งานประชุมวิชาการ และนวัตกรรม กฟภ. ปี 2564
Data Driven Business in Digital Utility Era
ขับเคลื่อนธุรกิจด้วยฐานข้อมูลในยุค Digital Utility

การปรับปรุงการรักษาความมั่นคงปลอดภัยของระบบควบคุมระบบไฟฟ้า ของ การไฟฟ้านครหลวง
(Cybersecurity Improvement for MEA Power Control System)

นางฐิติมา คงเมือง, CSSA, GCIP, IRCA 27001 Lead Auditor
ฝ่ายควบคุมระบบไฟฟ้า การไฟฟ้านครหลวง thitima.pcd@mea.or.th

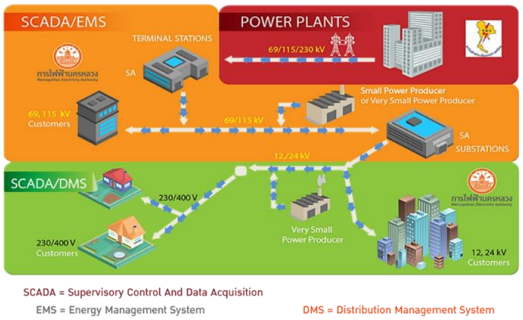
บทคัดย่อ

ระบบควบคุมระบบไฟฟ้า เป็นส่วนสำคัญต่อการจ่ายกระแสไฟฟ้าให้แก่ประชาชน ซึ่งมีความต้องการใช้ข้อมูลจากระบบควบคุมระบบไฟฟ้ามากขึ้น เพื่อปรับปรุงการบริการให้แก่ผู้ใช้ไฟฟ้าได้อย่างรวดเร็ว ในปัจจุบันมีภัยคุกคามต่อระบบคอมพิวเตอร์และเครือข่ายมากขึ้น ดังนั้น การไฟฟ้านครหลวง (กฟน.) จึงต้องปรับปรุงระบบการรักษาความมั่นคงปลอดภัยของระบบควบคุมระบบไฟฟ้าหลักของ กฟน. ให้มีความมั่นคงปลอดภัยเพิ่มขึ้น โดยได้ศึกษา วิเคราะห์ มาตรฐานที่ใช้ในต่างประเทศ มาตรฐานสากล กรอบการดำเนินการ รวมทั้ง พิจารณา พรบ. ระเบียบปฏิบัติ ของประเทศไทยที่ต้องดำเนินการ สังเคราะห์ข้อมูลเพื่อนำมาสู่การพิจารณาเพิ่มเติมกระบวนการบริหารจัดการการรักษาความมั่นคงปลอดภัย และ นำส่วนเทคนิคที่ต้องเพิ่มเติมมาปรับปรุง ออกแบบ และพัฒนาระบบควบคุมระบบไฟฟ้าใหม่ ผลการศึกษาพบว่า ส่วนที่ต้องเพิ่มเติมมากที่สุดในกระบวนการ ได้แก่ กระบวนการตรวจจับความผิดปกติในระบบ และ กระบวนการรวบรวมข้อมูล วิเคราะห์ และตอบโต้หรือแก้ไข ช่องโหว่ต่าง ๆ ของระบบควบคุม เพื่อให้ กฟน. ให้มีความพร้อมต่อการรักษาความมั่นคงปลอดภัย สามารถป้องกันภัยคุกคาม และ ตอบโต้หรือกู้คืนระบบงานได้อย่างรวดเร็ว ทำให้การบริการจำหน่ายไฟฟ้าแก่ประชาชนดำเนินการได้อย่างต่อเนื่อง

คำสำคัญ: ระบบควบคุม การรักษาความมั่นคงปลอดภัย การออกแบบระบบ มาตรฐาน

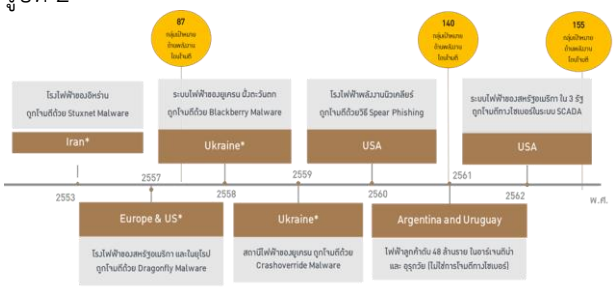
1. บทนำ

ปัจจุบัน การไฟฟ้านครหลวง (กฟน.) มีระบบควบคุมระบบไฟฟ้าหลักที่ใช้ ณ ศูนย์ควบคุมระบบไฟฟ้า คือ ระบบ Supervisory Control and Data Acquisition (SCADA) ซึ่งเป็นระบบคอมพิวเตอร์ที่ใช้สำหรับควบคุมอุปกรณ์ไฟฟ้าระยะไกลจากศูนย์ควบคุมระบบไฟฟ้า ไปยังสถานีต้นทาง สถานีย่อย สถานีไฟฟ้าของลูกค้า ผู้ผลิตไฟฟ้าขนาดเล็ก และผู้ผลิตไฟฟ้าขนาดเล็กมาก โดยติดต่อสื่อสารกับ Station Remote Terminal Unit (SRTUs) หรือSubstation Automation (SA) ผ่านเครือข่ายสื่อสารไฟเบอร์ออฟติกเฉพาะของ กฟน. ดังรูปที่ 1



