แนวทางการประเมินคุณภาพซอฟต์แวร์สำหรับการประยุกต์ใช้ทางการทหาร: กรณีศึกษาบนระบบซอฟต์แวร์สำหรับการถอดรหัสและแสดงผลข้อมูลเรดาร์

Military Software Quality Assessment (MSQA) Framework: A Case Study of the Air Situation Display (ASD) System

สุทธิชัย รอดแก้ว[1, 2], ภูจนา ปาลิยะวรรณ[1], กิ่งกาญจน์ สุขคณาภิบาล[1*], วรวัฒน์ เชิญสวัสดิ์[1]

Sutthichai Rodkaew[1, 2], Pujana Paliyawan[1], Kingkarn Sookhanaphibarn[1*], Worawat Choensawat[1]

[1]ศูนย์นวัตกรรมเฉพาะทาง มหาวิทยาลัยกรุงเทพ 10120 ประเทศไทย

[1]Center of Specialty Innovation (CoSI), Bangkok University 10120, Thailand

[2]หน่วยบัญชาการป้องกันภัยทางอากาศกองทัพบก, ประเทศไทย

[2]Army Air Defense Command, Thailand

**Corresponding Author. E-mail : kingkarn.s@bu.ac.th*

(Received: March 27, 2025, Revised: July 23, 2025, Accepted: August 13, 2025)

บทคัดย่อ: การประเมินคุณภาพซอฟต์แวร์เป็นปัจจัยสำคัญในการพัฒนาและรับรองความสามารถของระบบซอฟต์แวร์ให้สอดคล้องกับมาตรฐานและข้อกำหนดเฉพาะทาง โดยเฉพาะสำหรับระบบซอฟต์แวร์ทางทหารที่มีความซับซ้อนสูงและต้องทำงานในสภาพแวดล้อมที่ท้าทาย การประเมินคุณภาพที่มีประสิทธิภาพจะช่วยให้ระบบสามารถทำงานได้อย่างถูกต้องตามที่คาดหวัง และลดความเสี่ยงจากข้อผิดพลาดที่อาจเกิดขึ้นในกระบวนการพัฒนาและบำรุงรักษา บทความนี้นำเสนอกรอบการประเมินคุณภาพซอฟต์แวร์ใหม่ในชื่อ Military Software Quality Assessment (MSQA) Framework ซึ่งพัฒนาขึ้นบนพื้นฐานของมาตรฐาน ISO/IEC 25010 พร้อมบูรณาการมาตรฐานสำคัญอื่น ๆ เช่น MIL-STD-498 MIL-STD-882 MIL-STD-1397C MIL-STD-810 MIL-STD-461 ISO/IEC 12207 ISO/IEC15504 และ ISO/IEC27001 เพื่อเพิ่มความครอบคลุมและเหมาะสมกับการใช้งานในบริบททางทหาร บทความยังนำเสนอกรณีศึกษาการพัฒนาระบบแสดงผลเรดาร์ของกองทัพบกไทย เพื่อแสดงการประยุกต์ใช้ MSQA ในการประเมินและปรับปรุงคุณภาพซอฟต์แวร์จริงอย่างเป็นระบบ

คำสำคัญ: การประเมินคุณภาพซอฟต์แวร์ IEC25010 มาตรฐานซอฟต์แวร์ ระบบซอฟต์แวร์ทางการทหาร การบูรณาการมาตรฐาน

Abstract: Software quality assessment is a critical factor in developing and validating software systems to ensure compliance with specific standards and requirements, especially for military software systems that are highly complex and must operate in challenging environments. Effective quality assessment ensures systems perform as expected and reduces risks from errors during

development and maintenance. This paper presents a novel software quality assessment framework, called the Military Software Quality Assessment (MSQA) Framework, developed based on the ISO/IEC 25010 standard and integrating key related standards such as MIL-STD-498, MIL-STD-882, MIL-STD-1397C, MIL-STD-810, MIL-STD-461, ISO/IEC 12207, ISO/IEC 15504, and ISO/IEC 27001 to enhance comprehensiveness and suitability for military applications. A case study on the development of a radar display system for the Royal Thai Army demonstrates the practical application of MSQA in systematically assessing and improving software quality in a real-world military context.

Keywords: Software Quality Assessment, IEC 25010, Software Standards, Military Software Systems, Standards Integration

1. บทนำ

ซอฟต์แวร์ทางทหารมีบทบาทสำคัญอย่างยิ่งในการสนับสนุนภารกิจที่เกี่ยวข้องกับความมั่นคงและความปลอดภัยของประเทศ ด้วยความซับซ้อนและสภาพแวดล้อมที่ต้องเผชิญกับความท้าทายต่าง ๆ เช่น การโจมตีทางไซเบอร์ สภาวะทางภูมิอากาศที่รุนแรง และสถานการณ์ฉุกเฉินอื่น ๆ การประเมินคุณภาพซอฟต์แวร์สำหรับระบบทหารจึงมีความสำคัญเพื่อให้มั่นใจว่าซอฟต์แวร์สามารถทำงานได้อย่างแม่นยำเชื่อถือได้ ในสภาพแวดล้อมและสถานการณ์ต่างๆ

