กรมการขนส่งทางราง
Department of Rail Transport

มขร. – SC – 005 -2567
มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติ ด้านระบบอาณัติสัญญาณ
(Automated People Mover Standard: Signaling system part)

กองมาตรฐานความปลอดภัยและบำรุงทาง

514/1 Lan Luang Road, Dusit, Bangkok, Thailand 10300
http://www.drt.go.th/
Facebook/DRT.OfficialFanpage

รายนามคณะกรรมการจัดทำมาตรฐานการขนส่งทางราง

คณะกรรมการ

๑.	นายพิเชฐ คุณาธรรมรักษ์ กรมการขนส่งทางราง	ประธานกรรมการ
๒.	นายอธิภู จิตรานุเคราะห์ กรมการขนส่งทางราง	รองประธานกรรมการ
๓.	นายชัยวัฒน์ สังขภาคย์ สำนักงานนโยบายและแผนการขนส่งและจราจร	กรรมการ
๔.	นายอภิชาติ พันธ์สุโต การรถไฟแห่งประเทศไทย	กรรมการ
๕.	นายสุพพัต พิพัฒนกุล การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย	กรรมการ
๖.	นายอานุภาพ เกียรติกำจร บริษัท รถไฟฟ้า ร.ฟ.ท. จำกัด	กรรมการ
๗.	นางสลักษณ์ พิสุทธิพัทธยา สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม	กรรมการ
๘.	นายอาณัติ หาทรัพย์ สถาบันวิจัยวิทยาศาสตร์และเทคโนโลยีแห่งประเทศไทย	กรรมการ
๙.	นายสุธี โอฬารฤทธินันท์ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ	กรรมการ
๑๐.	นายกิตติพงษ์ ชะเอมเทศ สถาบันมาตรวิทยาแห่งชาติ	กรรมการ
๑๑.	นายบัณฑิต ประดับสุข สมาคมสถาปนิกสยาม ในพระบรมราชูปถัมภ์	กรรมการ
๑๒.	นายทินกฤต สุขสงวน บริษัท ระบบขนส่งมวลชนกรุงเทพ จำกัด (มหาชน)	กรรมการ
๑๓.	นายพรศักดิ์ ครุฑกุล บริษัท ทางด่วนและรถไฟฟ้ากรุงเทพ จำกัด (มหาชน)	กรรมการ
๑๔.	นายทยากร จันทรางศุ กรมการขนส่งทางราง	กรรมการ และเลขานุการ
๑๕.	นางสาวอนาอีส อารีย์ กรมการขนส่งทางราง	กรรมการ และผู้ช่วยเลขานุการ

****

รายนามคณะอนุกรรมการจัดทำมาตรฐานด้านไฟฟ้าและอาณัติสัญญาณของระบบราง

คณะอนุกรรมการ

๑.	นายอธิภู จิตรานุเคราะห์ กรมการขนส่งทางราง	ประธานอนุกรรมการ
๒.	นายทยากร จันทรางศุ กรมการขนส่งทางราง	รองประธานอนุกรรมการ
๓.	นายศัลยวิทย์ อภิชาตะพงศ์ การรถไฟแห่งประเทศไทย	อนุกรรมการ
๔.	นายนิธินันต์ วิทูรแก้วศิริ การรถไฟฟ้าขนส่งมวลชนแห่งประเทศไทย	อนุกรรมการ
๕.	นายธนา ภู่เผือกรัตน์ บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)	อนุกรรมการ
๖.	นายสฤษฏ์โรจ จันทร์เพิ่มพูนผล สถาบันวิจัยและพัฒนาเทคโนโลยีระบบราง (องค์การมหาชน)	อนุกรรมการ
๗.	นางสาวนีรนุช อารีราชการัณย์ บริษัท รถไฟฟ้า ร.ฟ.ท. จำกัด	อนุกรรมการ
๘.	นายหลักฐาน ทองนพคุณ บริษัท ทางด่วนและรถไฟฟ้ากรุงเทพ จำกัด (มหาชน)	อนุกรรมการ
๙.	นายปิยชัย ชูเอม บริษัท ระบบขนส่งมวลชนกรุงเทพ จำกัด (มหาชน)	อนุกรรมการ
๑๐.	นายเอนก มีมูซอ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ	อนุกรรมการ
๑๑.	นายเอนก วุฒยวนิข การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย	อนุกรรมการ
๑๒.	นายปิยะชัย สุขปลั่ง การไฟฟ้านครหลวง	อนุกรรมการ
๑๓.	นายนวพงศ์ นุตาดี การไฟฟ้าส่วนภูมิภาค	อนุกรรมการ
๑๔.	นายพลากร กลัดเจริญ กรมการขนส่งทางราง	อนุกรรมการ และเลขานุการ
๑๕.	นางสาวอนาอีส อารีย์ กรมการขนส่งทางราง	อนุกรรมการ และผู้ช่วยเลขานุการ

****

รายนามคณะทำงานจัดทำมาตรฐานระบบบขนส่งผู้โดยสารอัตโนมัติ
โดย ศูนย์รวมผู้เชี่ยวชาญระบบราง (Thailand Railway Research Network)

คณะทำงาน

๑. นายพรศักดิ์ ศรีสังสิทธิสันติ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

๒. นายชัยยุทธ์ สัมภวะคุปต์
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

๓. นายวัลลภ กิติสาธร
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

๔. นายสมภพ ตลับแก้ว
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

๕. นางสาวปานรวี รุ่งสกุลโรจน์
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

๖. นางสาวพิชยพัชยา ศรีคร้าม
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

****

มขร – SC – 005 – 2567
มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านระบบอาณัติสัญญาณ
(Automated People Mover Standards: Signaling system part)

บทที่ 1
ทั่วไป

1.1 ขอบเขต

มาตรฐานนี้เป็นส่วนหนึ่งของมาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติ (Automated People Mover Standards) ซึ่งถูกแบ่งออกเป็นทั้งหมด 4 มาตรฐาน ได้แก่

(1) มขร. – S – 003 – 2567 มาตรฐานความปลอดภัยทั่วไปของระบบขนส่งผู้โดยสารอัตโนมัติ

(2) มขร. – C – 010 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติโครงสร้างพื้นฐานและงานโยธา

(3) มขร. – R – 007 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านเครื่องกลและตัวรถ

(4) มขร. – SC – 005 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านระบบอาณัติสัญญาณ

โดยที่มาตรฐานนี้มีเนื้อหาประกอบด้วย

บทที่ 1 ทั่วไป

บทที่ 2 ข้อกำหนดความปลอดภัย

บทที่ 3 ความน่าเชื่อถือของระบบ (System Dependability)

บทที่ 4 ระบบควบคุมการเดินรถอัตโนมัติ (Automatic Train Control)

บทที่ 5 การสื่อสารด้วยเสียงและภาพ (audio and vistual communications)

ภาคผนวก ก ข้อกำหนดแผนความปลอดภัยของระบบ

ภาคผนวก ข อุปกรณ์ทางไฟฟ้า

ภาคผนวก ค ข้อแนะนำสำหรับการวัดค่าความพร้อมใช้งาน (service availability)

ภาคผนวก ง แนวทางการประเมินความปลอดภัยอิสระ (Independent Safety Assessment)

1.2 การใช้งานที่มีอยู่

การติดตั้งและโครงการที่มีอยู่ซึ่งอยู่ระหว่างดำเนินการก่อนวันที่มาตรฐานนี้มีผลบังคับใช้ไม่จำเป็นต้องเป็นไปตามข้อกำหนดใหม่หรือที่มีการแก้ไขของมาตรฐานฉบับนี้ ยกเว้นในกรณีที่หน่วยงานที่มีอำนาจตัดสินกำหนดไว้เป็นพิเศษ โดยที่ APM ที่มีอยู่ เมื่อมีการเลิกใช้งานจากระบบเดิมและติดตั้งใหม่ทั้งหมดแล้ว จะต้องจัดประเภทเป็นการติดตั้งใหม่

1.3 การใช้งานใหม่

การติดตั้งระบบขนส่งผู้โดยสารอัตโนมัติใหม่ที่เริ่มต้นหลังจากวันที่มาตรฐานนี้มีผลบังคับใช้จะต้องเป็นไปตามข้อกำหนดใหม่หรือแก้ไขของมาตรฐานฉบับนี้

1.4 มาตรฐานอ้างอิง

เอกสารหรือส่วนต่อไปนี้รวมอยู่ในการอ้างอิงในมาตรฐานนี้

ASCE : Automated People Mover Standards, ANSI/ASCE/T&DI 21-21

ASTM International : Formerly American Society for Testing and Materials

ASTM D635-06 (2006a). Standard Test Method for Rate of Burning and/or Extent and Time of Burning of Plastics in a Horizontal Position

IEEE: Institute of Electrical and Electronic Engineers

IEEE Standard 1474.1-2004 (2004). IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements

IEEE Standard 242-2001 (2001). Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems, Section 1.0, First Principles

IEEE Standard 519-1992 (1992). IEEE Recommended Practices and Requirements for Harmonic Control in Electrical Power Systems

IEEE Standard 142-1991 (ANSI C114.1-1991) (1991). IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems

NACE: National Association of Corrosion Engineers

NACE Standard RP0169-2002 (2002). Control of External Corrosion on Underground or Submerged Metallic Piping Systems

NFPA Publications: National Fire Protection Association

NFPA 72-2002 (2002). National Fire Alarm Code

NFPA 70 (2017). National Electrical Code

NFPA 130 (2017). Fixed Guideway Transit and Passenger Rail Systems

TIA: Telecommunications Industry Association

Wireless Communications Systems:

Performance in Noise and Interference-Limited Situations— Recommended Methods for Technology-Independent Modeling, Simulation, and Verification, Addendum 1, TIA/EIA Telecommunications Systems Bulletin TSB-88-A-1, January 2002

UL: Underwriters Laboratories

UL 813-1993. (1993). Commercial Audio Equipment

1.5 คำนิยาม

ระบบขนส่งผู้โดยสารอัตโนมัติ (Automated People Mover: APM) คือ รูปแบบการขนส่งแบบมีทางวิ่งบังคับพร้อมการทำงานแบบอัตโนมัติเต็มรูปแบบ โดยมียานพาหนะที่ทำงานบนทางที่มีสิทธิพิเศษเฉพาะทาง

ระบบควบคุมการเดินรถอัตโนมัติ (Automatic Train Control: ATC) คือ ระบบควบคุมการเคลื่อนที่ของรถอัตโนมัติ ที่มีการบังคับในเรื่องความปลอดภัย และควบคุมทิศทางการเดินรถไฟฟ้า โดยที่ระบบย่อย ATC ประกอบด้วย ระบบการเดินรถอัตโนมัติ (ATO) ระบบป้องกันเหตุอันตรายของรถอัตโนมัติ (ATP) และระบบติดตามการเดินรถอัตโนมัติ (ATS)

ระบบการเดินรถอัตโนมัติ (Automatic Train Operation: ATO) คือ ระบบย่อยภายในระบบ ATC ที่ทำหน้าที่ เช่น การควบคุมความเร็ว การหยุดตามโปรแกรม การควบคุมเวลาในการเปิดปิดประตู และฟังก์ชันอื่นๆ ที่กำหนดให้กับผู้ควบคุมขบวนรถ

ระบบป้องกันเหตุอันตรายของรถอัตโนมัติ (Automatic Train Protection: ATP) คือ ระบบย่อยภายในระบบ ATC ที่มีการป้องกันเบื้องต้นสำหรับผู้โดยสาร พนักงานและอุปกรณ์จากอันตรายในการปฏิบัติงานภายใต้การควบคุมอัตโนมัติ

ระบบติดตามการเดินรถอัตโนมัติ (Automatic Train Supervision: ATS) คือ ระบบย่อยภายในระบบ ATC ที่ตรวจสอบและจัดการการทำงานโดยรวมของระบบ APM และจัดให้มีการเชื่อมต่อระหว่างระบบและผู้ควบคุมส่วนกลาง (central control operator)

เครือข่ายระบบขนส่งมวลชนอัตโนมัติขนาดเล็ก (Automated Transit Network: ATN) คือ ระบบย่อยของระบบขนส่งผู้โดยสารอัตโนมัติที่ไม่มีสถานีให้บริการเป็นหลัก เดินทางจากจุดหนึ่งไปยังอีกจุดหนึ่ง ซึ่งมีการสับเปลี่ยนที่ไม่ต้องใช้ชิ้นส่วนที่เคลื่อนที่ตามทางรางและมีความจุของขบวนรถที่มีผู้โดยสารน้อยกว่า 25 คน

การเบรกฉุกเฉิน (emergency braking) คือ การเบรกต่อเนื่องจนหยุดสนิท ในอัตราที่ไม่ต่ำกว่าอัตราการรับประกันขั้นต่ำ (guaranteed rate)

ตัวถังรถ (carbody) คือ โครงสร้างตัวรถที่มีห้องโดยสาร

เวลารถหยุดในสถานี (dwell time) คือ เวลาทั้งหมดที่ขบวนรถให้บริการที่สถานี

ป้ายแบบเปลี่ยนแปลงข้อมูลได้ (dynamic sign) คือ ป้ายซึ่งสามารถเปลี่ยนแปลงข้อความได้

ความปลอดภัยในกรณีขัดข้อง (fail-safe) คือ คุณลักษณะหรือองค์ประกอบของระบบเมื่อเกิดการทำงานล้มเหลวแล้วยังอยู่ในสถานะปลอดภัย (Known safe state)

ความล้มเหลว (failure) คือ การทำงานที่ไม่สามารถทำตามหน้าที่ตามที่ต้องการได้

ทางวิ่งบังคับ (guideway) คือ ลู่ทางหรือพื้นผิวในการขับขี่อื่น ๆ รวมถึงโครงสร้างรองรับ ซึ่งรองรับและนำทางทางกายภาพของยานพาหนะขนส่งที่ออกแบบเป็นพิเศษเพื่อการเดินทางบนทางนั้นโดยเฉพาะ

อันตราย (hazard) คือ สภาวะที่มีอยู่หรือที่อาจเกิดขึ้นซึ่งอาจส่งผลให้เกิดอุบัติเหตุได้

ระยะเวลาระหว่างขบวน (headway) คือ การแบ่งเวลาระหว่างขบวนรถสองขบวน ซึ่งทั้งสองขบวนเดินทางในทิศทางเดียวกันบนทางวิ่งบังคับเดียวกัน ซึ่งวัดจากเวลาที่ส่วนหัวของรถขบวนหลักผ่านจุดอ้างอิงที่กำหนด จนถึงเวลาที่ส่วนหัวของรถที่ตามมาผ่านจุดอ้างอิงเดียวกัน

การบังคับสัมพันธ์ (interlock) คือ การจัดเรียงองค์ประกอบในการควบคุมให้เชื่อมโยงถึงกันจนการปฏิบัติงานสำเร็จซึ่งกันและกันตามลำดับที่เหมาะสม

การกระชาก (jerk) คือ อัตราเวลาที่เปลี่ยนแปลงของการเร่งความเร็วหรือการลดความเร็ว

Mean Time Between Hazardous Events (MTBHE) คือ เวลาเฉลี่ยระหว่างเหตุการณ์อันตราย (ตารางที่ 2-1)

สถานีนอกเส้นทาง (offline station) คือ สถานีที่มีชานชาลาการขนถ่ายของที่ตั้งอยู่บริเวณด้านข้างทางผ่าน (through guideway) เพื่อให้รถสามารถเลี่ยงผ่านสถานีได้และหลีกเลี่ยงการรอรถขบวนก่อน ๆ ที่หยุดที่สถานี

ความเร็วเกินกำหนด (overspeed) คือ ความเร็วของขบวนรถที่เกินขีดจำกัดความเร็วที่กำหนดไว้สำหรับจุดที่เกี่ยวข้องบนทางวิ่งบังคับ

การจอด/หยุดรถเกินระยะที่กำหนด (overtravel) คือ การเคลื่อนขบวนรถอย่างต่อเนื่องเกินกว่าจุดหยุดรถ (stopping point) ที่กำหนด

ห้องโดยสาร (passenger compartment) คือ ตัวรถถูกแบ่งออกเป็นพื้นที่ ซึ่งผู้โดยสารไม่สามารถหรือไม่ได้รับอนุญาตให้เคลื่อนย้าย โดยในแต่ละพื้นที่ดังกล่าวจะถูกกำหนดให้เป็นห้องโดยสาร ทั้งนี้ถ้าพื้นที่ไม่ได้แบ่งแยก รถทั้งคันต้องเป็นห้องโดยสาร

คำสั่งที่ได้รับอนุญาต (permissive decision) คือ การให้อนุญาตหรืออำนาจแก่ระบบหรือส่วนหนึ่งของระบบในการเข้าสู่สถานะอื่น ๆ นอกเหนือจากสถานะปลอดภัย (safe state)

ความเสี่ยง (risk) คือ ตัวชี้วัดความรุนแรงและความน่าจะเป็นของการเกิดอุบัติเหตุ

สถานะปลอดภัย (safe state) คือ สถานะของระบบที่ถือว่ายอมรับได้จากกระบวนการแก้ไขความเสี่ยงในหัวข้อที่ 2.1.2

มีความสำคัญต่อความปลอดภัย (safety-critical) คือ การออกแบบบนระบบ ระบบย่อย องค์ประกอบส่วนประกอบ อุปกรณ์ หรือฟังก์ชันที่แสดงว่าการดำเนินการดังกล่าวเป็นสิ่งจำเป็นในการบรรเทาผลกระทบที่ไม่สามารถยอมรับได้และอันตรายที่ไม่พึงประสงค์ตามที่กำหนดไว้ในตาราง 2-1

ระยะห่างปลอดภัย (Separation Assurance Zone (SAZ)) คือ ระยะห่างระหว่างส่วนท้ายของรถขบวนหลักและด้านหน้าของรถขบวนถัดไป ที่มีการรับรองอย่างต่อเนื่องว่ารถขบวนถัดไปสามารถหยุดได้โดยไม่ชนกับรถขบวนหลัก แม้ในกรณีที่เกิดความล้มเหลวกับรถขบวนหลักก็ตาม

ต้อง คือ ข้อกำหนดบังคับในมาตรฐานนี้

ควร คือ คำแนะนำในมาตรฐานนี้

ระบบย่อย (subsystem) คือ ส่วนประกอบย่อยในการทำงานหลักหรือการจัดกลุ่มรายการหรืออุปกรณ์ที่จำเป็นต่อความสมบูรณ์ในการปฏิบัติงานของระบบ

ระบบ (system) ประกอบด้วยผู้คน ขั้นตอน สิ่งอำนวยความสะดวกและอุปกรณ์ที่บูรณาการเพื่อปฏิบัติงานหรือหน้าที่การทำงานภายในสภาพแวดล้อมเฉพาะ

ความน่าเชื่อถือของระบบ (system dependability) คือ ชุดเกณฑ์โดยรวมที่ใช้ในการวัดประสิทธิภาพของระบบปฏิบัติการในแง่ของความน่าเชื่อถือ การบำรุงรักษาและความพร้อมใช้งาน

ความปลอดภัยของระบบ (system safety) คือ การใช้หลักการ เกณฑ์ และเทคนิคทางวิศวกรรมและการจัดการเพื่อเพิ่มประสิทธิภาพความปลอดภัยในทุกด้าน ภายใต้ข้อจำกัดด้านประสิทธิภาพ เวลาและต้นทุนในการปฏิบัติงานตลอดอายุการใช้งานของระบบ

ทางผ่าน (through guideway) คือ ทางวิ่งบังคับหลักที่รวมถึงการผสมและการแยกขบวนรถที่วิ่งผ่านสถานีนอกเส้นทาง สิ่งอำนวยความสะดวกในการบำรุงรักษาหรือที่จัดเก็บ และอื่น ๆ

ขบวนรถ (train) คือ ตัวรถที่ต่อกันตั้งแต่หนึ่งคันขึ้นไป รวมกันเป็นหน่วยปฏิบัติการ

ตัวรถ (vehicle) คือ หน่วยที่เล็กที่สุดที่สามารถทำงานได้โดยลำพัง

ความเร็วเป็นศูนย์ (zero speed) คือ ความเร็วที่ระบุในหัวข้อ 4.1.8 ซึ่งเป็นความเร็วที่ระบบ ATC จะพิจารณาว่าขบวนรถจะหยุด

บทที่ 2
ข้อกำหนดความปลอดภัย

แผนความปลอดภัยของระบบ (system safety program) ในหัวข้อที่ 2.1 ต้องมีการถูกจัดทำขึ้นในระหว่างกระบวนการวางแผน (planning) และการออกแบบ (design) อีกทั้งยังต้องดำเนินการต่อตลอดกระบวนการก่อสร้าง (construction) และให้บริการ (operation) โดยที่แนวทางของระบบความปลอดภัยนี้ต้องคำนึงถึงหลักการสำคัญของการป้องกันอุบัติเหตุด้วยกับการแก้ไขความเสี่ยงที่สอดคล้องกับหัวข้อย่อยที่ 2.1.2 กระบวนการแก้ไขความเสี่ยง (Hazard Resolution Process)

2.1 แผนความปลอดภัยของระบบ (system safety program)

แผนนี้ต้องถูกนำมาปฏิบัติใช้งานเพื่อระบุและแก้ไขความเสี่ยง ซึ่งผู้ประกอบการ (owner) ต้องมีการวางแผนความปลอดภัยของระบบ (System Safety Program Plan: SSPP) เพื่อสนับสนุนการดำเนินการ (implementing) และรวบรวมบันทึก (documenting) ของแผนนี้ โดยที่ SSSP ต้องระบุถึงหน้าที่ความรับผิดชอบของทุกหน่วยงานที่เกี่ยวข้องในการดำเนินการวางแผนความปลอดภัยของระบบ

แผนความปลอดภัยของระบบและ SSSP ต้องเป็นไปตามข้อกำหนดดังนี้

(1) ต้องมีวัตถุประสงค์ เพื่อจัดให้มีความปลอดภัยของผู้โดยสาร พนักงาน สาธารณะชนทั่วไป และอุปกรณ์ต่าง ๆ

(2) ต้องครอบคลุมทุกองค์ประกอบและหน่วยงานภายในระบบขนส่งผู้โดยสารอัตโนมัติ (Automated People Mover: APM)

(3) ต้องระบุบทบาทและความรับผิดชอบในด้านความปลอดภัยของทุกหน่วยงาน รวมถึงต้องมีผู้รับผิดชอบในงานนั้น ๆ (accountability)

(4) ต้องกำหนดบุคคลหนึ่งคน ในการรับผิดชอบระบบความปลอดภัย ซึ่งมีบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนผ่านนโยบายที่เป็นลายลักษณ์อักษร

(5) ต้องมีกระบวนการแก้ไขความเสี่ยง (Hazard Resolution Process) ที่มีขั้นตอนที่จำเป็นในการระบุและแก้ไขความเสี่ยงตลอดวงจรชีวิตของระบบ (system life cycle)

(6) ต้องจัดให้มีผู้ประกอบการและข้อผูกมัดในการบริหาร ในรูปแบบของนโยบายที่นำมาใช้และการจัดสรรทรัพยากร

ทั้งนี้ บุคคลที่ถูกกำหนดให้ดำเนินการวางแผนความปลอดภัยของระบบ ต้องมีหลักฐานที่ชัดเจนในอำนาจหน้าที่ เพื่อให้แน่ใจว่ามีการดำเนินการในระบบดังกล่าว และต้องรายงานโดยตรงต่อผู้บริหารสูงสุด

2.1.1 การวางแผนความปลอดภัยของระบบ (System Safety Program Plan: SSSP)

(1) SSSP ต้องมีการพัฒนาขึ้นในระหว่างกระบวนการวางแผน (planning) และการออกแบบ (design) ของโครงการ APM และต้องดำเนินการต่อตลอดวงจรชีวิตของโครงการ APM

(2) SSSP ต้องเป็นไปตามภาคผนวก ก หัวข้อ ก.1 การวางแผนความปลอดภัยของระบบ (System Safety Program Plan) หรือข้อกำหนดที่เทียบเท่า อีกทั้ง ต้องระบุขอบเขตขั้นต่ำของกิจกรรมในแผนความปลอดภัยของระบบ รวมถึงข้อกำหนดที่ได้ระบุไว้ในหัวข้อ 2.1

2.1.2 กระบวนการแก้ไขความเสี่ยง (Hazard Resolution Process)

กระบวนการแก้ไขความเสี่ยงนี้ต้องเริ่มต้นจากการกำหนดคุณลักษณะทางกายภาพและการทำงานของระบบ APM ที่จะวิเคราะห์ โดยคุณลักษณะเหล่านี้ต้องถูกนำเสนอในรูปแบบขององค์ประกอบหลัก (major elements) ที่ประกอบขึ้นเป็นระบบและสภาพแวดล้อม รวมถึงอุปกรณ์สิ่งอำนวยความสะดวก วิธีการ และบุคคลากร

เทคนิคและขั้นตอนต่าง ๆ ต้องถูกระบุความเสี่ยงที่มีรายละเอียดดังต่อไปนี้

(1) ข้อมูลจากอุบัติเหตุครั้งก่อน หรือประสบการณ์ในการให้บริการ

(2) ข้อคิดเห็นจากผู้เชี่ยวชาญ และสถานการณ์ที่เป็นความเสี่ยง (hazards scenarios)

(3) รายการความเสี่ยงที่อาจเกิดขึ้น

(4) การวิเคราะห์อันตรายครั้งก่อน

(5) เทคนิคการวิเคราะห์อื่น ๆ ตามความเหมาะสม

ความเสี่ยงทั้งหมดต้องถูกประเมินในแง่ของความรุนแรง (severity) หรือผลที่ตามมาของความเสี่ยง และความน่าจะเป็นของเหตุการณ์ที่อาจเกิดขึ้น

การประเมินความเสี่ยง (risk assessment) ในตารางที่ 2-1 ตาม Mean Time Between Hazardous Events (MTBHE) ต้องถูกใช้เป็นพื้นฐานในกระบวนการตัดสินใจ ในการพิจารณาความเสี่ยงของระบบ APM หรือระบบย่อยต่าง ๆ โดยความเสี่ยงต้องถูกกำจัด บรรเทาลง หรือทำให้ยอมรับได้ และต้องได้รับการแก้ไขผ่านกระบวนการออกแบบที่มุ่งเน้นถึงการกำจัดความเสี่ยง ซึ่งกลยุทธ์ในการแก้ไขหรือการบรรเทาที่ใช้ เรียงลำดับความสำคัญ ได้ดังนี้

(1) กำจัดความเสี่ยง

(2) ออกแบบเพื่อควบคุมความเสี่ยง

(3) ใช้อุปกรณ์รักษาความปลอดภัย (safety devices)

(4) ใช้อุปกรณ์แจ้งเตือนเหตุอันตราย (warning devices)

(5) ดำเนินการขั้นตอนพิเศษ

(6) ยอมรับความเสี่ยง

(7) นำระบบหลัก ระบบย่อย หรืออุปกรณ์ออกจากการให้บริการ

กระบวนการนี้ต้องรวมบันทึกฉบับสมบูรณ์ของความเสี่ยงที่ระบุไว้ทั้งหมด การประเมินความเสี่ยง และกิจกรรมการแก้ไขความเสี่ยงใน Hazard Tracking Log ซึ่งประสิทธิภาพในการบรรเทาความเสี่ยงต้องถูกตรวจสอบเพื่อพิจารณาว่าไม่มีความเสี่ยงใหม่เกิดขึ้น อีกทั้ง เมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้นกับระบบ ต้องดำเนินการวิเคราะห์เพื่อระบุและแก้ไขความเสี่ยงใหม่ที่อาจเกิดขึ้น

2.1.2.1 การวิเคราะห์อันตราย (hazard analyses)

(1) การวิเคราะห์อันตรายต้องใช้เพื่อประเมินความเสี่ยงหรืออันตรายที่อาจเกิดขึ้นและบันทึกการแก้ไขปัญหาดังกล่าว โดยในขั้นต่ำ การวิเคราะห์ Preliminary Hazard Analysis (PHA) ต้องดำเนินการในโครงการใหม่ของระบบ APM และสำหรับการวิเคราะห์อย่างละเอียดอื่น ๆ รวมถึงการวิเคราะห์ Subsystem Hazard Analysis (SSHA) System Hazard Analysis (SHA) และ Operating and Support Hazard Analysis (O&SHA) ต้องดำเนินการเช่นกันหากเป็นข้อบังคับใน SSSP

(2) การดำเนินการข้างต้นต้องเป็นไปตามภาคผนวก ก หัวข้อ ก.2 (PHA) ก.3 (SSHA) ก.4 (SHA) และ ก.5 (O&SHA) หรือข้อกำหนดอื่นที่เทียบเท่าตามลำดับ ทั้งนี้ ข้อกำหนดความปลอดภัย

และข้อกำหนดต่าง ๆ ที่ถูกระบุจากการวิเคราะห์อันตรายและการตรวจสอบเหล่านั้น ต้องบันทึกจัดทำเป็นเอกสาร

หมายเหตุ การวิเคราะห์ที่เฉพาะเจาะจงมีความจำเป็นในหัวข้ออื่น ๆ ของมาตรฐานฉบับนี้ ซึ่งแสดงอยู่ในตารางที่ 2-2 และอ้างอิงไปยังส่วนที่เกี่ยวข้อง เพื่อสะดวกแก่การวางแผนและตรวจสอบกิจกรรมต่าง ๆ

ตารางที่ 2-1 การประเมินความเสี่ยง (risk assessment)

ความถี่ในการเกิดเหตุ	ความรุนแรง (hazard severity)			
	I - รุนแรงมาก (catastrophic)	II – ร้ายแรง (critical)	III – ไม่รุนแรง (marginal)	IV – เล็กน้อย (negligible)
A - เป็นประจำ	IA	IIA	IIIA	IVA
B - เป็นไปได้มาก	IB	IIB	IIIB	IVB
C – เป็นครั้งคราว	IC	IIC	IIIC	IVC
D - นานครั้ง	ID	IID	IIID	IVD
E - ไม่มีความเป็นไปได้	IE	IIE	IIIE	IVE

IA IIA IIIA IB IIB และ IC ไม่สามารถยอมรับได้ (unacceptable)

ID IIC และ IIIB ไม่เป็นที่ต้องการ (undesirable) เป็นที่อนุญาตโดยมีการตกลงจากหน่วยงานที่มีอำนาจตัดสิน

IE IID IIE IIIC IIID IVA และ IVB ยอมรับได้โดยแจ้งไปยังหน่วยงานที่มีอำนาจตัดสิน

IIIE IVC IVD และ IVE ยอมรับได้ (acceptable)

โดยที่

A – เป็นประจำ คือ มี MTBHE น้อยกว่า 1,000 operating hour

B - เป็นไปได้มาก คือ มี MTBHE เท่ากับหรือมากกว่า 1,000 operating hour แต่น้อยกว่า 100,000 operating hour

C - เป็นครั้งคราว คือ มี MTBHE เท่ากับหรือมากกว่า 100,000 operating hour แต่น้อยกว่า 1,000,000 operating hour

D - นานครั้ง คือ มี MTBHE เท่ากับหรือมากกว่า 1,000,000 operating hour แต่น้อยกว่า 100,000,000 operating hour

E – ไม่มีความเป็นไปได้ คือ มี MTBHE เท่ากับหรือมากกว่า 100,000,000 operating hour

ทั้งนี้ ปริมาณความน่าจะเป็นหรือความถี่ของการเกิดเหตุขององค์ประกอบต่าง ๆ ภายในกระบวนการตรวจสอบความปลอดภัยอาจถูกกำหนดโดยขึ้นอยู่กับแต่ละบุคคล เช่น กำหนดในเชิงคุณภาพ ดังนั้น ต้องระบุการกำหนดปริมาณที่ขึ้นอยู่กับแต่ละบุคคล และอธิบายเหตุผลการประเมินนั้นด้วย

I – รุนแรงมาก คือ การเสียชีวิต ระบบล่ม หรือเกิดความเสียหายต่อสิ่งแวดล้อมอย่างรุนแรง

II – ร้ายแรง คือ การบาดเจ็บสาหัส การเจ็บป่วยขั้นรุนแรงที่เกิดจากการทำงาน หรือความเสียหายส่วนมากของระบบหรือสิ่งแวดล้อม

III – ไม่รุนแรง คือ การบาดเจ็บเล็กน้อย การเจ็บป่วยเล็กน้อยที่เกิดจากการทำงาน หรือความเสียหายส่วนน้อยของระบบหรือสิ่งแวดล้อม

IV – เล็กน้อย คือ น้อยกว่าการบาดเจ็บเล็กน้อย การเจ็บป่วยที่เกิดจากการทำงาน หรือน้อยกว่าความเสียหายส่วนน้อยของระบบหรือสิ่งแวดล้อม

2.2 หลักการความปลอดภัย

หลักการความปลอดภัยต่อไปนี้ต้องถูกตรวจสอบในระบบ APM โดยตารางที่ 2-1 ได้กำหนดความเสี่ยงที่ไม่สามารถยอมรับได้และความเสี่ยงที่ไม่เป็นที่ต้องการไว้แล้ว

(1) เมื่อระบบทำงานหรือให้บริการในสภาวะปกติ ระบบจะต้องไม่มีสภาวะความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) และความเสี่ยงที่ไม่เป็นที่ต้องการ (undesirable)

(2) การออกแบบระบบต้องมีการดำเนินการในเชิงบวก (positive actions) ตามที่ได้กำหนดไว้เพื่อเริ่มการทำงานหรือทำงานต่อของระบบ

(3) ความปลอดภัยของระบบในสภาวะการทำงานโหมดอัตโนมัติแบบปกติ ต้องไม่ขึ้นกับการกระทำหรือขั้นตอนที่ผู้ปฏิบัติงานใช้

(4) ต้องไม่มีความล้มเหลวใด ๆ ในระบบ (single-point failures) ที่จะทำให้เกิดสภาวะความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) และความเสี่ยงที่ไม่เป็นที่ต้องการ (undesirable)