รูปที่ 1 ระบบควบคุมระบบไฟฟ้าของการไฟฟ้านครหลวงในปัจจุบัน

ในปัจจุบัน จะเห็นภัยคุกคามเกิดขึ้นในโลกของอินเทอร์เน็ต ระบบเครือข่าย และระบบงานต่าง ๆ มากขึ้น โดยแนวโน้มของภัยคุกคาม เริ่มที่จะมีเป้าหมายมาสู่ระบบควบคุมของระบบโครงสร้างพื้นฐานต่าง ๆ โดยเฉพาะ ระบบควบคุมระบบไฟฟ้า โดยมีแนวโน้มและความรุนแรงเพิ่มขึ้น [1] โดยจำนวนครั้งของความพยายามที่จะโจมตีระบบไฟฟ้าเพิ่มมากขึ้นเรื่อย ๆ โดยในปี พ.ศ. 2558 มีความพยายาม 87 ครั้ง และ ปี พ.ศ. 2561 และ พ.ศ. 2562 เพิ่มขึ้นเป็น 140 ครั้ง และ 155 ครั้ง ตามลำดับ ดังรูปที่ 2



รูปที่ 2 เหตุภัยคุกคามที่เกิดขึ้นในระบบควบคุมระบบไฟฟ้าต่าง ๆ

จากผลการวิเคราะห์เหตุการณ์ภัยคุกคามสำคัญที่มีผลต่อระบบไฟฟ้า 4 กรณีศึกษา ได้แก่ กรณีศึกษาของประเทศอิหร่าน ระบบ SCADA ของโรงไฟฟ้า ถูกโจมตีด้วยมัลแวร์ Stuxnet [2] ในปี พ.ศ. 2553 กรณีศึกษาของประเทศในกลุ่มสหภาพยุโรป และสหรัฐอเมริกา โดนลักลอบข้อมูลสำคัญของระบบงานภาคพลังงานและภาคเภสัชกรรม ด้วยมัลแวร์ Dragonfly [3] ในปี พ.ศ. 2557 และ กรณีศึกษาของประเทศยูเครน ระบบ SCADA

ของศูนย์ควบคุมระบบไฟฟ้า โดนโจมตีโดยมัลแวร์ Blackberry [4] ในปี พ.ศ. 2558 และ ระบบ Substation Automation ภายในสถานีไฟฟ้าที่ใช้มาตรฐาน IEC 61850 และ IEC 60870-5-104 โดนโจมตีด้วยมัลแวร์ Crashoverride [5] ในปี พ.ศ. 2559 จากกรณีศึกษาดังกล่าวสามารถสรุปลักษณะการโจมตีที่มีผลกระทบกับระบบไฟฟ้า มีช่องทางเข้ามาของมัลแวร์ต่างๆ ผ่านทาง อีเมลของพนักงาน หรือ USB drive แล้วมัลแวร์มีการเข้ามาแฝงตัวอยู่ในเครือข่ายขององค์กรระยะหนึ่ง หรือในเครื่องคอมพิวเตอร์ พยายามจะบุกรุกเข้าในในเครือข่ายขององค์กร เข้าโจมตีระบบควบคุมระบบไฟฟ้าโดยเข้าควบคุมระบบ SCADA หรือระบบควบคุมภายในสถานีไฟฟ้า ควบคุมอุปกรณ์ระบบไฟฟ้า แล้วทำการดับไฟฟ้า ตามลำดับ ส่งผลให้เกิดไฟฟ้าดับต่อลูกค้าหลายรายเป็นระยะเวลาหลายชั่วโมง จะเห็นว่า ภัยคุกคามมีหลายรูปแบบ และ สามารถเข้าได้หลายช่องทาง รวมทั้งมักจะอาศัยพนักงานภายในองค์กรที่อาจจะขาดความรู้หรือความตระหนักด้านความมั่นคงปลอดภัย โดยใช้ช่องโหว่ของซอฟท์แวร์ระบบควบคุม ระบบปฏิบัติการของระบบควบคุม โปรโตคอลที่ใช้สื่อสารของระบบควบคุม และเครือข่าย เข้ามาจนทำให้เกิดความเสียหายต่อระบบควบคุมระบบไฟฟ้าขององค์กรได้

จากภัยคุกคามเหล่านี้ย่อมส่งผลกระทบอย่างมากทำให้ประชาชนไม่มีไฟฟ้าใช้เป็นระยะเวลานาน ดังนั้นระบบไฟฟ้าซึ่งถือเป็นโครงสร้างพื้นฐานที่สำคัญต่อการดำรงชีวิต ความปลอดภัยสาธารณะ เศรษฐกิจของประเทศ หากเกิดภัยคุกคามเช่นเดียวกับกรณีศึกษาต่าง ๆของต่างประเทศ อาจส่งผลต่อการควบคุมระบบไฟฟ้าในพื้นที่บริการของ กฟน. จนทำให้เกิดเหตุการณ์ไฟฟ้าดับเป็นบริเวณกว้าง รวมทั้งจะสูญเสียความมั่นคงปลอดภัยของประเทศไทยได้เนื่องจากเป็นพื้นที่ที่มีหน่วยงานสำคัญ เป็นศูนย์กลางของเศรษฐกิจของประเทศ ทำให้มีผลกระทบที่อาจประเมินค่าไม่ได้อีกและมีผลต่อชื่อเสียงของประเทศได้