กรณีตัวอย่างเหตุการณ์จริงที่แสดงผลกระทบในทางลบจากการขาดการบริหารจัดการซอฟต์แวร์อย่างเหมาะสม สามารถอ้างอิงจากข่าวตามเอกสารอ้างอิงที่ [1] และ [2] เช่น กรณีของระบบ Joint Disability Evaluation Tracking System (JDETS) ของกองทัพเรือสหรัฐฯ เคยเกิดเหตุระบบล่มจนไม่สามารถประมวลผล เพื่อปลดทหารกว่า 3,000 นาย เป็นเวลานานเกือบหนึ่งสัปดาห์ ส่งผลกระทบต่อการเข้าถึงบริการสำคัญต่อบุคลากร (อ้างอิง [1]) และกรณีของเฮลิคอปเตอร์ MRH-90 Taipan ของกองทัพออสเตรเลียที่ต้องลงจอดฉุกเฉินเนื่องจากการละเลยการติดตั้งแพตช์ซอฟต์แวร์สำคัญ (อ้างอิง [2]) เหตุการณ์เหล่านี้แสดงให้เห็นถึงต้นทุนและความเสียหายที่อาจเกิดขึ้นหากไม่บริหารจัดการคุณภาพซอฟต์แวร์อย่างเคร่งครัด

ในประเทศไทย ซอฟต์แวร์มีบทบาทสำคัญอย่างยิ่งต่อการปฏิบัติภารกิจทั้งในด้านการควบคุมระบบยุทโธปกรณ์ การวิเคราะห์ข้อมูลสถานการณ์ และการสื่อสารทางยุทธวิธี หน่วยทหารบางแห่ง เช่น ศูนย์ต่อสู้ป้องกันภัยทางอากาศกองทัพบก (ศปภอ.ทบ.) มีการพัฒนาซอฟต์แวร์สำหรับงานทางทหารเอง ทั้งในรูปแบบของการสร้างระบบใหม่และการปรับปรุงระบบเดิมเพื่อให้ทันต่อภารกิจที่เปลี่ยนแปลง อย่างไรก็ตาม แม้จะมีการทดสอบระบบอย่างเข้มงวดโดยเจ้าหน้าที่ผู้ใช้งานจริง รวมถึงการประเมินผลการใช้งานโดยผู้บังคับบัญชา แต่กระบวนการเหล่านี้ยังขาดแนวทางการประเมินคุณภาพซอฟต์แวร์ที่เป็นมาตรฐานกลาง ทำให้การพิจารณาด้านคุณภาพขึ้นอยู่กับบริบทของแต่ละระบบและมุมมองของผู้ประเมินในแต่ละครั้ง ซึ่งอาจส่งผลให้คุณลักษณะสำคัญบางประการไม่ได้รับการพิจารณาอย่างครบถ้วน

ด้วยเหตุนี้ จึงเกิดความต้องการในการกำหนดแนวทางการควบคุมและประเมินคุณภาพซอฟต์แวร์อย่างเหมาะสม จนเป็นจุดเริ่มต้นของการศึกษาและวิจัยเกี่ยวกับการประเมินคุณภาพซอฟต์แวร์ในบริบททางทหาร ซึ่งนำไปสู่การทบทวนมาตรฐานที่มีอยู่และข้อค้นพบว่ามาตรฐานเดิมยังไม่ตอบโจทย์อย่างครบถ้วน ส่งผลให้มีการเสนอกรอบการประเมินคุณภาพซอฟต์แวร์ใหม่ที่เหมาะสมกับสภาพแวดล้อมและความต้องการเฉพาะของกองทัพบกไทยในปัจจุบัน

มาตรฐานสากลที่ใช้เป็นกรอบอ้างอิงสำหรับการประเมินคุณภาพซอฟต์แวร์มีอยู่หลายรายการ โดยสามารถแบ่งออกเป็นกลุ่มหลัก ๆ เช่น กลุ่ม MIL (Military Standards) ซึ่งเป็นชุดมาตรฐานที่พัฒนาโดยกระทรวงกลาโหมสหรัฐอเมริกาเพื่อควบคุมคุณภาพของระบบและซอฟต์แวร์ทางทหารโดยเฉพาะ และกลุ่ม IEC (International Electrotechnical Commission) ซึ่งทำโดยองค์กรระหว่างประเทศที่กำหนดมาตรฐานทางเทคนิคสำหรับระบบไฟฟ้า อิเล็กทรอนิกส์ และเทคโนโลยีสารสนเทศ รวมถึงมาตรฐานคุณภาพซอฟต์แวร์สำหรับการใช้งานทั่วไป ทีมวิจัยได้ทำการสำรวจและวิเคราะห์มาตรฐานจากทั้งสองกลุ่ม และพบว่ามาตรฐานที่เกี่ยวพันธ์ข้องกับการควบคุมคุณภาพซอฟแวร์มากที่สุด ได้แก่ MIL-STD-498 ซึ่งครอบคลุมขั้นตอนการพัฒนาและควบคุมเอกสารในโครงการทางทหาร และ ISO/IEC 25010 ซึ่งเน้นคุณลักษณะด้านคุณภาพของซอฟต์แวร์ทั่วไป ทีมวิจัยจึงได้นำทั้งสองมาตรฐานมาเป็นรากฐานหลักเพื่อการพัฒนาแนวทางการประเมินสำหรับกองทัพบกไทย

