทดสอบการคำนวณและการจัดการข้อมูล ให้ป้อนค่าพารามิเตอร์ทางไฟฟ้าแต่ละชนิดจากภายนอกที่มีผลต่อหน้าที่ความปลอดภัย โดยการทดสอบต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) ค่าปกติภายในช่วงการทำงาน
- (ข) ค่าที่ขอบเขตต่ำ
- (ค) ค่าต่ำกว่าขอบเขตต่ำ
- (ง) ค่าที่ขอบเขตสูง
- (จ) ค่าสูงกว่าขอบเขตสูง
- (ฉ) การเปลี่ยนค่าจากช่วงปกติไปยังค่านอกขอบเขต
- (ช) การเปลี่ยนค่าจากค่านอกขอบเขตกลับเข้าสู่ช่วงปกติ

ค่าที่อยู่ภายในช่วงการทำงาน ต้องตรวจสอบว่าผลการประมวลผลที่สามารถสังเกตได้จากภายนอก และการตอบสนองของเครื่องตัวจริงเป็นไปตามที่กำหนด

ค่านอกขอบเขตหรือข้อมูลที่ไม่ถูกต้องหรือไม่สมเหตุผล ต้องตรวจสอบว่าข้อมูลดังกล่าวไม่ถูกนำไปใช้ในลักษณะที่ทำให้หน้าที่ความปลอดภัยลดลง และเมื่อไม่สามารถประมวลผลข้อมูลได้อย่างปลอดภัย เครื่องตัวจริงต้องคงไว้ซึ่งหน้าที่ความปลอดภัยหรือเข้าสู่สภาวะปลอดภัยตามที่กำหนด

ค.๒.๑.๖ การทดสอบความคงที่ของตรรกะการควบคุม

การทดสอบตามข้อนี้ให้ดำเนินการเฉพาะกรณีที่ตรรกะการควบคุมใช้ขอบเขตสำหรับการเปลี่ยนเข้าสู่สถานะและขอบเขตสำหรับการกลับสู่สถานะเดิม โดยใช้ขอบเขตที่ผู้ทำกำหนดสำหรับพารามิเตอร์ทางไฟฟ้าแต่ละชนิดที่ใช้กำหนดการเปลี่ยนสถานะของตรรกะการควบคุม

เริ่มจากสภาวะที่เครื่องตัวจริงอยู่ในสถานะปกติ แล้วเปลี่ยนค่าพารามิเตอร์ทางไฟฟ้าในทิศทางที่ทำให้เกิดการเปลี่ยนสถานะจนผ่านขอบเขตสำหรับการเปลี่ยนเข้าสู่สถานะ จากนั้นเปลี่ยนค่าพารามิเตอร์กลับในทิศทางตรงข้ามจนผ่านขอบเขตสำหรับการกลับสู่สถานะเดิม ให้เปลี่ยนค่าพารามิเตอร์ผ่านขอบเขตสำหรับการเปลี่ยนเข้าสู่สถานะและขอบเขตสำหรับการกลับสู่สถานะเดิม สลับไปมา เพื่อทดสอบความคงที่ของการเปลี่ยนสถานะ

ภายในช่วงระหว่างขอบเขตทั้งสอง ให้ตรวจสอบว่าเครื่องตัวจริงไม่เกิดการเปลี่ยนสถานะกลับโดยไม่เป็นไปตามตรรกะการควบคุมที่ผู้ทำกำหนด

ตรวจสอบว่าเครื่องตัวจริงเปลี่ยนสถานะและกลับสู่สถานะเดิมตามขอบเขตและเงื่อนไขที่ผู้ทำกำหนด และไม่เกิดการเปิดและปิดวงจรสลับกันโดยไม่ตั้งใจ

ค.๒.๑.๗ การทดสอบลำดับการดำเนินงานและการเปลี่ยนสถานะ

การทดสอบลำดับการดำเนินงานและการเปลี่ยนสถานะ ต้องดำเนินการกับลำดับคำสั่งหรือเหตุการณ์ที่ผู้ทำกำหนดให้มีผลต่อหน้าที่ความปลอดภัยหรือการเปลี่ยนสถานะของเครื่องตัวจริง โดยให้ดำเนินการตามลำดับปกติที่ผู้ทำกำหนดก่อน เพื่อยืนยันสถานะและการตอบสนองที่กำหนด การทดสอบต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) การเปลี่ยนลำดับของคำสั่งหรือเหตุการณ์ที่ผู้ทำกำหนดให้มีลำดับก่อนและหลัง
- (ข) การละเว้นคำสั่งหรือเหตุการณ์ที่เป็นส่วนหนึ่งของลำดับ
- (ค) การส่งคำสั่งหรือเหตุการณ์เดิมซ้ำในระหว่างลำดับ
- (ง) กรณีที่ลำดับดำเนินการผ่านช่องทางสื่อสาร ให้ชัดเจนการสื่อสารระหว่างการเปลี่ยนสถานะ

- (จ) กรณีที่การเปลี่ยนสถานะขึ้นอยู่กับแรงดันไฟเลี้ยงระบบควบคุม ให้ทำให้แรงดันไฟเลี้ยงขาดหายระหว่างการเปลี่ยนสถานะ

ให้ตรวจสอบว่าเครื่องตัดวงจรตรวจพบหรือจัดการลำดับหรือการเปลี่ยนสถานะที่ไม่เป็นไปตามที่กำหนด ไม่ยอมรับคำสั่งหรือสถานะที่ขัดกับเงื่อนไขด้านความปลอดภัย และไม่เข้าสู่สถานะที่ไม่ปลอดภัย เมื่อไม่สามารถยืนยันสถานะการทำงานที่ปลอดภัยได้ เครื่องตัดวงจรต้องเข้าสู่สภาวะปลอดภัยภายในเวลาที่กำหนด และแสดงหรือส่งสัญญาณสถานะตามข้อกำหนดความต้องการด้านความปลอดภัย