(5) หากความล้มเหลวครั้งแรกรวมกับความล้มเหลวครั้งที่สอง ทำให้เกิดสภาวะความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) และความเสี่ยงที่ไม่เป็นที่ต้องการ (undesirable) ความล้มเหลวครั้งแรกนั้น ต้องถูกตรวจจับได้และระบบต้องอยู่ในสถานะปลอดภัย (Known safe state) ก่อนที่ความล้มเหลวครั้งที่สองจะเกิดขึ้น

(6) ความผิดพลาดของซอฟต์แวร์ต้องไม่ก่อให้เกิดสภาวะความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) และความเสี่ยงที่ไม่เป็นที่ต้องการ (undesirable)

(7) ความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) ต้องถูกกำจัดหรือถูกควบคุมโดยการออกแบบระบบ เพื่อไม่ให้ความเสี่ยงนั้นถูกประเมินเป็นความเสี่ยงที่ไม่สามารถยอมรับได้อีกต่อไป

(8) การซ่อมบำรุง (maintenance activities) ให้เป็นไปตามความเสี่ยงในตารางที่ 2-1 ต้องถูกกำหนดให้มีบุคคลที่รับผิดชอบในแผนความปลอดภัยของระบบ (system safety program) ตามหัวข้อที่ 2.1 ในช่วงของกระบวนการออกแบบ โดยที่การซ่อมบำรุงนี้ต้องลดความถี่และความซับซ้อนของการปฏิบัติงาน อีกทั้ง คุณสมบัติของบุคลากรที่จำเป็นในการดำเนินการเหล่านี้ต้องถูกระบุไว้ด้วย

2.3 การออกแบบความปลอดภัยในกรณีขัดข้องของระบบ ATC (ATC system fail-safe design)

ทุกองค์ประกอบที่มีความสำคัญต่อความปลอดภัยของระบบ ATC ตามหัวข้อที่ 4 การควบคุมรถอัตโนมัติ (Automatic Train Control) ต้องถูกออกแบบและปฏิบัติใช้ตามหลักการความปลอดภัยในกรณีขัดข้อง (fail-safe) และต้องใช้หนึ่งหรือหลายเทคนิคตามหัวข้อด้านล่างนี้ หรือเทคนิคที่เทียบเท่า เพื่อตรวจจับรูปแบบความล้มเหลวที่อาจเป็นอันตรายและบังคับให้อยู่ในสถานะปลอดภัย (Known safe state) โดยที่หลักการความปลอดภัยในกรณีขัดข้อง ต้องถูกคำนึงจากการออกแบบระบบ เพื่อให้มีคุณลักษณะความล้มเหลวที่ปลอดภัยภายในตัวระบบเอง หรือโดยการออกแบบระบบด้วยกับเทคนิคที่สามารถตรวจสอบได้ ทั้งนี้ ทุก ๆ ระบบหลักหรือระบบย่อยที่มีความสำคัญต่อความปลอดภัย ต้องมีเอกสารวิธีการใช้งานและการพิสูจน์ว่าเป็นไปตามหลักการความปลอดภัยในกรณีขัดข้อง

2.3.1 การออกแบบความปลอดภัยในกรณีขัดข้องภายในตัวระบบเอง

ความปลอดภัยในกรณีขัดข้องภายในตัวระบบเองจะต้องได้รับการออกแบบโดยใช้คุณลักษณะทางกายภาพ ทางเครื่องกล และ/หรือทางไฟฟ้าที่ตรวจสอบได้ ซึ่งผลกระทบจากความล้มเหลวที่เกี่ยวข้องต่อการทำงานทั้งหมดของระบบต้องได้รับการพิจารณา วิเคราะห์ และจัดทำเป็นเอกสารที่ครอบคลุมและมีการวิเคราะห์ผลกระทบ (effects analysis) หรือรูปแบบอื่นเทียบเท่า

2.3.2 ทางเลือกอื่นสำหรับการออกแบบความปลอดภัยในกรณีขัดข้องภายในตัวระบบเอง

การออกแบบระบบการควบคุมจำนวนมากใช้วงจรรวม (integrated circuits) ไมโครโปรเซสเซอร์ (microprocessor) และซอฟต์แวร์เพื่อให้ได้คุณลักษณะการทำงานที่ต้องการ โดยหากการออกแบบที่ไม่ได้มีการแสดงการทำงานภายในของระบบความปลอดภัยในกรณีขัดข้อง ต้องใช้เทคนิคหนึ่งหรือหลายเทคนิคตามหัวข้อที่ 2.3.2.1 ถึง 2.3.2.4 อีกทั้ง ประสิทธิภาพและความครบถ้วนของเทคนิคเหล่านี้จะต้องจัดทำเป็นเอกสารและเป็นส่วนหนึ่งของการตรวจสอบและรับรองของระบบ ตามหัวข้อที่ 2.4 ซึ่งการวัดประสิทธิภาพ

ของเทคนิคต้องมีสามารถตรวจจับความบกพร่องและรับรองได้ว่าเทคนิคนั้นได้รับการติดตั้งตามที่ออกแบบไว้และตามความจำเป็นสำหรับการทำงานของระบบ

ตารางที่ 2-2 ตัวชี้วัดในการวิเคราะห์อันตรายที่จำเป็น

อ้างอิงตามมาตรฐาน ASCE 21	ข้อกำหนดในการวิเคราะห์อันตราย
มขร. – SC – 005 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านระบบอาณัติสัญญาณ หัวข้อ 2.1 แผนความปลอดภัยของระบบ (system safety program)	
2.1.2.1 การวิเคราะห์อันตราย (hazard analyses)	การวิเคราะห์ Preliminary Hazard Analysis (PHA) การวิเคราะห์ Subsystem Hazard Analysis (SSHA) การวิเคราะห์ System Hazard Analysis (SHA) และ การวิเคราะห์ Operting and Support Hazard Analysis (O&SHA)
มขร. – SC – 005 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านระบบอาณัติสัญญาณ 4.1 ฟังก์ชั่นระบบป้องกันเหตุอันตรายของรถอัตโนมัติ (Automatic Train Protection functions)	
4.1.2 การรักษาระยะห่าง	เงื่อนไขการเบรกฉุกเฉินขั้นต่ำ
4.1.2.1 การรักษาระยะห่างสำหรับรถ APM	เงื่อนไขการเบรกฉุกเฉินขั้นต่ำ
4.1.2.2 การรักษาระยะห่างสำหรับ ATN	เงื่อนไขการเบรกฉุกเฉินขั้นต่ำและอัตราการลดความเร็วหัวขบวนรถ
4.1.10 ระบบป้องกันในการควบคุมการเปิดประตู (เมื่อขบวนรถไม่สามารถหยุดได้โดยสมบูรณ์ เพื่อให้ผู้โดยสารที่ขึ้นลง)	อัตราการเร่งความเร็วและการกระชาก (jerk rates) การเปิด-ปิดประตูรถภายในเขตระบบ (designed zone)
4.1.13 การบังคับสัมพันธ์ของระบบขับเคลื่อนและเบรก (Propulsion and Braking Interlocks)	การรีเซ็ตของเบรกฉุกเฉิน เว้นแต่จะใช้ตามหัวข้อที่ 4
4.1.14 การบังคับสัมพันธ์ของทางประแจ (Guideway Switch Interlocks)	การบังคับสัมพันธ์ของทางประแจบนตัวรถ (Onboard guideway switch interlocks)
4.1.15 การทำงานในเขตออฟไลน์ — เงื่อนไขพิเศษ (O&SHA)	จุดเชื่อมต่อระหว่างรถสองคันในเขตหมุนเวียน (circulating zone)
4.1.15 การทำงานในเขตออฟไลน์ — เงื่อนไขพิเศษ	จุดเชื่อมต่อระหว่างรถสองคันในเขตจอดรถ (docking zone)
4.4 ข้อจำกัดในการทำงานแบบใช้คนขับ	การเดินรถแบบใช้คนขับ (manual mode operation)
มขร. – SC – 005 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านระบบอาณัติสัญญาณ 5. การสื่อสารทางเสียงและภาพ (Audio and Visual communication)	ระยะเวลาการทำงานของ UPS สำหรับการสื่อสารทางเสียงและภาพ
5.3.2 สถานี	การเปลี่ยนถ่ายผู้โดยสารเมื่อขบวนรถหยุดไม่สนิท
มขร. – R – 007 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านเครื่องกลและตัวรถ 2. ตัวรถ	

2.4.4.9.2 การชนของขบวนรถกับอุปกรณ์ป้องกันการจอด/หยุดรถเกินระยะที่กำหนด (Vehicle–Overtravel protection device collision)	ความเร็วสูงสุดของจุดสัมผัสที่มีการป้องกันการจอด/หยุดรถเกินระยะที่กำหนด แบบมีคนบังคับ
2.6 การกันสะเทือนและตัวบังคับการวิ่ง (Suspension and Guidance)	ความบกพร่องของความดันลมยาง (pneumatic tire pressure)
2.7.2 การระบายอากาศ (Ventilation)	ระยะเวลาการทำงานของลมจ่าย (fresh air supply)
2.8 ประตู การเข้าถึง และการออก (Doors, Access, and Egress)	การทำงานของทางออกฉุกเฉิน (emergency exit)
2.11.2 ไฟแสงสว่างฉุกเฉิน (Emergency Lighting)	ระยะเวลาการทำงานของพลังงานไฟแสงสว่างฉุกเฉิน
2.12.2.3 ไฟกำลังฉุกเฉิน (Emergency Power)	ระยะเวลาการทำงานของไฟกำลังฉุกเฉินที่ระบบย่อยสำคัญ
มขร. – R – 007 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านเครื่องกลและตัวรถ 3. การขับเคลื่อนและการเบรก (Propulsion and Braking)	
3.3.2 การเบรกฉุกเฉิน (Emergency Braking)	แรงฉุด (traction effort) และระยะเบรก (stopping distance) สำหรับระบบเบรกฉุกเฉินข้างทาง (wayside emergency braking system)
3.4 การออกแบบอุปกรณ์สำหรับระบบขับเคลื่อนและเบรก	การทำงานของระบบขับเคลื่อนและเบรก (PBS)
3.4 การออกแบบอุปกรณ์สำหรับระบบขับเคลื่อนและเบรก	อายุการใช้งานของเบรกแบบใช้แรงเสียดทาน (friction brakes)
3.5 การติดตั้งและการป้องกัน	การเข้าถึงการบำรุงรักษาของอุปกรณ์ระบบขับเคลื่อนและเบรก (PBS) ตามทางวิ่งบังคับ (guideway) หรือในสถานี
3.7 การทดสอบเบรก	รอบการทดสอบระบบเบรก
มขร. – SC – 005 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านระบบอาณัติสัญญาณ ภาคผนวก ข อุปกรณ์ทางไฟฟ้า (Electrical Equipment)	
ข.1.4 การต่อลงดิน (Grounding)	อันตรายทางไฟฟ้า (electrical hazards)
ข.1.4.2 การต่อลงดินสำหรับอุปกรณ์อำนวยความสะดวกและโครงสร้าง	กราวนด์ทางไฟฟ้าขณะการอพยพฉุกเฉิน (emergency evacuation)
ข.2.5 อุปกรณ์จ่ายพลังงานไฟฟ้ากลับคืน (Power Regeneration Equipment)	การจ่ายพลังงานไฟฟ้ากลับคืนไปยังรางนำไฟที่ตัดพลังงานไฟฟ้าออก (deenergized power rail) (ถ้ามี)
ข.2.8 การจ่ายไฟฟ้ากลับคืน (Restoring Power)	การปิดวงจรซ้ำอัตโนมัติ (automatic reclosing) ของอุปกรณ์สำหรับจ่ายกำลังไฟฟ้า (power distribution equipment)
ข.5 Uninterrubtible Power Supply (UPS)	ระยะเวลาการทำงานของ UPS สำหรับระบบ ATP ระบบสื่อสารภาพและเสียง (AV) ระบบเพลิงไหม้ และอุปกรณ์รักษาความปลอดภัย ระบบจ่ายกำลังไฟฟ้าและการควบคุมพลังงานที่สถานีไฟฟ้าย่อย

มขร. – C – 010 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านโครงสร้างพื้นฐานและงานโยธา 2. สถานี (stations)	
2.2 การป้องกันที่ขอบชานชาลา (Platform Edge Protection)	การป้องกันที่ขอบชานชาลา
2.2.3 ระบบตรวจจับการรุกล้ำ (Intrusion Detection System)	คำสั่งเบรกเพื่อเข้าสถานี วิธีการรีเซ็ตระบบตรวจจับและกู้คืนการเดินรถ (restore traffic)
2.5.1 ระบบตรวจจับเพลิงไหม้ (Fire detection)	การตอบสนองของระบบตรวจสอบเพลิงไหม้หรือควัน
2.5.2 การควบคุมเพลิงไหม้ (Fire containment)	การแยกพื้นที่เพลิงไหม้ของสถานี (fire separation)
มขร. – C – 010 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านโครงสร้างพื้นฐานและงานโยธา 3. ทางวิ่งบังคับ (guideways)	
3.2 การป้องกันและตรวจจับการรุกล้ำ	รูปแบบของการป้องกันและตรวจจับการบุกรุก
3.3 การอพยพฉุกเฉินและการเข้าถึง	การเปิดใช้งานประตูรถ (vehicle door release)
3.3.3 ทางวิ่งบังคับยกระดับ (Elevated Guideway)	ทางเลือกอื่นในการอพยพและระยะเวลาในการใช้ทางเดินยกระดับฉุกเฉิน (elevated emergency walkway)
3.8.1 ช่องว่างในการจัดแนวทางวิ่งบังคับ	ระยะห่างสำหรับส่วนประกอบของระบบที่ไม่ใช่โครงสร้าง
3.9 หลักเกณฑ์โครงสร้าง แรงตามยาว (longitudinal force) และแรงจากแผ่นดินไหว (seismic force)	การออกแบบทางวิ่งบังคับสำหรับการรับน้ำหนักที่รุนแรง (severe loads) จากความล้มเหลวต่างๆ
มขร. – S – 003 – 2567 มาตรฐานความปลอดภัยทั่วไปของระบบขนส่งผู้โดยสารอัตโนมัติ 7. กระบวนการตรวจสอบการดำเนินงาน (Operational monitering)	
7.5 การจัดการตั้งค่า (Configuration management)	การเปลี่ยนการออกแบบของชิ้นส่วนที่มีความสำคัญต่อความปลอดภัย (safety-critical items)

2.3.2.1 การตรวจสอบซ้ำ (Checked Redundancy)

การใช้หลักการของ Checked Redundancy นี้ต้องมีอย่างน้อย 2 ระบบในลักษณะคู่ขนานกันและทำหน้าที่เหมือนกัน ซึ่งจะต้องมีวิธีการเปรียบเทียบผลลัพธ์ (output) ของระบบคู่ขนานนั้น หากทั้งสองระบบไม่สอดคล้องกัน ฟังก์ชันที่สำคัญต่อความปลอดภัยที่กำลังทำงานอยู่ ต้องตั้งค่าเริ่มต้น (default) เป็นสถานะปลอดภัย (Known safe state) โดยการออกแบบ Checked Redundancy จะต้องมีการตรวจสอบและมีคุณลักษณะดังต่อไปนี้

(1) กระบวนการตรวจสอบต้องให้แน่ใจว่าไม่มีการแจ้งว่าระบบมีความสอดคล้องกัน เว้นแต่ว่าผลลัพธ์ที่ตรวจสอบซ้ำ (redundance output) จะสอดคล้องกัน ทั้งนี้ หากไม่มีความสอดคล้องกันในขั้นตอนการตรวจสอบต้องส่งผลให้อยู่ในสถานะปลอดภัย (Known safe state)

(2) กระบวนการตรวจสอบต้องมีการเปรียบเทียบกันของผลลัพธ์ที่สำคัญต่อความปลอดภัยกับฟังก์ชันที่สำคัญต่อความปลอดภัยทั้งหมด

(3) ความล้มเหลวใดๆ ที่อาจส่งผลต่อความปลอดภัยของระบบในหน่วยสำรอง (redundance units) ตัวใดตัวหนึ่งต้องส่งผลให้อยู่ในสถานะปลอดภัย (Known safe state)

(4) หน่วยสำรอง (redundance units) ต้องเป็นอิสระจากกัน เพื่อไม่ให้เกิดความผันผวนของสภาพแวดล้อมหรือพลังงานทั่วไปและไม่ให้เกิด errors และ/หรือ faults ที่สามารถก่อให้เกิดความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) และความเสี่ยงที่ไม่เป็นที่ต้องการ (undesirable) ตามตารางที่ 2-1

(5) กระบวนการตรวจสอบจะต้องครอบคลุมถึงฟังก์ชันที่ทดสอบและอัตราต่าง ๆ ในการทดสอบฟังก์ชันนั้น เพื่อให้มั่นใจว่าความน่าจะเป็นของความล้มเหลวหรือความเสียหาย ซึ่งเป็นความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) และความเสี่ยงที่ไม่เป็นที่ต้องการ (undesirable) อยู่ในระดับที่สามารถยอมรับได้ (acceptable level) ตามตารางที่ 2-1

(6) สำหรับหน่วยการทำงานที่ใช้โปรแกรมซอฟต์แวร์ (software-programmed elements) ซอฟต์แวร์นั้นต้องแสดงให้เห็นว่าไม่มีข้อผิดพลาด รวมถึงข้อผิดพลาดใด ๆ ที่เกิดขึ้นระหว่างกระบวนการทำงานร่วมกัน (compilation process) โดยมีการพิสูจน์และมีแนวทางปฏิบัติในการตรวจสอบและรับรอง ตามหัวข้อที่ 2.4

2.3.2.2 N-Version Programming

การใช้หลักการของ N-Version Programming นี้ต้องมีอย่างน้อย 2 ระบบในลักษณะคู่ขนานกันและทำหน้าที่เหมือนกัน โดยที่ในแต่ละระบบต้องมีเอกลักษณ์เฉพาะตัวและถูกเขียนอย่างอิสระจากบุคคลหรือทีมที่แตกต่างกัน ใช้ภาษาและเครื่องมือที่แตกต่างกัน ทั้งนี้ ฮาร์ดแวร์อาจจะเหมือนกันหรือไม่เหมือนกันก็ได้ หรืออาจจะเป็น 2 ระบบที่ถูกติดตั้งโปรแกรมไว้ภายในฮาร์ดแวร์ประมวลผลตัวเดียวกัน (hardware processing unit) อีกทั้ง ต้องมีวิธีการเปรียบเทียบกันของผลลัพธ์ (output) ในระบบที่ถูกติดตั้งโปรแกรมแบบขนานกัน หากทั้งสองระบบไม่สอดคล้องกัน ฟังก์ชันที่มีความสำคัญต่อความปลอดภัยที่กำลังทำงานอยู่จะต้องตั้งค่าเริ่มต้น (default) เป็นสถานะปลอดภัย (Known safe state) โดยการออกแบบจะต้องมีการตรวจสอบและมีคุณลักษณะดังต่อไปนี้

(1) กระบวนการตรวจสอบต้องอยู่ในรูปแบบความปลอดภัยในกรณีขัดข้อง (fail-safe) และจะต้องไม่มีการแจ้งว่าระบบมีความสอดคล้องกัน เว้นแต่ว่าผลลัพธ์ที่ตรวจสอบซ้ำ (redundance output) สอดคล้องกัน ทั้งนี้ หากไม่มีความสอดคล้องกันในขั้นตอนการตรวจสอบต้องส่งผลให้อยู่ในสถานะปลอดภัย (Known safe state)

(2) กระบวนการตรวจสอบต้องมีการเปรียบเทียบกันของผลลัพธ์กับฟังก์ชันที่มีความสำคัญต่อความปลอดภัยทั้งหมด

(3) ความล้มเหลวใดๆ ที่อาจส่งผลต่อความปลอดภัยของระบบในหน่วยสำรอง (redundance units) ตัวใดตัวหนึ่งต้องส่งผลให้อยู่ในสถานะปลอดภัย (Known safe state)

(4) โปรแกรมแบบขนานกันนั้น ต้องเป็นอิสระต่อกัน เพื่อไม่ให้เกิดความผันผวนของสภาพแวดล้อมหรือพลังงานทั่วไปและไม่ให้เกิด errors และ/หรือ faults ที่สามารถก่อให้เกิดความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) และความเสี่ยงที่ไม่เป็นที่ต้องการ (undesirable) ตามตารางที่ 2-1

(5) กระบวนการตรวจสอบจะต้องครอบคลุมถึงฟังก์ชันที่ทดสอบและอัตราต่าง ๆ ในการทดสอบฟังก์ชันนั้น เพื่อให้มั่นใจว่าความน่าจะเป็นของความล้มเหลวหรือการชดเชยความเสียหายมีความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) และความเสี่ยงที่ไม่เป็นที่ต้องการ (undesirable) อยู่ในระดับที่สามารถยอมรับได้ (acceptable level) ตามตารางที่ 2-1

(6) ซอฟต์แวร์ที่ประมวลผลโดยระบบซึ่งถูกติดตั้งโปรแกรมแบบขนานกัน ต้องได้รับการยืนยันแล้วว่าเป็นอิสระต่อกัน

2.3.2.3 การทำงานหลายวิธีและการตรวจสอบตัวเอง (Diversity and Self-Checking)

การใช้หลักการของ Diversity and Self-Checking ต้องกำหนดให้ฟังก์ชันที่สำคัญทั้งหมดมีการทำงานในหลายวิธี โดยใช้ซอฟต์แวร์ที่หลากหลาย และ/หรือช่องทางฮาร์ดแวร์ที่หลากหลาย อีกทั้งฮาร์ดแวร์หลักของระบบต้องถูกทดสอบด้วยตนเองเป็นกิจวัตร (self-checking routine) ทั้งนี้ ผลลัพธ์ที่ได้รับอนุญาต (permissive output) ต้องได้รับอนุญาตก็ต่อเมื่อความสอดคล้องกันจากการทำงานหลายวิธีและการตรวจสอบตัวเอง ไม่พบความล้มเหลวเท่านั้น โดยการออกแบบจะต้องมีการตรวจสอบและมีคุณลักษณะดังต่อไปนี้

(1) กระบวนการตรวจสอบในการทำงานหลายวิธีของระบบต้องอยู่ในรูปแบบความปลอดภัยในกรณีขัดข้อง (fail-safe) และจะต้องไม่มีการแจ้งว่าระบบได้มีคำสั่งอนุญาต (permissive decisions) เว้นแต่ว่าผลลัพธ์ในหลายวิธีนั้น มีความสอดคล้องกัน ทั้งนี้ หากไม่มีความสอดคล้องกันในขั้นตอนการตรวจสอบในการทำงานหลายวิธีและการตรวจสอบตัวเอง ต้องส่งผลให้อยู่ในสถานะปลอดภัย (Known safe state)

(2) การทำงานหลายวิธีและการตรวจสอบตัวเองต้องมีการรับรองผลลัพธ์ของฟังก์ชันทั้งหมดที่มีความสำคัญต่อความปลอดภัย

(3) ความล้มเหลวใดๆ ที่อาจส่งผลต่อความปลอดภัยของระบบต้องส่งผลให้อยู่ในสถานะปลอดภัย (Known safe state)

(4) การทำงานหลายวิธีและการตรวจสอบตัวเองที่มีการตรวจสอบเป็นกิจวัตรต้องครอบคลุมถึงฟังก์ชันที่ทดสอบ และอัตราต่าง ๆ ในการทดสอบฟังก์ชันนั้น เพื่อให้มั่นใจว่าความน่าจะเป็นของความล้มเหลวหรือความเสียหาย ซึ่งมีความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) และความเสี่ยงที่ไม่เป็นที่ต้องการ (undesirable) อยู่ในระดับที่สามารถยอมรับได้ (acceptable level) ตามตารางที่ 2-1

(5) สำหรับหน่วยการทำงานที่ใช้โปรแกรมซอฟต์แวร์ (software-programmed elements) ซอฟต์แวร์นั้นต้องแสดงให้เห็นว่าไม่มี error รวมถึงข้อผิดพลาดใด ๆ ที่เกิดขึ้นในระหว่างกระบวนการทำงานร่วมกัน (compilation process) โดยมีการพิสูจน์และมีแนวทางปฏิบัติในการตรวจสอบและรับรอง ตามหัวข้อที่ 2.4

2.3.2.4 Numerical Assurance

การใช้หลักการของ Numerical Assurance ต้องมีคำสั่งที่ได้รับอนุญาต (permissive decisions) เพื่อแสดงผลด้วยค่าตัวเลขขนาดใหญ่ที่ไม่ซ้ำกัน ซึ่งคำนวณจากการรวมค่าตัวเลขของแต่ละองค์ประกอบที่สำคัญใน permissive decisions โดยการออกแบบจะต้องมีการตรวจสอบและมีคุณลักษณะดังต่อไปนี้

(1) ค่าตัวเลขจาก permissive decisions ต้องมีการรับรองได้ว่าไม่ซ้ำกันและมีการเพิ่มค่าที่ไม่ซ้ำกันจากแต่ละองค์ประกอบที่สำคัญของ permissive decisions

(2) กระบวนการสำคัญทั้งหมดที่ไม่มีการเพิ่มค่าตัวเลขตามข้อ (1) ต้องสร้างค่าตัวเลขที่ไม่ซ้ำกันในการตรวจสอบความถูกต้อง

(3) ระบบการคำนวณผลตัวเลขต้องไม่มีการรับรู้ค่าตัวเลขที่ถูกต้องมาก่อน

(4) กระบวนการที่ใช้ในการตรวจสอบความถูกต้องของผลลัพธ์ตัวเลข (numerical results) ต้องอยู่ในรูปแบบความปลอดภัยในกรณีขัดข้อง (fail-safe)

(5) ความล้มเหลวใดๆ ที่อาจส่งผลต่อความปลอดภัยของระบบต้องส่งผลให้อยู่ในสถานะปลอดภัย (Known safe state)

(6) หากไม่มีความถูกต้องในผลลัพธ์ตัวเลขใดก็ตาม ต้องส่งผลให้อยู่ในสถานะปลอดภัย (Known safe state)

(7) กระบวนการเชิงนี้ต้องมีความครอบคลุมรวมไปถึงฟังก์ชันต่างๆ ที่มีการป้องกันโดยการใช้ค่าตัวเลข และความถี่ในการคำนวณและตรวจสอบค่าตัวเลขนี้ เพื่อให้มั่นใจว่าความน่าจะเป็นของความล้มเหลวหรือความเสียหาย ซึ่งเป็นความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable) และความเสี่ยงที่ไม่เป็นที่ต้องการ (undesirable) อยู่ในระดับที่สามารถยอมรับได้ (acceptable level) ตามตารางที่ 2-1

2.4 การตรวจสอบและการรับรองความถูกต้อง

การออกแบบและการใช้งานสำหรับองค์ประกอบฮาร์ดแวร์และซอฟต์แวร์ที่มีความสำคัญต่อความปลอดภัยทั้งหมดของระบบตามที่ได้ระบุไว้ในกระบวนการแก้ไขความเสี่ยง (Hazard Resolution Process) หัวข้อที่ 2.1.2 ต้องถูกตรวจสอบและรับรองความถูกต้อง โดยกระบวนการนี้รวมองค์ประกอบที่ออกแบบและดำเนินการตามหัวข้อที่ 2.2 หลักการความปลอดภัย และหัวข้อที่ 2.3 การออกแบบความปลอดภัยในกรณีขัดข้องของระบบ ATC โดยวัตถุประสงค์ของการตรวจสอบและการรับรองความถูกต้อง เพื่อตรวจสอบว่าองค์ประกอบสำคัญด้านความปลอดภัยทั้งหมดที่ได้ออกแบบและนำไปใช้มีการทำงานมีความปลอดภัยและตรวจสอบระดับความปลอดภัย ซึ่งการตรวจสอบและการรับรองความถูกต้องมีดังต่อไปนี้

(1) การระบุปัจจัยทั้งหมดที่ขึ้นอยู่กับการรับรองความปลอดภัย ซึ่งปัจจัยดังกล่าวต้องเกี่ยวข้องโดยตรงกับการออกแบบการใช้งาน เช่น Checked Redundancy N-Version Programming Diversity and Self-Checking หรือ Numerical Assurance

(2) การระบุฟังก์ชันที่มีความสำคัญต่อความปลอดภัยทั้งหมดที่ดำเนินการโดยระบบ

(3) การวิเคราะห์ต่างๆ ที่แสดงปัจจัยที่มีความเกี่ยวข้องทั้งหมด และในแต่ละฟังก์ชันที่มีความสำคัญต่อความปลอดภัยที่นำมาใช้เป็นไปตามหลักการของความปลอดภัย

ทั้งนี้ รายงานการรับรองความปลอดภัยของระบบ (System Safety Certification Report: SSCR) ต้องบันทึกเป็นสถานะในการตรวจสอบและรับรองความถูกต้องของกิจกรรมในโครงการ APM โดย SSCR ต้องเริ่มต้นด้วย PHA ต่อจากนั้นมีการอัปเดตเป็นระยะและทำต่อไปตลอดอายุการใช้งานของ APM

2.5 Mean Time Between Hazardous Events (MTBHE) ของระบบ ATC

นอกเหนือจากข้อกำหนดของระบบ ATC ในหัวข้อที่ 2.4 แล้ว ระบบ ATC ต้องมีการคำนวณ MTBHE ซึ่งรวมไปถึงความเสี่ยงที่รุนแรงมาก (catastrophic hazard) และความเสี่ยงที่ร้ายแรง (critical hazard) ที่มีค่าเท่ากับหรือมากกว่า 10^8 หรือ 1 x E8 ชั่วโมงการทำงานของระบบ ทั้งนี้ เอกสารความปลอดภัยของระบบต้องเป็นไปในทางเดียวกันกับการคำนวณ MTBHE และมีการรับรองวิธีการที่ใช้ เพื่อให้บรรลุผล

2.6 ข้อแนะนำเพิ่มเติมในหัวข้อที่ 2 และส่วนย่อยต่างๆ

1) หัวข้อที่ 2.4 ของมาตรฐานนี้ อธิบายขั้นตอนในการตรวจสอบเพื่อระบุและแก้ไขปัญหาความเสี่ยงที่มีความสำคัญต่อความปลอดภัย และหัวข้อที่ 2.4 ไม่ได้ใช้เฉพาะกับระบบ ATC แต่ต้องมีการตรวจสอบและการรับรองในทุกๆ องค์ประกอบของฮาร์ดแวร์และซอฟท์แวร์ที่มีความสำคัญต่อความปลอดภัยของระบบ APM ทั้งหมด ซึ่งกระบวนการแก้ไขความเสี่ยง (Hazard Resolution Process) นี้ ได้ระบุในหัวข้อที่ 2.1.2

2) หัวข้อที่ 2.4 และ 2.5 เป็นข้อกำหนดเพิ่มเติมของ MTBHE ที่ใช้กับระบบ ATC เท่านั้น

3) ตามที่ระบุในหัวข้อ 2.1.2 ความเสี่ยงทั้งหมดของระบบ APM หรือระบบย่อย ต้องได้รับการประเมินในแง่ของความรุนแรงและผลหรือความน่าจะเป็นที่ตามมาของความเสี่ยงนั้น โดยการประเมินความเสี่ยงตามตารางที่ 2-1 ใช้เป็นพื้นฐานในการตัดสินใจว่าความเสี่ยงนั้นจำเป็นที่ต้องกำจัด บรรเทาลง หรือเป็นความเสี่ยงที่ยอมรับได้ อีกทั้ง ตารางนี้เป็นแนวทางในการพิจารณาระดับความเสี่ยง โดยที่ระดับความเสี่ยงที่ยอมรับได้จะมีการแจ้งไปยังหน่วยงานที่มีอำนาจตัดสิน ซึ่งต้องได้รับการอนุมัติจากหน่วยงานที่มีอำนาจตัดสินเท่านั้น และความเสี่ยงที่รุนแรงและไม่สามารถยอมรับได้ต้องถูกกำจัดหรือบรรเทาลง

4) การประเมินความเสี่ยงในระบบที่แยกส่วนหรือระบบย่อยสำหรับระบบ APM ถูกระบุไว้ในตารางที่ 2-1 ซึ่งเป็นที่เข้าใจว่าการคาดการณ์เชิงปริมาณของความน่าจะเป็นหรือความถี่ในการเกิดเหตุอาจไม่สามารถใช้ได้เสมอไป ในกรณีเช่นนี้ สามารถทำการประเมินความเสี่ยงในเชิงคุณภาพได้ โดยที่จะต้องมีการให้เหตุผลในการประเมินดังกล่าวไว้ด้วย

5) โดยปกติแล้ว ผลลัพธ์ของกระบวนการนี้จะเป็นชุดของแบบฟอร์มการแก้ไขความเสี่ยงที่จะอธิบายในแต่ละความเสี่ยงถึงผลที่จะตามมาของความเสี่ยงและความรุนแรง รวมไปถึงขั้นตอนการบรรเทาหรือกำจัดความเสี่ยงหากเป็นความเสี่ยงที่ไม่สามารถยอมรับได้ อีกทั้ง แบบฟอร์มนี้จะมีการบันทึกระดับความเสี่ยงที่ยอมรับได้หลังจากการบรรเทาความเสี่ยงลงแล้ว ซึ่งจะยังเป็นกรณีที่ไม่ถูกกำจัดไปอย่างสมบูรณ์

6) หัวข้อที่ 2.1.2 ในมาตรฐานนี้ ได้ระบุแนวทางที่อนุญาตในการบรรเทาหรือกำจัดความเสี่ยง โดยที่แนวทางการแก้ไขที่แนะนำ คือ การเปลี่ยนการออกแบบ ทั้งนี้ หากไม่สามารถแก้ไขความเสี่ยงดังกล่าวได้ สามารถใช้อุปกรณ์ความปลอดภัยหรืออุปกรณ์แจ้งเตือนได้ และหากยังไม่สามารถทำได้ แนะนำให้ดำเนินการตรวจสภาพระบบเป็นวาระ (periodic inspection) และท้ายที่สุด อุปกรณ์ที่ทำให้เกิดความเสี่ยงจะสามารถถูกกำจัดออกจากการออกแบบได้ ทั้งนี้ ความเสี่ยงที่ยอมรับได้ต้องไม่อยู่ในประเภทความเสี่ยงที่ถูกแรงเงาในตารางที่ 2-1 ซึ่งพื้นที่ความเสี่ยงที่ถูกแรงเงาเหล่านั้น คือ ความเสี่ยงที่ไม่สามารถยอมรับได้ที่มาจากความรุนแรงและความน่าจะเป็นของการเกิดเหตุที่ไม่สามารถยอมรับได้