แม้ว่า MIL-STD-498 และ ISO/IEC 25010 จะเป็นมาตรฐานสากลที่ได้รับการยอมรับอย่างกว้างขวางและมีความเกี่ยวข้องกับการประเมินคุณภาพซอฟต์แวร์ในระดับทั่วไปและทางทหาร แต่ทั้งสองมาตรฐานก็ยังมีข้อจำกัดสำคัญที่ทำให้ไม่สามารถนำมาใช้ได้โดยตรงในบริบทของกองทัพบกไทย โดย MIL-STD-498 ซึ่งประกาศใช้ในปี 1994 นั้น มุ่งเน้นที่การควบคุมเอกสารและกระบวนการพัฒนาซอฟต์แวร์อย่างเป็นระบบเป็นหลัก และสะท้อนแนวคิดของการจัดการคุณภาพในยุคต้นของระบบดิจิทัล อีกทั้ง MIL-STD-498 ได้ถูกยกเลิกอย่างเป็นทางการ และแทนที่ด้วย IEEE/EIA 12207 ซึ่งต่อมาได้รับการยอมรับเป็น ISO/IEC 12207 สำหรับการจัดการกระบวนการพัฒนาซอฟต์แวร์ อย่างไรก็ตาม ISO/IEC 12207 มุ่งเน้นที่การจัดการและควบคุมกระบวนการพัฒนาเป็นหลัก มากกว่าการประเมินคุณภาพของตัวซอฟต์แวร์ที่พัฒนาแล้วโดยตรง จึงไม่เหมาะสำหรับใช้เป็นโครงสร้างหลักในการประเมินคุณภาพเชิงเทคนิคในบริบทเฉพาะของระบบทางทหาร

ในขณะที่ ISO/IEC 25010 แม้จะครอบคลุมคุณภาพเชิงเทคนิคของซอฟต์แวร์ในหลากหลายมิติ เช่น ความน่าเชื่อถือ ความปลอดภัย และการใช้งานง่าย แต่ก็ยังไม่สามารถสะท้อนความต้องการเฉพาะของซอฟต์แวร์ทางทหารได้อย่างครบถ้วน เช่น ความทนทานภายใต้สภาวะฉุกเฉิน ความสามารถในการบำรุงรักษาภายใต้ข้อจำกัดของสนามรบ และมาตรการด้านความมั่นคงปลอดภัยในระดับสูง กรอบการประเมินใหม่จึงจำเป็นต้องได้รับการออกแบบให้มีความครอบคลุมมากขึ้น เพื่อให้ตอบสนองต่อบริบทและภารกิจของกองทัพได้อย่างแท้จริง

2. วัตถุประสงค์และขอบเขตของงานวิจัย

งานวิจัยนี้มีเป้าหมายเพื่อพัฒนา กรอบการประเมินคุณภาพซอฟต์แวร์สำหรับงานด้านการทหาร ที่มีชื่อว่า Military Software Quality Assessment (MSQA) Framework โดยมุ่งเน้นให้สามารถประเมินคุณภาพซอฟต์แวร์ได้อย่างครอบคลุม สอดคล้องกับบริบทเฉพาะของระบบทางทหาร ซึ่งมักต้องเผชิญกับข้อจำกัดด้านทรัพยากร สภาพแวดล้อมที่ท้าทาย และความต้องการด้านความมั่นคงปลอดภัยในระดับสูง

MSQA พัฒนาขึ้นโดยอิงโครงสร้างหลักจากมาตรฐาน ISO/IEC 25010 ที่เน้นคุณลักษณะด้านคุณภาพของผลิตภัณฑ์ซอฟต์แวร์ พร้อมทั้งผสานมาตรฐานอื่นที่เกี่ยวข้อง เช่น MIL-STD-498 สำหรับเอกสารด้านเทคนิค, MIL-STD-882 สำหรับการจัดการความปลอดภัย, ISO/IEC 12207 สำหรับวงจรชีวิตซอฟต์แวร์, ISO/IEC 15504 สำหรับการประเมินกระบวนการ และ ISO/IEC 27001 สำหรับการจัดการความมั่นคงปลอดภัยของข้อมูล การผสมผสานนี้ช่วยให้กรอบ MSQA มีความยืดหยุ่นเพียงพอในการประเมินทั้งซอฟต์แวร์ที่มีอยู่เพื่อการปรับปรุง และซอฟต์แวร์ใหม่ที่จะพัฒนาในอนาคต

ขอบเขตของงานวิจัยนี้ยังเสนอการประยุกต์ใช้ MSQA กับระบบที่มีข้อกำหนดเฉพาะ คือ ระบบซอฟต์แวร์สำหรับการถอดรหัสและแสดงผลข้อมูลเรดาร์ (Air Situation Display: ASD) เรียกโดยย่อว่า ระบบ

ASD โดยนำเสนอกรณีศึกษาจริง เพื่อทดสอบประสิทธิภาพและความเหมาะสมของกรอบการประเมินที่พัฒนาขึ้น ข้อจำกัดที่สำคัญ ได้แก่ การประเมินเน้นที่ซอฟต์แวร์เป็นหลัก ไม่รวมฮาร์ดแวร์ และมุ่งเน้นบริบทของภารกิจทางทหารเท่านั้น ซึ่งอาจจำเป็นต้องปรับเปลี่ยนกรอบเมื่อนำไปใช้กับระบบหรือภาคส่วนอื่น