ค.๒.๑.๘ การทดสอบคำสั่งที่ขัดแย้งกับหน้าที่ความปลอดภัย

การทดสอบคำสั่งที่ขัดแย้งกับหน้าที่ความปลอดภัย ต้องดำเนินการกับหน้าที่ความปลอดภัยแต่ละหน้าที่ที่เครื่องตัดวงจรรองรับคำสั่งหรือการเปลี่ยนแปลงค่าซึ่งอาจขัดแย้งกับการทำงานของหน้าที่ดังกล่าว โดยให้กระตุ้นหน้าที่ความปลอดภัยและดำเนินการคำสั่งหรือการเปลี่ยนแปลงค่าที่อาจขัดแย้งกับหน้าที่ความปลอดภัยในขณะที่หน้าที่นั้นกำลังทำงาน

การทดสอบต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) การส่งคำสั่งที่หากมีผลแล้วจะทำให้เครื่องตัดวงจรอยู่ในสถานะที่ขัดแย้งกับหน้าที่ความปลอดภัย
- (ข) การเปลี่ยนแปลงค่าที่หากมีผลแล้วจะทำให้การทำงานหรือการตอบสนองของหน้าที่ความปลอดภัยเปลี่ยนแปลงไปจากที่กำหนด

กรณีที่คำสั่งหรือการเปลี่ยนแปลงค่าดังกล่าวสามารถดำเนินการได้มากกว่าหนึ่งช่องทาง ให้ดำเนินการทดสอบผ่านแต่ละช่องทางที่เครื่องตัดวงจรรองรับ

ตรวจสอบว่าเครื่องตัดวงจรจัดการคำสั่งหรือการเปลี่ยนแปลงค่าตามลำดับความสำคัญด้านความปลอดภัยที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย และคำสั่งหรือการเปลี่ยนแปลงค่าดังกล่าวไม่ทำให้หน้าที่ความปลอดภัยถูกยกเลิก ขัดขวาง หรือหน่วงรั้งจนไม่สามารถบรรลุผลการตอบสนองและระยะเวลาที่กำหนด

ค.๒.๒ การทดสอบการปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์

การทดสอบการปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์ ให้บันทึกรุ่นซอฟต์แวร์หรือเฟิร์มแวร์ ค่าตรวจสอบความถูกต้องสมบูรณ์ และพารามิเตอร์ด้านความปลอดภัยก่อนดำเนินการทดสอบ

การทดสอบต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) ปรับปรุงด้วยชุดซอฟต์แวร์หรือเฟิร์มแวร์ที่ผู้ทำอนุญาตจนสำเร็จ และทวนสอบหน้าที่ความปลอดภัยที่ได้รับผลกระทบ
- (ข) ดำเนินการปรับปรุงด้วยชุดซอฟต์แวร์หรือเฟิร์มแวร์ที่ไม่ผ่านการพิสูจน์ความแท้จริงหรือการตรวจสอบความถูกต้องสมบูรณ์ และตรวจสอบว่าชุดดังกล่าวถูกปฏิเสธ
- (ค) กรณีที่สามารถดำเนินการได้ตามข้อ ค.๑.๔ ให้ชัดเจนกระบวนการปรับปรุงในระหว่างที่กระบวนการปรับปรุงกำลังดำเนินอยู่ โดยทำให้แรงดันไฟเลี้ยงหรือการสื่อสารที่จำเป็นต่อกระบวนการปรับปรุงขาดหายตามวิธีการปรับปรุงของเครื่องตัวจริง จากนั้นคืนสภาพและตรวจสอบการกู้คืน
- (ง) ภายหลังการทดสอบตาม (ก) ถึง (ค) ให้ตรวจสอบรุ่นซอฟต์แวร์หรือเฟิร์มแวร์ ค่าตรวจสอบความถูกต้องสมบูรณ์ พารามิเตอร์ด้านความปลอดภัย และหน้าที่ความปลอดภัย รวมทั้งตรวจสอบว่าเครื่องตัวจริงยังคงรักษาหน้าที่ความปลอดภัยได้ตามที่กำหนด หรือเข้าสู่สภาวะปลอดภัยเมื่อไม่สามารถดำเนินการต่อได้อย่างปลอดภัย

ระหว่างกระบวนการดาวน์โหลด การติดตั้ง การปรับปรุง หรือการกู้คืน ให้ตรวจสอบว่าหน้าที่ความปลอดภัยไม่ถูกระงับหรือลดทอนเกินระยะเวลาที่กำหนดในข้อกำหนดความต้องการด้านความปลอดภัย กรณีที่ไม่สามารถรักษาหน้าที่ความปลอดภัยได้ ให้ตรวจสอบว่าเครื่องตัวจริงเข้าสู่สภาวะปลอดภัยและยับยั้งการจ่ายพลังงานหรือการต่อกลับที่ไม่ปลอดภัยตามที่กำหนด

ค.๒.๓ การทดสอบความถูกต้องสมบูรณ์ของข้อมูลและการบันทึกเหตุการณ์

ค.๒.๓.๑ การทดสอบความถูกต้องสมบูรณ์ของข้อมูล

การทดสอบความถูกต้องสมบูรณ์ของข้อมูล ต้องดำเนินการกับข้อมูลพารามิเตอร์ด้านความปลอดภัยและซอฟต์แวร์หรือเฟิร์มแวร์ที่ใช้ในการดำเนินหน้าที่ความปลอดภัยและสามารถป้อน ส่งผ่าน หรือเปลี่ยนแปลงจากภายนอกได้