7) หลังจากที่ได้กำหนดความเสี่ยงและกำหนดประเภทความเสี่ยงให้กับเหตุอันตรายแล้ว ควรมีการอ้างอิงหลักการทั่วไปในการประเมินความเสี่ยงที่ยอมรับได้ ตัวอย่างเช่น

(1) หลักการ As Low As Reasonably Practicable (ALARP) ซึ่งเป็นหลักการที่ใช้ในสหราชอาณาจักร

(2) หลักการ Globalement Au Moins Aussi Bon (GAMAB) ซึ่งเป็นหลักการที่ใช้ในสาธารณรัฐฝรั่งเศส

(3) หลักการ Minimum Endogenous Mortality (MEM) ซึ่งเป็นหลักการที่ใช้ในสหพันธ์สาธารณรัฐเยอรมนี

8) หัวข้อที่ 2.5 กำหนดหลักเกณฑ์ความปลอดภัยเพิ่มเติมสำหรับระบบ ATC นอกเหนือจากการบรรเทาหรือกำจัดความเสี่ยงในหัวข้อที่ 2.4 โดยที่หลักเกณฑ์ความปลอดภัยเพิ่มเติมนี้ คือ ผลรวมของ MTBHE นั่นคือ ผลรวมทั้งหมดของความเสี่ยงที่รุนแรงมาก (catastrophic hazard) และความเสี่ยงที่ร้ายแรง (critical hazard) สำหรับระบบ ATC เท่านั้น โดยที่ตัวเลข MTBHE นี้ต้องมีเอกสารประกอบด้านความปลอดภัยรับรอง

9) มีการระบุค่า MTBHE สองค่าที่แตกต่างกัน หากระบบไม่ได้ใช้การควบคุมแบบ Communications-Based Train Control (CBTC) ผลรวมของ MTBHE จะเท่ากับหรือมากกว่า 10^8 หรือ 1 x E8 ชั่วโมงการทำงานของทั้งระบบ ATC และหากระบบ ATC ใช้การควบคุมแบบ CBTC ค่า MTBHE จะเป็นไปตาม

มาตรฐาน IEEE 1474.1 หรือมาตรฐานอื่นที่เทียบเท่า ซึ่งได้ระบุค่า MTBHE ไว้อย่างน้อย 10^9 หรือ 1 x E9 ชั่วโมงการทำงานของอุปกรณ์ระบบควบคุม CBTC ข้างทาง (wayside equipment) และอุปกรณ์บนรถ (train-born equipment) ทั้งหมดตลอดเส้นทางการเดินรถทางเดียว (one-way route) ที่สามารถเดินรถด้วยความเร็วสูงสุดตามที่กำหนดไว้เป็นเวลา 1 ชั่วโมงหรือน้อยกว่านั้น อีกทั้ง ควรมีจำนวนขบวนสูงที่สุดในช่วงให้บริการที่มีความต้องการสูง (peak operating headway)

10) ข้อสังเกต: ค่า 10^8 หรือ 1 x E8 ในมาตรฐานนี้ครอบคลุมระบบ ATC ทั้งหมด ในขณะที่ค่า 10^9 หรือ 1 x E9 ครอบคลุมเฉพาะตัวรถและอุปกรณ์ CBTC ข้างทางในบางส่วนของเส้นทางการเดินรถจากเส้นทางทั้งหมด ทั้งนี้ 2 ค่านี้ไม่สามารถเปรียบเทียบกันโดยตรงได้

บทที่ 3
ความน่าเชื่อถือของระบบ (System Dependability)

ความน่าเชื่อถือของระบบ คือ การวัดประสิทธิภาพการทำงานของระบบ ที่ประกอบไปด้วยการวัดความน่าเชื่อถือ (reliability) ความสามารถการบำรุงรักษา (maintainability) และความพร้อมใช้งาน (availability)

โดยเนื้อหาในบทนี้กล่าวถึงระบบหลักที่อาจจะประกอบด้วยระบบย่อยหลายๆ ส่วน และความน่าเชื่อถือของระบบย่อยแต่ละส่วนจะนำไปสู่การประมาณค่าความน่าเชื่อถือของระบบหลัก

ระบบที่ทำงานได้บางส่วนหรือระบบที่ทำงานไม่สมบูรณ์จะถูกนำไปวิเคราะห์เพื่อประเมินความเชื่อถือโดยรวมของระบบ โดยอาศัยวิธีการใช้ตัวแปร อัตราส่วน หรือการคำนวณ

ข้อสังเกตุ: รายละเอียดการวัดค่าความพร้อมใช้งานสามารถดูได้ที่ภาคผนวก ค ของมาตรฐานฉบับนี้ โดยเป็นการวัดเวลาหยุดทำงาน (downtime) ของอุปกรณ์ที่มีผลต่อการให้บริการผู้โดยสารอย่างมีนัยสำคัญ ซึ่งการคำนวณหาความพร้อมใช้งานของระบบจะใช้เป็นตัวแปรสำคัญของบทนี้

3.1 ความน่าเชื่อถือ (Service Reliability)

ความน่าเชื่อถือคำนวณจากเวลาเฉลี่ยการทำงานของระบบหรืออุปกรณ์ระหว่างเกิดความล้มเหลวในแต่ละครั้ง (Mean Time Between Failures service: MTBFs) (สมการ 3-1)

เวลาเฉลี่ยการทำงานของระบบหรืออุปกรณ์ระหว่างเกิดความล้มเหลวแต่ละครั้งมีค่าเท่ากับ

$$\text{MTBFs} = \frac{\text{จำนวนชั่วโมงการทำงาน}}{\text{จำนวนครั้งที่เกิดความล้มเหลว}} = \frac{\text{OH}_\text{S}}{\text{NF}_\text{S}} \qquad \text{สมการ 3-1}$$

โดยที่ OH_S คือ จำนวนชั่วโมงการทำงานทั้งหมดของระบบตามแผน ซึ่งค่าความน่าเชื่อถือถูกกำหนดโดยชั่วโมงการทำงาน

NF_S คือ จำนวนครั้งที่เกิดความล้มเหลว ความผิดปกติ และการเกิดเหตุขัดข้องของระบบในขณะทำงาน

3.1.1 การเกิดเหตุขัดข้อง

คือ เหตุการณ์หรือความล้มเหลวของระบบหรืออุปกรณ์ที่ทำให้ผู้โดยสารไม่สามารถใช้งานระบบหรืออุปกรณ์นั้นได้อย่างปกติ โดยการเกิดเหตุขัดข้องคำนวณตามน้ำหนักหรือความสำคัญของอุปกรณ์เหล่านั้น โดยการเกิดเหตุขัดข้องต้องรวมถึงกรณีดังต่อไปนี้

1. การเกิดเหตุขัดข้องของรถที่อยู่นอกเหนือแผน
2. การสับเปลี่ยนเส้นทางเดินรถอันเนื่องมาจากความเสียหายของอุปกรณ์ที่ใช้งานประจำสถานี ทำให้ไม่สามารถใช้งานได้อย่างปกติ
3. ความผิดปกติที่สถานีที่ทำให้ผู้โดยสารไม่สามารถเข้าหรือออกจากขบวนรถได้
4. อุปกรณ์บางอย่างที่อยู่ในระบบ APM มีความผิดปกติทำให้ผู้โดยสารไม่สามารถใช้บริการรถ APM ได้
5. ความผิดปกติที่ส่งผลให้เกิดอุบัติเหตุ

นอกจากนี้ยังรวมไปถึงความผิดพลาดของผู้ปฏิบัติงานที่อาจส่งผลทำให้เกิดผลกระทบต่อการให้บริการ

3.1.2 ข้อยกเว้นต่อไปนี้ไม่จัดว่าเป็นผลกระทบต่อการเกิดเหตุขัดข้อง

กรณีต่อไปนี้ไม่จัดว่าเป็นการเกิดเหตุขัดข้อง

1. ความผิดปกติที่เป็นเหตุให้เกิดเหตุขัดข้อง แต่ช่วงเวลาที่เกิดเหตุขัดข้องไม่เกินกว่าเวลาที่กำหนดไว้ตามแผน (grace time)

2. ความผิดปกติหรือเหตุฉุกเฉินที่เกิดขึ้นจากการที่ผู้โดยสารทำลายทรัพย์สิน ผู้โดยสารใช้อุปกรณ์ผิด หรือผู้โดยสารทำให้ขบวนรถต้องล่าช้า

3. เหตุฉุกเฉินที่เกิดจากบุคคลที่ไม่ได้รับอนุญาตหรือมีสัตว์เลี้ยงรุกล้ำเข้าไปในเขตพื้นที่หวงห้าม จนส่งผลให้เกิดความล้มเหลวของอุปกรณ์ความปลอดภัย ซึ่งความเสียหายของอุปกรณ์ความปลอดภัยเกิดจากการป้องกันการรุกล้ำของบุคคลหรือสัตว์เลี้ยงดังกล่าว

4. เหตุฉุกเฉินที่เกิดจากปัจจัยภายนอก เช่น ระบบพลังงานไฟฟ้ามีปัญหา การหยุดตามคำสั่งของเจ้าพนักงาน (เช่น ตำรวจ) การเกิดเหตุสุดวิสัย ค่าสภาวะแวดล้อมที่เกินค่าปกติ

5. เหตุฉุกเฉินที่เกิดจากการฝึกอบรมในกรณีพิเศษ การตรวจสอบทางวิ่งบังคับ หรือการขยายเวลาซ่อมเพิ่มเติมจากที่กำหนดไว้ในแผน

6. การหยุดที่มีสาเหตุมาจากการตรวจสอบประสิทธิภาพการทำงานของระบบควบคุมการเดินรถอัตโนมัติเพื่อให้มั่นใจได้ว่าเป็นไปตามข้อกำหนดอย่างแท้จริง

3.2 ความสามารถการบำรุงรักษา (Service Maintainability)

คือ เวลาเฉลี่ยในการซ่อมบำรุง (Mean Time To Restore service: MTTRs) หลังจากที่ระบบมีการหยุดซ่อม (สมการ 3-2)

$$\mathrm{MTTR_s} = \frac{\text{ผลรวมของเวลาทั้งหมดในการซ่อมบำรุง}}{\text{จำนวนครั้งที่เกิดความล้มเหลว}} \qquad \text{สมการ 3-2}$$

$$\mathrm{MTTR_s} = \left(\frac{1}{NF_s}\right)\sum_{i=1}^{NF_s} TTR_i$$

โดยที่ $\mathrm{TTR_i}$ คือ เวลาในการซ่อมบำรุงหลังจากเกิดการหยุดฉุกเฉินในแต่ละครั้ง i (หรือช่วงเวลาการหยุดงาน)

$\mathrm{NF_s}$ คือ จำนวนความล้มเหลว ความผิดปกติ และการหยุดฉุกเฉินที่กระทบต่อชั่วโมงการเดินรถ

ในการคำนวณเวลาสะสมในการซ่อมบำรุงจากจำนวนความล้มเหลวทั้งหมด $(\mathrm{NF_s})$ จะคิดเฉพาะความเสียหายที่มีเวลาการซ่อมเกินกว่าเวลาการหยุดซ่อมตามแผน (grace time) เท่านั้น เวลาการซ่อมที่กำหนดไว้ตามแผนนี้จะเป็นค่าคงที่และไม่มีการขยายเวลาเพิ่ม ดังนั้นเวลาการซ่อมที่เกินกว่าเวลาที่กำหนดไว้ให้นับว่าเป็นเวลาหยุดงาน (downtime)

นอกจากนี้ ช่วงเวลาการหยุดงานของแต่ละเหตุการณ์ ความเสียหายต้องพิจารณาจากช่วงเวลาที่ระบบเกิดเหตุขัดข้องฉุกเฉิน โดยที่

(1) เวลาการหยุดซ่อมตามแผน (grace time) ต้องไม่นำไปลบออกจากเวลาในการซ่อม $(\mathrm{TTR_i})$ ของการเกิดเหตุขัดข้องฉุกเฉินในแต่ละครั้ง

(2) เวลาการหยุดงาน (downtime) ต้องเริ่มวัดจากเวลาที่ระบบหยุดฉุกเฉิน ระบบมีอาการผิดปกติ และได้ทำการซ่อมบำรุงจนสามารถกลับมาใช้งานได้เป็นปกติ โดยที่การซ่อมบำรุงอาจจะเป็นวิธีการซ่อมหรือวิธีการเปลี่ยนอะไหล่ทดแทนก็ได้

3.3 ความพร้อมใช้งาน (Service Availability)

สามารถคำนวณความพร้อมใช้งาน (Service Availability: As) จากสมการ 3-3

$$\mathrm{As} = \frac{MTBF_s}{MTBF_s + MTTR_s} \qquad \text{สมการ 3-3}$$

ค่าความพร้อมใช้งานต้องคำนวณได้จากชั่วโมงการทำงานที่แท้จริง หรือเอาชั่วโมงการทำงานรวมตามแผนลบด้วยเวลาหยุดงานทั้งหมด (Total operation time - Total downtime) หารด้วยชั่วโมงการทำงานทั้งหมดตามแผน (Total operation time)

บทที่ 4
ระบบควบคุมการเดินรถอัตโนมัติ (Automatic Train Control)

ระบบควบคุมการเดินรถอัตโนมัติ (ATC) ต้องประกอบด้วยระบบป้องกันเหตุอันตรายของรถอัตโนมัติ (Automatic train protection: ATP) ระบบการเดินรถอัตโนมัติ (Automatic train operation: ATO) และระบบติดตามการเดินรถอัตโนมัติ (Automatic train supervision: ATS) โดย ATP ต้องให้การคุ้มครองพื้นฐานสำหรับผู้โดยสาร บุคลากรและอุปกรณ์ต่างๆ ในระบบ จากความเสี่ยงที่เกิดขึ้น ในการดำเนินการภายใต้การควบคุมแบบอัตโนมัติ ต้องให้ความสำคัญฟังก์ชัน ATP มากกว่าฟังก์ชัน ATO และ ATS

ฟังก์ชัน ATO ต้องควบคุมการทำงานเบื้องต้นแทนพนักงานที่ปฏิบัติงาน ภายใต้ขีดจำกัดของระบบ ATP และในส่วนของระบบ ATS ต้องให้ข้อมูลสถานะของระบบและมีวิธีตรวจสอบและการแทนที่เพื่อควบคุมอัตโนมัติในฟังก์ชั่นต่าง ๆ ของระบบแก่ผู้ดำเนินการควบคุม

ระบบ APM ที่ใช้การควบคุมการสื่อสารแบบ Communications-Based Train Control (CBTC) ของ ATC ต้องอ้างอิงข้อกำหนดตามมาตรฐาน IEEE 1474.1 หรือมาตรฐานอื่นที่เทียบเท่า แทนข้อกำหนดในข้อ 4.1 และ 4.2 แต่ระบบ ATN ตามข้อ 4.1.2.2 ไม่จำเป็นต้องเป็นไปตามมาตรฐาน IEEE 1474.1 หรือมาตรฐานอื่นที่เทียบเท่า นั้น

4.1 ฟังก์ชันระบบป้องกันเหตุอันตรายของรถอัตโนมัติ (ATP)

ฟังก์ชัน ATP ทั้งหมดต้องถูกออกแบบและนำมาใช้ตามหัวข้อ 2.2 หลักการความปลอดภัย และหัวข้อ 2.3 การออกแบบความปลอดภัยในกรณีขัดข้องของระบบ ATC (ATC system fail-safe design)

4.1.1 การตรวจจับการมีอยู่ (ตำแหน่งรถ)

ฟังก์ชันของ ATP ต้องมีการตรวจจับการมีอยู่ของรถเพื่อให้มั่นใจในความปลอดภัยของฟังก์ชัน ATP อื่น ๆ เช่น การรักษาระยะห่างขบวนรถ และ/หรือ การบังคับสัมพันธ์ของทางประแจ (guideway switch)

การตรวจจับการมีอยู่ของขบวนรถต้องทำอย่างต่อเนื่องตามข้อ 4.1.7 ในพื้นที่อัตโนมัติทั้งหมดของทางวิ่งบังคับ โดยที่รถทุกคันและยานพาหนะอื่น ๆ ที่ทำงานบนระบบที่ตรวจจับขบวนรถอัตโนมัติต้องถูกตรวจจับได้ ไม่ว่าจะมีการเดินรถในโหมดอัตโนมัติหรือการควบคุมด้วยมือก็ตาม

ก่อนเริ่มการเดินรถแบบอัตโนมัติ ฟังก์ชั่นการตรวจจับความมีอยู่ของขบวนรถต้องถูกตั้งค่าใหม่และขบวนรถทั้งหมดต้องถูกระบุตำแหน่งและตัวตนให้เจอ โดยที่ไม่อนุญาตให้สามารถป้อนข้อมูลตำแหน่งของรถด้วยมือในการเดินรถอัตโนมัติได้

4.1.2 การรักษาระยะห่าง

หัวข้อ 4.1.2.1 กำหนดมาตรฐานการรักษาระยะห่างสำหรับรถ APM

หัวข้อ 4.1.2.2 ใช้แทนข้อ 4.1.2.1 สำหรับระบบ APM ที่มีข้อกำหนดตรงตามระบบ ATN และมีความตั้งใจที่จะเดินรถในระยะห่างระหว่างขบวนรถที่ใกล้กว่าส่วน 4.1.2.1 อนุญาต

4.1.2.1 การรักษาระยะห่างสำหรับรถ APM

ฟังก์ชัน ATP ต้องมีการรักษาระยะห่าง ซึ่งเป็นองค์ประกอบของระบบ APM ที่ให้บริการเดินรถตลอดเส้นทางของทางวิ่งบังคับ

การรักษาระยะห่างต้องป้องกันการชนท้ายรถ (rear-end collision) โดยรักษาระยะห่างที่ด้านหลังของรถทุกคันให้มีระยะหยุดรถที่เพียงพอสำหรับรถที่ตามมาในกรณีที่รถข้างหน้าหยุดกระทันหัน ซึ่งระยะหยุดรถนั้นต้องถูกคำนวณจากการใช้คุณลักษณะขององค์ประกอบที่เกี่ยวข้องในกรณีที่แย่ที่สุดที่ให้มีระยะหยุดรถมากที่สุด ซึ่งมีคุณลักษณะดังต่อไปนี้

1. ความเร่งวิ่งสูงสุด
2. เงื่อนไขการเบรคฉุกเฉินขั้นต่ำ
3. ความล่าช้าสะสมทั้งหมด
4. ความเร็วเกินกำหนด
5. ความชัน (grade)
6. ภาระบรรทุกที่มากที่สุด
7. แรงยึดเกาะ (adhesion) น้อยที่สุดและแรงขับเคลื่อน (traction) และ
8. แรงลมท้ายรถ (tailwind) มากที่สุดที่ออกแบบไว้

ทั้งนี้ เงื่อนไขการเบรคฉุกเฉินขั้นต่ำต้องขึ้นอยู่กับความล้มเหลวที่แย่ที่สุดหนึ่งกรณีของระบบเบรคตามที่กำหนดไว้ในการวิเคราะห์ที่เหมาะสมตามหัวข้อ 2.1.2.1 การวิเคราะห์อันตราย

สำหรับระบบ APM ที่อนุญาตให้มีการเดินรถอัตโนมัติในทิศทางตรงกันข้ามบนทางเดียวกัน การรักษาระยะห่างที่คำนวนระยะหยุดของทั้งสองรถต้องถูกนำมาใช้เพื่อป้องกันการชน

สำหรับระบบ APM ที่ใช้ขอพ่วงแบบอัตโนมัติ การต่อพ่วงต้องดำเนินการภายใต้ระบบ ATP และสามารถทำการตรวจสอบได้ตามหัวข้อ 2.3

สำหรับระบบ APM ที่มีการรักษาระยะห่างระหว่างขบวน โดยการใช้กลไกทางกายภาพ เช่น ระบบที่ใช้การขับเคลื่อนดวยสายเคเบิ้ล (cable-propelled system) และขบวนรถที่วิเคราะห์ตามหัวข้อ 2.1.2.1 ต้องมีการตรวจจับการเลื่อนหลุดของกลไกระหว่างขบวนรถ หากพบการหลุดหรือการถอดชิ้นส่วนเหล่านี้จะต้องเริ่มกระบวนการเบรคฉุกเฉินเพื่อหยุดรถขบวนนั้น และขบวนรถทั้งหมดที่พ่วงต่อกับกลไกนั้น

สำหรับระบบ APM ที่ใช้วิธีการอื่นในการรักษาระยะห่างระหว่างรถ การรักษาระยะห่างนั้นต้องถูกกำหนดด้วยวิธีการอื่นที่มีความคล้ายคลึงกัน

4.1.2.2 การรักษาระยะห่างสำหรับเครือข่ายระบบขนส่งมวลชนอัตโนมัติ (Automated Transit Network: ATN)

ส่วนนี้จะใช้แทนข้อ 4.1.2.1 สำหรับระบบ ATN ในกรณีที่จะไม่เกิดความล้มเหลวปลอดจากความเสี่ยงที่ยอมรับไม่ได้ ตามที่กำหนดไว้ในหัวข้อ 2.2 โดยมาจากการประเมินความเสี่ยงในกรณีที่มีการหยุดของรถขบวนนำ ตามข้อ 2.1.2 และข้อบังคับเพิ่มเติมทั้งหมดที่เพิ่มเข้ามาในหัวข้อ 4.1.2.2 ด้วย

ไม่อนุญาตให้มีการเดินรถอัตโนมัติของขบวนรถที่วิ่งสวนทางกันในเวลาเดียวกันบนทางวิ่งบังคับเดียวกัน

การรักษาระยะห่างต้องมีฟังก์ชันของ ATP ที่เป็นไปตามหัวข้อ 2.3 ในการกำหนดค่าใด ๆ ของระบบ ATN ที่เดินรถรอบเส้นทางของทางวิ่งบังคับ อีกทั้ง ระบบ ATP ต้องป้องกันไม่ให้ขบวนรถมีสิทธิ์ในการเคลื่อนที่ของรถเกินขีดจำกัด หรือเกินความเร็วปลอดภัยที่กำหนด

การรักษาระยะห่างต้องมีการป้องกันในกรณีที่ขบวนรถตามหลังมีความเสี่ยงที่จะชนกับรถขบวนนำ โดยมีการรักษาระยะห่างปลอดภัยไว้ (Separation Assurance Zone: SAZ)

ข้อกำหนด การออกแบบ การคำนวณ การวิเคราะห์อันตรายและมาตรการความปลอดภัยด้านผลกระทบด้านความปลอดภัยในการรักษาระยะห่าง ต้องถูกตรวจสอบโดยผู้ประเมินความปลอดภัยที่เป็นอิสระ (Independent Safety Assessor: ISA) ที่ได้รับการอนุมัติจากหน่วยงานที่มีอำนาจตัดสิน (Authority Having Jurisdiction: AHJ) โดยอ้างอิงตามแนวทางการปฏิบัติแนะนำสำหรับการประเมินความปลอดภัยอิสระ ภาคผนวก ค

ในการคำนวณการรักษาระยะห่าง (SAZ) ข้อมูลตำแหน่งและความเร็วของรถที่ตามหลัง ต้องรวมค่าคลาดเคลื่อนของเครื่องมือ ความล่าช้าของข้อมูล และการล่าช้าในการสื่อสารตั้งแต่เวลาการส่งข้อมูลตำแหน่งและความเร็วจากรถด้านหน้า นอกจากนี้ ต้องคำนึงถึงข้อจำกัดของสิ่งแวดล้อมในโครงการ เช่น ทัศนวิสัยไม่ดี บริเวณที่มีแสงน้อย การรบกวนจากคลื่นแม่เหล็กไฟฟ้า (EMI) และกรณีฉุกเฉินและความล้มเหลวของอุปกรณ์ระบุตำแหน่งต่าง ๆ

ระยะหยุดรถสำหรับรถที่ตามหลังต้องถูกคำนวณด้วยวิธีการใช้คุณลักษณะขององค์ประกอบที่เกี่ยวข้องในกรณีที่แย่ที่สุด โดยทำให้มีระยะหยุดรถมากที่สุด ซึ่งมีคุณลักษณะดังต่อไปนี้

1. ความเร่งในการวิ่งสูงสุด
2. เงื่อนไขการเบรคฉุกเฉินขั้นต่ำ
3. ความล่าช้าทั้งหมด
4. ความเร็วเกินกำหนดสูงสุด
5. รูปร่างและคุณสมบัติของราง (track geometry) รวมถึงความชัน
6. โหลดในกรณีแย่ที่สุด (worst-case load)
7. การยึดเกาะและแรงยึดที่น้อยที่สุด หรือมีการแปรผัน
8. แรงลมท้ายรถ (tailwind) มากที่สุดที่ออกแบบไว้

ทั้งนี้ เงื่อนไขการเบรคฉุกเฉินขั้นต่ำต้องขึ้นอยู่กับความล้มเหลวที่แย่ที่สุดหนึ่งของระบบเบรคตามที่กำหนดไว้ในการวิเคราะห์ที่เหมาะสมตามหัวข้อ 2.1.2.1 การวิเคราะห์อันตราย

หากไม่สามารถสมมุติฐานได้ว่าขบวนรถข้างหน้าสามารถหยุดได้ทันที อัตราการเบรคของรถคันหน้าต้องถูกวิเคราะห์ตามข้อกำหนดในข้อ 2.1.2.1 การวิเคราะห์อันตรายและตาราง 2-1 การประเมินความเสี่ยง

อันตรายที่อาจเกิดขึ้นหรือเหตุการณ์ที่เสี่ยง อย่างน้อยได้แก่

1. การชนกับสิ่งกีดขวางอิสระบนทางวิ่งบังคับซึ่งมีน้ำหนักมากกว่าร้อยละ 10 ของน้ำหนักรถแบบ AW0

2. การชนกับขบวนรถที่ไม่ได้ตรวจพบการหยุดบนทางวิ่งบังคับและขบวนที่ตามมามากกว่า 1 ขบวน โดยที่นิยามของขบวนรถที่ไม่ได้ตรวจพบ คือ ขบวนรถที่เกิดความล้มเหลวในการตรวจจับหรือการสื่อสาร จึงไม่ได้รับตำแหน่งจากเทคโนโลยีที่ใช้ตรวจจับตำแหน่งรถ เมื่อสูญเสียการตรวจจับรถให้สมมุติว่ารถคันหน้าได้รับคำสั่งให้หยุดทันทีในอัตราการเบรคสูงสุดที่ SAZ กำหนด

3. ความล้มเหลวของประแจส่งผลให้ขบวนรถหลุดออกจากทางวิ่งบังคับเมื่อผ่านจุดทางแยกหรือบริเวณชุมทางบนทางราง

4. ความล้มเหลวของการอุปกรณ์นำทางด้านข้างหรือกลไกกันตกรางที่ทำให้ขบวนรถได้รับความเสี่ยงที่จะมีการสัมผัสหรือชนกับรางจ่ายไฟ (power rails) พื้นผิวนำทาง (guidance surfaces) ทางวิ่งบังคับ หรือชิ้นส่วนอื่นๆ ภายนอก

5. ความล้มเหลวของล้อหรือระบบกันสะเทือนที่อาจนำไปสู่การสัมผัสหรือชนกับรางจ่ายไฟ พื้นผิวนำทาง ทางวิ่งบังคับ หรือ ชิ้นส่วนอื่นๆภายนอก

6. การเอียงตัวออกจากแนวเดิมของตัวรถ (rollover)

7. ขบวนรถชนกับสิ่งกีดขวางบนทางวิ่งบังคับเนื่องจากมีระยะห่างข้างทางวิ่งบังคับไม่เพียงพอ

8. ขบวนรถชนกับสิ่งกีดขวางบนทางวิ่งบังคับเนื่องจากมีระยะห่างข้างทางวิ่งบังคับไม่เพียงพอ โดยที่สิ่งกีดขวางนั้นถูกออกแบบให้ถูกชนได้อย่างปลอดภัยและทำให้ขบวนรถด้านหน้าเบรคในอัตราที่ไม่เกิน SAZ กำหนด

9. การชนกับสิ่งกีดขวางอิสระบนทางวิ่งบังคับซึ่งมีน้ำหนักน้อยกว่าร้อยละ10 ของน้ำหนักรถแบบ AW0

10. การเปลี่ยนทิศทางการขับเคลื่อนเองจากอุปกรณ์ขับเคลื่อนของขบวนรถ

11. การใช้ระบบเบรคที่ไม่ได้กำหนดไว้ (เบรกปกติ เบรกฉุกเฉิน และเบรกจอด (หากมี)) บนรถที่มีโหลดแบบ AW0 ในอัตราการเบรกสูงที่สุด

12. การขัดกันของลูกปืนล้อ (wheel bearing)

13. การล็อคของระบบขับเคลื่อน

14. รถด้านหน้าชนกับแท่นหยุดรถที่ปลายทางวิ่งบังคับ

เหตุการณ์ที่ 1 ถึง 7 ต้องถูกนำไปในการวิเคราะห์อันตรายตามตาราง 2-1 และไม่ถูกรวมในการคำนวณ SAZ ทั้งนี้ อัตราการหยุดรถไม่สามารถคำนวณได้อย่างแม่นยำสำหรับเหตุการณ์ที่ 1 ถึง 7

ในส่วนของอันตรายที่เหลืออื่นๆ ต้องถูกกำจัดด้วยการรวมอัตราการหยุดที่แย่ที่สุดในการคำนวณ SAZ หรือถูกนำไปในการวิเคราะห์อันตรายตามตาราง 2-1

ในการคำนวณอัตราการหยุดที่แย่ที่สุดต้องเลือกใช้น้ำหนักของขบวนรถที่ทำให้เกิดอัตราการหยุดที่แย่ที่สุด อีกทั้ง ต้องพิจารณาผลจากความลาดชัน โหลดของผู้โดยสารที่น้อยที่สุด แรงลมสูงสุด ขีดจำกัดการยึดเกาะและการขับเคลื่อนสูงสุด และความเร็วเริ่มต้นที่ต่ำที่สุด

ในการใช้ตาราง 2-1 ความถี่ของเหตุการณ์ในระบบ ATN ทั้งหมดต้องถูกคำนวณจากการใช้ชั่วโมงการวิ่งของขบวนรถตลอดปีต่อค่าพารามิเตอร์ตามการออกแบบที่กำหนด โดยที่ความรุนแรงของเหตุการณ์ที่ 1 ถึง 7 ต้องเป็น "I – เหตุการณ์รุนแรงมาก (Catastrophic) " ความรุนแรงของเหตุการณ์ที่ 8 ถึง 14 ต้องเป็นอย่างน้อยสุด "II – เหตุการณ์ร้ายแรง (Critical) " อีกทั้ง ความถี่ของเหตุการณ์ต้องถูกบรรเทาให้ไปสู่ระดับ "ยอมรับได้พร้อมแจ้งเตือนไปยังหน่วยงานที่มีอำนาจตัดสิน" ตามข้อ 2.2 ของมาตรฐาน APM

เหตุการณ์ที่กล่าวถึงทั้งหมดที่มีขบวนรถมากกว่าหนึ่งขบวน และวัตถุภายนอกต้องถูกพิจารณาว่าเป็น "I - เหตุการณ์รุนแรงมาก" และเหตุการณ์ที่กล่าวถึงทั้งหมดที่มีขบวนรถมากกว่าสองขบวน ต้องถือว่าเป็น "I - เหตุการณ์รุนแรงมาก" ทั้งนี้ อันตรายที่ไม่สามารถยอมรับได้ต้องถูกกำจัดด้วยการออกแบบ

หากต้องการเปลี่ยนระดับความรุนแรงของความล้มเหลวจาก "I - เหตุการณ์รุนแรงมาก" เป็น "II - เหตุการณ์ร้ายแรง" ต้องดำเนินการตามมาตรการด้านความปลอดภัยการชนทั้ง 3 มาตรการต่อไปนี้

1. ผู้โดยสารทุกคนต้องมีที่นั่งและอาจมีเข็มขัดนิรภัย โดยที่มีการเตือนทั้งเสียงและภาพเพื่อเตือนภัยให้รัดเข็มขัดนิรภัยก่อนการเดินรถ

2. ขบวนรถทุกขบวนต้องมีความปลอดภัยหากชนกับกำแพงแข็งที่อยู่กับที่ด้วยความเร็วครึ่งหนึ่งของความเร็วสูงสุด (รวมค่าความคลาดเคลื่อน)

3. ต้องมีการป้องกันผู้โดยสารจากการชนกระแทกภายในตัวรถ รวมถึงการป้องกันส่วนศีรษะผู้โดยสารสำหรับที่นั่งที่หันไปทางหน้ารถและที่หันไปทางหลังรถ และการใช้วัสดุดูดซับที่มีความทนทานต่อการกระแทก

นอกจากนี้ ระบบตรวจจับและกำจัดสิ่งกีดขวางอาจถูกนำใช้เพื่อลดความเสี่ยงจากวัตถุต่าง ๆ บนทางวิ่งบังคับ รวมถึงมีมาตรการความปลอดภัยอื่น ๆ ความคงทนของการออกแบบฮาร์ดแวร์ ซอฟต์แวร์ วิธีการบำรุงรักษา และขั้นตอนการทำงาน เพื่อควบคุมความเสี่ยงตามหัวข้อ 3.2

4.1.3 การตรวจจับการเคลื่อนที่ของขบวนรถโดยไม่ได้ตั้งใจ

ฟังก์ชันระบบ ATP ของระบบ APM ทั้งหมด ต้องตรวจจับการเคลื่อนไหวของขบวนรถที่เคลื่อนที่เองแบบไม่ได้ตั้งใจ

ระบบ ATP ต้องเริ่มการเบรกฉุกเฉินในกรณีที่พบว่าขบวนรถกำลังเคลื่อนที่โดยไม่ได้รับคำสั่งให้เคลื่อนที่ และเมื่อพบว่าขบวนรถกำลังเคลื่อนที่นอกเหนือจากที่ได้รับอนุญาต (การถอยหลัง) ต้องเริ่มการเบรกฉุกเฉินทันที

4.1.4 การป้องกันความเร็วเกินกำหนด (overspeed protection)

ฟังก์ชันระบบ ATP ของระบบ APM ทั้งหมด ต้องป้องกันความเร็วเกินกำหนด

แนวทางวิ่งบังคับ ข้อจำกัดทางโครงสร้าง และเงื่อนไขการเดินรถตามที่ระบบ ATP กำหนด เป็นตัวกำหนดความเร็วสูงสุดที่ได้รับอนุญาตของขบวนรถที่ตำแหน่งใด ๆ บนทางวิ่งบังคับ

ฟังก์ชันการป้องกันความเร็วเกินกำหนดต้องบังคับความเร็วให้ไม่เกินความเร็วของขบวนรถที่กำหนดไว้ทุกตำแหน่งบนทางวิ่งบังคับ และอุปกรณ์การป้องกันความเร็วเกินกำหนดต้องวัดความเร็วตามมาตราวัดความเร็วจริงของขบวนรถ หากความเร็วจริงของขบวนรถเกินค่าความเร็วที่กำหนด อุปกรณ์การป้องกันต้องสั่งเบรกฉุกเฉินทันที

4.1.5 การป้องกันการจอด/หยุดรถเกินระยะที่กำหนด (overtravel protection)

ฟังก์ชันระบบ ATP ของระบบ APM ที่อนุญาตให้ขบวนรถเคลื่อนที่อัตโนมัติไปถึงปลายทางต้องป้องกันการจอด/หยุดรถเกินระยะที่กำหนด

การป้องกันการจอด/หยุดรถเกินระยะที่กำหนด ต้องทำงานร่วมกับการป้องกันความเร็วเกินกำหนดเพื่อป้องกันขบวนรถไม่ให้เดินรถเกินปลายทางของทางวิ่งบังคับและป้องกันไม่ให้กระแทกกับกันชนที่ปลายทางวิ่งบังคับ (end-of-guideway buffer)

การออกแบบการป้องกันการจอด/หยุดรถเกินระยะที่กำหนด ต้องอ้างอิงตามการคำนวณระยะหยุดที่ใช้ในกรณีที่แย่ที่สุดรวมกันขององค์ประกอบที่เกี่ยวข้องตามข้อ 4.1.2.