3. เอกสารและงานวิจัยที่เกี่ยวข้อง

หัวข้อนี้จะนำเสนอมาตรฐานที่เกี่ยวข้องกับการควบคุมคุณภาพซอฟแวร์ โดยเนื้อหาแบ่งเป็นสองส่วนหลักๆ คือ ส่วนของ ISO/IEC 25010 [3, 4] ได้ใช้เป็นโครงสร้างหลักของ MSQA และส่วนของมาตรฐานอื่นๆ ที่เกี่ยวข้อง [5–13]

3.1 มาตรฐานหลักที่อ้างอิง (ISO/IEC 25010)

ISO/IEC 25010 [3, 4] มีชื่อเรียกว่า “System and Software Quality Models” ใช้สำหรับประเมินคุณภาพระบบและซอฟต์แวร์ โดยมีการกำหนดลักษณะคุณภาพที่ต้องพิจารณา โดยระบบจะถือว่ามีคุณภาพก็ต่อเมื่อสามารถตอบสนองความต้องการทั้งที่ระบุไว้และที่ไม่ได้ระบุของผู้มีส่วนเกี่ยวข้องได้อย่างเหมาะสม ซึ่งมีการแบ่งคุณภาพออกเป็นลักษณะหลักและลักษณะย่อยดังนี้

1) ความเหมาะสมของฟังก์ชันการทำงาน (Functional Suitability) คือ การวัดระดับที่ระบบสามารถตอบสนองความต้องการที่ระบุและแฝงไว้ภายใต้เงื่อนไขที่กำหนด ซึ่งมีองค์ประกอบดังนี้ ความครบถ้วนของฟังก์ชัน (Functional Completeness) ความถูกต้องของฟังก์ชัน (Functional Correctness) และความเหมาะสมของฟังก์ชัน (Functional Appropriateness)
2) ประสิทธิภาพการทำงาน (Performance Efficiency) คือ การวัดระดับที่ระบบสามารถดำเนินการตามเวลาที่กำหนดและทรัพยากรอย่างเหมาะสม ซึ่งมีองค์ประกอบดังนี้ ประสิทธิภาพด้านเวลา (Time Behavior) ประสิทธิภาพในการใช้ทรัพยากร (Resource Utilization) และขีดความสามารถในการรองรับงาน (Capacity)
3) ความสามารถในการทำงานร่วมกัน (Compatibility) คือ การวัดระดับที่ระบบสามารถแลกเปลี่ยนข้อมูลกับผลิตภัณฑ์อื่น ๆ และทำงานร่วมกันได้ ซึ่งมีองค์ประกอบดังนี้ การอยู่ร่วมกัน (Co-existence) และความสามารถในการทำงานร่วมกัน (Interoperability)
4) ความสามารถในการโต้ตอบ (Interaction Capability) คือ การวัดระดับที่ระบบสามารถโต้ตอบกับผู้ใช้เพื่อแลกเปลี่ยนข้อมูลผ่านอินเทอร์เฟซ ซึ่งมีองค์ประกอบดังนี้ ความเหมาะสมในการจดจำ (Appropriateness Recognizability) ความสามารถ ในการเรียนรู้ (Learnability) ความสามารถในการใช้งาน (Operability) การป้องกันข้อผิดพลาดของผู้ใช้ (User Error Protection) การมีส่วนร่วมของผู้ใช้ (User Engagement) ความครอบคลุมสำหรับผู้ใช้ทุกกลุ่ม (Inclusivity) การช่วยเหลือผู้ใช้ (User Assistance) และความสามารถในการอธิบายตนเอง (Self-descriptiveness)
5) ความน่าเชื่อถือ (Reliability) คือ การวัดระดับที่ระบบสามารถทำงานได้อย่างต่อเนื่องภายใต้เงื่อนไขที่กำหนด ซึ่งมีองค์ประกอบดังนี้ ความถูกต้องแม่นยำ (Faultlessness) ความพร้อมใช้งาน (Availability) ความสามารถในการทนต่อข้อผิดพลาด (Fault Tolerance) และความสามารถในการกู้คืนข้อมูล (Recoverability)
6) ความปลอดภัย (Security) คือ การวัดระดับที่ระบบสามารถป้องกันการโจมตีและปกป้องข้อมูล ซึ่งมีองค์ประกอบดังนี้ การรักษาความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) การป้องกันการปฏิเสธความรับผิดชอบ (Non-repudiation) ความสามารถในการตรวจสอบความรับผิดชอบ (Accountability) ความแท้จริงของข้อมูล (Authenticity) และความสามารถในการต้านทานการโจมตี (Resistance)

7) ความสามารถในการบำรุงรักษา (Maintainability) คือ การวัดระดับที่ระบบสามารถแก้ไข ปรับปรุง หรือปรับเปลี่ยนเพื่อตอบสนองต่อการเปลี่ยนแปลง ซึ่งมีองค์ประกอบดังนี้ การออกแบบเป็นโมดูล (Modularity) การนำกลับมาใช้ใหม่ (Reusability) และความ สามารถในการวิเคราะห์ (Analyzability)