การทดสอบต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) ข้อมูลที่ถูกต้องและสมบูรณ์
- (ข) ข้อมูลที่ถูกเปลี่ยนแปลงจนไม่ผ่านกลไกตรวจสอบความถูกต้องสมบูรณ์
- (ค) ข้อมูลที่ไม่ครบถ้วน

ให้ตรวจสอบว่าข้อมูลตาม (ก) สามารถผ่านการทวนสอบและถูกนำไปใช้ตามที่กำหนด และข้อมูลตาม (ข) และ (ค) ถูกตรวจพบและไม่ถูกนำไปใช้ในการดำเนินหน้าที่ความปลอดภัย

เมื่อไม่สามารถใช้ข้อมูลที่ถูกต้องและสมบูรณ์ในการดำเนินหน้าที่ความปลอดภัยได้ ให้ตรวจสอบว่าเครื่องตัดวงจรคงไว้ซึ่งหน้าที่ความปลอดภัยหรือเข้าสู่สภาวะปลอดภัยตามที่กำหนด

ค.๒.๓.๒ การทดสอบการบันทึกเหตุการณ์

การทดสอบการบันทึกเหตุการณ์ ต้องดำเนินการกับเหตุการณ์ตามข้อ ๘.๒.๑ (ก) (ข) และ (ง) แต่ละชนิดที่เครื่องตัดวงจรรองรับและกำหนดให้มีการบันทึก

ให้สร้างเหตุการณ์แต่ละชนิดดังกล่าว แล้วอ่านข้อมูลที่บันทึกตามวิธีที่ผู้ทำกำหนด

ให้ตรวจสอบว่าบันทึกเหตุการณ์แต่ละรายการมีข้อมูลวันและเวลา ชนิดหรือรหัสเหตุการณ์ และสถานะการทำงานของเครื่องตัดวงจรที่เกี่ยวข้องกับเหตุการณ์นั้นอย่างถูกต้องและครบถ้วน และสามารถสลับไปยังเหตุการณ์ที่สร้างขึ้นได้

ให้ตัดแหล่งจ่ายไฟฟ้าของเครื่องตัดวงจรภายหลังเกิดเหตุการณ์ที่กำหนดให้ต้องบันทึก แล้วคืนแหล่งจ่ายไฟฟ้าและตรวจสอบว่าบันทึกเหตุการณ์ดังกล่าวยังคงอยู่และสามารถเรียกคืนได้

กรณีที่สามารถทำให้พื้นที่จัดเก็บถึงหรือจำลองให้ถึงขีดจำกัดได้โดยวิธีที่เครื่องตัดวงจรรองรับจากภายนอก ให้ดำเนินการตามวิธีที่ผู้ทำกำหนด และตรวจสอบว่าบันทึกเหตุการณ์ที่ยังอยู่ภายในระยะเวลาเก็บรักษาไม่น้อยกว่า ๑ ปีไม่สูญหาย ไม่ถูกเขียนทับ และยังสามารถเรียกคืนได้ รวมทั้งตรวจสอบว่าหลักเกณฑ์การจัดการข้อมูลสอดคล้องกับข้อ ๘.๒.๑

กรณีที่ใช้ระบบเครือข่ายหรือระบบประมวลผลภายนอกสำหรับการเก็บรักษาข้อมูล ให้ทำให้ระบบดังกล่าวไม่พร้อมใช้งาน แล้วสร้างเหตุการณ์ที่กำหนดให้ต้องบันทึก และตรวจสอบว่าข้อมูลยังคงได้รับการบันทึกและเก็บรักษาไว้ จากนั้นคืนการเชื่อมต่อและตรวจสอบว่าสามารถส่งต่อข้อมูลดังกล่าวได้ตามเงื่อนไขที่ผู้ทำกำหนด

ค.๒.๔ การทดสอบการบันทึกรูปคลื่นสัญญาณหรือข้อมูลโปรไฟล์พารามิเตอร์ทางไฟฟ้าเชิงเวลา

การทดสอบการบันทึกรูปคลื่นสัญญาณหรือข้อมูลโปรไฟล์พารามิเตอร์ทางไฟฟ้าเชิงเวลา ต้องดำเนินการกับข้อมูลแต่ละประเภทที่เครื่องตัดวงจรรองรับตามข้อ ๘.๒.๓

ให้จัดเครื่องตัดวงจรในสภาวะใช้งานปกติ วัดและบันทึกแรงดันไฟฟ้า กระแสไฟฟ้า และเวลาอ้างอิงตลอดช่วงเวลาที่ดำเนินการทดสอบ สร้างเหตุการณ์ที่ทำให้เกิดการบันทึกข้อมูลตามที่ผู้ทำกำหนด และเรียกข้อมูลที่บันทึกออกจากเครื่องตัดวงจรตามวิธีที่ผู้ทำกำหนด

การทดสอบต้องตรวจสอบอย่างน้อย ดังต่อไปนี้

- (ก) ข้อมูลที่บันทึกครอบคลุมช่วงเวลาก่อนเกิดเหตุการณ์ไม่น้อยกว่าช่วงเวลาที่ผู้ทำระบุ