4.1.6 การป้องกันขบวนรถแยกออกจากกัน (parted consist protection)

ฟังก์ชันระบบ ATP ของระบบ APM ที่ใช้ตัวรถต่อพ่วงกันสองคันหรือมากกว่าเพื่อประกอบเป็นขบวนรถ ต้องป้องกันขบวนรถแยกออกจากกัน โดยที่การป้องกันการแยกขบวนรถต้องใช้กับตัวรถที่ต่อพ่วงแบบถาวรหรือตัวรถที่ต้องแยกเป็นประจำสำหรับการซ่อมบำรุงหรือการเดินรถ

การป้องกันขบวนรถแยกออกจากกันต้องตรวจจับการแยกตัว การปลดล็อค และ/หรือการแยกตัวรถภายในขบวนและจะสั่งเบรกทันทีกับรถทุกคันในขบวนที่ต่อกันก่อนหน้า ให้หยุดสนิท

การตรวจจับการมีอยู่ของขบวนรถ หากมีการใช้ข้อกำหนดในข้อ 4.1.1 ต้องตรวจจับการมีอยู่และตำแหน่งที่แน่นอนของแต่ละขบวนที่แยกกันเท่าที่ทำได้ภายในเขตการแบ่งส่วนที่ตรวจจับขบวนรถ (presence detection segmentation)

4.1.7 การป้องกันสัญญาณสูญหาย (lost signal protection)

สัญญาณที่สำคัญต่อการทำงานของ ATP ของระบบ APM ทั้งหมด ต้องเป็นสัญญาณต่อเนื่องหรือมีลักษณะที่ทำซ้ำๆ โดยสามารถตรวจจับการขัดข้องของสัญญาณได้

เมื่อเกิดกรณีสัญญาณขัดข้องต้องสั่งการเบรกฉุกเฉินโดยระบบ ATP ให้ทันเวลา เพื่อไม่ให้เกิดความเสี่ยงต่อความปลอดภัยในการทำงานของระบบ ATP ใด ๆ ตามการออกแบบ

4.1.8 การตรวจจับความเร็วเป็นศูนย์ (zero speed detection)

ฟังก์ชันระบบ ATP ของระบบ APM ต้องตรวจจับความเร็วเป็นศูนย์เมื่อมีการหยุดของขบวนรถ

ความเร็วขบวนรถเป็นศูนย์ต้องยังไม่ขึ้นสถานะจนกว่าความเร็วจะลดลงจนมีค่าน้อยกว่าหรือเท่ากับ 0.30 เมตรต่อวินาที (0.95 ฟุตต่อวินาที) และมีการสั่งเบรก

4.1.9 การป้องกันการเปิดประตูที่ไม่ได้กำหนดไว้ (unscheduled door opening protection)

ฟังก์ชันระบบ ATP ของระบบ APM ทั้งหมด ต้องป้องกันการเปิดประตูที่ไม่ได้กำหนดไว้

หากประตูอัตโนมัติหรือประตูทางออกฉุกเฉินบนขบวนรถถูกปลดล็อกด้วยสาเหตุใดๆ ขณะที่ขบวนรถกำลังเคลื่อนที่ (มีความเร็วมากกว่าศูนย์ตามที่กำหนดไว้ในข้อ 4.1.8) ขบวนรถนั้นต้องเบรกทันทีจนหยุดสนิท

สำหรับระบบที่ติดตั้งประตูกั้นชานชาลา ต้องมีการป้องกันการเปิดประตูที่ไม่ได้กำหนดไว้ด้วยระบบ ATP เช่นกัน หากประตูอัตโนมัติใด ๆ ถูกปลดล็อกด้วยสาเหตุใด ๆ ต้องห้ามให้ขบวนรถเข้าหรือออกจากสถานีนั้น และต้องเบรกทันทีจนหยุดสนิท

ในกรณีของการเปิดประตูที่ไม่ได้กำหนดไว้ (ของขบวนรถหรือสถานี) ต้องกำหนดให้มีการรีเซ็ตด้วยมือโดยบุคคลที่ได้รับอนุญาตก่อนที่จะคืนสถานะการทำงานของขบวนรถแบบอัตโนมัติ

4.1.10 ระบบป้องกันการควบคุมการเปิดประตู (door control protection interlocks)

ระบบ ATP ของระบบ APM ทั้งหมด ต้องมีระบบป้องกันการควบคุมการเปิดประตู

การควบคุมการเปิดประตูนี้ต้องตรวจสอบว่าเงื่อนไขต่อไปนี้ ถูกปฏิบัติตามก่อนที่จะเปิดประตูขบวนรถแบบอัตโนมัติและประตูสถานี (หากมี)

1. ตำแหน่งของขบวนรถจอดตรงกับสถานีอย่างถูกต้องตามเกณฑ์ในข้อ 4.2.2
2. ตรวจจับความเร็วขบวนรถเป็นศูนย์
3. ปิดระบบขับมอเตอร์ และ
4. ขบวนรถถูกล็อคไว้ไม่ให้เคลื่อนที่ได้

สำหรับระบบ APM ที่ขบวนรถไม่สามารถหยุดได้โดยสมบูรณ์ เพื่อให้ผู้โดยสารที่ขึ้นลงเงื่อนไขต่อไปนี้ควรถูกปฏิบัติตามก่อนปลดล็อกและเปิดประตูขบวนรถและประตูสถานี (หากมี)

1. ความเร็วต้องไม่เกิน 0.35 เมตรต่อวินาที (1.1 ฟุตต่อวินาที)
2. อัตราเร่งและอัตราการกระชากต้องเป็นค่าที่ยอมรับได้โดยการวิเคราะห์ตามข้อกำหนดของข้อ 2.1.2.1 Hazard Analyses
3. ลำดับการเปิดประตูและปิดประตูทั้งหมดต้องเกิดภายในเขตที่กำหนดไว้ตามการวิเคราะห์ตามข้อ 2.1.2.1

4.1.11 ระบบป้องกันขบวนรถออกจากสถานี (departure interlocks)

ระบบ ATP ของระบบ APM ทั้งหมด ต้องมีระบบป้องกันขบวนรถออกจากสถานี

ขบวนรถที่จอดในสถานีต้องไม่ได้รับอนุญาตให้เคลื่อนที่จนกว่าประตูทั้งหมด (ขบวนรถและประตูสถานี(ถ้ามี)) จะถูกปิดและล็อคอย่างถูกต้อง ทั้งนี้ การป้องกันการเคลื่อนที่ต้องถูกปลดล็อคก่อนที่จะสั่งให้มอเตอร์ขับเคลื่อนทำงาน

สำหรับระบบ APM ที่ขบวนรถไม่ได้จอดสนิทให้ผู้โดยสารที่ขึ้นลง ระบบป้องกันขบวนรถออกจากสถานีต้องถูกใช้เพื่อหยุดขบวนรถไม่ให้ออกจากสถานีหากประตูทั้งหมดยังไม่ได้ปิดและล็อค

4.1.12 ระบบป้องกันขบวนรถเปลี่ยนทิศทางการเคลื่อนที่ (direction reversal interlocks)

ระบบ ATP ของระบบ APM ทั้งหมด ต้องป้องกันขบวนรถเปลี่ยนทิศทางการเคลื่อนที่บนทางวิ่งบังคับที่เป็นการเดินรถสองทิศทาง (bidirectional operation)

การเปลี่ยนทิศทางการเคลื่อนที่ขบวนรถต้องเกิดขึ้นหลังจากมีการตรวจจับความเร็วเป็นศูนย์เท่านั้น (ตามข้อ 4.1.8) และการเปลี่ยนทิศทางการเคลื่อนที่ต้องเกิดขึ้นโดยอัตโนมัติที่สถานีหรือเขตสิ้นสุดของทางวิ่งบังคับตามที่กำหนดจากการตั้งค่าของระบบ เพื่อรองรับโหมดการเดินรถแบบ pinched loop แบบ intermediate turnback loop แบบ reverse direction loop หรือแบบ shuttle modes

การเปลี่ยนทิศทางการเคลื่อนที่ขบวนรถต้องสามารถสั่งงานแบบมีคนขับ จากระบบควบคุมกลางได้ (remote manual command)

4.1.13 ระบบบังคับสัมพันธ์ของระบบขับเคลื่อนและเบรก (propulsion and braking interlocks)

ระบบ ATP ของระบบ APM ทั้งหมด ต้องมีการบังคับสัมพันธ์ของขับเคลื่อนและเบรกที่เชื่อมต่อกัน

ระบบเบรกฉุกเฉินต้องเป็นระบบที่ไม่สามารถยกเลิกได้ กล่าวคือ หากระบบเบรกฉุกเฉินเริ่มทำงาน ต้องคงการทำงานจนกระทั่งขบวนรถหยุดโดยสมบูรณ์ หลังจากขบวนหยุดจึงสามารถรีเซ็ตระบบเบรกฉุกเฉินให้กลับมาทำงานปกติเพื่อกลับมาดำเนินการต่อได้ สำหรับวิธีการรีเซ็ตที่ไม่ได้ระบุในบทที่ 4 วิธีการนี้ต้องถูกวิเคราะห์ตามข้อกำหนดที่ระบุไว้ในหัวข้อ 2.1.2.1 Hazard Analyses

หากเงื่อนไขที่กำหนดโดยระบบ ATP ไม่อนุญาตให้มีการเคลื่อนที่ของขบวนรถ การเบรกฉุกเฉินต้องยังคงทำงานไม่ว่าจะมีสัญญาณหรือการกระทำใด ๆ ในการรีเซ็ต ยกเว้นกรณีที่ต้องเปลี่ยนไปทำงานแบบมีคนขับ ซึ่งจะทำให้ฟังก์ชัน ATP ของขบวนนั้นถูกปิดใช้งาน หากเงื่อนไขของระบบ ATP ถูกต้องตรงตามที่กำหนดหลังจากเอาเบรกฉุกเฉินที่ไม่สามารถยกเลิกได้ออกแล้ว ขบวนรถต้องได้รับอนุญาตให้เคลื่อนที่ได้ แต่ถ้าหากเกิดขัดข้องขึ้นอีก การเบรกฉุกเฉินที่ไม่สามารถยกเลิกได้ต้องถูกใช้งานเช่นเดิม

ระบบควบคุมการเบรกฉุกเฉินต้องเชื่อมโยงกับการควบคุมการขับเคลื่อน โดยกำหนดให้คำสั่งเบรกฉุกเฉินมีอำนาจเหนือกว่า

4.1.14 การบังคับสัมพันธ์ของทางประแจ (guideway switch interlocks)

การบังคับสัมพันธ์ทางประแจต้องถูกกำหนดโดยระบบ ATP ของระบบ APM ที่มีการควบคุมขบวนรถโดยอัตโนมัติผ่านประแจที่ติดตั้งไว้ตามทางวิ่งบังคับ โดยที่กลไกการสับประแจที่ติดตั้งบนตัวรถต้องกำหนดการบังคับสัมพันธ์ทางประแจที่เทียบเท่ากับข้อกำหนดของหัวข้อนี้ ตามการวิเคราะห์ในหัวข้อ 2.1.2.1 Hazard Analyses

ระบบ ATP ต้องป้องกันขบวนรถไม่ให้เข้าทางประแจที่ไม่ได้ตั้งให้ถูกตำแหน่งและล็อคอย่างถูกต้อง และต้องป้องกันทางประแจไม่ให้ถูกปลดล็อคและ/หรือมีการเคลื่อนไหวเมื่อขบวนรถได้ถูกสั่งให้ออกตัวแล้ว

วงจรควบคุม (control circuits) ต้องอยู่ในลักษณะที่ประแจถูกล็อคไว้ให้ไม่สามารถรับสัญญาณเตรียมเส้นทางจนกว่าทางประแจจะถูกตรวจสอบและยืนยันว่าอยู่ในตำแหน่งที่ถูกต้อง กรณีที่เงื่อนไขของทางประแจไม่ถูกต้อง (ไม่ว่าทางประแจจะได้รับการเปิดใช้งานโดยอัตโนมัติหรือแบบมีคนขับ) สัญญาณควบคุมที่ถูกส่งให้กับขบวนรถที่กำลังเคลื่อนที่เข้ามา ต้องแน่ใจว่าขบวนรถที่กำลังเคลื่อนที่เข้ามาในโหมดอัติโนมัติต้องหยุดก่อนที่จะถึงทางเข้าทางประแจ

เมื่อขบวนรถอยู่ในเขตที่มีการป้องกันทางประแจหรือชุดทางประแจ การล็อคเส้นทาง (route locking) ต้องป้องกันการเคลื่อนไหวอัตโนมัติหรือการเคลื่อนไหวด้วยระบบควบคุมระยะไกลแบบมีคนขับ ของทางประแจใด ๆ ในเขตที่ได้รับการป้องกัน และต้องป้องกันการเคลื่อนที่ของขบวนรถที่เกิดความขัดแย้งกันในระบบ

การล็อคด้วยการตรวจจับการมีอยู่ของขบวนรถ (presence detection locking) ต้องถูกใช้งานเพื่อป้องกันการเคลื่อนที่ของทางประแจหากมีขบวนรถเคลื่อนที่อยู่บริเวณนั้น ไม่ว่าประแจจะทำงานในโหมดอัตโนมัติหรือควบคุมระยะไกลแบบ มีคนบังคับ

การล็อคเวลา (time locking) กับการปลดล็อคหลังจากล็อคเวลา (approach release) ต้องถูกใช้ในวงจรการสับประแจ โดยที่หากส่วนของทางเข้าประแจได้รับการเคลียร์ทางสำหรับการเคลื่อนที่ผ่านประแจนั้น ซึ่งมีความเร็วเข้าใกล้ทางประแจเป็นศูนย์และประแจมีสถานะว่าง ประแจต้องไม่สามารถเคลื่อนที่ได้จนกว่าจะผ่านเวลาที่แน่นอนไปแล้ว ทั้งนี้ ค่าเผื่อเวลา (time allowance) ต้องกำหนดไว้อย่างน้อยร้อยละ 10 ของเวลาที่ขบวนรถเคลื่อนที่ไปตามระยะหยุด (stopping distance) ซึ่งคำนวณตามข้อ 4.1.2 โดยถ้ามีการใช้การปลดล็อคหลังจากล็อคเวลา (approach release) เวลาสามารถเป็นศูนย์ได้หากไม่มีส่วนใดส่วนหนึ่งของขบวนอยู่บนทางนั้น (approach section) ซึ่งความยาวของส่วนใดส่วนหนึ่งของขบวนบนทางประแจ (approach section) ต้องมากกว่าระยะเบรคในกรณีที่แย่ที่สุดที่ใช้หยุดบนทางวิ่งบังคับนั้น

ระบบ ATP ต้องป้องกันการปลดล็อกทางประแจโดยอัตโนมัติหรือจากระยะไกลแบบ มีคนบังคับ หลังจากที่ขบวนรถเตรียมการเคลื่อนที่ผ่านไปจนกระทั่งขบวนรถผ่านไปแล้ว และมีระบบป้องกันเพื่อไม่ให้เกิดการปลดล็อกโดยไม่ตั้งใจจากการสูญเสียพลังงานชั่วขณะหรือสูญเสียการตรวจจับขบวนรถชั่วคราว

4.1.15 การทำงานในเขตออฟไลน์—เงื่อนไขพิเศษ เขตออฟไลน์เป็นส่วนของทางวิ่งบังคับที่มีการทำงานอัตโนมัติซึ่งควบคุมความเร็ว เช่น สถานีนอกเส้นทาง (offline station) หรือพื้นที่จัดเก็บรถ (storage areas) โดยการทำงานในเขตออฟไลน์นี้ พิจารณาเป็นโซนได้ดังนี้

1. เขตเปลี่ยนผ่านจากเส้นทางหลัก (transition zone)
2. เขตหมุนเวียน (circulation zone)
3. เขตการจอด (docking zone)

เขตเปลี่ยนผ่าน (transition zoce) เมื่อเข้าหรือออกจากเส้นทางหลักหรือออกจากเขตออฟไลน์ ตัวรถต้องถูกตรวจจับโดยระบบ ATP ของเขตออฟไลน์ และความเร็วต้องถูกปรับให้เหมาะสม ทั้งนี้ การเคลื่อนที่ของขบวนรถระหว่างเส้นหลักและเขตออฟไลน์ต้องดำเนินการตามข้อที่ 4.1.14

เขตหมุนเวียน (circulation zone) เป็นบริเวณจุดเชื่อมต่อระหว่างตัวรถที่กำลังเคลื่อนที่ 2 คัน ที่อนุญาตให้ใช้ความเร็วต่ำภายใต้เงื่อนไขที่มีความล้มเหลวเกิดขึ้นเท่านั้น ตามข้อกำหนดในข้อ 2.1.2.1 เพื่อป้องกันไม่ให้เกิดความเสียหายต่อตัวรถ (อาจใช้ตัวดูดซับแรงกระแทกแบบย้อนกลับได้) และป้องกันไม่ให้ผู้โดยสารเกิดการบาดเจ็บ (ผลกระทบจากการชนต้องตรงตามเกณฑ์ทั้งหมดใน

มขร. – R – 007 - 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านเครื่องกลและตัวรถ ข้อ 2.4.4.9.2) ทั้งนี้ ความเร็วของจุดเชื่อมต่อที่อนุญาตต้องกำหนดโดยระบบ ATP

เขตการจอด (docking zone) เป็นบริเวณจุดเชื่อมต่อระหว่างรถที่กำลังเคลื่อนที่และรถที่หยุดที่จุดจอด (พร้อมประตูเปิดและเบรกทำงานตามข้อ 4.1.8) อาจยอมรับได้ในความเร็วต่ำที่อนุญาตให้ใช้ความเร็วต่ำภายใต้เงื่อนไขที่มีความล้มเหลวเกิดขึ้นเท่านั้น ตามข้อกำหนดในข้อ 2.1.2.1 เพื่อ

(1) ป้องกันไม่ให้เกิดความเสียหายต่อตัวรถ (อาจใช้ตัวดูดซับแรงกระแทกแบบย้อนกลับได้)

(2) ป้องกันไม่ให้ผู้โดยสารเกิดการบาดเจ็บ (ผลกระทบจากการชนต้องตรงตามเกณฑ์ทั้งหมดใน มขร. – R – 007 - 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านเครื่องกลและตัวรถ ข้อ 2.4.4.9.2) และ

(3) ป้องกันไม่ให้เกิดการเคลื่อนที่ของรถที่หยุดนิ่ง

ความปลอดภัยของผู้โดยสารที่อยู่บนชานชาลาและการขึ้นลงขบวนรถจะต้องเป็นไปตาม มขร. – C – 010 - 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติโครงสร้างพื้นฐานและงานโยธา ข้อ 2.2 การป้องกันที่ขอบชานชาลา และการป้องกันการควบคุมประตูและการล็อคการออกจากสถานีจะต้องเป็นไปตามข้อ 4.1.10 และ 4.1.11 ตามลำดับ

4.2 ฟังก์ชันการเดินรถอัตโนมัติ (ATO)

ระบบ ATO จะต้องมีการเดินรถโดยอัตโนมัติรอบระบบตามเกณฑ์การทำงานที่กำหนดไว้แต่อยู่ภายใต้ข้อจำกัดด้านความปลอดภัยที่เป็นผลมาจากระบบ ATP

4.2.1 ควบคุมการเคลื่อนที่ การเริ่มต้น การหยุดและการควบคุมความเร็วของขบวนรถขณะเคลื่อนที่ตลอดทางวิ่งบังคับ ต้องถูกควบคุมโดยระบบ ATO โดยที่มีความเร่ง การชะลอความเร็วและการกระชากอยู่ในระดับความสบายของผู้โดยสารที่สามารถยอมรับได้ และความเร็วต้องถูกรักษาให้ต่ำกว่าความเร็วเกินกำหนด (overspeed limits) ที่มาจากระบบ ATP

4.2.2 การจอดที่สถานีตามที่ตั้งโปรแกรม ต้องอยู่ในระดับความสบายของผู้โดยสารที่สามารถยอมรับได้ และในขณะที่มีการขึ้นและลงขบวนของผู้โดยสาร ประตูขบวนรถจะต้องมีช่องเปิดที่ชัดเจนอย่างน้อย 82 เซนติเมตร (32.5 นิ้ว) ในเขตที่กำหนดไว้สำหรับการขึ้นรถ (boarding zone) โดยที่ช่องเปิดนี้ต้องอนุญาตให้ผู้โดยสารออกไปยังชานชาลาเท่านั้น

หากประตูรถและประตูสถานีไม่ได้จอดตรงตามระยะทางที่อนุญาต ประตูต้องไม่เปิดโดยอัตโนมัติ และต้องส่งสัญญาณเตือนไปยังศูนย์ควบคุมส่วนกลาง

4.2.3 ควบคุมประตูและเวลารถหยุดในสถานี (dwell time) ประตูรถต้องถูกควบคุมอัตโนมัติโดยระบบ ATO โดยในขณะที่ผู้โดยสารขึ้นและลง หากมีประตูอัตโนมัติที่สถานี ต้องถูกควบคุมเป็นชุดที่เข้าคู่กับประตูรถ ซึ่งประตูรถและประตูสถานีที่จับคู่กัน ต้องเปิดและปิดพร้อมกัน

ระบบนี้ต้องสามารถปิดการทำงานของชุดประตูใด ๆ (บนรถหรือที่สถานี) ได้ด้วยวิธีมีคนขับ โดยที่ไม่มีผลกระทบต่อการทำงานแบบอัตโนมัติของชุดประตูอื่นที่ไม่ได้รับผลกระทบ

ในกรณีที่มีประตูอัตโนมัติที่สถานีและชุดประตู (ของรถหรือที่สถานี) ไม่สามารถใช้งานได้ ชุดประตูที่จับคู่กันนั้นต้องถูกปิดใช้งานตามการทำงานอัตโนมัติด้วย แต่ยังใช้งานแบบมีคนขับ ได้

หากประตูเกิดขัดข้องในการเปิดหรือปิดภายใน 10 วินาทีหลังจากได้รับคำสั่ง ต้องมีการส่งสัญญาณเตือนไปยังศูนย์ควบคุมส่วนกลาง

ระยะเวลาที่ขบวนรถอยู่ในสถานีและระยะเวลาประตูเปิด ต้องถูกกำหนดจากผู้ออกแบบระบบและมีการควบคุมอัตโนมัติด้วยระบบ ATS ซึ่งเป็นฟังก์ชันการทำงานอัตโนมัติเต็มรูปแบบ โดยที่เมื่อเวลาเปิดประตูหมดลงและคำสั่งที่ให้ประตูเปิดค้างไว้ (hold door open) จากระบบ ATS หรือผู้ควบคุมที่ศูนย์ควบคุมส่วนกลางถูกนำออกแล้ว ต้องมีคำสั่งให้ปิดประตูทั้งหมด

เมื่อขบวนรถที่ควบคุมแบบมีคนขับ จอดในสถานีและผู้ควบคุมรถสั่งให้ประตูรถเปิดหรือปิด หากมีการใช้ประตูที่สถานี ต้องมีการเปิดหรือปิดตามไปด้วย หรือปฏิบัติตามคู่มือปฏิบัติงาน (operation manual)

4.3 ฟังก์ชั่นระบบติดตามการเดินรถอัตโนมัติ (ATS)

ระบบ ATS ต้องติดตามและจัดการการเดินรถโดยรวมของระบบ โดยระบบ ATS ต้องจัดให้มีการเชื่อมต่อระหว่างระบบและผู้ปฏิบัติการควบคุมส่วนกลาง การแสดงภาพและเสียง โดยที่ข้อมูลต้องถูกนำเสนอสถานะของระบบแบบเวลาจริง (real-time) ซึ่งข้อมูลนี้ต้องช่วยให้ผู้ปฏิบัติการควบคุมส่วนกลางประเมินสภาวะทั่วทั้งระบบและดำเนินการตามความเหมาะสมได้ ผู้ปฏิบัติงานควบคุมส่วนกลางต้องสามารถออกคำสั่งเพื่อเริ่มและยุติการทำงานของระบบได้ มีการแทนที่คำสั่งอัตโนมัติและการทำงานที่เลือก และทำหน้าที่จัดการระบบอื่นๆ

สำหรับระบบ APM ที่ไม่มีสถานที่ตั้งศูนย์ควบคุมส่วนกลาง สัญญาณเตือนและความผิดปกติข้อมูลจะต้องถูกส่งไปยังบุคคลที่รับผิดชอบซึ่งมีอำนาจตอบสนองต่อสถานการณ์ได้ทันท่วงที

4.3.1 ข้อจำกัดของระบบ ATS

หาก ATS ไม่ทำงานด้วยเหตุผลใดก็ตาม ระบบ ATP และระบบ ATO ต้องยังคงทำงานได้ เว้นแต่จะมีการสั่งปิดระบบโดยผู้ปฏิบัติงานศูนย์ควบคุมส่วนกลาง ทั้งนี้ การควบคุมเหตุฉุกเฉินบนคอนโซลควบคุมส่วนกลางต้องเป็นอิสระจากอุปกรณ์ ATS โดยมีฟังก์ชันการปิดระบบฉุกเฉินอย่างน้อย 2 ฟังก์ชัน ได้แก่

(1) การหยุดขบวนรถทุกขบวน และ

(2) การปิดกำลังขับเคลื่อนทั้งหมด

4.3.2 การติดตามสถานะและการปฏิบัติงาน ข้อมูลการปฏิบัติงานและสถานะของระบบต้องนำเสนอต่อผู้ปฏิบัติงานศูนย์ควบคุมส่วนกลาง โดยแยกส่วนจอแสดงผลเป็นจอแสดงผลการทำงานของระบบ (system operations display) และจอแสดงผลแผนผังกำลังไฟฟ้า (Power Schematic Display)

4.3.2.1 จอแสดงผลการทำงานของระบบ (system operations display)

จอแสดงผลการทำงานของระบบต้องแสดงภาพการทำงานแบบ real-time ทั่วทั้งระบบ โดยที่การออกแบบจอแสดงผลต้องมีสิ่งต่อไปนี้

(1) มีขนาดและ/หรือปริมาณที่เพียงพอและมีความละเอียดของจอแสดงผลที่สามารถเห็นได้สะดวกจากบริเวณที่นั่งปกติบริเวณคอนโซลควบคุมส่วนกลางของผู้ควบคุมเครื่อง

(2) แสดงผลแผนผังโดยรวมของทางวิ่งบังคับและตำแหน่งของพื้นที่ทำงานทางกายภาพที่เกี่ยวข้อง เช่น สถานีผู้โดยสาร ทางประแจ และ/หรือศูนย์ซ่อมบำรุงและลานจัดเก็บ

(3) รายงานสภาพการทำงานของระบบในเวลาจริงที่เกี่ยวข้องกับการกำหนดค่าของระบบ ดังนี้

(ก) ที่ตั้งและการระบุขบวนรถทุกขบวนในทุกส่วนของระบบที่ออกแบบให้ทำงานอัตโนมัติ

(ข) ทิศทางการเดินรถของขบวนที่ยังวิ่งอยู่ทั้งหมด

(ค) จำนวนตู้ที่ประกอบกันในแต่ละขบวน (หากมีการประกอบของขบวนที่หลากหลาย)

(ง) หมายเลขประจำขบวนรถที่ใช้โต้ตอบกับขบวนรถ (หากหมายเลขประจำขบวนรถไม่มีความชัดเจนจากการกำหนดค่าของระบบ)

(จ) สถานะของทางประแจในระบบ

(ฉ) โหมดการทำงานและสถานะของอุปกรณ์ของระบบที่เลือก

(ช) สถานะของแต่ละสถานี รวมถึงสถานีที่ใช้งานอยู่ในขณะนั้น

(4) มีการทำงานร่วมกับอุปกรณ์ช่วยการมองเห็นอื่น ๆ ตามความจำเป็นเพื่ออนุญาตให้ผู้ปฏิบัติงานศูนย์ควบคุมส่วนกลางจัดการระบบได้อย่างมีประสิทธิภาพ

4.3.2.2 จอแสดงผลแผนผังกำลังไฟฟ้า (Power Schematic Display: PSD) ต้องจัดให้มีการแสดงภาพสถานะการจ่ายพลังงานทั่วทั้งระบบ โดย PSD ต้องมีขนาด จำนวนและความละเอียดในการแสดงผลเพียงพอต่อการมองเห็นได้ง่ายจากบริเวณที่นั่งปกติบริเวณที่คอนโซลผู้ควบคุมเครื่อง

PSD ต้องแสดงเงื่อนไขดังต่อไปนี้อย่างชัดเจนเป็นอย่างน้อย

(1) การมีหรือการไม่มีพลังงานไฟฟ้าในวงจรกำลังขับเคลื่อนทุกวงจรที่สามารถเปิดหรือปิดได้ในแต่ละวงจร

(2) การมีหรือการไม่มีพลังงานที่จ่ายไฟตามแต่ละส่วนของทางวิ่งบังคับที่สามารถเปิดหรือปิดได้แต่ละวงจร

(3) สถานะของ circuit breaker และ/หรือสวิตช์ของระบบจ่ายไฟทั้งหมด (หากมีการสะดุดใด ๆ ต้องมีแจ้งเตือน)

(4) การมีหรือไม่มีพลังงานสำรอง (backup power)

(5) การแสดงเงื่อนไขการแจ้งเตือนใด ๆ

ตัวบ่งชี้ (indication) ของสถานะกำลังไฟฟ้าต้องมาจากการตรวจวัดแรงดันไฟฟ้าและการระบุตำแหน่งอุปกรณ์ โดยที่ตัวบ่งชี้และการควบคุมของ PSD ต้องไม่ได้รับผลกระทบจากความล้มเหลวของใดๆ ในระบบ (single-point failure)

4.3.3 การควบคุมและการแทนที่การทำงาน การจัดการและการทำงานของระบบต้องถูกดำเนินการด้วยฟังก์ชันการควบคุมและการแทนที่ (override) โดยต้องมีทั้งการควบคุมแบบอัตโนมัติและการเริ่มต้นการควบคุมและการแทนที่แบบมีคนขับ ตามที่อธิบายในส่วนนี้

4.3.3.1 ฟังก์ชันการควบคุมอัตโนมัติ ระบบ ATS ต้องมีฟังก์ชันการควบคุมและการประสานงานที่จำเป็น เพื่อทำให้การทำงานของระบบเป็นการดูแลแบบอัตโนมัติอย่างสมบูรณ์

4.3.3.1.1 การจัดการโหมดในการทำงาน (mode management)

ระบบ ATS ต้องบริหารจัดการทุกโหมดการทำงานที่ระบุ ซึ่งโหมดที่มีการใช้อยู่นั้นต้องขึ้นอยู่กับเทคโนโลยีของระบบ การกำหนดรูปแบบของทางวิ่งบังคับ แผนการเดินรถ และแผนการรีเซตโหมดเมื่อเกิดความล้มเหลว

4.3.3.1.2 การติดตามขบวนรถ (train tracking)

ระบบ ATS ต้องติดตามแต่ละขบวนทั้งระบบตามความเหมาะสมของรูปแบบของระบบ และเป็นไปตามข้อกำหนดการบริหารโหมดการทำงานที่กำหนดไว้

4.3.3.1.3 การจัดการระยะเวลาระหว่างขบวน (headway management)

เพื่อให้มีความสอดคล้องกับโหมดการทำงานที่เลือกและระดับการควบคุมขบวนรถแบบโต้ตอบกัน (interactive train regulation) ระบบ ATS ต้องรักษาระยะเวลาเท่าที่จำเป็นตามการวัดที่จุดคงที่บนทางวิ่งบังคับ และ/หรือระยะห่างระหว่างขบวนในการทำงานแบบอัตโนมัติในระบบ

4.3.3.1.4 การกำหนดเส้นทางของขบวนรถ (train routing)