8) ความยืดหยุ่น (Flexibility) คือ การวัดระดับที่ระบบสามารถปรับตัวให้เข้ากับการเปลี่ยนแปลงของสภาพแวดล้อมและความต้องการ ซึ่งมีองค์ประกอบดังนี้ ความสามารถในการปรับตัว (Adaptability) ความสามารถในการขยายขนาด (Scalability) การติดตั้ง (Installability) และการทดแทน (Replac- eability)

9) ความปลอดภัย (Safety) คือ การวัดระดับที่ระบบสามารถหลีกเลี่ยงอันตรายต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อม ซึ่งมีองค์ประกอบดังนี้ ข้อจำกัดในการปฏิบัติการ (Operational Constraints) การระบุความเสี่ยง (Risk Identification) ระบบป้องกันความล้มเหลว (Failure Prevention) การเตือนภัยอันตราย (Hazard Warning) และการรวมระบบอย่างปลอดภัย (Safe System Integration)

3.1.1 การยอมรับและการใช้งานของมาตรฐาน ISO/IEC 25010

ISO/IEC 25010 เป็นมาตรฐานที่ได้รับการยอมรับอย่างกว้างขวางในทั้งภาคอุตสาหกรรมและงานวิจัย โดยงานศึกษาของ Wagner et al. (2017) [14] ชี้ให้เห็นว่าองค์กรต่างๆ ใช้มาตรฐานนี้ในการกำหนดและจัดการความต้องการด้านคุณภาพซอฟต์แวร์ ขณะที่งานของ Alnanih et al. (2014) [15] แสดงให้เห็นถึงการประยุกต์ใช้ ISO/IEC 25010 อย่างเป็นระบบในการประเมินคุณภาพซอฟต์แวร์ ทำให้มาตรฐานนี้เป็นเครื่องมือที่ครบถ้วนและมีประสิทธิภาพสำหรับการวัดและประเมินคุณภาพซอฟต์แวร์ในทางปฏิบัติและทางวิชาการ

3.1.2 ข้อจำกัดของ ISO/IEC 25010

ในบริบทของการประเมินคุณภาพซอฟต์แวร์สำหรับระบบที่มีความซับซ้อนหรือใช้งานในสภาพแวดล้อมเฉพาะทาง เช่น ระบบทางทหาร มาตรฐาน ISO/IEC 25010 แม้จะเป็นกรอบการประเมินที่ครอบคลุมและได้รับการยอมรับในระดับสากล แต่ก็ยังมีข้อจำกัดบางประการที่ควรพิจารณา

ประการแรก มาตรฐานนี้ไม่ได้ออกแบบมาเพื่อรองรับบริบทเฉพาะ เช่น การใช้งานในสถานการณ์วิกฤต ความจำเป็นในการทำงานแบบต่อเนื่อง หรือสภาพแวดล้อมที่มีความเสี่ยงสูง ซึ่งพบได้บ่อยในระบบที่เกี่ยวข้องกับความมั่นคงและความปลอดภัย

ประการที่สอง ISO/IEC 25010 ไม่มีหมวดประเมินที่มุ่งเน้นความทนทานของระบบ (durability) และความสามารถในการบูรณาการกับระบบเดิม (legacy systems) อย่างชัดเจน ทั้งที่เป็นปัจจัยสำคัญในการออกแบบและใช้งานระบบในระยะยาว

ประการที่สาม มาตรฐานนี้ยังขาดการประเมินความสอดคล้องกับข้อกำหนดด้านกฎหมายหรือมาตรฐานเฉพาะทาง เช่น มาตรฐานด้านความปลอดภัยสารสนเทศหรือมาตรฐานทางการทหาร ซึ่งมีบทบาทสำคัญในการรับรองความปลอดภัยและความน่าเชื่อถือของระบบ

สุดท้าย ประเด็นด้านการติดตั้ง การใช้งานจริง และผลกระทบต่อระบบเดิมยังไม่ได้รับการกล่าวถึงอย่างชัดเจนใน ISO/IEC 25010 แม้จะเป็นปัจจัยสำคัญต่อความสำเร็จของการนำระบบไปใช้ในบริบทที่มีข้อจำกัดเฉพาะทาง เช่น การใช้งานในภาคสนามในสภาพการณ์ที่มีข้อจำกัดด้านเวลาและทรัพยากร

จากข้อจำกัดเหล่านี้ แสดงให้เห็นว่าแม้มาตรฐาน ISO/IEC 25010 จะมีความครอบคลุมในมุมมองทั่วไป แต่ก็ยังไม่เพียงพอสำหรับการประเมินซอฟต์แวร์ในบริบทที่มีความเฉพาะเจาะจงหรือมีข้อกำหนดด้านความปลอดภัยและความน่าเชื่อถือสูง