- (ข) ข้อมูลที่บันทึกมีข้อมูลอ้างอิงเวลาและสามารถระบุกรอบเวลาที่สัมพันธ์กับเหตุการณ์ที่สร้างขึ้นได้
- (ค) ข้อมูลที่บันทึกมีความต่อเนื่องและครบถ้วนตามรูปแบบและความละเอียดที่ผู้ทำกำหนด
- (ง) ข้อมูลที่บันทึกสามารถนำกลับมาประมวลผลเพื่อจำลองรูปคลื่นสัญญาณย้อนหลังหรือแสดงเส้นแนวโน้มพฤติกรรมทางไฟฟ้าตามประเภทข้อมูลที่บันทึก
- (จ) ผลที่ได้จากการประมวลผลข้อมูลที่บันทึกสอดคล้องกับค่าที่วัดและบันทึกไว้ระหว่างการทดสอบ โดยความแตกต่างต้องไม่เกินขีดจำกัดความถูกต้องที่ผู้ทำกำหนดสำหรับหน้าที่การบันทึกดังกล่าว

ค.๒.๕ การทดสอบการจำกัดการปรับตั้งค่าที่ไม่ปลอดภัย

การทดสอบการจำกัดการปรับตั้งค่าที่ไม่ปลอดภัย ต้องดำเนินการกับพารามิเตอร์ด้านความปลอดภัยแต่ละชนิดที่สามารถปรับตั้งค่าจากภายนอกได้ โดยดำเนินการผ่านช่องทางการปรับตั้งค่าแต่ละช่องทางที่ผู้ทำอนุญาต

การทดสอบต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) ค่าที่ขอบเขตต่ำสุด
- (ข) ค่าต่ำกว่าขอบเขตต่ำสุด
- (ค) ค่าที่ขอบเขตสูงสุด
- (ง) ค่าสูงกว่าขอบเขตสูงสุด

กรณีที่สามารถกำหนดค่าพารามิเตอร์ที่ขัดกับขีดจำกัดความสามารถทางกายภาพของเครื่องตัวจริงได้ ต้องทดสอบค่าดังกล่าวด้วย

ค่านอกขอบเขตให้กำหนดตามข้อ ค.๑.๔

ให้ตรวจสอบว่าค่าที่ขอบเขตต่ำสุดและขอบเขตสูงสุดสามารถบันทึกหรือบังคับใช้ได้ตามที่กำหนด และค่าต่ำกว่าขอบเขตต่ำสุด ค่าสูงกว่าขอบเขตสูงสุด หรือค่าที่ขัดกับขีดจำกัดความสามารถทางกายภาพของเครื่องตัวจริงถูกปฏิเสธ ไม่ถูกบันทึกหรือบังคับใช้ และค่าปลอดภัยที่มีผลอยู่ก่อนการทดสอบยังคงอยู่

ค.๒.๖ การทดสอบความเป็นอิสระจากระบบภายนอก

การทดสอบความเป็นอิสระจากระบบภายนอก ต้องดำเนินการกับการเชื่อมต่อสื่อสารภายนอก บริการหรือระบบประมวลผลภายนอกแต่ละรายการที่เครื่องตัวจริงใช้งานตามปกติและเกี่ยวข้องกับหน้าที่ความปลอดภัยที่ประเมิน

ให้เชื่อมต่อเครื่องตัดวงจรกับระบบหรือบริการภายนอกดังกล่าวตามสภาวะใช้งานปกติ และทวนสอบ
หน้าที่ความปลอดภัยและหน้าที่ป้องกันพื้นฐานที่เกี่ยวข้องเพื่อใช้เป็นค่าฐาน

การทดสอบต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) กรณีที่เครื่องตัดวงจรมีหน้าที่สื่อสาร หน้าที่อัจฉริยะ หรือหน้าที่อื่นที่ไม่เกี่ยวข้องกับความ
ปลอดภัยและอาจมีผลต่อหน้าที่ความปลอดภัย ให้ใช้งานหน้าที่ดังกล่าวตามสภาวะใช้งานปกติ
ในขณะที่กระตุ้นหน้าที่ความปลอดภัยที่เกี่ยวข้อง
- (ข) ทำให้การเชื่อมต่อสื่อสารภายนอก บริการ หรือระบบประมวลผลภายนอกแต่ละรายการไม่
พร้อมใช้งาน แล้วกระตุ้นหน้าที่ความปลอดภัยและหน้าที่ป้องกันพื้นฐานที่เกี่ยวข้อง
- (ค) คั่นการเชื่อมต่อสื่อสารภายนอก บริการ หรือระบบประมวลผลภายนอกแต่ละรายการสู่สภาวะ
พร้อมใช้งานภายหลังการทดสอบตาม (ข)

ระหว่างการทดสอบตาม (ก) ให้ตรวจสอบว่าหน้าที่สื่อสาร หน้าที่อัจฉริยะ หรือหน้าที่อื่นที่ไม่เกี่ยวข้อง
กับความปลอดภัยไม่รบกวน หน่วงรั้ง หรือทำให้ความสามารถของหน้าที่ความปลอดภัยลดลงเกินเกณฑ์
ที่กำหนด

ระหว่างการทดสอบตาม (ข) ให้ตรวจสอบว่าหน้าที่ความปลอดภัยยังคงตอบสนองและบรรลุผลภายใน
ระยะเวลาที่กำหนดตามข้อกำหนดความต้องการด้านความปลอดภัย และหน้าที่ป้องกันพื้นฐานยังคง
ตอบสนองได้ตามข้อกำหนด

ภายหลังการคั่นการเชื่อมต่อสื่อสารภายนอก บริการ หรือระบบประมวลผลภายนอกสู่สภาวะพร้อมใช้
งาน ให้ตรวจสอบว่าไม่เกิดการต่อวงจร การเปลี่ยนสถานะ การเปลี่ยนแปลงพารามิเตอร์ด้านความ
ปลอดภัย หรือการทำงานที่ไม่ปลอดภัยโดยไม่ตั้งใจ