ที่ผ่านมา กฟน. ได้นำกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยทางสารสนเทศ หรือ Information Security Management System (ISMS) ตามมาตรฐานสากล คือ ISO/IEC 27001:2013 มาใช้บริหารจัดการความมั่นคงปลอดภัยทางสารสนเทศสำหรับระบบควบคุม โดยมีขอบเขตระบบควบคุมหลัก (ระบบ SCADA) ของศูนย์ควบคุมระบบไฟฟ้าทุกแห่ง และได้กำหนดให้มีการตรวจสอบมาตรฐานทุกปี ทั้งจากผู้ตรวจประเมินภายใน (Internal Auditor) และผู้ตรวจสอบภายนอก (External Auditor) อีกทั้งยังได้ผ่านการตรวจประเมินและรับรองมาตรฐานจากผู้ตรวจประเมินภายนอก คือ บริษัท บีเอสไอ กรุ๊ป (ประเทศไทย) จำกัด (BSI Certification Services Co. Ltd.) ซึ่งเป็นสถาบันรับรองมาตรฐานแห่งชาติของประเทศอังกฤษ เมื่อปี พ.ศ. 2562 ตลอดจนมีการประเมินความเสี่ยงและทบทวนโดยผู้บริหารระดับสูงเป็นประจำ รวมถึงการแก้ไขข้อบกพร่องต่าง ๆ ที่ไม่เป็นไปตามข้อกำหนดเพื่อให้เกิดความมั่นใจได้ว่าระบบ SCADA/EMS สามารถใช้งานได้อย่างต่อเนื่อง มีความปลอดภัย ลดความเสี่ยงจากภัยคุกคามต่าง ๆ ทั้งจากระบบภายนอกและภายใน

ถึงแม้ว่า ระบบ SCADA/EMS จะได้รับการรับรองตามมาตรฐาน ISO/IEC 27001 แต่ก็สามารถดำเนินการได้อย่างมีข้อจำกัด เนื่องจากการออกแบบระบบเดิม ไม่ได้รองรับการเชื่อมต่อกับระบบงานภายนอก ประกอบกับ ซอฟท์แวร์และฮาร์ดแวร์ของระบบเอง เป็นระบบเฉพาะทาง ใช้งานเป็นเวลานาน มีข้อจำกัด จึงทำให้ไม่สามารถบริการข้อมูลระบบไฟฟ้าให้ระบบงานอื่น ๆ ได้อย่างรวดเร็ว ซึ่งปัจจุบันมีความต้องการใช้ข้อมูลและบูรณาการข้อมูลระบบไฟฟ้า เพื่อนำไปใช้ในการวางแผน วิเคราะห์ และพัฒนาระบบงานต่าง ๆ มากขึ้น ทำให้มีความต้องการเชื่อมต่อกับระบบควบคุมระบบไฟฟ้ามากขึ้น ดังนั้น กฟน. ได้มีแผนงานทดแทนระบบควบคุมปัจจุบัน เพื่อให้รองรับความต้องการใช้งานเพิ่มขึ้นและมีการบริการข้อมูลระบบไฟฟ้าให้แก่ระบบต่าง ๆ ได้อย่างรวดเร็ว ประกอบกับ รัฐบาลไทยได้ประกาศ พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อให้หน่วยงานของรัฐมีมาตรการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ซึ่ง กฟน. เป็นหน่วยงานของรัฐที่ต้องปฏิบัติตาม พรบ. ดังกล่าวอย่างเคร่งครัด

จากปัจจัยดังกล่าวข้างต้น ทำให้ กฟน. จะต้องเตรียมการรับมือ และออกแบบให้ระบบควบคุมระบบไฟฟ้ารองรับความต้องการและสอดคล้องตามข้อกำหนดต่าง ๆ ตามมาตรฐานและที่จะถูกบังคับใช้กับ กฟน. ในอนาคต โดยต้องคำนึงถึงเรื่องความมั่นคงปลอดภัยของระบบควบคุมระบบไฟฟ้า ทั้งความมั่นคงปลอดภัยทางกายภาพและทาง ไซเบอร์ เนื่องด้วยระบบใหม่นี้จะสื่อสารข้อมูลผ่านระบบเครือข่าย และมีการแลกเปลี่ยนข้อมูลกับระบบงานต่าง ๆ ขององค์กร รวมทั้งมีการบริการข้อมูลผ่านเครือข่ายอินเตอร์เน็ตให้แก่หน่วยงานภายนอก ดังนั้น พนักงานของ กฟน. ที่เกี่ยวข้องกับระบบควบคุม และระบบงาน IT ต่างๆ ขององค์กร จะต้องมีความรู้ ความเข้าใจ และมีความตระหนักในภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ เพื่อช่วยกันปกป้องภัยคุกคามต่างๆ ที่จะเข้ามาในองค์กร และอาจส่งผลต่อความมั่นคงปลอดภัยของระบบสารสนเทศและระบบควบคุมระบบไฟฟ้า ซึ่งเป็นสิ่งที่สำคัญต่อชื่อเสียง และความมั่นคงปลอดภัยขององค์กร และเพื่อให้ประชาชนที่ใช้บริการของ กฟน. มีความมั่นใจต่อการบริการที่ต่อเนื่องของ กฟน.