3.2 มาตรฐานอื่นๆ ที่พิจารณา

แม้ว่ากรอบ MSQA จะอิงกับ ISO/IEC 25010 เป็นหลัก แต่มาตรฐานนี้เน้นเฉพาะคุณภาพของซอฟต์แวร์เท่านั้น ในบริบทของระบบทหาร ซึ่งมีความซับซ้อนและสภาพแวดล้อมการทำงานที่ท้าทาย จำเป็นต้องพิจารณามาตรฐานเสริมเพิ่มเติมทั้งจากกลุ่ม MIL-STD และ ISO/IEC เพื่อครอบคลุมในทุกมิติของคุณภาพ ทั้งด้านกายภาพ ความปลอดภัย ความเชื่อถือได้ และความสามารถในการบำรุงรักษา

MIL-STD-498 [5] เป็นมาตรฐานของกระทรวงกลาโหมสหรัฐฯ ที่กำหนดกระบวนการพัฒนาซอฟต์แวร์และการจัดทำเอกสารอย่างเข้มงวด โดยให้ความสำคัญกับการตรวจสอบย้อนกลับ (Traceability) และการควบคุมเวอร์ชัน (Version Control) ซึ่ง MSQA ได้นำแนวทางดังกล่าวมาเสริมในด้านการบำรุงรักษา (Maintainability) และความสามารถในการติดตั้ง (Installability) เพื่อให้แน่ใจว่าระบบสามารถปรับปรุงและดูแลได้ตลอดอายุการใช้งาน

MIL-STD-882 [6] เป็นมาตรฐานด้านความปลอดภัยของระบบ (System Safety) ที่เน้นการวิเคราะห์อันตราย (Hazard Analysis) การประเมินความเสี่ยง (Risk Assessment) และการกำหนดมาตรการลดความเสี่ยง (Risk Mitigation) ตลอดวงจรชีวิตของระบบ MSQA ได้นำแนวทางนี้มาเสริมในมิติด้านความปลอดภัย (Safety) และความสอดคล้องกับข้อกำหนด (Compliance) โดยเน้นการประเมินระดับความรุนแรงและความถี่ของความเสี่ยง เพื่อนำไปสู่การวางแผนป้องกันหรือบรรเทาผลกระทบที่อาจเกิดขึ้นในระบบที่ทำงานภายใต้สภาพแวดล้อมที่มีความเสี่ยงสูง เช่น ระบบอัตโนมัติทางทหารหรือระบบควบคุมในภารกิจที่ต้องการความปลอดภัยสูง

MIL-STD-1397C [7] เป็นมาตรฐานที่กำหนดรูปแบบและโปรโตคอลสำหรับการสื่อสารทางดิจิทัลระหว่างระบบต่าง ๆ ภายในบริบททางทหาร โดยเฉพาะการเชื่อมต่อผ่านอินเตอร์เฟซของอุปกรณ์จากผู้ผลิตหลากหลาย เพื่อให้มั่นใจว่าสามารถแลกเปลี่ยนข้อมูลแบบเรียลไทม์ได้อย่างมีประสิทธิภาพและเชื่อถือได้ MSQA ได้นำแนวคิดจากมาตรฐานนี้มาใช้เพื่อสนับสนุนการประเมินด้าน ความสามารถในการทำงานร่วมกัน (Interoperability) และ การบูรณาการระบบ (System Integration) โดยเน้นให้ซอฟต์แวร์สามารถสื่อสารและทำงานร่วมกับฮาร์ดแวร์หรือระบบอื่นได้แม้จะไม่ได้ควบคุมการออกแบบอินเตอร์เฟซโดยตรง ทั้งนี้เพื่อให้ระบบมีความยืดหยุ่นและสามารถปรับใช้ในบริบทภาคสนามที่หลากหลาย

MIL-STD-810 [8] เป็นมาตรฐานที่ครอบคลุมการทดสอบภายใต้สภาพแวดล้อมที่รุนแรง เช่น อุณหภูมิ ความชื้น ฝุ่น การกระแทก และการสั่นสะเทือน การนำแนวทางนี้มาใช้ช่วยให้การประเมินด้านความทนทาน (Durability) ความน่าเชื่อถือ (Reliability) และความสอดคล้องกับภาคสนาม (Operational Compliance) ของระบบมีความสมจริงยิ่งขึ้น โดยมีตัวอย่างการประยุกต์ ได้แก่ การทดสอบอุณหภูมิ (Temperature Test) สำหรับการใช้งานในสภาพอากาศร้อนจัดหรือเย็นจัด การทดสอบแรงกระแทก (Shock Test) โดยจำลองแรงระเบิดหรือการตกหล่นของอุปกรณ์ และการทดสอบการสั่นสะเทือน (Vibration Test) ที่ประเมินประสิทธิภาพขณะติดตั้งบนพาหนะทางทหาร

MIL-STD-461 [9] เป็นมาตรฐานที่เกี่ยวข้องกับการควบคุมการรบกวนทางแม่เหล็กไฟฟ้า (EMI) และความเข้ากันได้ทางแม่เหล็กไฟฟ้า (EMC) MSQA นำมาประยุกต์ใช้ในมิติด้านความปลอดภัย (Security) ความสามารถในการทำงานร่วมกัน (Compatibility) และความน่าเชื่อถือ (Reliability) โดยมีตัวอย่างการประยุกต์ ได้แก่ การทดสอบการแผ่คลื่นแม่เหล็กไฟฟ้า (Radiated Emissions) และการทดสอบภูมิคุ้มกันต่อคลื่นรบกวน (Radiated Susceptibility)