ระบบ ATS ต้องกำหนดเส้นทางที่จำเป็นโดยอัตโนมัติตามโหมดการทำงานที่เลือก ชุดฟังก์ชันเหล่านี้ต้องรวมไปถึงการขอเส้นทาง ท่าประแจและคำขอการเปลี่ยนทิศทางการเดินรถตามความเหมาะสม

4.3.3.2 ฟังก์ชันการควบคุมและการแทนที่แบบมีคนขับ ความสามารถและฟังก์ชันที่อธิบายในส่วนนี้ต้องถูกรวมอยู่ในคอนโซลควบคุมส่วนกลาง โดยที่การควบคุมและการแสดงผลที่เกี่ยวข้องกับระบบ ATC ต้องรวมอยู่กับการควบคุมและการแสดงผลของระบบสื่อสาร (ตามบทที่ 5 การสื่อสารด้วยเสียงและภาพ) และระบบไฟฟ้า (ตามหัวข้อที่ 4.3.2.2 จอแสดงผลแผนผังกำลังไฟฟ้า) เพื่อให้การจัดการทุกระบบเป็นไปอย่างมีประสิทธิภาพโดยผู้ปฏิบัติการคนเดียวที่หน้าคอนโซล

ต้องมีการควบคุมแบบ มีคนบังคับ เพื่อให้ผู้ปฏิบัติการควบคุมส่วนกลางทำหน้าที่ดังต่อไปนี้

(1) การส่งขบวนรถ (train dispatching) ผู้ปฏิบัติการศูนย์ควบคุมส่วนกลางต้องสามารถส่งขบวนรถในการให้บริการจากจุดปล่อยภายนอกที่กำหนดได้

(2) การกำหนดเส้นทาง (train routing) โดยขึ้นอยู่กับการกำหนดค่าของระบบ ซึ่งระบบ ATS ต้องถูกออกแบบให้แต่ละขบวนสามารถกำหนดโหมดการทำงานหรือเส้นทางวิ่งบังคับ ผ่านคำสั่งจากผู้ปฏิบัติการควบคุมส่วนกลางได้

(3) เริ่มการให้บริการ (initiation of service) ผู้ปฏิบัติการควบคุมส่วนกลางต้องสามารถเริ่มการให้บริการของระบบได้

(4) สิ้นสุดการให้บริการ (termination of service) ผู้ปฏิบัติการควบคุมส่วนกลางต้องสามารถสิ้นสุดการให้บริการของระบบได้

(5) ปรับเปลี่ยนการทำงานของขบวนรถ (modify train operations) ผู้ปฏิบัติการควบคุมส่วนกลางต้องสามารถให้คำสั่งที่ปรับเปลี่ยนการทำงานตามปกติของขบวนรถได้

(6) นำขบวนรถออกจากระบบ (remove trains) สำหรับระบบที่มีการจัดเก็บนอกเส้นทาง (off-line storage) ผู้ปฏิบัติการควบคุมส่วนกลางต้องสามารถสั่งให้ขบวนรถออกจากบริการได้

(7) เริ่มการทำงานโหมดความล้มเหลว (initiate failure mode operatins) ผู้ปฏิบัติการควบคุมส่วนกลางต้องสามารถแปลงระบบจากโหมดการทำงานปกติไปยังโหมดการทำงานทางเลือกที่มีไว้สำหรับการจัดการความล้มเหลว

(8) ควบคุมการจอดขบวนรถ (hold trains) ผู้ปฏิบัติการควบคุมส่วนกลางต้องสามารถสั่งให้ขบวนรถจอดพักที่สถานีได้

(9) คำสั่งประแจ (command switches) เมื่อมีการทำงานของประแจ ผู้ปฏิบัติการควบคุมส่วนกลางต้องสามารถสั่งการประแจแต่ละอันให้เคลื่อนที่ได้

(10) หยุดขบวนรถทั้งหมด (stop all trains) ผู้ปฏิบัติการควบคุมส่วนกลางต้องสามารถหยุดขบวนรถทั้งหมดบนทางวิ่งบังคับด้วยคำสั่งเดียวได้

(11) คำสั่งปิดหรือเปิดพลังงานไฟฟ้า (command power off or on) ผู้ปฏิบัติการควบคุมส่วนกลางต้องสามารถสั่งให้พลังงานขับเคลื่อนปิดหรือเปิดให้กับระบบทั้งหมดหรือวงจรไฟฟ้าบางส่วนได้โดยขึ้นอยู่กับการแบ่งส่วนพื้นที่ให้บริการ

(12) ยืนยันและประมวลผลการแจ้งเตือน (acknowledge and process alarms) ผู้ปฏิบัติการควบคุมส่วนกลางต้องสามารถรับ จัดเก็บ และเรียกคืนการแสดงข้อความเตือนจากระบบย่อยหลายระบบ และรับทราบเสียงเตือนที่มาพร้อมกันได้

ทั้งนี้ ได้ยกเว้นสำหรับคำสั่งเหตุการณ์เดียว (single-event command) โดยหากมีคำสั่งหนึ่งจากผู้ปฏิบัติการควบคุมส่วนกลางและได้รับการยินยอมจากระบบ ATS การดำเนินการนั้นต้องยังคงมีผลใช้งานจนกว่าจะถูกยกเลิกจากผู้ปฏิบัติการในภายหลัง

4.3.3.3 สัญญาณเตือนและการรายงานความผิดปกติ ส่วนประกอบสำคัญของระบบต้องถูกติดตามโดยอัตโนมัติ และต้องมีการแจ้งเตือนเมื่อมีความผิดปกติและความล้มเหลวของส่วนเหล่านั้น นอกจากนี้ สิ่งอำนวยความสะดวกที่เกี่ยวข้องกับระบบต่างๆ ต้องถูกติดตามเช่นเดียวกัน รวมถึงมีการแจ้งเตือนเมื่อพบปัญหาเกี่ยวกับเพลิงไหม้และความปลอดภัยต่อชีวิต และ/หรือการบุกรุก

คอนโซลควบคุมส่วนกลางต้องมีทั้งการแสดงรายละเอียดของเหตุการณ์ (ข้อความ) และเสียงเตือน เพื่อเป็นประโยชน์ต่อผู้ปฏิบัติการควบคุมส่วนกลาง โดยที่ภายใน 2 วินาที หลังจากตรวจพบเหตุการณ์หรือเงื่อนไขที่เกิดขึ้น ข้อมูลเหตุการณ์นั้นต้องถูกรายงานบนหน้าจอ โดยระบุเวลาของเหตุการณ์ ลักษณะและเงื่อนไขของเหตุการณ์ ระบุตัวรถและขบวนรถ และ/หรือตำแหน่งที่เฉพาะเจาะจงบนทางวิ่งบังคับหรือสถานี ซึ่งแต่ละการแจ้งเตือนต้องถูกจัดทำรายการดัชนีและมีการติดตามเวลา (time-tagged) ที่ตรวจพบข้อผิดพลาด โดยที่สัญญาณเตือนภัยต้องถูกจัดเก็บและความสามารถเรียกคืนและ/หรือแสดงผลซ้ำด้วยหมายเลขดัชนีหรือตามประเภทฮาร์ดแวร์ที่เกี่ยวข้อง (เช่น ขบวนรถ สถานีย่อย สถานีโดยสารหรือประแจ)

การตอบรับสัญญาณเตือนจากผู้ปฏิบัติการควบคุมส่วนกลางต้องทำให้เสียงเตือนหยุดลง อย่างไรก็ตาม การแจ้งเตือนที่เกี่ยวข้องต้องยังอยู่จนกว่าสถานการณ์จะได้รับการแก้ไข ซึ่งการรายงานสัญญาณเตือนทั้งหมดและการเคลียร์ข้อมูลต้องถูกบันทึกไว้ในหน่วยความจำและพิมพ์บนเครื่องพิมพ์บรรทัด (line printer)

การสื่อสารข้อมูลระหว่างศูนย์ควบคุมส่วนกลางและขบวนรถต้องได้รับการจัดเก็บและมีการยืนยันข้อมูล โดยหากไม่มีขบวนรถตอบสนองต้องแจ้งเตือนไปยังศูนย์ควบคุมส่วนกลาง

4.3.3.3.1 การแจ้งเตือนระบบ การขัดข้องในการทำงาน การแจ้งเตือนและการรายงานผลของระบบ ต้องมีเพื่อรักษาความปลอดภัย ให้มีความปลอดภัยของระบบและแจ้งปัญหาการหยุดทำงานโดยที่ไม่ได้แจ้งเตือนล่วงหน้า

อย่างน้อยที่สุด การขัดข้องในการทำงานของระบบต้องถูกรายงานอย่างใดอย่างหนึ่งจาก 2 ประเภทต่อไปนี้ โดยที่การจัดประเภทและการรายงานข้อบกพร่องต้องมีรายละเอียดเพียงพอเพื่อให้บุคลากรที่ดำเนินการและซ่อมบำรุงสามารถตัดสินใจได้ตรงกับความต้องการในแผนการดำเนินงาน ขั้นตอนและคู่มือ

การขัดข้องระดับ I ก่อให้เกิดความเสี่ยงทันทีต่อความปลอดภัยของผู้โดยสารและ/หรือความเสี่ยงที่จะเสียหายต่ออุปกรณ์ของระบบ

การขัดข้องระดับ II ไม่ก่อให้เกิดความเสี่ยงทันที แต่อาจทำให้เกิดความเสี่ยงต่อผู้โดยสารหรืออุปกรณ์ได้ หากไม่ได้รับการแก้ไขเร็ว ๆ นี้

4.3.3.3.2 สัญญาณเตือนเหตุการณ์เพลิงไหม้และการบุกรุก หากมีการแจ้งเตือนเกี่ยวกับเหตุการณ์เพลิงไหม้และ/หรือควัน และการบุกรุก ต้องถูกประกาศแยกต่างหากและมีการทำควบคู่กันทั้งทางเสียงและภาพ บนคอนโซลควบคุมส่วนกลาง โดยต้องระบุตำแหน่งของจุดแจ้งเตือนด้วย

4.3.3.4 การบันทึกและรายงานข้อมูล ระบบย่อยของระบบ ATS ต้องมีการบันทึกข้อมูลที่เลือกไว้ระหว่างศูนย์ควบคุมส่วนกลางและส่วนอื่น ๆ ของระบบ โดยข้อมูลเหล่านี้ต้องถูกบันทึกในรูปแบบที่มีวันที่และเวลาที่แน่นอนของการส่งข้อมูลแต่ละครั้ง และเก็บไว้ในรูปแบบที่เหมาะสมทั้งไฟล์ถาวรและมีการเข้าถึงได้แบบสุ่ม อีกทั้ง เพื่อใช้กับซอฟต์แวร์ประมวลผลข้อมูลของระบบในการสร้างรายงานผล (หากมี) ทั้งนี้ ชุดข้อมูลที่บันทึกไว้นี้ต้องสามารถพิมพ์ได้แบบ real-time บนเครื่องพิมพ์ที่ศูนย์ควบคุมจากส่วนกลาง โดยเอกสารที่พิมพ์ออกมานี้ต้องประกอบไปเป็นบันทึกการปฏิบัติงานประจำวัน (daily operations log)

4.4 ข้อจำกัดในการทำงานแบบมีคนขับ

มาตรฐานนี้ได้รับการออกแบบมาเพื่อให้บริการในโหมดการทำงานแบบอัตโนมัติเท่านั้น และไม่ได้มีการให้บริการโดยใช้โหมดมีคนขับ เป็นระยะเวลานาน โดยที่การทำงานในโหมดมีคนขับ อาจถูกใช้สำหรับการทดสอบ การกู้คืนระบบ การซ่อมบำรุงและการจัดการความล้มเหลวของระบบ หรือสถานการณ์ที่ผิดปกติอื่น ๆ ซึ่งกระบวนการแก้ปัญหาความเสี่ยงตามข้อ 2.1.2 ต้องทำการคำนึงถึงความเสี่ยงที่เกี่ยวข้องกับการให้บริการในโหมดมีคนขับ

สำหรับการให้บริการในโหมดมีคนขับ ที่มีข้อจำกัดนั้น การออกแบบระบบต้องทำให้ผู้ปฏิบัติการสามารถสังเกตเห็นเงื่อนไขของทางวิ่งบังคับ มีการสื่อสารกับศูนย์ควบคุมส่วนกลางและผู้โดยสาร สามารถสังเกตเห็นสถานะของตัวรถและควบคุมการขับเคลื่อนของตัวรถ การเบรกและประตูได้เมื่อไม่ได้มีการใช้งานโดยที่ตัวควบคุมและตัวบ่งชี้สถานะต้องไม่ให้ผู้โดยสารเข้าถึงได้

บทที่ 5
การสื่อสารด้วยเสียงและภาพ

อุปกรณ์สื่อสารด้วยภาพและเสียงทั้งหมดต้องทำงานโดยอิสระจากพลังงานไฟฟ้าของทางวิ่งบังคับ และต้องทำงานอย่างเต็มที่ภายใต้สภาวะแวดล้อมที่อาจสัมผัสกับอากาศภายนอกได้ ทั้งนี้ อุปกรณ์สื่อสารด้วยภาพและเสียงทั้งหมดที่กำหนดโดยมาตรฐานนี้ต้องมีพลังงานสำรองเป็นระยะเวลาตามที่กำหนดในหัวข้อที่ 2.1.2.1 การวิเคราะห์อันตราย

5.1 การสื่อสารด้วยเสียง

ต้องจัดให้มีสิ่งอำนวยความสะดวกและอุปกรณ์เพื่อให้สามารถสื่อสารด้วยเสียงระหว่างผู้ควบคุมที่ศูนย์ควบคุมส่วนกลางกับ (1) ผู้โดยสารและ (2) เจ้าหน้าที่ปฏิบัติการและซ่อมบำรุงที่อยู่ทั่วทั้งระบบ

ระบบการสื่อสารด้วยเสียงและระบบเสียงประกาศสาธารณะที่จำเป็นทั้งหมดในที่นี้ ต้องเป็นไปตามข้อกำหนดในหัวข้อที่ 5.1.6

5.1.1 เสียงประกาศสาธารณะของสถานี

ระบบเสียงประกาศสาธารณะของสถานีจะต้องทำให้สามารถประกาศสดจากศูนย์ควบคุมส่วนกลางไปยังพื้นที่สาธารณะทั้งหมดของชานชาลาบนสถานีได้

ถ้ามีการใช้ข้อความสด (live message) ต้องประกาศแทนข้อความที่บันทึกไว้ล่วงหน้า ซึ่งลำโพงทุกตัวในเขตสถานีต้องประกาศพร้อมกันเมื่อได้เลือกสถานีหรือเขตนั้น และการแบ่งเขตระบบเสียงประกาศสาธารณะต้องครอบคลุมพื้นที่สาธารณะทั้งหมดของแต่ละสถานีอย่างครบถ้วน

5.1.2 ระบบการสื่อสารฉุกเฉินบนสถานีและอุปกรณ์ข้างทาง (emergency station and wayside communications)

ต้องมีการสื่อสารด้วยเสียงกรณีฉุกเฉินแบบสองทิศทางที่ได้เชื่อมโยงศูนย์ควบคุมส่วนกลางกับสถานีของผู้โดยสารทั้งหมดและ blue light station [ตามที่ระบุในหัวข้อที่ 10.4 ของมาตรฐาน NFPA 130] อีกทั้ง อุปกรณ์สื่อสารฉุกเฉิน (ECD) แต่ละตัวต้องโทรหาศูนย์ควบคุมส่วนกลางโดยอัตโนมัติเมื่อมีการเปิดใช้งาน และจอแสดงผลที่ศูนย์ควบคุมส่วนกลางต้องสามารถระบุตัว ECD ที่สื่อสาร และระบุได้ว่ามี ECD ที่เปิดใช้งานเพิ่มเติมหรือไม่

อุปกรณ์ ECD ทั้งหมดต้องได้รับการออกแบบให้ทนทานต่อภาระหนัก (heavy-duty) ทนต่อการงัดแงะและทนต่อสภาพอากาศและอุณหภูมิต่างๆ ได้ ทั้งนี้ การสื่อสารด้วยเสียงฉุกเฉินเหล่านี้จะต้องไม่ขึ้นอยู่กับระบบการสื่อสารอื่นๆ

ผู้ปฏิบัติงาน ECD ต้องได้รับสัญญาณเสียงว่าเครื่องกำลังใช้งานการโทรอยู่

คำแนะนำในการใช้งานต้องระบุไว้ในป้ายป้องกันการทุบทำลายที่อยู่บน ECD หรือติดกับ ECD

5.1.3 การสื่อสารด้วยเสียงและเสียงประกาศสาธารณะในขบวนรถ

ต้องจัดให้มีระบบการสื่อสารแบบเชื่อมสองทิศทาง (full-duplex comminication) เพื่อให้สามารถสื่อสารด้วยเสียงแบบสองทิศทางระหว่างผู้ควบคุมที่ศูนย์ควบคุมส่วนกลางกับผู้โดยสารหรือบุคลากรภายในห้องโดยสารแต่ละตู้ของขบวนรถแต่ละขบวน และต้องจัดให้ครอบคลุมขบวนรถทั่วทั้งระบบ ทั้งนี้ การเปิดใช้งานการสื่อสารด้วยเสียงแบบสองทิศทางระหว่างศูนย์ควบคุมส่วนกลางและขบวนรถต้องทำได้จากศูนย์ควบคุมส่วนกลางเท่านั้น โดยที่คำขอการสื่อสารที่เริ่มโดยผู้โดยสารบนขบวนรถ รวมถึงหมายเลข

ประจำตัวห้องโดยสาร ต้องแสดงโดยอัตโนมัติที่ศูนย์ควบคุมส่วนกลาง เพื่อให้ผู้ควบคุมที่ศูนย์ควบคุมส่วนกลางเปิดใช้งานการเชื่อมต่อสื่อสาร ซึ่งคำขอการสื่อสารจากผู้โดยสารต้องมีสัญญาณภาพและเสียงบนเครื่องว่ามีการร้องขอให้มีการโทร

ต้องจัดให้มีฟังก์ชันเสียงประกาศสาธารณะของขบวนรถสำหรับผู้ควบคุมที่ศูนย์ควบคุมส่วนกลางได้ 2 โหมด ดังนี้

(1) การประกาศด้วยเสียงในห้องโดยสารทั้งหมดของขบวนรถขบวนใดขบวนหนึ่ง

(2) การประกาศด้วยเสียงในห้องโดยสารทั้งหมดของขบวนรถทุกขบวนในระบบ

ถ้ามีการใช้ข้อความสด (live message) ต้องประกาศแทนข้อความที่บันทึกไว้ล่วงหน้า อีกทั้ง การทนไฟของลำโพงต้องเป็นไปตามข้อกำหนดของ UL 813-1993 หรือมาตรฐานอื่นที่เทียบเท่า และสำหรับขบวนรถที่สามารถเดินรถแบบโหมดมีคนขับ ได้ ต้องจัดให้มีวิธีการที่ผู้ควบคุมขบวนรถสามารถทำการประกาศได้ตลอดขบวนรถ

5.1.4 การสื่อสารของบุคลากรฝ่ายปฏิบัติการ (operation) และซ่อมบำรุง (maintenance)

ระบบ APM ต้องมีระบบโทรศัพท์ภายในหรือระบบอินเตอร์คอมที่เชื่อมต่อกับศูนย์ควบคุมส่วนกลาง อย่างน้อยบริเวณพื้นที่สำนักงานบริหาร พื้นที่บำรุงรักษา รวมถึงห้องจัดเก็บและห้องอุปกรณ์ ทั้งนี้ โทรศัพท์หรืออินเตอร์คอมที่ไม่ได้รับการป้องกันใดๆ ต้องออกแบบให้มีที่หุ้มที่ทนทานต่อภาระหนัก ป้องกันการงัดแงะ และทนต่อสภาพอากาศ

ต้องจัดให้มีระบบวิทยุในการปฏิบัติการและการบำรุงรักษา (O&M) สำหรับการสื่อสารระหว่างผู้ควบคุมที่ศูนย์ควบคุมส่วนกลางและเจ้าหน้าที่ของ O&M ทั้งนี้ เจ้าหน้าที่ O&M แต่ละคนที่ปฏิบัติหน้าที่แล้วไม่สามารถเข้าถึงโทรศัพท์ภายในหรือระบบอินเตอร์คอมได้โดยตรง ต้องมีวิทยุแบบพกพาตลอดเวลา

5.1.5 การบันทึกเสียง

ต้องจัดให้มีอุปกรณ์บันทึกเสียงเพื่อบันทึกการสื่อสารทั้งหมดที่มีการสื่อสารด้วยเสียงของขบวนรถ อุปกรณ์ ECD และระบบเสียงประกาศสาธารณะต่างๆ กับผู้ควบคุมส่วนกลาง โดยที่อุปกรณ์นี้ต้องมีความสามารถในการบันทึกเสียงต่อเนื่องอย่างน้อย 24 ชั่วโมง ซึ่งเป็นไปตามหัวข้อ 5.1.1 ถึง 5.1.3 โดยมีการระบุวันที่และเวลา และต้องมีตัวกลางบันทึก (recording media) เพื่อให้สามารถจัดเก็บบันทึกในแต่ละวันได้

5.1.6 ความเข้าใจทางภาษาในการสื่อสารด้วยเสียง

ระบบการสื่อสารด้วยเสียงต้องเป็นไปตามข้อกำหนดดังต่อไปนี้

(1) ระบบเสียงประกาศสาธารณะของสถานี ระบบสื่อสารที่สถานีฉุกเฉินและข้างทาง และระบบโทรศัพท์ O&M ภายในหรือระบบอินเตอร์คอม ต้องเป็นไปตามข้อกำหนดด้านความเข้าใจทางภาษาของมาตรฐาน NFPA 72 โดยเกณฑ์การวัดต้องแสดงพื้นที่ผู้โดยสารทั้งหมดของสถานีหรือตำแหน่งของโทรศัพท์หรืออินเตอร์คอม และต้องมีผลลัพธ์โดยเฉลี่ยของสัญญาณที่สะท้อนและเสียงก้อง โดยที่ระบบรอง (auxiliary system) ทั้งหมดต้องอยู่ในการทำงานปกติ เสียงรบกวนรอบข้าง (ambient noise) จึงจะอยู่ที่ระดับสูงสุด ทั้งนี้ การทดสอบโทรศัพท์และอินเตอร์คอมต้องทำซ้ำตามจำนวนสถานที่ที่เลือกเป็นตัวอย่างจากทั้งระบบ

(2) การสื่อสารด้วยเสียงแบบไร้สายทั้งหมดระหว่างข้างทางกับบนขบวนรถ รวมถึงระบบควบคุมส่วนกลาง ต้องเป็นไปตาม DAQ 3 ของตารางที่ 1 ใน Appendix A ของ TIA/EIA TSB-88 หรือมาตรฐานอื่นที่เทียบเท่า สำหรับ 97% ของเส้นทางรถ (trainway) โดยที่พื้นที่ของเส้นทางที่ตรงตามมาตรฐานดังกล่าว ด้านความเข้าใจทางภาษา ต้องเป็นไปตามข้อกำหนดของมาตรฐาน NFPA 72 หรือมาตรฐานอื่นที่เทียบเท่า

เสียงรบกวนภายในรถต้องมีระดับอย่างน้อยที่ระดับเสียงภายในตัวรถสูงสุด (maximum interior level) ตามที่วัดใน มขร. – R – 007 - 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านเครื่องกลและตัวรถ หัวข้อที่ 2 ข้อ 7.7.4 ซึ่งการทดสอบนี้ต้องทำซ้ำตามจำนวนสถานที่ที่เลือกเป็นตัวอย่างจากทั้งระบบ

(3) การสื่อสารด้วยเสียงแบบพิเศษทั้งหมดภายในขบวนรถ ต้องเป็นไปตามข้อกำหนดด้านความเข้าใจทางภาษาของมาตรฐาน NFPA 72 โดยที่เสียงรบกวนภายในรถต้องมีระดับอย่างน้อยที่ระดับเสียงภายในสูงสุดตามที่วัดตาม มขร. – R – 007 – 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านเครื่องกลและตัวรถ หัวข้อที่ 2 ข้อ 7.7.4

(4) ระบบวิทยุ O&M ต้องครอบคลุมสัญญาณมากกว่าหรือเท่ากับที่อ้างอิงตาม DAQ 3 ไว้ก่อนหน้านี้ ซึ่งมีความน่าเชื่อถือ (reliability) ครอบคลุม 97% ของพื้นที่ภายในระบบที่บุคลากร O&M อาจทำงานอยู่

5.2 การเฝ้าระวังด้วยวิดีโอ (video surveilliance)

ต้องจัดให้มีระบบย่อยของกล้องวงจรปิด (Closed-circuit television: CCTV) เพื่อให้ศูนย์ควบคุมส่วนกลางติดตามกิจกรรมของผู้โดยสารบนชานชาลาของสถานีทั้งหมดได้ โดยเฉพาะบริเวณขึ้นรถและตลอดขอบของชานชาลาที่ไม่มีที่กั้น ทั้งนี้ ไม่จำเป็นต้องมีกล้องวงจรปิดสำหรับชานชาลาของสถานีที่มีการดูแลแล้ว

5.2.1 อุปกรณ์ควบคุมส่วนกลาง

การควบคุมส่วนกลางต้องติดตั้งจอภาพสำหรับแสดงผลเอาต์พุตของกล้อง โดยจัดเรียงตามลำดับอย่างมีตรรกะ พร้อมมีการระบุสิ่งต่าง ๆ บนแต่ละหน้าจอ เพื่อให้ผู้ควบคุมที่ศูนย์ควบคุมส่วนกลางเข้าใจได้และอำนวยความสะดวกในการระบุตำแหน่งของภาพ

จอภาพ CCTV ต้องมีภาพที่ชัดเจนในระดับแสงปกติโดยรอบของห้องควบคุมส่วนกลาง (central control room)

5.2.2 อุปกรณ์บนสถานีของผู้โดยสาร

กล้องต้องมีภาพที่ใช้งานได้ ซึ่งมีความสว่างของฉากตั้งแต่ 0.3 ลักซ์ (0.03 ฟุตแคนเดิล) จนถึงแสงแดดจ้า โดยใช้วิธีการชดเชยแสงอัตโนมัติ (automatic light compensation)

กล้องต้องป้องกันการงัดแงะและป้องกันการทุบทำลาย อีกทั้ง กล้องต้องปรับให้เข้ากับสภาพแวดล้อมและสภาพแสงโดยรอบของแต่ละสถานีโดยอัตโนมัติตลอดวันทำการ

ตำแหน่งกล้องในการดูชานชาลา โดยเฉพาะบริเวณขึ้นไปบนตัวรถและตลอดขอบของชานชาลาแบบเปิด ต้องติดอยู่กับที่และต้องไม่มีการควบคุมจากทางไกล กรณีที่มีการติดตั้งกล้องกลางแจ้ง ตัวยึดกล้องและตัวครอบกล้องต้องป้องกันการงัดแงะและป้องกันการทุบทำลายจากการใช้งานทุกประเภท และทนต่อสภาพอากาศ

5.2.3 การบันทึกวิดีโอ

ต้องจัดให้มีระบบเพื่อบันทึกภาพของกล้องแต่ละตัวในระบบ เพื่อระบุตัวกล้อง เวลาและวันที่ แต่ไม่จำเป็นต้องบันทึกกล้องทั้งหมดพร้อมกัน

5.3 อุปกรณ์ให้ข้อมูลสำหรับผู้โดยสาร

มีความจำเป็นที่จะมีเสียงประกาศและป้ายแบบเปลี่ยนแปลงข้อมูลได้ต่อไปนี้สำหรับระบบ APM

5.3.1 บนตัวรถ

ห้องโดยสารแต่ละห้องต้องมีเสียงประกาศอัตโนมัติบนรถซึ่งจะได้ประกาศเมื่อเข้าสู่แต่ละสถานี เพื่อแจ้งให้ผู้โดยสารทราบถึงจุดจอดที่กำลังจะถึง

สำหรับระบบ APM ที่มีขบวนรถวิ่งมากกว่าหนึ่งเส้นทางในชานชาลาเดียวกัน การประกาศด้วยเสียงจะต้องระบุชื่อของสถานีด้วย และต้องจัดให้มีป้ายแบบเปลี่ยนแปลงข้อมูลได้ในห้องโดยสารแต่ละห้อง ซึ่งระบุเส้นทางหรือจุดหมายปลายทางและชื่อของสถานีที่ขบวนรถกำลังเข้าใกล้หรือหยุด โดยที่ป้ายแบบเปลี่ยนแปลงข้อมูลได้เหล่านี้ต้องอยู่ในตำแหน่งให้ผู้โดยสารมองเห็นได้มากที่สุด

5.3.2 บนสถานี

ในแต่ละชานชาลาของสถานีต้องมีการเตือนด้วยเสียงและภาพอัตโนมัติ หรือวิธีการอื่นใดที่ทำให้ผู้โดยสารรับทราบเรื่องการเข้า-ออกของขบวนรถ เพื่อแจ้งเตือนการมาถึงและออกจากขบวนรถ โดยที่การแจ้งเตือนการมาถึงต้องทำก่อนที่ขบวนรถจะเข้าสู่สถานี และการแจ้งเตือนการออกเดินรถที่ระบุว่าประตูกำลังจะปิดต้องแจ้งให้ผู้โดยสารทั้งในขบวนรถและบนชานชาลาทราบ ทั้งนี้ หากขบวนรถไม่สามารถหยุดได้โดยสมบูรณ์ เพื่อให้ผู้โดยสารที่ขึ้นลง ต้องจัดให้มีสัญญาณเตือนหรือประกาศแจ้งเตือนที่ตรงตามการอำนวยความสะดวก ในหัวข้อที่ 2.1.2.1 การวิเคราะห์อันตราย

ระบบ APM ที่มีขบวนรถวิ่งมากกว่าหนึ่งเส้นทางในชานชาลาเดียวกันต้องประกาศเส้นทางหรือจุดหมายปลายทางด้วยเสียง และต้องจัดให้มีป้ายสถานีแบบเปลี่ยนแปลงได้บนชานชาลาแต่ละสถานีเพื่อแจ้งให้ผู้โดยสารทราบเส้นทางหรือจุดหมายปลายทาง โดยที่ป้ายแบบเปลี่ยนแปลงข้อมูลได้ของตัวรถอาจติดข้อความไว้ที่ด้านนอกของตัวรถด้วย เพื่อให้ผู้โดยสารสามารถอ่านได้จากชานชาลาของสถานี

ภาคผนวก ก
ข้อกำหนดแผนความปลอดภัยของระบบ

ภาคผนวกนี้เป็นภาคบังคับสำหรับมาตรฐานนี้ ตามที่ได้ระบุไว้ในหัวข้อที่ 2 ข้อกำหนดความปลอดภัย เทคนิคที่เทียบเท่าอาจใช้แทนเทคนิคในภาคผนวกนี้ได้

ก.1 การวางแผนความปลอดภัยของระบบ (System Safety Program Plan)

ก.1.1 วัตถุประสงค์

การวางแผนความปลอดภัยของระบบ (SSSP) นี้ ต้องอธิบายรายละเอียดงานและกิจกรรมต่าง ๆ ของการจัดการความปลอดภัยระบบ วิศวกรรมด้านความปลอดภัยระบบ และกระบวนการรับรองความปลอดภัยที่จำเป็นในการระบุ ประเมิน และกำจัดหรือควบคุมอันตราย หรือลดความเสี่ยงที่เกี่ยวข้องให้อยู่ในระดับที่ยอมรับได้ของหน่วยงานที่มีอำนาจในการตัดสินตลอดการใช้งานของระบบ

ก.1.2 รายละเอียด

SSSP ต้องได้รับการพัฒนาเพื่อให้มีพื้นฐานความเข้าใจเกี่ยวกับแผนความปลอดภัยของระบบให้เป็นไปตามข้อกำหนดความปลอดภัย โดยแผนที่ได้รับอนุมัติ ต้องอธิบายงานและความรับผิดชอบที่จำเป็นทั้งหมดทีละรายการ ซึ่ง SSSP ต้องมีรายละเอียดดังต่อไปนี้

ก.1.2.1 ขอบเขตและวัตถุประสงค์ของแผน

ในแต่ละ SSSP ต้องอธิบายอย่างน้อย 4 องค์ประกอบของแผนระบบความปลอดภัยที่มีประสิทธิภาพ ได้แก่ แนวทางที่วางแผนไว้เพื่อบรรลุผลสำเร็จของงาน บุคลากรที่มีคุณสมบัติเหมาะสมที่จะบรรลุภารกิจ อำนาจในการปฏิบัติงานผ่านฝ่ายบริหารทุกระดับ และข้อผูกมัดของทรัพยากรทั้งพนักงานและทุนเพื่อรับรองความสมบูรณ์ของภารกิจ โดยที่ SSSP ต้องกำหนดแผนให้เป็นไปตามข้อกำหนดความปลอดภัยของระบบ ในส่วนนี้ต้องมีรายละเอียดดังต่อนี้

(1) รายละเอียดขอบเขตของแผนภาพรวมและแผนความปลอดภัยของระบบที่เกี่ยวข้อง

(2) รายการงานและกิจกรรมต่าง ๆ ของการจัดการและวิศวกรรมทางด้านความปลอดภัยของระบบ โดยอธิบายความสัมพันธ์กันระหว่างความปลอดภัยของระบบกับองค์ประกอบในการทำงานอื่นๆ ของแผน รวมไปถึงรายการข้อกำหนดของแผนและงานอื่น ๆ ที่ใช้งานกับความปลอดภัยของระบบ ซึ่งระบุไว้ในที่ที่รายละเอียดถูกระบุ

(3) การอธิบายงานและความรับผิดชอบทั้งหมดที่จำเป็น โดยต้องจัดให้เป็นแถวและคอลัมน์ (matrix) เพื่อเชื่อมโยงข้อกำหนดกับ SSSP ที่มีการระบุข้อกำหนด