2. วิธีการดำเนินการวิจัย

1. ศึกษา วิเคราะห์ มาตรฐานที่ใช้ในต่างประเทศ มาตรฐานสากล ที่เกี่ยวข้อง กรอบการดำเนินการ แนวทางปฏิบัติที่ดี รวมทั้ง พิจารณาข้อกฎหมาย พรบ. ระเบียบปฏิบัติของประเทศไทยที่ต้องดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย

2. ศึกษาดูงาน และสัมภาษณ์ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยของหน่วยงานการไฟฟ้าในประเทศไทยและในประเทศสหรัฐอเมริกา เพื่อแลกเปลี่ยนประสบการณ์และหาแนวปฏิบัติที่ดีในการดำเนินการและปรับใช้กับ กฟน.

3. นำมาเพิ่มเติมกระบวนการบริหารจัดการการรักษาความมั่นคงปลอดภัย และ นำส่วนเทคนิคที่ต้องเพิ่มเติมมาปรับปรุง ออกแบบ และพัฒนาระบบควบคุมระบบไฟฟ้าใหม่ต่อไป

3. ผลการวิจัย

กฟน. ได้พิจารณาและออกแบบระบบควบคุมใหม่ของ กฟน. โดยพิจารณาระบบงานต่าง ๆ ที่ กฟน. ต้องแลกเปลี่ยนข้อมูล ระบบสื่อสารที่จะเปลี่ยนไปของระบบควบคุม รวมทั้งศึกษา วิเคราะห์ และพิจารณานำมาตรฐานสากลและมาตรฐานการรักษาความมั่นคงปลอดภัยที่ใช้กับงานควบคุมระบบไฟฟ้า มาใช้ในการออกแบบ และ กำหนดข้อกำหนดของระบบควบคุมระบบไฟฟ้าใหม่ โดยมีกรอบการพิจารณาจากมาตรฐานปัจจุบันที่ กฟน. ดำเนินการอยู่ คือ ISO 27001:2013 เทียบกับมาตรฐานที่บังคับใช้กับหน่วยงานการไฟฟ้าและพลังงานทั้งในประเทศและต่างประเทศ โดยมาตรฐานที่นำมาพิจารณา สรุปได้ดังนี้

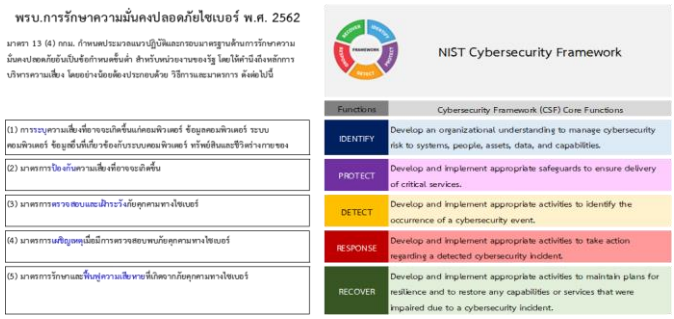
มาตรฐาน	ขอบเขต	ประเทศที่นำไปใช้	ปีที่ตีพิมพ์	หน่วยงานที่นำไปประยุกต์ใช้
ISO/IEC 27001 [6]	การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	- ทั่วโลก - ประเทศไทย (กฟน.)	2556	หน่วยงานทั่วไปที่ใช้ระบบสารสนเทศ (IT) รวมทั้งหน่วยงานไฟฟ้าและอุตสาหกรรม
NERC CIP-002 to 013 [7]	การรักษาความมั่นคงปลอดภัยที่กำหนดให้ผู้ประกอบกิจการไฟฟ้าสำหรับส่วนการผลิต การส่งไฟฟ้าระบบจำหน่าย และศูนย์ควบคุมระบบไฟฟ้า **ต้อง** ปฏิบัติตามมาตรฐาน	- ประเทศสหรัฐอเมริกา แคนาดา, เม็กซิโก และบางส่วนในทวีปยุโรป - ประเทศไทย (กฟผ.)	2551-2563	หน่วยงานด้านไฟฟ้า
IEC 62443 [8]	การรักษาความมั่นคงปลอดภัยสำหรับระบบควบคุมและระบบอัตโนมัติทางอุตสาหกรรม	- ทั่วโลก	2552-2563	หน่วยงานที่ใช้หรือพัฒนาระบบควบคุมและระบบอัตโนมัติทางอุตสาหกรรม
(ครอบคลุมทั้งหน่วยงานและผู้ผลิตอุปกรณ์หรือระบบควบคุม)				
NIST Cyber Security Framework V1.1	เป็นกรอบการปรับปรุงโครงสร้างพื้นฐานสำคัญด้านความปลอดภัยทางไซเบอร์	- ประเทศสหรัฐอเมริกา - ประเทศออสเตรเลีย	2561	หน่วยงานโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure)