ISO/IEC 12207 [10] เป็นมาตรฐานสากลที่กำหนดกรอบกระบวนการวงจรชีวิตของซอฟต์แวร์ (Software Life Cycle Process Framework) โดยครอบคลุมตั้งแต่กระบวนการเริ่มต้น เช่น การกำหนดความต้องการ (Requirement Definition) การวางแผน (Planning) การออกแบบและพัฒนา (Design and Implementation) ไปจนถึงกระบวนการบำรุงรักษา (Maintenance) การติดตั้ง (Deployment) และการยุติระบบ (Retirement)

MSQA ได้นำโครงสร้างและแนวทางจาก ISO/IEC 12207 มาใช้ในการจัดหมวดหมู่และตรวจสอบคุณภาพในแต่ละช่วงของการพัฒนา โดยเฉพาะในมิติของความสามารถในการบำรุงรักษา (Maintainability) และความสามารถในการจัดการกระบวนการ (Process Maturity) ซึ่งช่วยให้สามารถประเมินว่าโครงการมีการวางโครงสร้างที่เป็นระบบหรือไม่ มีการควบคุมการเปลี่ยนแปลง และสามารถปรับปรุงหรือแก้ไขซอฟต์แวร์ได้ในระยะยาวหรือไม่

ISO/IEC 15504 [11] หรือที่เรียกว่า Software Process Improvement and Capability Determina- tion (SPICE) เป็นมาตรฐานที่เน้นการวัดระดับความสามารถของกระบวนการ (Process Capability Level) และให้กรอบสำหรับการปรับปรุงกระบวนการ พัฒนาซอฟต์แวร์อย่างต่อเนื่อง โดยมาตรฐานนี้มีการแบ่งระดับความสามารถของกระบวนการออกเป็น 6 ระดับ ตั้งแต่ “Incomplete Process” จนถึง “Opti- mizing Process” ซึ่งช่วยให้สามารถประเมินว่ากระบวนการพัฒนามีความเป็นระบบและมีการควบคุมที่ดีเพียงใด ดังนั้น MSQA ได้นำแนวคิดนี้มาใช้เสริมในมิติด้าน ประสิทธิภาพ (Performance Efficiency) และ ความทนทาน (Durability) เพื่อให้การประเมินไม่ได้จำกัดเฉพาะตัวซอฟต์แวร์เท่านั้น แต่รวมถึงกระบวนการที่สร้างซอฟต์แวร์นั้นด้วย เช่น การจัดการทรัพยากร การวิเคราะห์ข้อผิดพลาด และการปรับปรุงกระบวนการอย่างต่อเนื่อง

ISO/IEC 27001 [12] เป็นมาตรฐานด้านการจัดการความปลอดภัยของข้อมูล (Information Security Management Systems – ISMS) ที่ได้รับการยอมรับอย่างกว้างขวางในระดับองค์กรและโครงการขนาดใหญ่ มาตรฐานนี้กำหนดข้อกำหนดที่เกี่ยวข้องกับการป้องกันข้อมูล ได้แก่ ความลับ (Confidentiality) หมายถึง ข้อมูลไม่สามารถเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ความสมบูรณ์ (Integrity) หมายถึง ข้อมูลถูกต้อง ไม่สามารถดัดแปลง และความพร้อมใช้งาน (Availability) หมายถึง ข้อมูลสามารถเข้าถึงได้เมื่อต้องการ ดังนั้น MSQA ได้นำแนวทางจาก ISO/IEC 27001 มาเสริมในระบบที่เกี่ยวข้องกับการจัดเก็บและส่งข้อมูลในสภาพแวดล้อมทางทหาร เช่น การจัดการข้อมูลภารกิจหรือข้อมูลอาวุธ โดยเน้นการป้องกันข้อมูลสำคัญทั้งในเชิงเทคนิค (Technical Controls) และเชิงองค์กร (Organiza- tional Controls)

ISO/IEC 29110 [13] เป็นมาตรฐานที่ออกแบบมาโดยเฉพาะสำหรับ องค์กรขนาดเล็ก (Very Small Entities - VSEs) ซึ่งมีบุคลากรไม่เกิน 25 คน และมีข้อจำกัดด้านทรัพยากร มาตรฐานนี้ให้แนวทางในการวางแผน พัฒนา และประเมินซอฟต์แวร์ในลักษณะที่เรียบง่ายแต่มีประสิทธิภาพ โดยไม่จำเป็นต้องใช้เครื่องมือหรือเอกสารที่ซับซ้อน แม้ว่า MSQA ได้ออกแบบให้ใช้ในระบบขนาดใหญ่ แต่หลักการบางประการจาก ISO/IEC 29110 เช่น การปรับกระบวนการให้เหมาะสมกับทรัพยากรที่มี (Tailoring) และการติดตามคุณภาพในระดับโครงการขนาดเล็กสามารถนำมาประยุกต์ใช้ในบริบทของระบบย่อย หรือโครงการเฉพาะกิจที่มีข้อจำกัดด้านกำลังคนและงบประมาณ เพื่อรักษามาตรฐานคุณภาพในระดับที่เหมาะสม