ก.1.2.2 องค์กรความปลอดภัยของระบบ

SSSP นี้ ต้องอธิบายตามหัวข้อต่อไปนี้

(1) องค์กรหรือหน้าที่ด้านความปลอดภัยของระบบภายในองค์กรของแผนทั้งหมด ซึ่งใช้แผนภูมิเพื่อแสดงความสัมพันธ์และการสื่อสารขององค์กรหรือหน้าที่ รวมถึงต้องแสดงความสัมพันธ์ขององค์กรระหว่างองค์ประกอบหน้าที่อื่น ๆ ที่มีความรับผิดชอบในงานซึ่งมีผลกระทบด้านความปลอดภัยของระบบกับองค์กรในการจัดการและวิศวกรรมทางด้านความปลอดภัยของระบบ อีกทั้ง ต้องอธิบายอำนาจในการตรวจสอบและอนุมัติโดยความปลอดภัยของระบบในภารกิจงานที่เกี่ยวข้อง

(2) หน้าที่ความรับผิดชอบและอำนาจของบุคคลด้านความปลอดภัยของระบบ รวมถึงองค์กรส่วนอื่นที่เกี่ยวข้องกับความปลอดภัยของระบบและกลุ่มระบบความปลอดภัย ทั้งนี้ ต้องอธิบายขั้นตอนการแจ้งประเด็นของบุคลากรความปลอดภัยโดยตรงไปยังผู้จัดการแผนหรือหัวหน้าการจัดการแผน โดยที่ต้องระบุหน่วยงานขององค์กรที่รับผิดชอบในการดำเนินงานในแต่ละงาน และต้องอำนาจในการแก้ไขปัญหาของความเสี่ยงที่ระบุไว้ทั้งหมด

(3) พนักงานขององค์กรด้านความปลอดภัยของระบบในระยะเวลาของสัญญา รวมถึงการบรรจุกำลังคน การควบคุมทรัพยากร และสรุปคุณสมบัติของบุคลากรด้านความปลอดภัยของระบบหลักที่ได้รับมอบหมายให้ปฏิบัติงาน รวมถึงผู้ประสานงานและ/หรือผู้ที่มีอำนาจในการจัดทำเอกสาร

(4) ขั้นตอนในการบูรณาการและประสานกันของความปลอดภัยของระบบ รวมถึงการมอบหมายข้อกำหนดด้านความปลอดภัยของระบบให้แก่องค์กรที่ปฏิบัติงาน การทำงานร่วมกันของแผนความปลอดภัยของระบบ การรวมการวิเคราะห์อันตราย การตรวจสอบแผนและการออกแบบ การรายงานผลสถานะของแผน และกลุ่มระบบความปลอดภัย

(5) กระบวนการในการตัดสินใจของฝ่ายบริหาร รวมถึงการแจ้งเตือนความเสี่ยงที่ไม่สามารถยอมรับได้ (unacceptable risks) ได้ทันเวลา การดำเนินการที่จำเป็น เหตุการณ์หรือการทำงานผิดปกติ การผ่อนผันข้อกำหนดความปลอดภัย และความคลาดเคลื่อนของแผน

(6) รายละเอียดวิธีการแก้ไขและการดำเนินการมีความสำคัญต่อความปลอดภัยของระบบว่าจะได้รับผลกระทบอย่างไรในระดับการจัดการแผนที่มีอำนาจในการแก้ไขปัญหา

ก.1.2.3 จุดสำคัญของแผนความปลอดภัยของระบบ (system safety program milstones) SSSP ต้องมีขั้นตอนดังต่อไปนี้

(1) กำหนดขั้นตอนของแผนความปลอดภัยของระบบ และเชื่อมโยงไปยังจุดสำคัญหลักของแผน หน้าที่ความรับผิดชอบของส่วนประกอบในแผน และอินพุต เอ้าต์พุต ที่จำเป็น

(2) จัดทำตารางแผนของงานด้านความปลอดภัย รวมถึงวันที่เริ่มต้นและวันที่เสร็จสิ้นรายงาน และการตรวจสอบ

(3) ระบุระบบย่อย ส่วนประกอบ และการฏิบัติงานด้านความปลอดภัยของซอฟต์แวร์ตลอดจนการฏิบัติงานระดับระบบที่บูรณาการแล้ว เช่น การวิเคราะห์การออกแบบ การทดสอบและการแสดงผล ที่ใช้งานกับแผนความปลอดภัยของระบบแต่ถูกระบุไว้ในผลการศึกษาและการพัฒนาทางวิศวกรรมอื่น ๆ เพื่อป้องกันไม่ให้เกิดความซับซ้อน

(4) จัดทำการบรรจุบุคลากรโดยประมาณที่จำเป็นสำหรับการปฏิบัติแต่ละงานให้เสร็จสิ้น

ก.1.2.4 ข้อกำหนดและเกณฑ์ทั่วไปในความปลอดภัยของระบบ SSSP ต้องเป็นไปตามข้อดังต่อไปนี้

(1) อธิบายข้อกำหนดทางวิศวกรรมทั่วไปและเกณฑ์การออกแบบด้านความปลอดภัย อีกทั้ง อธิบายข้อกำหนดความปลอดภัยเพื่อรองรับอุปกรณ์ และข้อกำหนดความปลอดภัยในการทำงานสำหรับทุกช่วงที่เหมาะสมตลอดอายุการใช้งาน รวมถึงการจัดการด้วย และมีรายการมาตรฐานความปลอดภัยและคุณลักษณะเฉพาะของระบบที่ต้องเป็นไปตามข้อกำหนดความปลอดภัย ซึ่งมีชื่อ วันที่ และเลขย่อหน้า (ถ้ามี)

(2) อธิบายขั้นตอนการประเมินความเสี่ยงและประเภทความรุนแรงของความเสี่ยงนั้น ระดับความน่าจะเป็นของความเสี่ยง และลำดับความสำคัญด้านความปลอดภัยของระบบ ซึ่งต้องเป็นไปตาม

ข้อกำหนดความปลอดภัยของแผน อีกทั้ง ต้องระบุตัวชี้วัดทางคุณภาพและปริมาณของความปลอดภัยที่ใช้ในการประเมินความเสี่ยง รวมถึงอธิบายระดับความเสี่ยงที่ยอมรับได้และไม่สามารถยอมรับได้ พร้อมทั้งมีคำจำกัดความของความปลอดภัยของระบบที่เป็นการแก้ไข คลาดเคลื่อน หรือเพิ่มเติมจากคำจำกัดความในมาตรฐานนี้

(3) อธิบายขั้นตอนแบบวงจรปิด (closed-loop procedures) ในการดำเนินการเพื่อแก้ไขความเสี่ยงที่ไม่สามารถยอมรับได้ รวมถึงความเสี่ยงที่เกี่ยวข้องกับสิ่งที่ไม่ได้รับการพัฒนา

(4) อธิบายกระบวนการและข้อกำหนดสำหรับการพัฒนาซอฟต์แวร์อ้างอิงตามระดับความสำคัญของความปลอดภัยที่เกี่ยวข้องกับแต่ละฟังก์ชัน

ก.1.2.5 การวิเคราะห์อันตราย

SSSP ต้องอธิบายตามข้อดังต่อไปนี้

(1) เทคนิคและรูปแบบในการวิเคราะห์ที่ใช้ในการวิเคราะห์เชิงคุณภาพและปริมาณเพื่อระบุความเสี่ยง สาเหตุและผลกระทบของความเสี่ยง การกำจัดความเสี่ยง หรือข้อกำหนดในการลดความเสี่ยง และวิธีที่ทำให้เป็นไปตามข้อกำหนดนั้น

(2) ความลึกภายในระบบที่ใช้ในแต่ละเทคนิค รวมถึงการระบุความเสี่ยงที่เกี่ยวข้องกับระบบหลัก ระบบย่อย ส่วนประกอบ ซอฟต์แวร์ วัตถุอันตราย บุคลากร อุปกรณ์สนับสนุนภาคพื้นดิน (ground support equipment) สิ่งที่ไม่ได้รับการพัฒนา สิ่งอำนวยความสะดวก และความสัมพันธ์ในการสนับสนุนด้านการขนส่ง การฝึกอบรม การซ่อมบำรุง การเดินรถ และการจัดการสภาพแวดล้อมที่รวมถึงขั้นตอนความปลอดภัยในการช่วยเหลือและการจัดการกรณีฉุกเฉิน

(3) การบูรณาการในการวิเคราะห์อันตราย ดำเนินการโดยผู้อื่นพร้อมกับการวิเคราะห์อันตรายภาพรวมของระบบ

(4) ความพยายามในการระบุและควบคุมความเสี่ยงที่เกี่ยวข้องกับวัตถุที่ใช้ระหว่างอายุการใช้งานของระบบ

(5) กระบวนการในการจัดการประวัติการติดตามความเสี่ยง (Hazard Tracking Log) และรูปแบบของ Hazard Tracking Log

ก.1.2.6 ข้อมูลความปลอดภัยของระบบ

SSSP ต้องเป็นไปตามข้อดังต่อไปนี้

(1) อธิบายแนวทางในการรวบรวมและประมวลผลข้อมูลที่เกี่ยวข้องโดยตรงกับอันตรายในอดีต (historical hazard) อุบัติเหตุ (mishap) และบทเรียนที่ได้รับในเรื่องความปลอดภัย

(2) ระบุข้อมูลที่ส่งตามชื่อ ตัวเลข และวิธีการในการส่ง เช่น สำเนาเอกสาร (hard copy) หรือ อิเล็กทรอนิกส์

(3) ระบุข้อมูลความปลอดภัยของระบบที่ไม่สามารถส่งได้ และอธิบายขั้นตอนในการเข้าถึงโดยหน่วยงานที่มีอำนาจตัดสิน และการเก็บรักษาข้อมูลที่มีค่าทางประวัติศาสตร์

(4) อธิบายกระบวนการในการติดตามประสิทธิภาพของการบรรเทาความเสี่ยงและรูปแบบในการนำเสนอข้อมูลสนับสนุน

ก.1.2.7 การยืนยันความปลอดภัย (safety verification)

SSSP ต้องเป็นไปตามข้อดังต่อไปนี้

(1) ข้อกำหนดในการยืนยันความถูกต้อง เช่น การทดสอบ การวิเคราะห์ หรือการตรวจตรา เพื่อให้แน่ใจว่ามีความปลอดภัยที่เพียงพอ และมีการระบุข้อกำหนดในการรับรอง

(certification requirements) สำหรับซอฟต์แวร์ อุปกรณ์ความปลอดภัย หรือการทำงานของความปลอดภัยพิเศษอื่น ๆ เช่น ขั้นตอนความปลอดภัยในการช่วยเหลือและการจัดการกรณีฉุกเฉิน

(2) ขั้นตอนเพื่อให้แน่ใจว่าข้อมูลที่เกี่ยวข้องกับความปลอดภัยถูกส่งไปยังหน่วยงานที่มีอำนาจตัดสินเพื่อตรวจสอบและวิเคราะห์ข้อมูล

(3) ขั้นตอนเพื่อให้แน่ใจว่ามีความปลอดภัยในทุกการทดสอบ

ก.1.2.8 แผนการตรวจสอบ (audit program)

SSSP ต้องอธิบายเทคนิคและขั้นตอนที่ใช้เพื่อให้แน่ใจว่าวัตถุประสงค์และข้อกำหนดของแผนความปลอดภัยของระบบจะบรรลุผลสำเร็จ

ก.1.2.9 การฝึกอบรม

SSSP ต้องอธิบายการฝึกอบรมความปลอดภัยสำหรับบุคลากรด้านวิศวกรรม ช่างเทคนิค เจ้าหน้าที่ปฏิบัติงาน และเจ้าหน้าที่ซ่อมบำรุง

ก.1.2.10 แบบรายงานอุบัติการณ์ (incident reporting)

SSSP ต้องอธิบายกระบวนการแจ้งเตือน การสืบสวน และการรายงานเหตุหรืออุบัติเหตุ รวมถึงการแจ้งเตือนของหน่วยงานที่มีอำนาจในการตัดสิน

ก.1.2.11 ส่วนเชื่อมต่อความปลอดภัยของระบบ (system safety interfaces)

SSSP ต้องระบุรายละเอียดดังต่อไปนี้

(1) ส่วนเชื่อมต่อระหว่างความปลอดภัยของระบบ วิศวกรรมของระบบ และส่วนที่สนับสนุนอื่นทั้งหมด เช่น การบำรุงรักษา (maintainability) การควบคุมคุณภาพ ความน่าเชื่อถือ (reliability) การพัฒนาซอฟต์แวร์ วิศวกรรมทางปัจจัยมนุษย์ การสนับสนุนทางการแพทย์หรือการประเมินความเสี่ยงทางสุขภาพ และอื่น ๆ

(2) ส่วนเชื่อมต่อระหว่างความปลอดภัยของระบบกับการรวมระบบและการทดสอบทั้งหมด

ก.1.2.12 การรับรองความปลอดภัย (safety certification)

SSSP ต้องมีรายละเอียดดังต่อไปนี้

(1) การอธิบายโดยละเอียดของกระบวนการรับรองความปลอดภัยของระบบ รวมถึงรายการและคำอธิบายขั้นตอนในการปฏิบัติตามกระบวนการนี้

(2) การอธิบายกระบวนการรับรองความปลอดภัยของระบบนี้ต้องรวมไปถึงแผนและกระบวนการการันตีของรายงานการรับรองความปลอดภัยของระบบ (System Safety Certifications Report: SSCR) โดยที่มีเนื้อหาของ SSCR แผนในการปรับปรุงและการเผยแพร่ภายหลังจากการทำ SSCR ตลอดอายุการใช้งานของโครงการ APM

(3) กระบวนการรับรองความปลอดภัยของระบบนี้ต้องอธิบายกระบวนการในการแก้ไขปัญหาผลจากหน่วยตรวจประเมินความปลอดภัยที่เป็นอิสระ (Independent Safety Assessment findings)

ก.2 การวิเคราะห์อันตรายเบื้องต้น (Preliminary Hazard Analysis)

ก.2.1 วัตถุประสงค์

การวิเคราะห์อันตรายเบื้องต้น (Preliminary Hazard Analysis: PHA) ต้องระบุพื้นที่ที่มีความสำคัญต่อความปลอดภัย โดยจัดให้มีการประเมินความเสี่ยงเริ่มต้นและระบุการควบคุมความเสี่ยงที่จำเป็นและการดำเนินการที่ตามมา

ก.2.2 รายละเอียด

การวิเคราะห์อันตรายเบื้องต้นต้องดำเนินการและจัดทำเป็นเอกสารเพื่อให้เป็นแนวคิดหรือระบบการประเมินความเสี่ยงเริ่มต้น ซึ่งอ้างอิงจากข้อมูลที่ดีที่สุดที่มีอยู่ รวมถึงข้อมูลอุบัติเหตุจากระบบที่คล้ายกันและบทเรียนอื่น ๆ (หากประเมินได้) โดยที่ความเสี่ยงที่เกี่ยวข้องกับการออกแบบหรือการทำงานที่เสนอไว้ต้องได้รับการประเมินของความรุนแรงของความเสี่ยง ความน่าจะเป็นของความเสี่ยง และข้อจำกัดในการปฏิบัติงาน อีกทั้งต้องมีข้อกำหนดความปลอดภัยและทางเลือกต่าง ๆ ที่จำเป็นในการกำจัดความเสี่ยงหรือลดความเสี่ยงที่เกี่ยวข้องให้อยู่ในระดับที่ยอมรับได้จากหน่วยงานที่มีอำนาจในการตัดสิน ซึ่ง PHA ต้องมีการพิจารณาอย่างน้อยในการระบุและการประเมินความเสี่ยงดังต่อไปนี้

(1) ส่วนประกอบที่มีเป็นอันตราย เช่น เชื้อเพลิง ก๊าซที่ใช้ขับเคลื่อน (propellants) เลเซอร์ สารพิษ วัสดุก่อสร้างที่มีอันตราย ระบบความดัน และแหล่งกำเนิดพลังงานอื่น ๆ

(2) ข้อพิจารณาส่วนเชื่อมต่อที่เกี่ยวข้องกับความปลอดภัยในองค์ประกอบต่าง ๆ ในระบบ เช่น ความเข้ากันได้ของวัสดุ การรบกวนทางแม่เหล็กไฟฟ้า การเปิดใช้งานโดยไม่ได้ตั้งใจ การจุดไฟหรือการ

ระเบิดและการแพร่กระจาย การควบคุมฮาร์ดแวร์และซอฟต์แวร์ โดยที่รายการนี้ต้องรวมถึงการพิจารณาการสนับสนุนจากซอฟต์แวร์ในระบบย่อยหรืออุบัติเหตุของระบบ ซึ่งรวมถึงซอฟต์แวร์ที่ถูกพัฒนาจากแหล่งอื่นด้วย

เกณฑ์การออกแบบความปลอดภัยในการควบคุมคำสั่งและการตอบสนองของซอฟต์แวร์ที่มีความสำคัญต่อความปลอดภัย เช่น การสั่งการโดยไม่ได้ตั้งใจ ความล้มเหลวในการสั่งการ คำสั่งหรือการตอบสนองก่อนเวลา ขนาดที่ไม่เหมาะสม หรือเหตุการณ์ที่ไม่พึงประสงค์อื่น ๆ ที่ออกแบบ ต้องได้รับการระบุและดำเนินการตามความเหมาะสมเพื่อเป็นไปตามคุณสมบัติของซอฟต์แวร์และฮาร์ดแวร์ที่เกี่ยวข้อง

(3) ข้อจำกัดทางสภาพแวดล้อม รวมถึงสภาพแวดล้อมในการทำงาน เช่น การตก (drop) การกระแทก (shock) การสั่นสะเทือน (vibration) อุณหูภูมิเกิน (extreme temperature) เสียงรบกวน การสัมผัสกับสารพิษ อันตรายต่อสุขภาพ เพลิงไหม้ การปล่อยประจุไฟฟ้าสถิต ฟ้าผ่า และผลกระทบต่อสิ่งแวดล้อมทางแม่เหล็กไฟฟ้า

(4) ขั้นตอนในการให้บริการ การทดสอบ การซ่อมบำรุง การทดสอบในตัว (built-in test) การวินิจฉัยและกรณีฉุกเฉิน เช่น วิศวกรรมทางปัจจัยมนุษย์ นั่นคือ การวิเคราะห์ความผิดพลาดของคนในการทำงานเป็นผู้ให้บริการ ในภารกิจ และในข้อกำหนด รวมถึงผลกระทบของปัจจัยต่าง ๆ เช่น แผนผังอุปกรณ์ ข้อกำหนดด้านแสงสว่าง การสัมผัสสารพิษ และผลกระทบทางเสียงหรือการแผ่รังสีในการปฏิบัติงานของมนุษย์

ขั้นตอนเหล่านี้ทดสอบความเสี่ยงที่มีลักษณะเฉพาะตัว ซึ่งจะทำให้เป็นผลโดยตรงจากการทดสอบและการประเมินของวัตถุหรือตัวรถ

(5) สิ่งอำนวยความสะดวก อสังหาริมทรัพย์ อุปกรณ์ที่ถูกติดตั้ง อุปกรณ์เสริม เช่น ข้อกำหนดสำหรับการจัดเก็บ การประกอบ การตรวจสอบ การพิสูจน์ หรือการทดสอบของระบบและส่วนประกอบที่มี

ความเสี่ยงเกี่ยวกับวัสดุหรือของเสียที่มีพิษ ไวไฟ ระเบิด กัดกร่อน หรือแข่แข็ง ตัวเครื่องแผ่รังสีหรือเสียง หรือแหล่งพลังงานไฟฟ้า รวมไปถึงการฝึกอบรม เช่น การฝึกอบรมและการรับรองในการปฏิบัติงาน และการบำรุงรักษาด้านความปลอดภัย

(6) อุปกรณ์ที่เกี่ยวข้องกับความปลอดภัย การป้องกัน และแนวทางเลือกที่เป็นไปได้ เช่น การบังคับสัมพันธ์ การสำรองของระบบ ข้อพิจารณาการออกแบบความปลอดภัยในกรณีขัดข้องโดยใช้การควบคุมฮาร์ดแวร์และซอฟต์แวร์ การป้องกันในระบบย่อย การตรวจจับและระงับเพลิงไหม้ รวมถึงอุปกรณ์ป้องกันส่วนบุคคล การทำความร้อน การระบายอากาศ เครื่องปรับอากาศ และที่กันเสียงหรือการแผ่รังสี

(7) ความผิดปกติในระบบหลัก ระบบย่อย หรือซอฟต์แวร์ โดยที่ในแต่ละความผิดปกตินี้ต้องระบุลำดับสาเหตุและผลที่ตามมาของเหตุการณ์ที่กำหนดไว้ ระดับความเสี่ยงที่กำหนดไว้ และคุณสมบัติและ/หรือการเปลี่ยนแปลงการออกแบบที่ได้รับการพัฒนา

ก.3 การวิเคราะห์อันตรายในระบบย่อย (Subsystem Hazard Analysis)

ก.3.1 วัตถุประสงค์

การวิเคราะห์อันตราย Subsystem Hazard Analysis (SSHA) ต้องเป็นไปตามข้อต่อไปนี้

(1) ต้องตรวจสอบระบบย่อยให้เป็นไปตามข้อกำหนดด้านความปลอดภัยที่อยู่ในคุณสมบัติของระบบย่อยและเอกสารที่เกี่ยวข้องอื่น ๆ

(2) ระบุความเสี่ยงที่ไม่สามารถระบุได้ก่อนหน้านี้ ซึ่งเกี่ยวข้องกับการออกแบบในระบบย่อย รวมไปถึงรูปแบบความล้มเหลวของส่วนประกอบ อินพุตสำคัญที่ผิดพลาดจากมนุษย์ และความเสี่ยงที่เป็นผลมาจากความสัมพันธ์ในการทำงานระหว่างส่วนประกอบต่าง ๆ และอุปกรณ์ที่ประกอบกันในแต่ละระบบย่อย

(3) การดำเนินการแนะนำที่จำเป็นในการกำจัดอันตรายที่สามารถระบุได้ หรือควบคุมความเสี่ยงที่เกี่ยวข้องให้อยู่ในระดับที่ยอมรับได้

ก.3.2 รายละเอียด

SSHA ต้องดำเนินการและจัดทำเป็นเอกสารเพื่อระบุส่วนประกอบและอุปกรณ์ทั้งหมดที่อาจเป็นผลทำให้เกิดความเสี่ยงหรือการออกแบบนั้นไม่เป็นไปตามข้อกำหนดด้านความปลอดภัย โดยที่ขอบเขตในการพิจารณา คือ ประสิทธิภาพ การลดลงของประสิทธิภาพการทำงาน ความผิดพลาดในการทำงาน ข้อผิดพลาดด้านเวลา (timing errors) ความล้มเหลวหรือข้อบกพร่องในการออกแบบ หรือการทำงานที่ประมาท ซึ่งมนุษย์ต้องถูกพิจารณาให้เป็นองค์ประกอบหนึ่งภายในระบบย่อย ทั้งอินพุตที่ได้รับและเอ้าท์พุตเริ่มต้น ตลอดการวิเคราะห์นี้ โดยที่ต้องรวมการพิจารณาดังต่อไปนี้

(1) รูปแบบความล้มเหลว รวมถึงความผิดพลาดจากมนุษย์ที่สมเหตุสมผล และความล้มเหลวแบบ single-point และแบบทั่วไป อีกทั้งผลกระทบต่อความปลอดภัยเมื่อเกิดความล้มเหลวในส่วนประกอบของระบบย่อย

(2) การมีส่วนร่วมในเหตุการณ์ของฮาร์ดแวร์และซอฟท์แวร์ (รวมถึงฮาร์ดแวร์และซอฟท์แวร์ที่ได้รับพัฒนาจากที่อื่น) ข้อผิดพลาดและเหตุที่เกิดกับความปลอดภัยของระบบย่อย เช่น การควบคุมเวลาที่ไม่เหมาะสม (inproper timimg)

(3) เป็นไปตามเกณฑ์การออกแบบความปลอดภัยในคุณสมบัติของฮาร์ดแวร์ ซอฟท์แวร์ และสิ่งอำนวยความสะดวก

(4) ขั้นตอนการปฏิบัติงานของข้อกำหนดการออกแบบฮาร์ดแวร์ ซอฟท์แวร์ และสิ่งอำนวยความสะดวก รวมไปถึงปฏิบัติการเชิงแก้ไข (corrective actions) ไม่ทำให้ความปลอดภัยของระบบย่อยลดลง หรือไม่ทำให้เกิดอันตรายหรือความเสี่ยงใด ๆ เพิ่มใหม่

(5) การปฏิบัติงานของข้อกำหนดการออกแบบความปลอดภัยจากคุณสมบัติระดับสูงสุด (top-level specifications) ถึงคุณสมบัติการออกแบบโดยละเอียดของระบบย่อย โดยการปฏิบัติงานตามข้อกำหนดการออกแบบความปลอดภัยที่พัฒนาเป็นส่วนหนึ่งของ PHA ต้องถูกวิเคราะห์เพื่อให้แน่ใจว่าเป็นไปตามเจตนาของข้อกำหนด

(6) แผนการทดสอบและคำแนะนำขั้นตอนเพื่อรวมการทดสอบความปลอดภัยเข้ากับโปรแกรมการทดสอบฮาร์ดแสร์และซอฟท์แวร์

(7) ความเสี่ยงในระดับระบบ (system-level hazards) ที่เกิดจากระบบย่อยนั้นได้รับการวิเคราะห์และมีการใช้การควบคุมความเสี่ยงที่อาจเกิดขึ้นในการออกแบบ

เมื่อมีการพัฒนาซอฟท์แวร์ที่ใช้ร่วมกับระบบย่อย บุคคลที่ดำเนินการ SSHA ต้องตรวจสอบ รับและใช้เอ้าพุตของแต่ละช่วงของกระบวนการพัฒนาซอฟท์แวร์อย่างเป็นทางการเพื่อประเมินซอฟท์แวร์ที่มีส่วนใน SSHA

SSHA นี้ต้องได้รับการอัปเดตที่เป็นผลมาจากการปลี่ยนแปลงการออกแบบของระบบ รวมถึงการเปลี่ยนแปลงการออกแบบซอฟท์แวร์ ซึ่งมีผลต่อความปลอดภัยของระบบ

ก.4 การวิเคราะห์อันตรายของระบบ (System Hazard Analysis)

ก.4.1 วัตถุประสงค์

การวิเคราะห์อันตราย System Hazard Analysis (SHA) ต้องเป็นไปตามข้อต่อไปนี้

(1) ต้องตรวจสอบระบบให้เป็นไปตามข้อกำหนดด้านความปลอดภัยที่อยู่ในคุณสมบัติของระบบและเอกสารที่เกี่ยวข้องอื่น ๆ

(2) ระบุความเสี่ยงที่ไม่สามารถระบุได้ก่อนหน้านี้ ซึ่งเกี่ยวข้องกับการเชื่อมต่อของระบบย่อยและความผิดพลาดในการทำงานของระบบ

(3) ประเมินความเสี่ยงที่เกี่ยวข้องกับการออกแบบระบบทั้งหมด รวมไปถึงซอฟท์แวร์และการเชื่อมต่อของระบบย่อย

(4) การดำเนินการแนะนำที่จำเป็นในการกำจัดอันตรายที่สามารถระบุได้ หรือควบคุมความเสี่ยงที่เกี่ยวข้องให้อยู่ในระดับที่ยอมรับได้

ก.4.2 รายละเอียด

SHA ต้องดำเนินการและจัดทำเป็นเอกสารเพื่อระบุอันตรายและประเมินความเสี่ยงของการออกแบบระบบทั้งหมด รวมไปถึงซอฟท์แวร์ และการเชื่อมต่อของระบบย่อย

การวิเคราะห์นี้ต้องรวมถึงการตรวจสอบความสัมพันธ์ของระบบย่อยดังต่อไปนี้

(1) เป็นไปตามเกณฑ์การออกแบบความปลอดภัยที่กำหนด

(2) เหตุการณ์อันตรายที่อาจเกิดขึ้นพร้อมกัน รวมถึงความล้มเหลวของระบบ อุปกรณ์ความปลอดภัย เหตุการณ์และความล้มเหลวจากสาเหตุทั่วไป และการทำงานร่วมกันของระบบที่อาจก่อให้เกิดอันตรายหรือส่งผลให้เพิ่มความเสี่ยงในการเกิดอุบัติเหตุ

(3) ความปลอดภัยที่ลดลงของระบบย่อยหรือระบบทั้งหมดจากการทำงานปกติของระบบย่อยอื่น ๆ

(4) การเปลี่ยนแปลงการออกแบบที่ส่งผลต่อระบบย่อย

(5) ผลกระทบของความผิดพลาดของมนุษย์ที่สมเหตุสมผล

(6) มีการกำหนดดังข้อต่อไปนี้

(6.1) มีส่วนร่วมในเหตุการณ์ของฮาร์ดแวร์และซอฟท์แวร์ (รวมถึงฮาร์ดแวร์และซอฟท์แวร์ที่ได้รับพัฒนาจากที่อื่นหรือที่มีจำหน่ายทั่วไปเชิงพาณิชย์) ข้อผิดพลาดและเหตุที่เกิดกับความปลอดภัยของระบบ เช่น การควบคุมเวลาที่ไม่เหมาะสม (inproper timimg)

(6.2) เป็นไปตามเกณฑ์การออกแบบความปลอดภัยในคุณสมบัติของฮาร์ดแวร์ ซอฟท์แวร์ และสิ่งอำนวยความสะดวก

(6.3) วิธีการปฏิบัติงานของข้อกำหนดการออกแบบฮาร์ดแวร์ ซอฟท์แวร์ และสิ่งอำนวยความสะดวก และการดำเนินการแก้ไขที่ไม่ทำให้ความปลอดภัยของระบบลดลงหรือเกิดอันตรายเพิ่มขึ้น

SHA อาจใช้ร่วมและ/หรือดำเนินการโดยใช้เทคนิคที่คล้ายกันกับกับเทคนิคที่ใช้สำหรับ SHA และเมื่อมีการพัฒนาซอฟท์แวร์ที่ใช้ร่วมกับระบบ บุคคลที่ดำเนินการ SHA ต้องตรวจสอบ รับและใช้เอ้าพุตของแต่ละช่วงของกระบวนการพัฒนาซอฟท์แวร์อย่างเป็นทางการเพื่อประเมินซอฟท์แวร์ที่มีส่วนใน SHA

SHA นี้ต้องได้รับการอัปเดตที่เป็นผลมาจากการปลี่ยนแปลงการออกแบบของระบบ รวมถึงการเปลี่ยนแปลงการออกแบบซอฟท์แวร์ ซึ่งมีผลต่อความปลอดภัยของระบบ

ก.5 การวิเคราะห์อันตรายจากการทำงานและสนับสนุน (Operating and Support Hazard Analysis)

ก.5.1 วัตถุประสงค์

การวิเคราะห์ Operating and Support Hazard Analysis (O&SHA) ต้องประเมินการปฏิบัติงานสำหรับอันตรายหรือความเสี่ยงที่นำมาใช้ในระบบ ซึ่งมาจากขั้นตอนในการทำงานและสนับสนุนเพื่อประเมินความเพียงพอของขั้นตอนที่ใช้ในการกำจัด ควบคุม หรือบรรเทาอันตรายหรือความเสี่ยงที่ระบุไว้ โดยที่ O&SHA ต้องรวมไปถึงการทำงานอัตโนมัติ (automatic operations) การทำงานด้วยคน (manual operations) ระเบียบการรักษาความปลอดภัย (ตามที่เลือกโดยการรักษาความปลอดภัยสำหรับการวิเคราะห์) ขั้นตอนในกรณีฉุกเฉิน และขั้นตอนการติดตั้งและซ่อมบำรุง

ก.5.2 รายละเอียด

O&SHA ต้องดำเนินการเพื่อตรวจสอบการฏิบัติงานที่ได้รับการควบคุมตามขั้นตอน โดยที่ O&SHA ได้ระบุและตรวจสอบความเสี่ยงที่มาจากการปฏิบัติงานหรือภารกิจโดยบุคคล โดยคำนึงถึงสิ่งต่อไปนี้

(1) การกำหนดรูปแบบตามแผนหรือสถานะในแต่ละช่วงของการปฏิบัติงานของระบบ

(2) การเชื่อมต่อของสิ่งอำนวยความสะดวก

(3) สภาพแวดล้อมที่วางแผนไว้ หรือขอบเขตดังกล่าว

(4) เครื่องมือในการสนับสนุนหรืออุปกรณ์อื่น รวมถึงซอฟท์แวร์ที่ควบคุมอุปกรณ์การทดสอบอัตโนมัติ ซึ่งถูกระบุสำหรับการใช้งาน ลำดับการทำงานหรือภารกิจ ผลกระทบและข้อจำกัดของงานที่ทำพร้อมกัน

(5) ความเป็นไปได้ของเหตุการณ์ที่ไม่ได้วางแผนไว้ รวมถึงความเสี่ยงที่มาจากความผิดพลาดของมนุษย์

มนุษย์ต้องถูกพิจารณาให้เป็นองค์ประกอบทั้งหมดในระบบ ทั้งอินพุตที่ได้รับและเอ้าท์พุตเริ่มต้น ตลอดการวิเคราะห์นี้ ซึ่ง O&SHA ต้องระบุข้อกำหนดด้านความปลอดภัยหรือทางเลือกอื่น ที่จำเป็น

ในการกำจัดหรือควบคุมความเสี่ยงที่ถูกระบุหรือเพื่อลดความเสี่ยงที่เกี่ยวข้องให้อยู่ในระดับที่ยอมรับได้ภายใต้เกณฑ์ที่กำหนดตามกฎระเบียบหรือตามสัญญา

โดยที่การวิเคราะห์นี้ต้องระบุตามข้อดังต่อไปนี้

(1) การปฏิบัติงานที่เกิดขึ้นภายใต้สภาวะอันตราย ช่วงเวลาและการดำเนินการที่จำเป็นเพื่อลดความเสี่ยงระหว่างการปฏิบัติงานและช่วงเวลาเหล่านั้น