ตารางที่ 1 เปรียบเทียบมาตรฐานที่บังคับใช้กับหน่วยงานการไฟฟ้า และพลังงาน

หมายเหตุ

- ที่ปรึกษาการพัฒนาระบบรักษาความมั่นคงความปลอดภัยด้านไซเบอร์ ของ สนพ. [9] สรุปผลการศึกษาว่า หน่วยงานทั่วโลกโดยทั่วไปที่หน่วยงานกำกับดูแลหรือภาครัฐยังไม่ได้มีการกำหนดระเบียบหรือมาตรฐานด้านความมั่นคงปลอดภัยที่ชัดเจน นิยมนำแนวทางขององค์กรมาตรฐานสากลมาใช้ คือ ISO/IEC 27001 และ IEC 62443
- มาตรฐาน ISO 27001 และ IEC 62443 เป็นมาตรฐานสากลองค์กรสามารถขอรับการรับรองจากหน่วยงานที่ได้รับอนุญาตในการออกใบรับรองได้
- มาตรฐาน NERC CIP ในภูมิภาคอเมริกาเหนือ ผู้วางนโยบาย คือ FERC และ ผู้ตรวจสอบและกำกับการดำเนินการ คือ หน่วยงานภายใต้ NERC ซึ่งหากมีหน่วยงานไฟฟ้าใดไม่ปฏิบัติหรือปฏิบัติไม่ได้ตามมาตรฐานที่กำหนดจะมีบทปรับกับหน่วยงานนั้น ๆ ส่วนในประเทศไทยนั้น กฟผ. ดำเนินการตามมาตรฐาน NERC CIP และ มีการตรวจประเมินระหว่างหน่วยงานภายใน

ปัจจุบันในประเทศไทยมี พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 บังคับใช้กับหน่วยงานของรัฐที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งได้กำหนดกรอบการดำเนินการที่หน่วยงานของรัฐจะต้องดำเนินการ ซึ่งอยู่ระหว่างพิจารณาข้อกำหนดแนวปฏิบัติอย่างชัดเจนสำหรับการรักษาความมั่นคงปลอดภัยของระบบไฟฟ้าต่อไปในอนาคต ซึ่ง ดร.ปริญญา หอมเอนก (2562) [10] อธิบายว่า แนวทางในการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ควรจะสอดคล้องกับ NIST Cybersecurity Framework (NIST CSF) ซึ่งพัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีของประเทศสหรัฐอเมริกา (National Institute of Standards and Technology, NIST) โดยจะเห็นปรากฏอยู่ในมาตรา 13 ของ พ.ร.บ. [11] ซึ่งสามารถเปรียบเทียบได้ ดังรูปที่ 3



รูปที่ 3 พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เทียบกับ NIST Cybersecurity Framework

ด้วยเหตุนี้ หน่วยงานกำกับดูแลด้านความมั่นคงปลอดภัยของประเทศไทย จึงมีแนวโน้มที่จะกำหนดแบบร่างของนโยบาย กฎหมาย ระเบียบข้อบังคับ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอ้างอิงตามจาก NIST CSF ซึ่งจะส่งผลให้ภาคส่วนไฟฟ้า จะต้องเตรียมความพร้อมในการกำหนดนโยบาย แนวทาง ระเบียบ ด้านความมั่นคงปลอดภัยไซเบอร์ของระบบไฟฟ้าให้มีความสอดคล้องกันในลำดับต่อไป ดังนั้น จึงได้ทำการเปรียบเทียบ NIST Cybersecurity Framework version 1.1 กับ มาตรฐานต่างๆ ที่ได้มีการนำมาประยุกต์ใช้กับศูนย์ควบคุมระบบไฟฟ้าของหน่วยงานด้านไฟฟ้าและพลังงานทั้งในต่างประเทศและประเทศไทย รวมทั้งมาตรฐานที่ กฟน. ได้ดำเนินการอยู่ เพื่อให้สอดคล้องกับแนวทางดำเนินการที่ พรบ. กำหนดให้ดำเนินการ

โดยผลการเปรียบเทียบกรอบการดำเนินการตาม NIST Cybersecurity Framework (NIST CFS) กับมาตรฐานต่าง ๆ สามารถสรุปส่วนที่มาตรฐานไม่มีเมื่อเทียบกับ NIST CFS ได้ดังนี้