ค.๒.๗ การทดสอบการตรวจสอบ การทวนสอบ และการบำรุงรักษา

การทดสอบการตรวจสอบ การทวนสอบ และการบำรุงรักษา ต้องดำเนินการกับวิธีที่เครื่องตัดวงจร
รองรับให้ดำเนินการในขณะที่ติดตั้งใช้งานและเกี่ยวข้องกับหน้าที่ความปลอดภัยหรือส่วนที่จำเป็นต่อการ
ปฏิบัติหน้าที่ความปลอดภัย

ก่อนดำเนินกิจกรรม ให้ทวนสอบหน้าที่ความปลอดภัยที่อาจได้รับผลกระทบเพื่อใช้เป็นค่าฐาน

การทดสอบต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) ดำเนินการตรวจสอบ การทวนสอบ หรือการบำรุงรักษาตามวิธีที่ผู้ทำกำหนด
- (ข) ระหว่างการดำเนินกิจกรรม ให้กระตุ้นหน้าที่ความปลอดภัยที่อาจได้รับผลกระทบ และตรวจ
สอบว่าหน้าที่ดังกล่าวยังคงปฏิบัติงานได้ตามข้อกำหนด

- (ค) กรณีที่เครื่องตัดวงจรไม่สามารถรักษาหน้าที่ความปลอดภัยที่จำเป็นไว้ได้ ให้ตรวจสอบว่าเครื่องตัดวงจรเข้าสู่สภาวะปลอดภัยตามที่กำหนด
- (ง) ภายหลังเสร็จสิ้นกิจกรรม ให้ทวนสอบหน้าที่ความปลอดภัยที่อาจได้รับผลกระทบซ้ำ และตรวจสอบว่าหน้าที่ดังกล่าวยังคงเป็นไปตามข้อกำหนด

ให้ตรวจสอบการแสดงผลสถานะ การแจ้งเตือน และข้อมูลบันทึกที่ผู้ทำกำหนดให้เกิดขึ้นจากกิจกรรมหรือผลการตรวจสอบดังกล่าว

ค.๒.๘ การทดสอบชิ้นส่วนทดแทน

การทดสอบชิ้นส่วนทดแทน ต้องดำเนินการกับชิ้นส่วนหรือมอดูลทดแทนที่ผู้ทำอนุญาตและอาจมีผลต่อหน้าที่ความปลอดภัย ก่อนเปลี่ยนชิ้นส่วนหรือมอดูล ให้ทวนสอบหน้าที่ความปลอดภัยที่อาจได้รับผลกระทบเพื่อใช้เป็นค่าฐาน

การทดสอบต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) เปลี่ยนชิ้นส่วนหรือมอดูลด้วยชิ้นส่วนหรือมอดูลทดแทนที่ผู้ทำอนุญาตตามวิธีที่ผู้ทำกำหนด แล้วตรวจสอบการระบุหรือข้อมูลที่ใช้อยืนยันความเข้ากันได้
- (ข) กรณีที่ชิ้นส่วนทดแทนเป็นมอดูลควบคุมที่มีซอฟต์แวร์หรือเฟิร์มแวร์ติดตั้งอยู่ภายใน ให้ตรวจสอบความเข้ากันได้ของรุ่นซอฟต์แวร์หรือเฟิร์มแวร์ก่อนการเปิดใช้งาน
- (ค) กรณีที่สามารถติดตั้งชิ้นส่วน มอดูล หรือรุ่นซอฟต์แวร์หรือเฟิร์มแวร์ที่ไม่เข้ากันได้โดยใช้วิธีการเปลี่ยนหรือบำรุงรักษาที่เครื่องตัดวงจรรองรับ ให้ทดสอบกรณีดังกล่าว และตรวจสอบว่าเครื่องตัดวงจรตรวจพบหรือจัดการความไม่เข้ากันก่อนการเปิดใช้งานหรือก่อนที่จะทำให้เกิดการทำงานที่ไม่ปลอดภัย

ภายหลังการเปลี่ยนชิ้นส่วนหรือมอดูลที่ผู้ทำอนุญาต ให้ทวนสอบหน้าที่ความปลอดภัยและเกณฑ์สมรรถนะที่ได้รับผลกระทบ และตรวจสอบว่าหน้าที่ความปลอดภัยและเกณฑ์สมรรถนะดังกล่าวยังคงเป็นไปตามข้อกำหนด

ค.๒.๙ การทดสอบการบันทึกกิจกรรมและการสอบกลับ

การทดสอบการบันทึกกิจกรรมและการสอบกลับ ต้องดำเนินการกับกิจกรรมตามข้อ ๘.๒.๑ (ค) และ (จ) ที่เครื่องตัดวงจรรองรับและกำหนดให้มีการบันทึก

การทดสอบต้องครอบคลุมอย่างน้อยกิจกรรมดังต่อไปนี้ที่เครื่องตัดวงจรรองรับ

- (ก) การบำรุงรักษา

(ข) การปรับตั้งหรือเปลี่ยนแปลงพารามิเตอร์ด้านความปลอดภัย

(ค) การเปลี่ยนแปลงซอฟต์แวร์หรือเฟิร์มแวร์ที่มีผลต่อหน้าที่ความปลอดภัย

ภายหลังแต่ละกิจกรรม ให้เรียกข้อมูลบันทึกตามวิธีที่ผู้ทำกำหนด และตรวจสอบว่าข้อมูลบันทึกสามารถ
สอบกลับไปยังกิจกรรมหรือการเปลี่ยนแปลงที่ดำเนินการได้ และมีข้อมูลอย่างน้อยเกี่ยวกับเหตุการณ์
หรือการเปลี่ยนแปลง วันเวลา รุ่นซอฟต์แวร์หรือเฟิร์มแวร์หรือการกำหนดค่าที่เกี่ยวข้อง และผลการทวน
สอบความถูกต้องสมบูรณ์เมื่อข้อกำหนดกำหนดให้มีข้อมูลดังกล่าว