(2) การเปลี่ยนแปลงที่จำเป็นในข้อกำหนดการทำงานหรือการออกแบบสำหรับฮาร์ดแวร์และซอฟท์แวร์ของระบบ สิ่งอำนวยความสะดวก เครื่องมือ หรืออุปกรณ์สนับสนุนและอุปกรณ์ทดสอบ เพื่อลดและควบคุมอันตราย หรือเพื่อลดความเสี่ยงที่เกี่ยวข้อง

(3) ข้อกำหนดสำหรับอุปกรณ์ด้านความปลอดภัย รวมถึงอุปกรณ์ป้องกันความปลอดภัยส่วนบุคคลและอุปกรณ์ช่วยชีวิต

(4) คำเตือน ข้อควรระวัง และขั้นตอนเหตุฉุกเฉินพิเศษ เช่น ทางออก การช่วยเหลือและการหลบหนี รวมถึงสิ่งที่จำเป็นจากความล้มเหลวของการทำงานที่ควบคุมด้วยซอฟท์แวร์คอมพิวเตอร์เพื่อให้ได้ผลลัพธ์หรือตัวบ่งชี้ที่ต้องการ

(5) ข้อกำหนดสำหรับการบรรจุ การจัดการ การจัดเก็บ การขนส่ง การบำรุงรักษา และการกำจัดวัตถุอันตราย

(6) ข้อกำหนดสำหรับการฝึกอบรมด้านความปลอดภัยและการรับรองบุคลากร

(7) ผลกระทบของฮาร์ดแวร์และซอฟต์แวร์ที่ไม่ได้รับการพัฒนาเชื่อมต่อกับส่วนประกอบอื่นของระบบหรือระบบย่อย

(8) สถานะของระบบที่อาจเป็นอันตรายภายใต้การควบคุมของผู้ปฏิบัติงาน

O&SHA ต้องจัดทำเอกสารการประเมินความปลอดภัยของระบบในขั้นตอนที่เกี่ยวกับการผลิต การใช้งาน การติดตั้ง การทดสอบ การเดินรถ การซ่อมบำรุง การให้บริการ การขนส่ง การจัดเก็บ การดัดแปลง การยกเลิกการควบคุม (demilitarization) และการกำจัดของระบบ

O&SHA ต้องได้รับการอัปเดตตามผลของการออกแบบระบบหรือการเปลี่ยนแปลงการทำงานใด ๆ

ก.6 รายงานการรับรองความปลอดภัยของระบบ (System Safety Certification Report)

ก.6.1 วัตถุประสงค์

System Safety Certification Report (SSCR) ต้องแสดง Hazard Tracking Log และจัดทำเอกสารการปฏิบัติงานการแก้ไขความเสี่ยง สรุปผลการตรวจสอบและยืนยันความถูกต้องขององค์ประกอบฮาร์ดแวร์และซอฟต์แวร์ที่สำคัญต่อความปลอดภัยทั้งหมดของระบบ รวมทั้งรักษาบันทึก (permannt record) ของใบรับรองความปลอดภัยทั้งหมด

ก.6.2 รายละเอียด

SSCR ต้องเริ่มต้นด้วย PHA ที่มีการอัปเดตเป็นระยะตลอดการออกแบบ การตรวจสอบและการรับรองความถูกต้องของโครงการ APM และรักษากระแสไฟตลอดอายุการใช้งานของ APM

โดยเป็นพื้นฐานให้เข้าใจสถานะของการรับรองความปลอดภัยของระบบที่ได้จากการดำเนินการ SSPP อีกทั้ง รายงานต้องพิจารณาการรับรององค์ประกอบฮาร์ดแวร์และซอฟท์แวร์ที่มีความสำคัญด้านความปลอดภัยแต่ละรายการของระบบ และระบบ APM ทั้งหมด โดยที่ SSCR ต้องมีรายละเอียดดังข้อต่อไปนี้

(1) รายงานสรุปผู้บริหาร ที่ระบุความคืบหน้าของการรับรอง ปัญหา การปฏิบัติถัดไป รายงานความปลอดภัยที่ใช้อยู่ แดชบอร์ดการจัดการขององค์ประกอบในการรับรอง และแดชบอร์ดการจัดการของ Hazard Tracking Log

(2) รายงานความปลอดภัยที่ใช้อยู่ (active safety bulletins)

(3) รายงานความปลอดภัยที่ได้รับการแก้ไข (resolved safety bulletins)

(4) สถานะการรับรองในแต่ละองค์ประกอบของฮาร์ดแวร์และซอฟท์แวร์ที่มีความสำคัญต่อความปลอดภัย

(5) สถานะการรับรองของระบบ APM

(6) Hazard Tracking Log ที่เป็นข้อมูลพื้นฐานในปัจจุบัน

(7) ประเด็นอื่น ๆ ที่ระบุไว้ในการตรวจสอบความปลอดภัยของ SSPP

ข้อแนะนำสำหรับภาคผนวก ก การวางแผนความปลอดภัยของระบบ (System Safety Program Plan)

ข้อกำหนดสำหรับ SSPP ที่ระบุในหัวข้ออื่นของมาตรฐานนี้ มีดังนี้

มขร. – SC – 005 - 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านระบบอาณัติสัญญาณ

2.1 แผนความปลอดภัยของระบบ (system safety program)

2.1.2 กระบวนการแก้ไขความเสี่ยง (hazard resolution process)

มขร. – S – 003 - 2567 มาตรฐานความปลอดภัยทั่วไปของระบบขนส่งผู้โดยสารอัตโนมัติ

4.1 แผนโครงการเตรียมความพร้อมในกรณีฉุกเฉิน

5.1 ข้อบังคับที่ระบบควรมีก่อนดำเนินการทวนสอบ

6.4 การวิเคราะห์การซ่อมแซมการให้บริการ (service restoration analysis)

6.7 การซ่อมบำรุง

7.2 ความรับผิดชอบในการตรวจสอบภายในแบบรายปี

7.5 การจัดการการตั้งค่า

7.8 แผนการเกี่ยวกับการละเมิดข้อบังคับเรื่องสารเสพติดและเครื่องดื่มและสุรา

7.9 กำหนดรายการเกี่ยวกับการควบคุมการใช้ยาและสุรา

7.11 กระบวนการการจัดซื้อ

ข้อแนะนำสำหรับภาคผนวก ก.2 การวิเคราะห์อันตรายเบื้องต้น (Preliminary Hazard Analysis)

รายการความเสี่ยงเบื้องต้น (Preliminary Hazard List: PHL) มักถูกใช้เป็นรากฐานสำหรับการวิเคราะห์อันตรายเบื้องต้น โดยในช่วงต้นของแผนนั้น การตรวจสอบรายละเอียดของระบบ APM แนวคิดในการให้บริการ และการตรวจสอบระบบที่คล้ายกัน รวมถึงรายงานผลอุบัติเหตุที่ใช้เพื่อรวบรวมรายการความเสี่ยง ตลอดจนอุบัติเหตุและสาเหตุที่อาจเกิดขึ้น โดยวัตถุประสงค์ของ PHL คือ เพื่อระบุอันตรายที่อาจเกิดขึ้น ระบุปัจจัยที่สำคัญต่อความปลอดภัย และกำหนดรูปแบบของอุบัติเหตุ ซึ่งการวิเคราะห์อันตรายที่ระบุไว้และการประเมินความเสี่ยง ถูกอ้างถึงจากการวิเคราะห์อันตรายเบื้องต้น (Preliminary Hazard Analysis) และการวิเคราะห์ถัดไป ทั้งนี้ ระบบนี้ต้องได้รับการประเมินในหลายรูปแบบการทำงาน เช่น รูปแบบอัตโนมัติ การซ่อมบำรุง กรณีฉุกเฉิน และการคืนสภาพ

เมื่อมีการพัฒนาความเสี่ยง ควรระวังในการเลือกใช้คำ และรายละเอียดความเสี่ยงควรอธิบายเงื่อนไขที่อาจทำให้เกิดอุบัติเหตุ โดยไม่ระบุอุบัติเหตุหรือสาเหตุที่อาจเกิดขึ้น ซึ่งการแยกอันตรายจากอุบัติเหตุและสาเหตุนั้น ช่วยให้วิเคราะห์และเลือกความเสี่ยงในการกำจัดหรือลดความเสี่ยงได้ โดยที่การบรรเทาความเสี่ยงสามารถกำจัดทั้งความเสี่ยงเองและสามารถบอกถึงสาเหตุที่เป็นไปได้

ยกตัวอย่างเช่น ความเสี่ยงที่คนจะสัมผัสกับขบวนรถที่กำลังเคลื่อนที่อยู่ในระบบ APM การวิเคราะห์สามารถระบุกลุ่มของผู้คนที่อาจได้รับผลกระทบความเสี่ยงนี้ อุบัติเหตุที่ตามมา และสาเหตุที่เป็นไปได้ ซึ่งรายการตัวอย่างของหมวดหมู่อุบัติเหตุและกลุ่มที่ได้รับผลกระทบระบุในตาราง ก-1 และตารางที่ ก-2 แสดง

ตัวอย่างการระบุความเสี่ยงเบื้องต้นและสาเหตุที่เป็นไปได้ ทั้งนี้ การวิเคราะห์อันตรายอย่างละเอียดทำตามที่เห็นสมควรและตามความเหมาะสม

ตาราง ก-1 รายการตัวอย่างหมวดหมู่อุบัติเหตุและกลุ่มที่ได้รับผลกระทบ

หมวดอุบัติเหตุ	กลุ่มที่ได้รับผลกระทบ	โหมดการทำงานของระบบ
การชนกันของขบวนรถต่อขบวนรถ การชนกันระหว่างขบวนรถกับโครงสร้าง ขบวนรถชนกับวัตถุอื่น ขบวนรถตกราง คนถูกขบวนรถชน คนบาดเจ็บในขบวนรถ คนบาดเจ็บจากอุปกรณ์ คนบาดเจ็บจากแหล่งพลังงาน คนบาดเจ็บจากสาเหตุอื่น ความเสียหายต่อโครงสร้างพื้นฐาน APM ความเสียหายต่ออุปกรณ์ APM ความเสียหายต่อทรัพย์สินของ APM ความเสียหายต่อทรัพย์สิน (ของผู้อื่น) ความเสียหายต่อสิ่งแวดล้อม ความล่าช้าในการให้บริการ ความล่าช้าของทางออกฉุกเฉิน ความล่าช้าในการเข้าถึงการช่วยเหลือ ไม่มี	พนักงาน ความปลอดภัย ผู้บุกรุก ผู้โดยสาร การตอบสนองฉุกเฉิน สาธารณะ สิ่งแวดล้อม โครงสร้างพื้นฐานของ APM ทรัพย์สิน APM อุปกรณ์ APM ทรัพย์สินของผู้อื่น ไม่มี	อัตโนมัติ การซ่อมบำรุง เหตุฉุกเฉิน/การคืนสภาพ (ขบวนรถ) เหตุฉุกเฉิน/กาคืนสภาพ (ระบบ)

ตาราง ก-2 ตัวอย่างการพัฒนารายการความเสี่ยงเบื้องต้น (preliminary hazard list)

คำอธิบายอันตราย	อุบัติเหตุ	กลุ่มที่ได้รับผลกระทบ	สาเหตุที่เป็นไปได้
1. บุคคลที่สัมผัสกับขบวนรถที่กำลังเคลื่อนที่			
1.01 คนที่ชานชาลาในเส้นทางของรถบริการที่กำลังเคลื่อนที่	คนถูกขบวนรถชน	ผู้โดยสาร พนักงาน รปภ. ผู้โดยสาร พนักงาน รปภ. ผู้โดยสาร พนักงาน รปภ. ผู้โดยสาร พนักงาน รปภ. ผู้โดยสาร พนักงาน รปภ.	บุคคลอยู่ใกล้ขอบชานชาลามากเกินไป ชานชาลาที่หนาแน่นเกินไป มีคนล้มลงบนทางวิ่งบังคับ บุคคลจงใจก้าวเข้าสู่ทางวิ่งบังคับ บุคคลถูกผลักเข้าสู่ทางวิ่งบังคับโดยเจตนา
1.02 คนที่ชานชาลาในเส้นทางการเคลื่อนย้ายรถซ่อมบำรุง	คนถูกขบวนรถชน	ผู้โดยสาร พนักงาน รปภ. ผู้โดยสาร พนักงาน รปภ. ผู้โดยสาร พนักงาน รปภ. ผู้โดยสาร พนักงาน รปภ. ผู้โดยสาร พนักงาน รปภ.	บุคคลอยู่ใกล้ขอบชานชาลามากเกินไป ชานชาลาที่หนาแน่นเกินไป มีคนล้มลงบนทางวิ่งบังคับ บุคคลจงใจก้าวเข้าสู่ทางวิ่งบังคับ บุคคลถูกผลักเข้าสู่ทางวิ่งบังคับโดยเจตนา
1.03 คนที่อยู่บนทางวิ่งบังคับของรถที่ให้ บริการที่กำลังเคลื่อนที่	คนถูกขบวนรถชน	พนักงาน รปภ. ผู้บุกรุก ผู้โดยสาร เจ้าหน้าที่ฉุกเฉิน	การซ่อมบำรุงบนหรือใกล้ทางวิ่งบังคับ การรักษาความปลอดภัยบนหรือใกล้ทางวิ่งบังคับ ผู้บุกรุกบนหรือใกล้ทางวิ่งบังคับ ทางออกฉุกเฉินบนหรือใกล้ทางวิ่งบังคับ การกู้ภัยบนหรือใกล้ทางวิ่งบังคับ
1.04 คนที่อยู่ในเส้นทางของรถบำรุงรักษาที่กำลังเคลื่อนที่	คนถูกขบวนรถชน	พนักงาน รปภ. ผู้โดยสาร เจ้าหน้าที่ฉุกเฉิน พนักงาน	การซ่อมบำรุงบนหรือใกล้ทางวิ่งบังคับ การรักษาความปลอดภัยบนหรือใกล้ทางวิ่งบังคับ ทางออกฉุกเฉินบนหรือใกล้ทางวิ่งบังคับ การกู้ภัยบนหรือใกล้ทางวิ่งบังคับ
1.05 การเคลื่อนย้ายผู้โดยสารระหว่างชานชาลาและรถบริการ	คนถูกขบวนรถชน	ผู้โดยสาร ผู้โดยสาร	รถให้บริการเคลื่อนย้ายระหว่างการขนย้ายผู้โดยสาร ผู้โดยสารติดอยู่ระหว่างแผงกั้นขอบขบวนรถและชานชาลา
1.06 การเคลื่อนตัวขบวนรถมากเกินไป	ผู้ได้รับบาดเจ็บจากอุบัติเหตุ	ผู้โดยสาร ผู้โดยสาร	ผู้โดยสารล้มเพราะรถกระชากมากเกินไป วัตถุในตัวรถเคลื่อนที่หรือตกใส่ผู้โดยสาร

ภาคผนวก ข
อุปกรณ์ทางไฟฟ้า

ข.1 ทั่วไป

ข้อกำหนดต่อไปนี้ จะต้องใช้กับอุปกรณ์ไฟฟ้าทั้งหมดของ APM

ข.1.1 ความปลอดภัย ผู้โดยสาร บุคลากรที่ควบคุมการทำงานและซ่อมบำรุง และบุคลากรที่ดูแลเหตุการณ์ฉุกเฉิน จะต้องได้รับการป้องกันจากการสัมผัสกับแรงดันไฟฟ้าที่อาจส่งผลให้เกิดการบาดเจ็บหรือเสียชีวิตได้

สำหรับระบบ APM ที่มี blue light station เช่น ระบบที่อยู่ในอุโมงค์ ต้องเป็นไปตามที่ได้ระบุไว้ในหัวข้อที่ 6.4.2 ของมาตรฐาน NFPA 130 หรือมาตรฐานอื่นที่เทียบเท่า

ข.1.2 การควบคุมการกัดกร่อน เพื่อที่จะหลีกเลี่ยงการเสื่อมสภาพของวัสดุที่มีโครงสร้างเป็นโลหะ การตรวจสอบป้องกันกระแสรั่วไหลจะต้องมีกระแสรั่วไหลลงดิน (stray earth currents) อยู่ในขอบเขตที่ยอมรับได้ โดยยังคงต้องรักษาค่าความต้านทานขั้นต่ำของรางย้อนกลับลบ (negative return rail) ไปยังกราวด์ ตามหัวข้อที่ ข.3.8 และตามข้อบังคับของมาตรฐาน NACE RP0169 หรือมาตรฐานอื่นที่เทียบเท่า อีกทั้ง สำหรับระบบขับเคลื่อนแบบไฟฟ้ากระแสตรง จะต้องมีการทดสอบบนโครงสร้างระบบที่ต่อด้วยไฟฟ้าทั้งหมดเพื่อวัดและเฝ้าระวังกระแสรั่วไหล

การป้องกันการกัดกร่อนด้วยปฏิกิริยาแคโทด (cathodic protection) อาจจะถูกนำมาประยุกต์ใช้เพื่อป้องกันการเกิดแบคทีเรียที่เจริญเติบโตได้โดยไม่ใช้ออกซิเจน (anaerobic bacteria) โดยจำเป็นต้องมีแผนการที่สามารถป้องกันร่วมกันในเรื่องข้อจำกัดของ cathodic ที่จะไม่สามารถเข้าถึงได้หลังจากการติดตั้งเสร็จสิ้น และมีวิธีในการทดสอบด้วย

ข.1.3 การป้องกันระบบไฟฟ้า มีการป้องกันอัตโนมัติเมื่อเกิดความผิดพร่องจาก กระแสเกิน กระแสย้อนกลับ แรงดันเกิน แรงดันต่ำเกิน การเปิดค้าง (lockout) ความผิดพร่องลงดิน (ground fault) และลำดับเฟส เมื่อปรับใช้กับระบบจ่ายกำลังไฟฟ้ากระแสสลับหรือกระแสตรง ระบบป้องกันต้องมีการเลือกใช้อย่างถูกต้อง เช่น อุปกรณ์ป้องกันทุกชิ้นจะต้องสามารถทำงานร่วมกันได้เพื่อเวลาที่เกิดการผิดพร่องหรือกระแสเกินจะส่งผลให้เกิดการตัดวงจรในส่วนที่เล็กที่สุดของระบบ ดังข้อแนะนำในหัวข้อที่ 1 First Principles จากมาตรฐาน IEEE 242 หรือมาตรฐานอื่นที่เทียบเท่า

การเกิดเฟสไม่สมดุล และรีเลย์ที่ไวต่อการเกิดฮาร์มอนิก จะต้องมีการติดตั้งตัวกรองฮาร์มอนิก (harmonic filters) เพื่อที่จะให้อุปกรณ์ที่เถียรภาพน้อยที่สุดยังคงสามารถทำงานได้ตามปกติ โดยอุปกรณ์และวงจรทั้งหมดต้องมีการป้องกันเสริจ์และป้องกันความผิดพร่องลงดิน โดยที่ระบบจะต้องทำงานร่วมกันกับเครื่องตัดวงจรเมื่อผิดพร่องลงดิน (ground-fault circuit interrupter) หรืออุปกรณ์อื่น ๆ ที่มีหน้าที่สำหรับป้องกันความปลอดภัยของบุคลากร อุปกรณ์ป้องกันความผิดพร่องลงดินจะทำงานโดยการตัดพลังงานของวงจรหรือส่วนใดส่วนหนึ่งของวงจรภายในระยะเวลาที่กำหนด โดยจะทำงานเมื่อมีกระแสไฟรั่วไหลลงดินเกินค่าที่กำหนดไว้ ซึ่งกระแสไฟฟ้าที่ทำให้อุปกรณ์ของความผิดพร่องลงดินทำงานนั้น จะต้องมีค่าที่น้อยกว่ากระแสที่ใช้ในการสั่งให้อุปกรณ์ป้องกันกระแสเกินทำงาน เมื่อเกิดการทริปของตัวตัดวงจรจะต้องมีสัญญาณแสดงและมีการแจ้งเตือนเกิดขึ้นที่ศูนย์ควบคุมส่วนกลาง และจะต้องมีอุปกรณ์ป้องกันการเกิดฟ้าผ่า ตามที่ได้

ระบุไว้ใน มขร. – S – 003 – 2567 มาตรฐานความปลอดภัยทั่วไปของระบบขนส่งผู้โดยสารอัตโนมัติ หัวข้อที่ 2.1.4

ข.1.4 การต่อลงดิน (Grounding) เนื้อหาในส่วนนี้จะกล่าวถึงข้อกำหนดสำหรับการต่อลงดินของระบบ APM ข้อกำหนดเกี่ยวกับการต่อลงดินของอุปกรณ์ตัวอื่นๆจะถูกระบุอยู่ใน มขร. – R – 007 - 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านเครื่องกลและตัวรถ บทที่ 2.12.5

ระบบการต่อลงดินนั้นจะต้องป้องกันอุปกรณ์จากการได้รับความเสียหายจากแรงดันไฟฟ้าและกระแสไฟฟ้า และจะต้องถูกออกแบบให้สามารถปกป้องอันตรายจากไฟดูด (electric shock) โดยข้อกำหนดที่ได้กล่าวไปข้างต้นจะเน้นไปที่เรื่องความปลอดภัย และการต่อลงดินเพิ่มเติมสำหรับป้องกันอุปกรณ์ประเภทไมโครโพรเซสเซอร์ หรืออุปกรณ์อื่น ๆ ต้องมีการคำนึงถึงอันตรายที่เกิดจากไฟฟ้าผ่านการวิเคราะห์อันตรายโดยอิงจากหัวข้อที่ 2.1.2

ข.1.4.1 การต่อลงดินสำหรับระบบขับเคลื่อน รางสายดินที่ไม่มีกระแสไหลผ่าน (non-current-carrying ground rail) จะต้องมีการต่อลงดินอย่างต่อเนื่องกับตัวรถ โดยความต้านทานระหว่างสายดินกับพื้นโลกต้องมีไม่มากไปกว่า 5 โอห์ม เมื่อวัดโดยอ้างอิงจากมาตรฐาน IEEE 142 หัวข้อที่ 44 หรือมาตรฐานอื่นที่เทียบเท่า

สำหรับระบบจ่ายกำลังไฟฟ้าสำหรับต้นกำลังในการขับเคลื่อนแบบกระแสตรง current-carrying return ห้ามมีการต่อประสานลงดินแบบจุดเดียว (single-point ground) มากกว่า 1 ตำแหน่งอยู่ในระบบ APM และต้องมีการป้องกันการกัดกร่อนด้วยปฏิกิริยาแคโทด เพื่อป้องกันโครงสร้างส่วนอื่น ๆ และอุปกรณ์อื่น ๆ ที่อยู่ในบริเวณเดียวกันกับสายดิน

ภายใต้สถานการณ์ที่มีกระแสไฟฟ้าทำงานสูงที่สุดหรือกระแสไฟฟ้าผิดพร่องบนตัวรถ สายดินสำหรับระบบขับเคลื่อนต้องไม่ยอมให้มีแรงดันสัมผัสมากกว่า 60 โวลต์ ไม่ว่าจะบริเวณใดก็ตามบนตัวรถ โดยเมื่อวัดระหว่างสายดินกับตัวรถ หรือกับชานชาลาของสถานีที่อยู่ติดกัน พื้นผิวอุปกรณ์ที่เป็นโลหะหรือโครงสร้างของทางวิ่งที่เป็นโลหะ ในขณะเดียวกัน ภายใต้สถานการณ์ที่มีกระแสผิดพร่องที่เลวร้ายที่สุดเกิดขึ้น ตัวระบบจะต้องไม่ยอมให้มีแรงดันมากกว่า 60 โวลต์ บนพื้นผิวใด ๆ เมื่อวัดระหว่างพื้นผิวกับจุดเชื่อมต่อกับสายดินในสถานีไฟฟ้านั้น ๆ

สำหรับระบบจ่ายกำลังไฟฟ้าขับเคลื่อนกระแสตรง การนำรางสายดินที่ไม่มีกระแสไหลผ่าน (non-current-carrying ground rail) ออกจากระบบนั้น สามารถนำมาพิจารณาได้ ถ้าหากว่ามีวิธีการอื่นใดในระดับเดียวกันที่จะสามารถป้องกันกระแสรั่วไหล และในกรณีที่เกิดการผิดพร่องในระบบไฟฟ้า สถานีไฟฟ้าย่อยต้องสามารถเข้าถึงบัสลบ (negative bus) เพื่อการตรวจสอบกระแสรั่วไหลได้ และแรงดันไฟฟ้าเมื่อวัดเทียบกับสายดินในรางย้อนกลับลบบนทางสายหลัก (mainline) จะต้องไม่เกิน 60 V และแรงดันไฟฟ้าเมื่อวัดเทียบกับสายดินในรางย้อนกลับลบบนลานจอด (yard) จะต้องไม่เกิน 10 V

ทางวิ่งภายในศูนย์ซ่อมบำรุง จะต้องต่อสายดินกับอาคารโรงซ่อมบำรุงและระบบสายดินของศูนย์ซ่อมบำรุง ระบบไฟฟ้าของทางวิ่งในศูนย์ซ่อมบำรุงต้องมีฉนวนกันระหว่างทางวิ่งในลานจอด

สำหรับระบบไฟฟ้ากระแสตรงที่ใช้สายดินแบบการต่อประสานลงดินแบบจุดเดียว (single-point ground) สายดินของอาคารศูนย์ซ่อมบำรุงจะต้องถูกแบ่งแยกจากในส่วนของลานจอดและระบบสายดินของทางวิ่งสายหลัก

การต่อไฟแบบขนานชั่วคราว (Temporary paralleling) อนุญาตให้ทำได้ในการสับเปลี่ยนขบวนระหว่างโรงซ่อมบำรุงกับลานจอดหรือลานจัดเก็บ

ข.1.4.2 การต่อลงดินสำหรับอุปกรณ์อำนวยความสะดวกและโครงสร้าง จะต้องมีการต่อลงดินสำหรับอุปกรณ์อำนวยความสะดวกที่ติดตั้งอยู่กับที่และบนโครงสร้าง ตามมาตรฐาน NFPA 70 โดยที่การต่อลงดินจะต้องมีกราวด์แมท (ground mat) ด้านใต้สถานีหรือสิ่งอำนวยความสะดวก และประกอบไปด้วยระบบการต่อลงดินแบบฝัง grid-and-rod อีกทั้ง ต้องจัดให้มีการต่อร่วมกับเสาเหล็กและโครงสร้างเหล็กเสริมแรง

การวิเคราะห์อันตรายจะต้องระบุความปลอดภัยของสายดินระหว่างการอพยพฉุกเฉินตามหัวข้อที่ 2.1.2.1

ข.1.5 ความซ้ำซ้อน (Redundancy) ระบบจ่ายกำลังไฟฟ้าจะต้องออกแบบให้มีความซ้ำซ้อนเพียงพอเพื่อป้องกันการหยุดทำงานของระบบ APM จากการผิดพร่องของอุปกรณ์ไฟฟ้าเพียงจุดเดียว การทำงานในรูปแบบลดประสิทธิภาพสามารถทำได้ ความผิดพร่องของอุปกรณ์ที่สำคัญในระบบจ่ายกำลังไฟฟ้าจะต้องมีการแจ้งเตือนตามที่ได้ระบุในหัวข้อที่ 4.3.2.2

หมายเหตุ: ข้อกำหนดในด้านความพร้อมใช้งานในการให้บริการในหัวข้อที่ 3.3 อ้างอิงจากระบบที่มีต้นกำลังหลักทำงานอยู่อย่างเต็มรูปแบบ

ข.1.6 อายุในการใช้งานตามการออกแบบ หม้อแปลง วงจรเรียงกระแส และสายไฟต่าง ๆ จะต้องออกแบบโดยอิงอายุการใช้งานอยู่ที่ 30 ปี เว้นเสียแต่ว่าถูกระบุอย่างชัดเจนจากเจ้าของโครงการ รางจ่ายไฟและอุปกรณ์ถาวรอื่น ๆ จะต้องถูกออกแบบให้มีอายุการใช้งานอยู่ที่ 15 ปี เว้นเสียแต่ว่าถูกระบุอย่างชัดเจนจากเจ้าของโครงการ

ข.1.7 การรักษาระดับแรงดันไฟฟ้า ระบบจ่ายกำลังไฟฟ้าจะต้องถูกออกแบบให้มีความมั่นคง กล่าวคือ ระหว่างการทำงานสภาวะปกติ จะต้องมีการรักษาระดับแรงดันให้อยู่ในระดับที่เหมาะสมเมื่อมีการใช้งาน โดยที่การรักษาระดับแรงดันไฟฟ้ายังรับประกันว่าอายุการใช้งานของมอเตอร์ต่าง ๆ บนตัวรถไม่เสื่อมลงก่อนเวลาอันควร

ข.1.8 ความจุ อุปกรณ์ต่าง ๆ รวมไปถึงสายส่งและรางจ่ายไฟจะต้องถูกออกแบบให้สามารถรองรับโหลดสูงสุดได้ ไม่ว่าจะเป็นโหมดเริ่มเดินเครื่อง โหมดทำงานตามปกติ โหมดทำงานตอนลดคุณภาพ และการทำงานในโหมดกู้คืนการทำงานของการปล่อยขบวนรถมาให้บริการเต็มรูปแบบตามที่วางแผนไว้ อุปกรณ์ของสถานีไฟฟ้าย่อยสำหรับต้นกำลังในการขับเคลื่อนและอุปกรณ์ที่เกี่ยวข้องกับสายไฟสำหรับจ่ายกำลังไฟฟ้าและอุปกรณ์อื่น ๆ จะต้องออกแบบให้มีอายุการใช้งานโดยอ้างอิงจากการทำงานที่มีโหลดขนาด AW2 ตามที่ได้ระบุใน มขร. – R – 007 - 2567 มาตรฐานระบบขนส่งผู้โดยสารอัตโนมัติด้านเครื่องกลและตัวรถ หัวข้อที่ 2.1

หากระบบ APM ดังกล่าว มีแผนที่จะขยายในเฟสข้างหน้า อุปกรณ์ทั้งหมดอาจไม่จำเป็นต้องระบุตั้งแต่ทีแรก อย่างไรก็ตาม การออกแบบควรจะคำนึงถึงการต่อเติมของอุปกรณ์ในอนาคตตามที่ระบบมีการขยาย

ข.2 อุปกรณ์ของสถานีไฟฟ้าย่อยสำหรับระบบขับเคลื่อน

อุปกรณ์สำหรับสถานีไฟฟ้าย่อยจะต้องถูกออกแบบด้วยเกณฑ์ในการเชื่อมต่อและการทำงานดังต่อไปนี้

ข.2.1 การเชื่อมต่อกับการไฟฟ้าท้องถิ่น ทุกอุปกรณ์ไฟฟ้าจะต้องสามารถเชื่อมต่อกันได้อย่างถูกต้องกับการไฟฟ้าท้องถิ่น

ข.2.2 ตัวประกอบกำลังไฟฟ้า (power factor) ค่าตัวประกอบกำลังไฟฟ้าของระบบเมื่อทำงานโดยเฉลี่ยมากกว่า 2 ชั่วโมง จะต้องได้อย่างน้อยค่าตัวประกอบกำลังแบบตามหลัง 0.8 (power factor 0.8 in lagging) และต้องไม่มีการได้ค่าตัวประกอบกำลังแบบนำหน้า ค่านี้อาจทำได้โดยการใช้อุปกรณ์แก้ไขตัวประกอบกำลังเมื่อจำเป็น โดยที่ตัวประกอบกำลังจะต้องถูกวัดที่จุดเชื่อมต่อระหว่างการไฟฟ้าท้องถิ่นกับระบบ APM ทั้งนี้ การประสานงานกับการไฟฟ้าท้องถิ่นจะต้องเกิดขึ้นในระหว่างการออกแบบระบบ

ข.2.3 ฮาร์มอนิก อุปกรณ์แปลงกำลังและองค์ประกอบโหลดภายในระบบจะต้องถูกออกแบบให้จุดเชื่อมต่อระหว่างการไฟฟ้ากับระบบ APM นั้นเป็นไปตามขีดจำกัดความเพี้ยนแรงดัน (voltage distortion limits) ตามข้อกำหนดในตารางที่ 11.1 ในมาตรฐาน IEEE 519 หรือมาตรฐานอื่นที่เทียบเท่า

ข.2.4 ระบบการเฝ้าติดตามและแจ้งเตือน อุปกรณ์สำหรับแสดงสถานะจะต้องถูกติดตั้งในแต่ละสถานีไฟฟ้าย่อยเพื่อที่จะแสดงแรงดันไฟฟ้า กระแสไฟฟ้า และกำลังไฟฟ้าที่ต้องการ สภาวะที่ไม่ปกติจะถูกส่งไปแจ้งเตือนยังศูนย์ควบคุมกลาง ตามหัวข้อที่ 4.3.2.2 และ 4.3.2.3 โดยค่าสถานะขั้นต่ำที่ต้องมีการแจ้งเตือน ได้แก่

1. แรงดันเกิน (Overvoltage)
2. แรงดันต่ำเกิน (Undervoltage)
3. กระแสเกิน (Overcurrent)
4. ความผิดพร่องลงดิน (Ground fault)
5. Switchgear local mode (ดูที่หัวข้อ ข.2.7)
6. อุณหภูมิเกิน (Overtemperature)
7. แรงดันเฟสใดเฟสหนึ่งหายไป (Loss of phase)
8. ไฟไหม้หรือกลุ่มควัน (Fire or smoke)

หม้อแปลงและวงจรเรียงกระแสทั้งหมดจะต้องมีการติดตั้งเซ็นเซอร์ตรวจวัดอุณหภูมิ ที่สามารถแจ้งเตือนไปยังศูนย์ควบคุมกลางและปิดการทำงานของอุปกรณ์โดยอัตโนมัติเมื่ออุณหภูมิเพิ่มขึ้นถึงค่าที่กำหนด สัญญาณเตือนจะถูงส่งเมื่ออุณหภูมิเกินค่าที่กำหนด และส่งสัญญาณเตือนอีกครั้งเมื่ออุณหภูมิสูงเกินค่าวิกฤตและปิดการทำงานของอุปกรณ์นั้น