มาตรา 13 ของ พรบ.ไซเบอร์ พ.ศ. 2562	NIST CFS V1.1	มาตรฐาน			ข้อกำหนดย่อยของ NIST CFS V1.1 ที่มาตรฐานนี้ไม่มี
	ข้อกำหนด/ข้อกำหนดย่อย	ISO 27001:2013	NERC CIP 002-013	IEC 62443	
การระบุความเสี่ยงที่อาจจะเกิดขึ้น	**การกำหนด**				
	การจัดการทรัพย์สิน	/	/	/***	*** ID.AM-4
	สภาพแวดล้อมทางธุรกิจ	/*	/**	/***	* ID.BE-3 ** ID.BE-1,3 *** ID.BE-1,2,5
	การดำเนินงานภาครัฐ	/	/**	/	** ID.GV-3,4
	การประเมินความเสี่ยง	/	/	/***	*** ID.RA-5
	กลยุทธ์การจัดการความเสี่ยง	/	/	/***	*** ID.RM-3
	กลยุทธ์การจัดการ supply chain	/	/**	/	** ID.SC-4,5
มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น	**การป้องกัน**				
	การควบคุมการเข้าถึง	/	/	/	
	การรับรู้และการฝึกอบรม	/	/	/	
	ความปลอดภัยของข้อมูล	/	/	/***	*** PR.DS-7
	กระบวนการป้องกันข้อมูล	/	/**	/***	** PR.IP-2 *** PR.IP-8
	การดูแลรักษา	/	/	/	
	เทคโนโลยีที่ใช้ในการป้องกัน	/	/**	/	** PR.PT-5
มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์	**การตรวจจับ**				
	ความผิดปกติและเหตุการณ์ต่างๆ	/	/**	/***	** DE.AE-1 *** DE.AE-4
	การสังเกตการณ์อย่างต่อเนื่อง	/*	/	/***	* DE.CM-1 *** DE.CM-6,7
	กระบวนการตรวจสอบ	/	/	/	
มาตรการการผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์	**การรับมือ**				
	การวางแผนรับมือ	/	/	/	
	การสื่อสาร	/	/**	/***	** RS.CO-5
	การวิเคราะห์	/*	/	/***	* RS.AN-5 *** RS.AN-5
	การลดความเสี่ยง	/	/	/***	*** RS.MI-3
	การปรับปรุงแก้ไข	/	/	/***	*** RS.IM-2
มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์	**การคืนสภาพ**				
	การวางแผนฟื้นฟู	/	/	-	
	การปรับปรุง	/	/	/***	*** RC.IM-2
	การสื่อสาร	/	/**	-	** RC.CO-1,2

หมายเหตุ / มีครบทุกข้อย่อยของ NIST CFS
/*, /**, /*** ไม่มีบางข้อย่อยของ NIST CFS
- ไม่มีทุกข้อย่อยของ NIST CFS

ตารางที่ 2 ตารางเปรียบเทียบ NIST Cybersecurity Framework version 1.1 กับ มาตรฐานต่าง ๆ

สามารถสรุปสิ่งที่ กฟน. ควรปรับปรุงเพิ่มเติมจากการดำเนินการในปัจจุบัน ตามมาตรฐาน ISO 27001:2013 และออกแบบระบบใหม่ให้รองรับกระบวนการเหล่านี้ด้วย ได้แก่

1. ควรมีกระบวนการตรวจจับความผิดปกติและการบุกรุกต่าง ๆ ทางเครือข่ายของระบบควบคุมระบบไฟฟ้า
2. ควรมีกระบวนการรวบรวมข้อมูล วิเคราะห์ และตอบโต้หรือแก้ไข ช่องโหว่ต่าง ๆ ของระบบควบคุมระบบไฟฟ้า โดยมีประสานงานจากหน่วยงานภายนอกทั้งในประเทศและต่างประเทศ รวมทั้งผู้ผลิตระบบควบคุม

จากผลการศึกษาและการแลกเปลี่ยนประสบการณ์กับการไฟฟ้าต่าง ๆ ในประเทศสหรัฐอเมริกา [12],[13] และ รวมทั้งการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย ซึ่งได้ดำเนินการนำมาตรฐานการรักษาความมั่นคงปลอดภัย NERC CIP มาใช้ในศูนย์ควบคุมระบบไฟฟ้าของหน่วยงานไฟฟ้าเป็นระยะเวลานานและสามารถป้องกันภัยคุกคามได้เป็นอย่างดี ดังนั้น กฟน. จึงพิจารณานำมาตรฐานการรักษาความมั่นคงปลอดภัย NERC CIP ซึ่งเป็นมาตรฐานที่บังคับใช้กับหน่วยงานการไฟฟ้าโดยตรง มาประยุกต์ใช้กับการออกแบบระบบควบคุมระบบไฟฟ้าใหม่ (ระบบ SCADA/EMS/DMS ใหม่) และจะนำมาปรับปรุงขั้นตอนหรือกระบวนการปฏิบัติจากเดิมที่ดำเนินการตามมาตรฐาน ISO 27001 ไม่ให้มีความซ้ำซ้อนและมีประสิทธิภาพขึ้น โดยมาตรฐาน NERC CIP นั้นมีการกำหนดกระบวนการ วิธีการ ทั้งในทางปฏิบัติและทางเทคนิคอย่าง

ชัดเจน เหมาะสมกับระบบควบคุมระบบไฟฟ้า โดยจะครอบคลุมทั้งการรักษาความมั่นคงปลอดภัยทางกายภาพและทางไซเบอร์ รวมทั้งเพิ่มการควบคุมสำหรับจัดการความเสี่ยงของห่วงโซ่อุปทาน (supply chain) ของผู้ผลิตซอฟท์แวร์และฮาร์ดแวร์ของระบบควบคุม ทั้งนี้จะพิจารณาเพิ่มเติมข้อกำหนดย่อยของ NIST CFS V.1.1 ที่ไม่มีในมาตรฐาน NERC CIP ตามผลการวิเคราะห์ที่ได้ต่อไป ซึ่งจะเป็นการเตรียมความพร้อมต่อข้อกำหนดแนวปฏิบัติที่จะบังคับใช้ในประเทศไทยต่อไปในอนาคต