ค.๒.๑๐ การทดสอบเครื่องมือซ่อมบำรุง

การทดสอบเครื่องมือซ่อมบำรุง ต้องดำเนินการกับเครื่องมือ อุปกรณ์ทดสอบ หรือซอฟต์แวร์ประยุกต์
ภายนอกแต่ละชนิดที่ผู้ทำกำหนดให้ใช้และสามารถเปลี่ยนแปลงพารามิเตอร์ การกำหนดค่า ซอฟต์แวร์
หรือเฟิร์มแวร์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัย

ให้เชื่อมต่อเครื่องมือซ่อมบำรุงกับเครื่องต้นวงจรตามวิธีที่ผู้ทำกำหนดและดำเนินการทดสอบ การ
ทดสอบต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

(ก) เข้าถึงและดำเนินการด้วยสิทธิ์ที่ถูกต้อง และตรวจสอบว่าสามารถดำเนินการได้เฉพาะภายใน
สิทธิ์ที่กำหนด

(ข) พยายามเข้าถึงหรือเปลี่ยนแปลงพารามิเตอร์ การกำหนดค่า ซอฟต์แวร์หรือเฟิร์มแวร์โดยไม่มี
สิทธิ์ที่กำหนด และตรวจสอบว่าไม่สามารถดำเนินการหรือทำให้การเปลี่ยนแปลงมีผลได้

(ค) ขัดจังหวะการสื่อสารระหว่างการเปลี่ยนพารามิเตอร์หรือการกำหนดค่า แล้วคืนการสื่อสาร และ
ตรวจสอบว่าเครื่องต้นวงจรคงการทำงานตามค่าพารามิเตอร์และการกำหนดค่าที่ผ่านการทวน
สอบและมีผลใช้งานอยู่ก่อนเริ่มการเปลี่ยนแปลงนั้น หรือเข้าสู่สภาวะปลอดภัยตามที่กำหนด

ค.๓ การทดสอบเพิ่มเติมกรณีหลักฐานไม่เพียงพอ

กรณีที่ผลการพิจารณาหลักฐานตามภาคผนวก ข. หรือผลการทดสอบตามภาคผนวกนี้มีความไม่ครบถ้วน
ความไม่สอดคล้อง ความไม่ชัดเจน หรือมีข้อมูลไม่เพียงพอสำหรับพิจารณาความเป็นไปตามข้อกำหนด อาจ
ดำเนินการทดสอบเพิ่มเติมเฉพาะเท่าที่จำเป็นเพื่อให้ได้ข้อมูลสำหรับประเด็นที่ยังไม่สามารถพิจารณาได้

ก่อนดำเนินการทดสอบเพิ่มเติม ต้องระบุข้อกำหนดที่ประเมิน ประเด็นที่ข้อมูลยังไม่เพียงพอ วัตถุประสงค์
ของการทดสอบเพิ่มเติม และข้อมูลที่จำเป็นต่อการพิจารณาประเด็นดังกล่าว และภายหลังการทดสอบให้
บันทึกเหตุผลในการทดสอบเพิ่มเติม วิธีการทดสอบ การกำหนดค่า สภาวะทดสอบ และผลที่ได้ไว้ในรายงาน
ผลการทดสอบ

กรณีทดสอบเพิ่มเติมให้กำหนดตามข้อ ค.๑.๑ โดยวิธีการทดสอบให้ใช้วิธีที่กำหนดในมาตรฐานที่เกี่ยวข้อง วิธีที่ผู้ใช้ในการทวนสอบ หรือหลักการทดสอบที่กำหนดในข้อ ค.๒ ตามที่เหมาะสม สภาวะทดสอบ การกำหนดค่าของเครื่องวัดจริง และเกณฑ์การยอมรับต้องสัมพันธ์โดยตรงกับข้อกำหนดและประเด็นที่ต้องตรวจสอบ และต้องกำหนดเกณฑ์การยอมรับก่อนดำเนินการทดสอบ

การทดสอบเพิ่มเติมต้องไม่ใช่เพื่อเปลี่ยนแปลงข้อกำหนดหรือเกณฑ์การยอมรับที่กำหนดไว้ในมาตรฐานนี้

ภาคผนวก ง.

แนวทางการตรวจ การทดสอบ และการบำรุงรักษาเครื่องตัดวงจร

(ข้อแนะนำ)

(ข้อ ๘)

ง.๑ ทัวไป

ผู้ทำควรถูกกำหนดกระบวนการตรวจ การทดสอบ การบำรุงรักษา และการจัดการการเปลี่ยนแปลงที่เกี่ยวข้องกับหน้าที่ความปลอดภัยตลอดวัฏจักรชีวิตด้านความปลอดภัยของเครื่องตัดวงจร และควรจัดให้มีหลักฐานที่สามารถสอบกลับการดำเนินการดังกล่าวได้

ง.๒ การจัดการการเปลี่ยนแปลงซอฟต์แวร์หรือเฟิร์มแวร์

เมื่อมีการเปลี่ยนแปลงซอฟต์แวร์หรือเฟิร์มแวร์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัย ผู้ทำควรประเมินผลกระทบของการเปลี่ยนแปลง กำหนดขอบเขตการทวนสอบหรือการทดสอบซ้ำในส่วนที่ได้รับผลกระทบ และบันทึกการซอฟต์แวร์หรือเฟิร์มแวร์ การกำหนดค่าที่เกี่ยวข้อง ความสัมพันธ์กับการกำหนดค่าฐานอ้างอิงเริ่มต้น และผลการทวนสอบ