ข.2.5 อุปกรณ์จ่ายพลังงานไฟฟ้ากลับคืน ระบบขับเคลื่อนแบบพลังงานกลับคืนอาจถูกระบุไว้ หากมีการระบุไว้ ระบบต้องใช้ความสามารถในการจ่ายพลังงานกลับคืนสำหรับขบวนรถได้อย่างมีประสิทธิภาพ ระบบต้องถูกออกแบบให้สามารถรองรับสภาวะแรงดันเกินสูงสุด ที่เกิดจากการจ่ายพลังงานไฟฟ้ากลับคืนในสภาวะความเร็วสูงสุด การบรรทุกสูงสุด และความยาวขบวนรถสูงสุด ซึ่งข้อกำหนดสำหรับการจ่ายพลังงานกลับคืนจะต้องป้องกันแรงดันเกินไหลกลับเข้าสู่แหล่งระบบไฟฟ้าหลัก ถ้าการจ่ายพลังงานไฟฟ้ากลับคืนถูกระบุไว้ จะต้องมีการวิเคราะห์อันตรายที่เกิดจากการจ่ายพลังงานไฟฟ้ากลับคืนไปยังรางนำไฟที่ตัดพลังงานไฟฟ้าออก ตามหัวข้อที่ 2.1.2.1

ข.2.6 การควบคุมและเฝ้าติดตามจากระยะไกล สถานีไฟฟ้าย่อยสำหรับระบบขับเคลื่อนจะต้องสามารถเฝ้าติดตามจากระยะไกลและควบคุมผ่านระบบ ATS (ตามหัวข้อที่ 4.3.2.2 และ 4.3.3.2 ข้อที่ 11) โดยการเฝ้าติดตามจะต้องมีการบันทึกข้อมูลด้วย (ตามหัวข้อที่ 4.3.3.4) โดยที่ทุกคำสั่งสำหรับการใช้พลังงานและการตัดพลังงานจะต้องถูกบันทึกพร้อมระบุเวลา

ข.2.7 การควบคุมด้วยตนเอง (local control) อุปกรณ์สำหรับจ่ายพลังจะต้องมีข้อกำหนดให้สามารถทำการควบคุมสวิตช์เกียร์โดยตนเองได้ (ทั้งการเปิดและปิด) เพิ่มเติมจากข้อกำหนดในส่วนที่สามารถควบคุมระยะไกลได้ สวิตช์เกียร์แต่ละตำแหน่งจะต้องมีสวิตช์สำหรับเปิดค้าง (lockout switch) เพื่อที่จะสามารถควบคุมสวิทช์เกียร์ได้ด้วยตนเอง และปิดกั้นการสั่งการจากระยะไกลเมื่ออยู่ในโหมดการควบคุมด้วยตนเอง ทั้งนี้ เมื่อมีการสั่งการและควบคุมด้วยตนเองจะต้องมีการประกาศที่ศูนย์ควบคุมกลาง

ข.2.8 การจ่ายไฟฟ้ากลับคืน (restoring power) อุปกรณ์สำหรับจ่ายกำลังไฟฟ้าจะต้องสามารถสั่งให้สวิตช์เกียร์หลักของสถานีจ่ายไฟย่อยอยู่ในสถานะวงจรปิด โดยจะสามารถสั่งการได้จากทั้งศูนย์ควบคุมส่วนกลาง และควบคุมด้วยตนเองได้จากที่สถานีย่อยสำหรับระบบขับเคลื่อน สำหรับจ่ายไฟฟ้ากลับคืนให้กับสถานีไฟฟ้าย่อยอีกครั้งนึง โดยการจ่ายไฟฟ้ากลับคืนจะต้องเป็นไปตามขั้นตอนการปฏิบัติงาน

การปิดวงจรซ้ำอัตโนมัติของอุปกรณ์สำหรับจ่ายกำลังไฟฟ้าจะสามารถทำได้ก็ต่อเมื่อวิเคราะห์อันตรายตามหัวข้อที่ 2.1.2.1 แล้ว หากนำไปใช้งาน การออกแบบจะต้องรองรับการปิดวงจรซ้ำได้ก็ต่อเมื่อมีการตรวจสอบสถานะของสายส่งแล้ว ไม่มีการลัดวงจรเกิดขึ้นในระบบ

ข.2.9 สิ่งอำนวยความสะดวกในสถานีไฟฟ้าย่อย สิ่งอำนวยความสะดวกในสถานีไฟฟ้าย่อย โครงสร้างภายนอก และอุปกรณ์สำหรับจ่ายกำลังไฟฟ้าจะต้องอ้างอิงตาม NFPA 70 หรือมาตรฐานอื่นที่เทียบเท่า อุปกรณ์เกี่ยวกับสถานีไฟฟ้าย่อยสำหรับระบบขับเคลื่อนจะต้องมีอุปกรณ์เสริมเป็นของตัวเอง และสามารถที่จะควบคุมกำลังไฟฟ้าได้

ระบบป้องกันอัคคีภัยจะต้องสามารถระบุได้ถึงการเกิดอัคคีภัย และระงับเหตุการณ์อัคคีภัย สถานีไฟฟ้าย่อยสำหรับระบบขับเคลื่อนต้องมีการออกแบบมาโดยคำนึงถึงการทำงานร่วมกันกับการออกแบบสถานีเพื่อปฏิบัติตามการรองรับอัคคีภัย โดยต้องผ่านการตรวจสอบโดยเจ้าหน้าที่ดับเพลิงท้องถิ่น สถานีไฟฟ้าย่อยสำหรับระบบขับเคลื่อนจะต้องเป็นไปตามที่ระบุไว้ในหัวข้อที่ 5.2.4.3 ของ NFPA 130 หรือมาตรฐานอื่นที่เทียบเท่าและหัวข้อที่ 4.3.3.3.2 เรื่อง สัญญาณเตือนเหตุการณ์เพลิงไหม้และการบุกรุก ในมาตรฐานเล่มนี้

ข.3 ชุดจ่ายกำลังไฟฟ้าข้างทาง (wayside power collection)

ในการเชื่อมต่อมายังชุดอุปกรณ์จ่ายกำลังไฟฟ้าบนตัวรถ ชุดอุปกรณ์สำหรับจ่ายกำลังไฟฟ้าข้างทางจะต้องเป็นไปตามหัวข้อต่อไปนี้

ข.3.1 การจ่ายกำลังไฟฟ้าสำหรับ Guideway-Mounted ระบบที่จ่ายพลังงานไฟฟ้าให้แก่ตัวรถจะต้องใช้รางจ่ายไฟ (power rails) ที่มีความแข็งแรงหรือเทียบเท่า โดยที่ระบบรางจ่ายไฟจะต้องประกอบไปด้วยรางจ่ายไฟ อุปกรณ์ยึดจับ (fastening) รอยต่อเผื่อขยาย (expansion joint) อุปกรณ์ป้องกัน (protection cover) และอุปกรณ์อื่น ๆ ซึ่งรางจ่ายไฟจะต้องมีการแยกการจ่ายไฟจากจุดอื่น ๆ และโครงสร้างข้าง ๆ โดยอ้างอิงตามแรงดันไฟฟ้าในการทำงาน ตำแหน่งติดตั้งและวิธีการสำหรับติดตั้งของรางจ่ายไฟจะต้องมีการคำนึงถึงการทำงานของพื้นที่โดยรอบของตัวรถ (dynamic envelope)

ระบบรางจ่ายไฟจะต้องมีการประมาณการณ์สำหรับกระแสไฟฟ้าและแรงดันตกคร่อมที่ต้องการและประมาณการณ์สำหรับความแข็งแรงของโครงสร้างสำหรับการเว้นระยะห่างที่เหมาะสม ทั้งนี้ ระบบรางจ่ายไฟจะต้องไม่ได้รับความเสียหายจากแรงทางแม่เหล็กไฟฟ้าซึ่งเกิดขึ้นขณะเกิดการลัดวงจร

ข.3.2 ช่วงการจ่ายพลังงาน (power zones) ที่ซึ่งระบบการจ่ายกำลังไฟฟ้าถูกแบ่งตามช่วงต่าง ๆ โดยลำดับการจ่ายพลังงานจะต้องสามารถปรับเปลี่ยนได้ในระดับที่เหมาะสมเพื่อที่จะให้ช่วงต่าง ๆ ของทางวิ่งบังคับได้รับการจ่ายไฟฟ้าอย่างเหมาะสม แม้ส่วนที่อยู่ด้านข้างถูกตัดไฟไปก็ยังคงสามารถทำงานได้ในรูปแบบการทำงานที่ลดประสิทธิภาพลงภายใต้สถานการณ์ที่เกิดความล้มเหลวต่าง ๆ หรือความบกพร่องจากการซ่อมบำรุง โดยช่วงการจ่ายพลังงานไฟฟ้าจะต้องทำงานควบคู่ไปกับบริเวณ blue light station (หัวข้อที่ ข.1.1)

ตัวรถเพียงขบวนเดียวจะต้องสามารถเชื่อมต่อช่องวางของการจ่ายกำลังไฟฟ้าระหว่างพื้นที่ได้เพื่อที่จะทำให้มีการจ่ายไฟต่อเนื่องกันตลอดเวลาที่ระบบ APM ยังคงให้บริการ เว้นแต่เมื่อ 2 พื้นที่ที่อยู่ติดกันมีความไม่เข้ากันทางไฟฟ้า ทำให้ต้องมีการเว้นระยะในการแบ่งแยกทางไฟฟ้าออกจากกัน เพื่อที่จะป้องกันการจ่ายพลังงานโดยไม่ได้ตั้งใจให้กับส่วนที่ไม่มีการจ่ายไฟของทางวิ่งบังคับ (เช่น ในระหว่างบำรุงรักษา) โดยอาจจะมีสาเหตุมาจากการเชื่อมต่อพลังงานไฟฟ้ากันผ่านทางตัวรถ

ข.3.3 ข้อกำหนดสำหรับการต่อกันของรอยต่อ (splice joint) รางจ่ายไฟกับแผ่นเชื่อม (splice plate) ระหว่างรางจะต้องมีรอยต่อที่มีความแข็งแรงและเป็นขั้วบวก ซึ่งความยาว พื้นที่หน้าตัด และภาพหน้าตัดของแผ่นเชื่อม จะต้องถูกออกแบบให้สามารถกระจายความร้อนที่พื้นผิวได้อย่างเพียงพอ ไปจนขีดจำกัด

ในการเพิ่มขึ้นของความร้อนไม่มากเกินไปกว่า 2 องศาเซลเซียส หรือ 3.5 องศาฟาเรนไฮต์เมื่อเทียบกับอุณหภูมิของรางจ่ายไฟขณะที่ทำงานตามปกติ

ข.3.4 รอยต่อเผื่อขยายและหน้าตัด (expansion joints and sections) รอยต่อเผื่อขยายและหน้าตัดจะต้องถูกคาดคะเนการขยายตัวและการหดตัวเนื่องจากความร้อนของรางจ่ายไฟ โดยมีสาเหตุมาจาก

การเปลี่ยนแปลงของอุณหภูมิสภาพแวดล้อม และความร้อนที่เพิ่มสูงขึ้นของตัวนำไฟฟ้าจากโหลดทางไฟฟ้า ผลจากการแผ่รังสี และการเคลื่อนตัวของทางวิ่งบังคับ

รอยต่อเผื่อขยายหรือหน้าตัดจะต้องสามารถทนรับแรงทางแม่เหล็กไฟฟ้าขณะเกิดการลัดวงจร โดยสายต่อพ่วงทุกจุดจะต้องทำให้กระแสไฟฟ้ามีความต่อเนื่องตลอด และต้องมีความจุไฟฟ้าเทียบเท่าหรือมากกว่าความจุไฟฟ้าของรางจ่ายไฟ

ข.3.5 ความต่อเนื่องของรางจ่ายไฟ (power rail transitions) ถ้าหากมีการชำรุดหรือความเสียหายเกิดขึ้นในทางวิ่งบังคับของรางจ่ายไฟ จะต้องมีวิธีการในการอำนวยความสะดวกในการเชื่อมต่อและปลดการเชื่อมต่อของขาตัวนำรับไฟ (current collector shoes) ที่ความเร็วพิกัดของขบวนรถ

ข.3.6 ฉนวนไฟฟ้า (insulator) พื้นผิวของวัสดุที่นำมาเป็นฉนวนจะต้องมีความราบเรียบ แข็ง สามารถต้านทาน UV และจะต้องถูกจัดให้สามารถดับไฟได้ด้วยตัวเอง หรือไม่ติดไฟ ตามมาตรฐาน ASTM D635-06 หรือมาตรฐานอื่นที่เทียบเท่า

รางตัวนำจ่ายไฟ (Power conductor rails) จะต้องถูกป้องกันจากการสัมผัสที่ไม่ได้เจตนา

ข.3.7 การยึด (mounting) ถ้ามีการใช้รางจ่ายไฟ จะต้องมีการยึดที่แข็งแรงเพื่อที่จะป้องกันการขยับทั้งทางด้านข้างและทางดิ่ง ในขณะที่ยังคงอนุญาตให้สามารถเคลื่อนที่ตามแนวยาวได้ เนื่องจากมีการขยายตัวจากความร้อน

ข.3.8 ความต้านทานของรางจ่ายไฟเทียบดิน (power rail to earth resistance) รางจ่ายไฟแต่ละจุดที่มีกระแสไหลจากระบบจ่ายกำลังไฟฟ้าของทางวิ่งบังคับ จะต้องมีค่าความต้านทาน ณ ขณะที่ให้บริการขั้นต่ำอยู่ที่ 1 เมกะโอห์มต่อระยะทาง 300 เมตร (1,000 ฟุต) ในทุก ๆ สภาวะ

สำหรับระบบจ่ายไฟกระแสตรง อุปกรณ์ขั้วลบย้อนกลับต้องถูกออกแบบให้มีความต้านทาน ณ ขณะที่ให้บริการขั้นต่ำอยู่ที่ 500 โอห์มต่อระยะทาง 300 เมตร (1,000 ฟุต) ในแต่ละทางวิ่ง

ข.3.9 ความร้อนของรางจ่ายไฟและรางกราวด์ ถ้ามีความจำเป็นต้องมีระบบระบายความร้อนสำหรับรางจ่ายไฟและรางกราวด์ จะต้องสามารถระบายความร้อนได้เหมาะสมกับสภาพอากาศในเขตที่ได้มีการติดตั้ง โดยระบบระบายความร้อนจะต้องมีการแบ่งเป็นช่วง และแต่ละช่วงจะต้องมีการควบคุมแยกกันไปอย่างอิสระ

ข.4 อุปกรณ์ทางไฟฟ้าสำหรับสถานีผู้โดยสาร

อุปกรณ์ในสถานีจะต้องมีการออกแบบเพื่อให้สามารถจ่ายกำลังไฟฟ้าและแสงสว่างสำหรับแผนกทำความสะอาดได้จากแหล่งเดียว อีกทั้ง ระบบสื่อสารและการแจ้งเตือนในสถานี ระบบไฟฉุกเฉิน และป้ายไฟจะต้องมีแหล่งจ่ายไฟสำรอง โดยโหลดทั่วไปจะใช้แหล่งจ่ายกำลังไฟฟ้าจากอุปกรณ์สนับสนุนภายในสถานีไฟฟ้าย่อย ซึ่งได้แก่ Automatic Train Control (ATC) UPS อุปกรณ์สื่อสาร และอุปกรณ์ประจำสถานีต่าง ๆ ซึ่งอุปกรณ์สนับสนุนภายในสถานีไฟฟ้าย่อยจะต้องถูกออกแบบโดยอ้างอิงจากมาตรฐาน NFPA 70 หรือมาตรฐานอื่นที่เทียบเท่า

ข.5 UPS (Uninterruptible Power Supply)

ในเหตุการณ์ที่แหล่งจ่ายไฟหลักนั้นไม่สามารถใช้งานได้ อุปกรณ์ต่าง ๆ ที่ต้องการใช้พลังงานไฟฟ้าจะต้องได้รับการสนับสนุนโดย UPS โดยที่ UPS จะต้องจ่ายไฟฟ้าสำรองอย่างต่อเนื่องสำหรับการทำงานของระบบต่อไปนี้

1. ATC (จากบทที่ 4)
2. ระบบการสื่อสาร (ทั้งภาพและเสียง จากบทที่ 5)
3. ระบบป้องกันอัคคีภัยและอุปกรณ์รักษาความปลอดภัยต่างๆ
4. ระบบจ่ายกำลังไฟฟ้าที่ซึ่งควบคุมกำลังไฟฟ้าที่สถานีไฟฟ้าย่อย

UPS จะต้องมีขนาดที่สามารถรองรับการทำงานทั้งหมดที่กล่าวมาข้างต้นได้ในระยะเวลาที่กำหนด ตามหัวข้อที่ 2.1.2.1 การวิเคราะห์อันตราย

ภาคผนวก ค
ข้อแนะนำสำหรับการวัดค่าความพร้อมใช้งาน (service availability)

ภาคผนวกนี้เป็นการให้ข้อมูลและไม่ได้เป็นการบังคับใช้ของมาตรฐานนี้

ค.1 บทนำ

วิธีการคำนวณค่าความน่าเชื่อถือ ความสามารถการบำรุงรักษา และความพร้อมใช้งาน เป็นวิธีที่ใช้กันอย่างแพร่หลาย (ดังรายละเอียดในบทที่ 3) ดังนั้นจึงสามารถนำมาใช้กับระบบต่างๆของรถ APM ได้ ซึ่งประกอบไปด้วยระบบย่อยและอุปกรณ์อยู่เป็นจำนวนมาก (เช่น ขบวนรถ สถานี การควบคุมการเดินรถ อุปกรณ์ทางวิ่งบังคับ ระบบสื่อสาร เป็นต้น) การคำนวณที่ซับซ้อนในขั้นตอนนี้จะใช้ข้อมูลการทำงานของระบบรถ APM ในขณะที่มีการเดินรถหลายเส้นทาง

การวัดค่าความพร้อมของขบวนรถ APM จะวัดทั้งด้านความพร้อมในการให้บริการผู้โดยสารและความพร้อมใช้งานของระบบหรืออุปกรณ์รถ APM เนื่องจากผู้โดยสารจะเกี่ยวข้องทั้งการใช้บริการภายในบริเวณสถานีและขบวนรถ วิธีการนี้จะเป็นแนวทางให้ผู้ปฏิบัติการเดินรถ APM ทราบถึงวิธีการวัดค่าความพร้อมใช้งานของขบวนรถ APM โดยเฉพาะ เพื่อให้สอดคล้องกับมาตรฐานที่กำหนดไว้ในบทที่ 3 ซึ่งค่าความพร้อมใช้งานจะวัดจากการนับจำนวนความล้มเหลวที่เกิดขึ้นกับรถ APM (เช่น ความเสียหายที่เกิดกับตัวรถหรือความเสียหายที่เกิดกับห้องโดยสารในขบวน) และความเสียหายที่เกิดบริเวณชานชาลาสถานี (เช่น ประตูเปิด-ปิดเข้าชานชาลาสถานี เป็นต้น) โดยทั่วไปแล้วข้อมูลความล้มเหลวเหล่านี้จะสามารถวัดหรือนับได้โดยตรงโดยการสร้างอัลกอริทึมลงบนซอฟท์แวร์ที่ใช้ควบคุมระบบหลัก

ค.2 การเกิดเหตุขัดข้องในการให้บริการ

คือ เหตุการณ์หรือความล้มเหลวที่ส่งผลให้ผู้โดยสารไม่สามารถใช้การบริการของระบบหลักหรือระบบย่อยได้ตามที่ต้องการ โดยที่การเกิดเหตุขัดข้องอย่างน้อยควรรวมไปถึงเหตุการณ์ต่อไปนี้

1. การหยุดการเดินรถหนึ่งขบวนหรือหลายขบวนที่อยู่นอกเหนือแผน
2. ความไม่พร้อมใช้งานของทั้งขบวนรถ ตัวรถหรือห้องของผู้โดยสาร
3. การเปลี่ยนเส้นทางการเดินรถอันเนื่องมาจากอุปกรณ์ประจำสถานีเกิดความเสียหายทำให้สถานีไม่สามารถเปิดใช้บริการได้
4. ความผิดปกติที่ทำให้ผู้โดยสารไม่สามารถเข้าหรือออกจากขบวนรถในสถานีที่มีการทำงานแบบอัตโนมัติ
5. ความผิดปกติที่บริเวณชานชาลาสถานีทำให้ผู้โดยสารไม่สามารถใช้บริการรถ APM ได้ตามตารางการเดินรถที่ให้บริการแบบอัตโนมัติ
6. ความผิดปกติที่ส่งผลต่อการให้บริการที่อาจเกิดอันตราย

ผู้ให้บริการการเดินรถอาจพิจารณาถึงสภาวะเหตุการณ์ที่ทำให้ห้องโดยสารหรือชานชาลาสถานี ไม่สามารถให้บริการได้ด้วยสาเหตุอื่นนอกเหนือจากความล้มเหลวอย่างสิ้นเชิง เช่น ระบบปรับอากาศ (HVAC) มีปัญหา ระบบแสงสว่างมีปัญหา อุปกรณ์ติดต่อสื่อสารกับผู้โดยสาร การตกแต่งภายในที่อาจก่อให้เกิดอันตราย เป็นต้น สภาวะเหล่านี้อาจจะส่งผลต่อการหยุดทำงานของขบวนรถ (down time) ตามรายละเอียดในหัวข้อ 2.1 และ/หรือ สถานีตามรายละเอียดในหัวข้อ 2.2 รวมทั้งความผิดพลาดของพนักงานผู้ปฏิบัติงานที่ส่งผลให้เกิดเหตุขัดข้องในการให้บริการ

ค.3 ข้อยกเว้น

ข้อต่อไปนี้ไม่ถือว่าเป็นการเกิดเหตุขัดข้องในการให้บริการ

1. ความผิดปกติที่ส่งผลให้การปฏิบัติงานปกติของขบวนเกิดเหตุขัดข้อง แต่ว่าช่วงเวลาที่เกิดเหตุขัดข้องไม่เกินกว่าเวลาที่กำหนดไว้ตามแผน (grace time)

2. ความผิดปกติหรือการหยุดฉุกเฉินที่เกิดขึ้นจากการที่ผู้โดยสารทำลายทรัพย์สิน ผู้โดยสารใช้อุปกรณ์ผิด หรือ ผู้โดยสารทำให้ขบวนรถต้องล่าช้า

3. การหยุดฉุกเฉินที่เกิดจากการที่มีบุคคลที่ไม่ได้รับอนุญาตหรือมีสัตว์เลี้ยงรุกล้ำเข้าไปในเขตพื้นที่หวงห้าม จนส่งผลให้เกิดความล้มเหลวของอุปกรณ์ความปลอดภัย ซึ่งความล้มเหลวของอุปกรณ์ความปลอดภัยเกิดจากการป้องกันการรุกล้ำของบุคคลหรือสัตว์เลี้ยงดังกล่าว

4. การหยุดฉุกเฉินที่เกิดจากปัจจัยภายนอก เช่น ระบบพลังงานไฟฟ้ามีปัญหา การหยุดตามคำสั่งของเจ้าพนักงาน (เช่น ตำรวจ) การเกิดเหตุสุดวิสัย หรือค่าสภาวะแวดล้อมที่เกินค่าปกติ

5. การหยุดฉุกเฉินที่เกิดจากการฝึกอบรมในกรณีพิเศษ การตรวจสอบทางวิ่งบังคับ หรือการขยายเวลาซ่อมเพิ่มเติมจากที่กำหนดไว้ในแผน

6. การหยุดที่มีสาเหตุมาจากการตรวจสอบประสิทธิภาพการทำงานของระบบควบคุมการเดินรถอัตโนมัติเพื่อให้มั่นใจได้ว่าเป็นไปตามข้อกำหนดอย่างแท้จริง

ค.4 ความพร้อมของระบบ (system availability)

ค่าความพร้อมใช้งานของอุปกรณ์ระบบและการให้บริการผู้โดยสาร คำนวณจากสูตรต่อไปนี้

$$A(i) = A_f(i)A_s(i) \qquad \text{(ค-1)}$$

โดยที่

$A(i)$ = ความพร้อมการบริการของระบบในช่วงเวลา i

$A_f(i)$ = ความพร้อมของขบวนรถในช่วงเวลา i

$A_s(i)$ = ความพร้อมของชานชาลาสถานี (หรือประตูชานชาลา) ในช่วงเวลา i

ค.4.1 ความพร้อมของขบวนรถ (fleet availability)

ค่าความพร้อมของขบวนรถ คำนวณจากสูตรต่อไปนี้

$$A_f(i) = (FTSi - FTDi)/\ FTSi \qquad \text{(ค-2)}$$

โดยที่

$FTSi$ = เวลารวมของตู้โดยสารทั้งหมดในขบวนรถที่มีการเดินรถตามตาราง ในช่วงเวลา i (ดูรายละเอียดได้ในหัวข้อ 1.5)

$FTDi$ = เวลาหยุดของตู้โดยสารทั้งหมดในขบวนรถที่มีการเดินรถตามตาราง ในช่วงเวลา i ซึ่งเหตุขัดข้องในการให้บริการผู้โดยสารเกิดจากความล้มเหลว หรือตู้โดยสารไม่สามารถให้บริการได้

$$FTDi = \sum CD_j \qquad \text{(ค-3)}$$

CD_j = เวลาหยุดของตู้โดยสารแต่ละตู้ ในช่วงเวลา i

ค.4.2 ความพร้อมของชานชาลา (station availability)

ค่าความพร้อมของชานชาลา คำนวณจากสูตรต่อไปนี้

$$A_s(i) = (STSi - STDi)/\ STSi \qquad \text{(ค-4)}$$

โดยที่

$STSi$ = เวลารวมที่ชานชาลาของสถานีเปิดให้บริการตามตารางการเดินรถของ ในช่วงเวลา i

$STDi$ = เวลาที่ชานชาลาของสถานีหยุดการให้บริการ อันเนื่องมาจากความล้มเหลวที่ผู้โดยสารไม่สามารถใช้การบริการรถ APM ได้ตามตาราง ในช่วงเวลา i หรือการงดบริการของชานชาลาของสถานี

ค.4.3 การชดเชยค่าความพร้อมสำหรับการบริการที่มีปัญหา

การชดเชยค่าความพร้อมใช้งานสำหรับการบริการที่มีปัญหาสามารถทำได้จากการกำหนดรูปแบบการบริการเฉพาะ (degraded service modes) ซึ่งสามารถให้บริการในเหตุการณ์ที่การบริการตามตารางไม่สามารถยอมรับได้และการบริการปกติไม่สามารถดำเนินการต่อตามเวลาที่เหมาะสม

ในการคำนวณค่าความพร้อมใช้งานสำหรับการบริการที่มีปัญหา จะมีการนำค่า K-factor มาคูณกับค่าความพร้อมใช้งาน โดยที่ค่า K-factor คือ อัตราส่วนระหว่างปริมาณและคุณภาพของการให้บริการผู้โดยสารที่ต้องเผชิญกับการบริการที่มีปัญหาเหล่านั้น กับปริมาณและคุณภาพของการให้บริการผู้โดยสารในสภาวะปกติ และค่า K-factor จะมีค่าน้อยกว่าหรือเท่ากับ 1 เสมอ ตัวอย่างเช่น ค่า K-factor อาจจะเป็นค่าอัตราส่วนระหว่างความสามารถในการรองรับผู้โดยสาร (line capacity) ของการให้บริการแบบ degraded service modes กับความสามารถในการรองรับผู้โดยสารสำหรับเหตุการณ์ที่อยู่ในสภาวะปกติ หรือเป็นฟังก์ชันทั้ง *headway* และ line capacity หรือรูปแบบอื่นที่เหมาะสม โดยที่ค่า K-factor สำหรับการให้บริการตามตารางเวลาจะมีค่าเท่ากับ 1 เสมอ

ค.4.4 ความพร้อมการบริการของระบบโดยรวม

ค่าความพร้อมการบริการของระบบโดยรวมสามารถวัดในรูปของช่วงเวลา (เช่น วัน สัปดาห์ เดือนหรือปี) และคำนวณจากผลรวมของค่าเฉลี่ยแบบถ่วงน้ำหนัก (weighted sum average)

จากสมการ (ค-5) ค่า $A(i)$ สำหรับแต่ละการบริการจะมีตัวถ่วงน้ำหนักคูณอยู่ นั่นคือ W_i และถ้าตัวถ่วงน้ำหนักสัมพันธ์กับช่วงเวลาในการบริการ ก็สามารถใช้ตัวแปร T_i แทนได้

ตัวถ่วงน้ำหนักที่สัมพันธ์กับช่วงเวลาอาจจะไม่ใช่วิธีที่เหมาะสม เนื่องจากอาจถ่วงน้ำหนักไม่เหมาะสมกับความพร้อมบริการในช่วงเวลาดังกล่าว ในกรณีนี้ ผู้ปฏิบัติการเดินรถอาจจะต้องกำหนดแฟคเตอร์ตัวถ่วงน้ำหนักที่ครอบคลุมทั้งด้านคุณภาพและปริมาณของการบริการตามตารางการเดินรถ ตัวอย่างเช่น แฟคเตอร์ตัวถ่วงน้ำหนักอาจจะเป็นผลคูณระหว่างค่า $T_i C_i$ โดยที่ T_i คือช่วงเวลา และ C_i คือความสามารถในการรองรับผู้โดยสารใช้บริการขบวนรถตามตาราง ดังนั้นผู้ปฏิบัติการเดินรถจึงควรกำหนดแฟคเตอร์ตัวถ่วงน้ำหนักที่เหมาะสมเฉพาะกับระบบรถ APM และการปฏิบัติการเดินรถ

$$A = \sum_i K_i W_i A(i) / \sum_i W_i \qquad \text{(ค-5)}$$

โดยที่

A = ค่าความพร้อมการให้บริการของระบบโดยรวมในช่วงเวลาที่กำหนด

K_i = K แฟคเตอร์ สำหรับการให้บริการที่เกิดในช่วงเวลา i

W_i = ตัวถ่วงน้ำหนักสำหรับการให้บริการ

$A(i)$ = ค่าความพร้อมการให้บริการในแต่ละช่วงการบริการ (ดูสมการ ค-1)

ภาคผนวก ง
แนวทางการประเมินความปลอดภัยอิสระ
(Idependent Safety Assessment)

ภาคผนวกนี้เป็นการให้ข้อมูลแต่ไม่ถือเป็นข้อบังคับตามมาตรฐาน

แนวทางแนะนำนี้จำเป็นอย่างยิ่งสำหรับการจัดทำในข้อกำหนดที่ 4.1.2 ระยะห่างปลอดภัย (separation assurance) เพื่อใช้ในกระบวนการประเมินความปลอดภัยอิสระสำหรับระบบ ATN เมื่อการออกแบบระบบไม่มีเกณฑ์การป้องกันการเกิดเหตุสุดวิสัยมาก่อน

จุดมุ่งหมายของแนวทางนี้ก็เพื่อใช้ในการประเมินความปลอดภัยอิสระให้เหมาะสมกับระบบ APM โดยมีแนวทางดังต่อไปนี้

1. คณะทำงานการประเมินความปลอดภัยควรประกอบด้วยผู้เชี่ยวชาญดังต่อไปนี้ ด้านการออกแบบ ด้านการก่อสร้าง ด้านการตรวจสอบ ด้านการปฏิบัติงาน และด้านการซ่อมบำรุง โดยอ้างอิงตาม มขร. – S – 003 - 2567 มาตรฐานความปลอดภัยทั่วไปของระบบขนส่งผู้โดยสารอัตโนมัติ หัวข้อ 7.3.1 ข้อกำหนดของผู้ตรวจสอบอิสระ ซึ่งควรนำมาปรับใช้กับคณะทำงานนี้

2. ผู้เชี่ยวชาญเฉพาะด้านที่ได้รับมอบหมายให้เป็นผู้ประเมินหลักด้านความปลอดภัยจากหน่วยงานตรวจสอบอิสระ ควรกำหนดบทบาทและหน้าที่ความรับผิดชอบให้ชัดเจน

3. ผู้ประเมินหลักด้านความปลอดภัยจากหน่วยงานตรวจสอบอิสระมีการจัดทำแผนการความปลอดภัยที่ประกอบไปด้วย ขั้นตอนการประเมิน วิธีการประเมิน และเทคนิควิธีการประเมิน

4. แผนการประเมินความปลอดภัยจากหน่วยงานอิสระควรมีรายละเอียดขั้นตอนการสื่อสารระหว่างผู้ที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบหลักด้านความปลอดภัยของระบบต่างๆ (รายละเอียดในหัวข้อ 2.1 ถึง 2.4) รวมถึงขั้นตอนการแก้ไขปัญหาจากการประเมินที่ตรวจเจอ โดยที่การแก้ไขปัญหาควรปฏิบัติตามมาตรการแก้ไขของโครงการซึ่งถือเป็นที่สิ้นสุด

5. แผนการประเมินความปลอดภัยจากหน่วยงานอิสระควรมีเอกสารยืนยันประสบการณ์และคุณสมบัติของคณะทำงานที่เกี่ยวข้องทั้งหมดกับขั้นตอนการประเมินความปลอดภัย

6. ผู้ประเมินด้านความปลอดภัยจากหน่วยงานอิสระปฏิบัติงานให้เป็นไปตามแผนงาน SSPP (System Safety Program Plan) SSCR (School of Social Care Research) ด้านที่มีความสัมพันธ์กับความปลอดภัยและด้านที่มีความสำคัญต่อความปลอดภัย โดยให้ระบุรายละเอียดการประเมินลงไปในขอบเขตการทำงานของผู้ประเมิน

7. ผู้ประเมินความปลอดภัยจากหน่วยงานอิสระมีการจัดทำรายงานการประเมินความปลอดภัยที่รวบรวมการประเมินทั้งหมด สิ่งที่ตรวจพบและวิธีการแก้ไข รวมทั้งข้อสรุปทั้งหมดที่เหมาะสมกับการใช้ระบบ APM

กรมการขนส่งทางราง
514/1 ถนนหลานหลวง แขวงสี่แยกมหานาค เขตดุสิต กรุงเทพ 10300
โทร: 02 164 2607 โทรสาร: 02 164 2606
https://www.drt.go.th