นอกจากการนำมาตรฐานการรักษาความมั่นคงปลอดภัย NERC CIP มาประยุกต์ใช้ในการออกแบบระบบควบคุมใหม่ กฟน. ได้ประเมินความเสี่ยงของระบบงานต่าง ๆ ที่ กฟน. ต้องการแลกเปลี่ยนข้อมูล ระบบสื่อสารที่จะเปลี่ยนไปของระบบควบคุม รวมทั้งพิจารณานำมาตรฐานสากลที่ใช้กับงานควบคุมระบบไฟฟ้า มาใช้ในการออกแบบ และ กำหนดข้อกำหนดของระบบควบคุมระบบไฟฟ้าใหม่ โดยได้เลือกใช้มาตรฐานสากลทางด้านเทคนิคสำหรับการสื่อสารข้อมูล คือ IEC 62351 [14] มาใช้กับการติดต่อสื่อสารระหว่างศูนย์ควบคุมระบบไฟฟ้ากับอุปกรณ์ต่าง ๆ ภายในสถานีไฟฟ้าหรืออุปกรณ์ที่ติดตั้งบนเสาไฟฟ้า การติดต่อสื่อสารระหว่างศูนย์ควบคุมระบบไฟฟ้าของ กฟน. และศูนย์ควบคุมกำลังไฟฟ้าแห่งชาติของ การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย ซึ่งจะสามารถป้องกันภัยคุกคามของการปลอมตัว (Spoofing) การแก้ไขข้อมูล (Modification) การทวนซ้ำข้อมูล (Replay) และการดักฟังข้อมูล (Eavesdropping) ซึ่งจะทำให้มั่นใจได้ว่าการสื่อสารข้อมูลระหว่างศูนย์ควบคุมระบบไฟฟ้ากับอุปกรณ์ไฟฟ้าต่าง ๆ ได้ดำเนินการจากระบบควบคุมจริง เนื่องจากมีการตรวจสอบพิสูจน์ตัวตน ของโปรโตคอลที่ใช้สื่อสารสำหรับการส่งคำสั่งสำคัญไปยังระบบไฟฟ้า ไม่ถูกการดักฟังข้อมูล แก้ไขข้อมูล จนทำลายระบบควบคุมระบบไฟฟ้าของ กฟน. ได้

การออกแบบระบบ SCADA/EMS/DMS ใหม่ ให้รองรับความต้องการและมีความมั่นคงปลอดภัยทางไซเบอร์และภัยคุกคามอื่น ๆ กฟน. ใช้แนวทางการออกแบบตามคำแนะนำแนวปฏิบัติที่ดี [16] ของ กระทรวงความมั่นคงแห่งมาตุภูมิของประเทศสหรัฐอเมริกา (U.S. Department of Homeland Security) โดยใช้หลักการออกแบบตามหลักยุทธศาสตร์การป้องกันเชิงลึก (Défense-in-Depth Strategy) ประกอบกับข้อกำหนดทางเทคนิคที่มาตรฐาน NERC CIP บังคับให้ระบบควบคุมระบบไฟฟ้าต้องมีและควบคุม โดยสรุปสำหรับสิ่งที่ได้ปรับปรุงเพิ่มเติมจากระบบปัจจุบันได้ ดังนี้

- แบ่งแยกระบบและเครือข่ายออกเป็นแต่ละ environment หรือโซน เพื่อกำหนดและควบคุมการไหลของข้อมูลและความปลอดภัยได้ดียิ่งขึ้น และต้องมีการควบคุมทุกจุดที่มีข้อมูลเข้าออก และมีการจัดเก็บข้อมูลเหตุการณ์ต่าง ๆ ของระบบ
- มีระบบบริหารจัดการรักษาความมั่นคงปลอดภัย เช่น การบริหารจัดการสิทธิ์ การตรวจจับการบุกรุกและการป้องกันการบุกรุก การควบคุมการเข้าถึงตามบทบาท เป็นต้น
- มีระบบสำรองข้อมูลของระบบทั้งหมด ติดตั้งนอกศูนย์ควบคุมระบบไฟฟ้า
- ระบบควบคุม ทั้งส่วน ฮาร์ดแวร์และซอฟท์แวร์ จะต้องควบคุมตามมาตรฐาน NERC CIP