กรณีที่มีการเปลี่ยนแปลงดังกล่าวมีผลต่อวิธีใช้งาน การบำรุงรักษา หรือข้อจำกัดด้านความปลอดภัย ผู้ทำควรปรับปรุงข้อมูลที่เกี่ยวข้องให้สอดคล้องกับการเปลี่ยนแปลงนั้น

ง.๓ การบำรุงรักษาและการตรวจสอบตามวาระ

ผู้ทำควรถูกกำหนดวิธีการและช่วงเวลาสำหรับการตรวจสอบหรือทวนสอบความพร้อมทำงานของส่วนที่เกี่ยวข้องกับหน้าที่ความปลอดภัย โดยพิจารณาจากผลการวิเคราะห์อันตราย ความล้มเหลว การเสื่อมสภาพ อายุการใช้งาน จำนวนครั้งการทริป หรือจำนวนครั้งการเปิดและปิดวงจร ตามที่เกี่ยวข้อง

ภายหลังการตรวจสอบหรือการบำรุงรักษา ผู้ทำควรถูกกำหนดวิธีการทวนสอบหน้าที่ความปลอดภัยและส่วนที่ได้รับผลกระทบ เพื่อยืนยันความพร้อมทำงานก่อนนำเครื่องตัดวงจรกลับมาใช้งาน

กรณีที่เครื่องตัดวงจรต้องถูกถอดออกจากระบบเพื่อการตรวจสอบหรือการบำรุงรักษา ผู้ทำควรถูกกำหนดวิธีการที่เหมาะสมสำหรับการแยกเครื่องตัดวงจรออกจากระบบและการนำกลับมาใช้งาน

ง.๔ การจัดการชิ้นส่วนทดแทน

ผู้ทำควรถูกกำหนดชิ้นส่วนหรือมอดูลทดแทนที่อนุญาตให้ใช้ วิธีการตรวจสอบความเข้ากันได้ และขอบเขตการทวนสอบหรือการทดสอบซ้ำของหน้าที่ความปลอดภัยและเกณฑ์สมรรถนะที่อาจได้รับผลกระทบจากการเปลี่ยนชิ้นส่วนหรือมอดูล

ง.๕ การบันทึกหลักฐานและการสอบกลับ

ผู้ทำควรกำหนดให้มีการบันทึกข้อมูลการบำรุงรักษา การตรวจสอบหรือทวนสอบตามวาระ การเปลี่ยนชิ้นส่วนหรือมอดูล และการเปลี่ยนแปลงซอฟต์แวร์หรือเฟิร์มแวร์ที่เกี่ยวข้องกับหน้าที่ความปลอดภัย โดยข้อมูลบันทึกควรสามารถระบุเหตุการณ์หรือกิจกรรม วันและเวลา รุ่นซอฟต์แวร์หรือเฟิร์มแวร์หรือการกำหนดค่าที่เกี่ยวข้อง และผลการทวนสอบตามที่เกี่ยวข้อง

ง.๖ เครื่องมือซ่อมบำรุง

ผู้ทำควรกำหนดเครื่องมือ อุปกรณ์ทดสอบ หรือซอฟต์แวร์ประยุกต์ภายนอกที่ใช้สำหรับการตรวจ การทดสอบ หรือการบำรุงรักษา รวมถึงวิธีการเชื่อมต่อ สิทธิการเข้าถึง เงื่อนไขความเข้ากันได้ และแนวทางการดำเนินการเมื่อการสื่อสารกับเครื่องตัวจริงขัดข้องหรือขาดหายในระหว่างการปรับตั้งหรือเปลี่ยนแปลงพารามิเตอร์หรือการกำหนดค่าที่เกี่ยวข้องกับหน้าที่ความปลอดภัย

ภาคผนวก จ.

ตัวอย่างรายงานผลการทดสอบ

(ข้อแนะนำ)

(ข้อ ๙)

	ชื่อและที่อยู่ของห้องปฏิบัติการทดสอบ 	
หมายเลขรายงาน		
หมายเลขตัวอย่างทดสอบ		
ชื่อและที่อยู่ของผู้ขอรับบริการ		
มาตรฐาน/วิธีการทดสอบ		
วันที่รับตัวอย่างทดสอบ		
วันที่ดำเนินการทดสอบ		
ผู้ทดสอบ	ผู้ทบทวน	ผู้อนุมัติ
.....		
(.....)	(.....)	(.....)
วันที่/...../.....	วันที่/...../.....	วันที่/...../.....

รายละเอียดของตัวอย่างทดสอบ

ข้อมูลการระบุตัวตนของผลิตภัณฑ์ (product identification)	
ชื่อตราสินค้า (brand)	
ชื่อรุ่น (model)	
หมายเลขประจำตัวเครื่อง (serial number)	
รูปถ่ายผลิตภัณฑ์ที่แสดงส่วนประกอบภายนอกและป้ายชื่อ (Nameplate)	
ข้อมูลชุดคำสั่งและรุ่นของอุปกรณ์ (software and hardware versioning)	
รุ่นของฮาร์ดแวร์ (hardware version/revision)	
รุ่นของซอฟต์แวร์หรือเฟิร์มแวร์ (software/firmware version)	
ค่าตรวจสอบความถูกต้องสมบูรณ์ของ ซอฟต์แวร์หรือเฟิร์มแวร์ (เช่น checksum) (integrity verification value)	
พิกัดและคุณลักษณะทางเทคนิค (technical characteristics and ratings)	
แรงดันไฟฟ้าที่กำหนด (rated voltage)	
ความถี่ที่กำหนด (rated frequency)	

พิกัดและคุณลักษณะทางเทคนิค (technical characteristics and ratings) (ต่อ)	
กระแสไฟฟ้าที่กำหนด (rated current)	
จำนวนขั้ว (number of poles)	
พิกัดการทนกระแสลัดวงจรสูงสุด (rated short-circuit capacity)	
พิกัดการทริป (trip threshold)	
อัตราส่วนการคืนตัว (reset ratio)	
เวลาหน่วงการตัด (trip delay time)	
ระดับบูรณาการความปลอดภัยที่กำหนดสำหรับ หน้าที่ความปลอดภัยที่เกี่ยวข้อง (ถ้ามี)	
รายการส่วนประกอบวิกฤต (list of critical components)	
หน่วยประมวลผลหลัก (main MCU)	
อุปกรณ์ตรวจวัด (current/voltage sensors)	
กลไกการทริป (trip mechanism/actuator)	

พารามิเตอร์การทดสอบและการกำหนดค่าของตัวอย่างทดสอบ

พารามิเตอร์ด้านความปลอดภัยและการกำหนดค่าอื่นที่มีผลต่อผลการทดสอบ

สภาพแวดล้อมและสิ่งอำนวยความสะดวกที่ใช้ในการทดสอบ

สรุปผลการประเมินความเป็นไปตามข้อกำหนด

ข้อกำหนด	ข้อย่อ/วิธีการประเมิน	ผลการประเมิน	หมายเหตุ
๑. ข้อกำหนดสมรรถนะด้านความปลอดภัย			
พึงสามารถในการรองรับ	ตามข้อ ๕.๑	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
ความปลอดภัยสำหรับหน้าที่พื้นฐาน	ตามข้อ ๕.๒	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
หน้าที่อื่น ๆ	ตามข้อ ๕.๓	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
๒. ข้อกำหนดด้านความปลอดภัยเชิงหน้าที่			
ทั่วไป	ตามข้อ ๖.๑	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
การตรวจวินิจฉัยและการตอบสนองต่อความผิดปกติของระบบควบคุมอิเล็กทรอนิกส์แบบโปรแกรมได้	ตามข้อ ๖.๒	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
การตรวจสอบความผิดปกติระดับซอฟต์แวร์และการประมวลผลเชิงตรรกะ	ตามข้อ ๖.๓	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
การทดสอบความทนทานต่อสภาวะแวดล้อม	ตามข้อ ๖.๔	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	

ข้อกำหนด	ข้อย่อ/วิธีการประเมิน	ผลการประเมิน	หมายเหตุ
๓. ข้อกำหนดด้านความมั่นคงปลอดภัย			
ความมั่นคงปลอดภัยทางไซเบอร์	ตามข้อ ๗.๑	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
๔. ข้อกำหนดด้านการคงไว้ซึ่งความปลอดภัยเชิงหน้าที่			
ทั่วไป	ตามข้อ ๘.๑	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
ความถูกต้องสมบูรณ์ของข้อมูลและการบันทึกเหตุการณ์	ตามข้อ ๘.๒	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
การจำกัดการปรับตั้งค่าที่ไม่ปลอดภัย	ตามข้อ ๘.๓	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
ความเป็นอิสระในการปฏิบัติงานของเครื่องตัดวงจร	ตามข้อ ๘.๔	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
การปรับปรุงซอฟต์แวร์หรือเฟิร์มแวร์	ตามข้อ ๘.๕	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
การเปลี่ยนชิ้นส่วนหรือมอดูล	ตามข้อ ๘.๖	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
การตรวจสอบ การทวนสอบ และการบำรุงรักษา	ตามข้อ ๘.๗	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	
ส่วนต่อประสานและเครื่องมือซ่อมบำรุง	ตามข้อ ๘.๘	☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง	

รายละเอียดผลการประเมินตามข้อกำหนด

ข้อกำหนด/ข้อย่อ:

วิธีการประเมิน: ☐ พิจารณาหลักฐาน ☐ ทดสอบ ☐ ทั้งสองวิธี

ผลการพิจารณาหลักฐาน:

.....

.....

.....

สรุปผลการทดสอบ (ถ้ามี):

.....

.....

.....

ผลการประเมิน: ☐ ผ่าน ☐ ไม่ผ่าน ☐ ไม่เกี่ยวข้อง

หลักฐานอ้างอิง:

.....

.....

.....

วิธีทดสอบด้านความปลอดภัยเชิงหน้าที่:

.....

.....

.....

รายละเอียดผลการทดสอบรายกรณี

กรณีทดสอบที่

รหัสกรณีทดสอบ:

ข้อกำหนดที่ประเมิน:

วิธีการทดสอบ:

.....

การกำหนดค่าที่ใช้:

.....

สถานะทดสอบ:

.....

.....

.....

เกณฑ์การยอมรับ:

.....

.....

.....

ผลที่ได้:

.....

.....

.....

ผลการทดสอบ: ☐ ผ่าน ☐ ไม่ผ่าน

หลักฐานอ้างอิง:

.....

.....

.....

กรณีทดสอบที่

รหัสกรณีทดสอบ:

ข้อกำหนดที่ประเมิน:

วิธีการทดสอบ:

.....

การกำหนดค่าที่ใช้:

.....

สถานะทดสอบ:

.....

.....

.....

เกณฑ์การยอมรับ:

.....

.....

.....

ผลที่ได้:

.....

.....

.....

ผลการทดสอบ: ☐ ผ่าน ☐ ไม่ผ่าน

หลักฐานอ้างอิง:

.....

.....

.....

รายละเอียดการดำเนินการเพิ่มเติม (ถ้ามี)

ประเด็นที่ต้องประเมินเพิ่มเติม:

.....

เหตุผล:

.....

.....

วิธีดำเนินการ:

.....

.....

ผลที่ได้:

.....

.....

หลักฐานอ้างอิง:

.....

.....

.....