4. สรุปอภิปรายผลและข้อเสนอแนะ

การดำเนินการรักษาความมั่นคงปลอดภัยของระบบควบคุมระบบไฟฟ้า ของการไฟฟ้านครหลวง จะต้องดำเนินการทั้งด้านบุคลากร กระบวนการทำงาน รวมทั้งการนำเทคโนโลยีที่เหมาะสมมาประยุกต์ใช้กับระบบของ กฟน. โดยประยุกต์ใช้มาตรฐานที่เหมาะสม เพื่อให้สอดคล้องกับแนวปฏิบัติที่ดี และกฎ ระเบียบ ข้อกำหนดต่างๆที่หน่วยงานโครงสร้างพื้นฐานสำคัญจะต้องปฏิบัติ รวมถึงจะต้องพิจารณาประเมินความเสี่ยงระบบงานอื่น ๆ ที่เป็นส่วนประกอบสำคัญของระบบควบคุมหลักด้วย และปรับปรุงระบบงานอื่น ๆ ที่ต้องเชื่อมต่อกับระบบควบคุมหลัก เพื่อให้เกิดความมั่นคงปลอดภัยต่อกระบวนการควบคุมระบบไฟฟ้าอย่างครบถ้วน ถึงแม้ว่า ระบบควบคุมระบบไฟฟ้าใหม่ หรือ ระบบ SCADA/EMS/DMS ของ กฟน. จะได้เตรียมการออกแบบให้รองรับกับความต้องการที่เพิ่มขึ้น รวมทั้ง ป้องกันภัยคุกคามอื่น ๆ ในเชิงเทคนิคแล้ว การดำเนินการด้านการบริหารจัดการและการรักษาความมั่นคงปลอดภัยของระบบควบคุมระบบไฟฟ้าจะต้องดำเนินการอย่างต่อเนื่องและปรับปรุงให้ทันสมัยอยู่เสมอ รวมทั้ง จะต้องเตรียมการในด้านการดำเนินการต่าง ๆ ให้สอดคล้องกับยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ รวมถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และข้อกำหนดอื่น ๆ ที่ทางรัฐบาลหรือหน่วยงานของประเทศไทยจะประกาศใช้ต่อไปในอนาคต

การเตรียมบุคลากรเป็นอีกเรื่องที่มีความสำคัญอย่างยิ่ง ทั้งในการกำหนดโครงสร้างหน่วยงานที่ดูแลรับผิดชอบด้านความมั่นคงปลอดภัยของระบบควบคุมระบบไฟฟ้าอย่างชัดเจน และเตรียมความรู้ของบุคลากร โดยการสร้างความตระหนัก ให้ความรู้เชิงลึก และ ทักษะของการรักษาความมั่นคงปลอดภัย เทคโนโลยี แนวปฏิบัติที่ถูกต้อง ทั้ง เทคโนโลยีสารสนเทศ (Information Technology, IT) และ เทคโนโลยีเชิงปฏิบัติการ (Operational Technology, OT) เพื่อให้บุคลากรที่ออกแบบ พัฒนา ติดตั้งและทดสอบ รวมทั้งดูแลระบบควบคุมระบบไฟฟ้าและระบบงานอื่น ๆ ของ กฟน. ให้มีความพร้อมต่อการรักษาความมั่นคงปลอดภัย สามารถป้องกันภัยคุกคาม และ ตอบโต้ หรือกู้คืนระบบงานได้อย่างรวดเร็ว

เพื่อให้การบริการจำหน่ายไฟฟ้าแก่ประชาชนดำเนินการได้อย่างต่อเนื่อง

เอกสารอ้างอิง

[1] “Cyber challenges to the energy transition”, World Energy Council, 2019, pp.6-7

[2] Eric Byres, Andrew Ginter, Joel Langill, “How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems”, 2011, pp.6-21

[3] Nell Nelson, “The Impact of Dragonfly Malware on Industrial Control Systems”, 2016, pp.4-15

[4] “TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case”, E-ISAC and SANS, 2016, pp.4-10

[5] “CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations”, Dragos, 2017, pp.16-25

[6] “ISO/IEC 27001:2013 Information technology – Security techniques – Information Security Management System – Requirements”, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2013

[7] “Critical Infrastructure Protection CIP-002 to CIP-011 and CIP-013 to CIP-014”, North American Electric Reliability Corporation, 2016-2021

[8] “IEC 62443 series for Industrial Automation and Control System (IACS) security”, International Electrotechnical Commission (IEC), 2009-2020

[9] “รายงานผลการดำเนินงานฉบับที่ 1 โครงการจ้างที่ปรึกษาการพัฒนาระบบรักษาความมั่นคงปลอดภัยด้านไซเบอร์ ของ สนพ.”, บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด, 2562, หน้า 5

[10] ดร. ปริญญา หอมเอนก, “การเตรียมองค์กร สอดรับ กม. ไซเบอร์”, 2562, (ออนไลน์) Available: https://www.bangkokbiznews.com/blogs/columnist/123072

[11] พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 “พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562”, สำนักงานราชกิจจานุเบกษา, 2562., หน้า 26-27

[12] “รายงานผลการศึกษาดูงานหลักสูตร Improvement on Management of Power System Operation and Utilities Visit”, คณะศึกษาดูงาน การไฟฟ้านครหลวง, 2559, หน้า 9,11-12,25

[13] “รายงานผลการศึกษาดูงาน Digital Substation for Smart Grid”, คณะศึกษาดูงาน การไฟฟ้านครหลวง, 2562, หน้า 1-12, 38-41

[14] “IEC 62351 Power systems management and associated information exchange - Data and communications security”, International Electrotechnical Commission (IEC), 2007-2020

[15] “IEC 62351-10 Security architecture guidelines”, International Electrotechnical Commission (IEC), 2012, page 23

[16] “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies”, U.S. Department of Homeland Security, 2016