4. วิธีดำเนินการศึกษา

4.1 หลักการและแนวคิดในการพัฒนา MSQA

การพัฒนา Military Software Quality Assessment (MSQA) มีจุดมุ่งหมายเพื่อสร้างกรอบการประเมินคุณภาพซอฟต์แวร์ที่ตอบสนองต่อบริบทการใช้งานในระบบทางทหาร ซึ่งมีความซับซ้อนสูง ต้องการความน่าเชื่อถือ และความทนทานต่อสภาพแวดล้อมที่หลากหลาย โดยมีหลักการสำคัญที่ใช้ในการออกแบบ MSQA ได้แก่

1) การอ้างอิงตามมาตรฐานสากล โดยใช้ ISO/IEC 25010 เป็นโครงสร้างหลักในการนิยามมิติด้านคุณภาพ (Quality Dimensions) และผนวกกับมาตรฐานอื่นที่เกี่ยวข้อง เช่น MIL-STD-810 MIL-STD-882 ISO/IEC12207 และ ISO/IEC 15504 เพื่อให้การประเมินครอบคลุมทั้งมิติด้าน

ซอฟต์แวร์ และความเหมาะสมทางยุทธวิธี

2) การออกแบบที่เหมาะสมกับบริบททางทหาร MSQA ได้ออกแบบให้มีความยืดหยุ่นในการใช้งานกับโครงการต่าง ๆ ในภาครัฐหรือกองทัพ โดยเน้นประเด็นด้านความปลอดภัย (Safety) ความน่าเชื่อถือ (Reliability) การบำรุงรักษา (Maintainability) และการทำงานร่วมกับระบบเดิม (Legacy Integration) ซึ่งเป็นข้อกำหนดสำคัญในระบบปฏิบัติการของกองทัพ

3) การประเมินตามลักษณะงานจริง: MSQA ไม่ได้จำกัดเฉพาะการประเมินเชิงเทคนิคในซอฟต์แวร์เท่านั้น แต่รวมถึงปัจจัยด้านกระบวนการพัฒนา (Process Maturity) ความสอดคล้องตามมาตรฐาน (Compliance) และความสามารถในการดำเนินงานภายใต้ข้อจำกัดเชิงทรัพยากรและโครงสร้าง

4) การมีส่วนร่วมจากหลายฝ่าย (Stakeholder-Driven Design): กระบวนการพัฒนา MSQA ขับเคลื่อนโดยการระดมความคิดเห็นจากผู้มีส่วนได้ส่วนเสียหลายฝ่าย ไม่ว่าจะเป็นนักพัฒนาระบบ ผู้ใช้งานจริงในภาคสนาม และหน่วยงานบริหาร เพื่อให้แน่ใจว่าเกณฑ์การประเมินมีความครอบคลุม และตอบโจทย์การปฏิบัติงานจริง

หลักการและแนวคิดเหล่านี้ช่วยให้ MSQA เป็นกรอบการประเมินที่มีความชัดเจน รองรับการนำไปประยุกต์ใช้ได้ในโครงการต่าง ๆ และส่งเสริมให้เกิดมาตรฐานกลางในการประเมินคุณภาพซอฟต์แวร์สำหรับภาคความมั่นคงและระบบสำคัญอื่น ๆ

4.2 ขั้นตอนการพัฒนา MSQA

การพัฒนา MSQA เกิดขึ้นผ่านกระบวนการ อภิปรายและระดมความคิดร่วมกับผู้เกี่ยวข้องและผู้มีส่วนได้ส่วนเสีย ที่เกี่ยวข้องในภาคสนาม ทั้งนักพัฒนา ผู้ใช้งานจริง และผู้บริหาร เพื่อให้มั่นใจว่าเกณฑ์การประเมินที่กำหนดขึ้นมีความครอบคลุม ตรงตามความต้องการ และเหมาะสมกับบริบททางทหารอย่างแท้จริง

ในกระบวนการนี้ ยังได้นำระบบจริงที่มีอยู่ คือ ระบบ ASD มาใช้เป็นกรณีศึกษา เพื่อทดลองและปรับใช้ MSQA โดยการวัดและประเมินประสิทธิภาพและคุณภาพของระบบเหล่านี้ตามมิติที่กำหนดไว้ ซึ่งช่วยให้ทีมพัฒนาเห็นภาพชัดเจนถึงข้อจำกัด ปัญหา และโอกาสในการปรับปรุงมาตรฐานประเมิน

ด้วยวิธีการนี้ MSQA จึงได้รับการออกแบบให้สามารถตอบสนองความต้องการใช้งานจริง และพร้อมนำไปใช้ในระบบทางทหารอื่นๆ ได้อย่างมีประสิทธิภาพ

4.3 มิติการประเมินในกรอบ MSQA และหลักการเชิงแนวคิด

มาตรฐาน ISO/IEC 25010 กำหนดไว้ทั้งหมด 9 มิติในการประเมินคุณภาพซอฟต์แวร์ ขณะที่กรอบการประเมิน MSQA ได้นำเสนอ 7 มิติ (รายละเอียดจะมีการขยายความในบท 4.4) โดยไม่ได้เป็นการตัดทอนมิติโดยตรง แต่เป็นการจัดกลุ่มและรวมมิติที่มีความเกี่ยวข้องกันใน ISO/IEC 25010 เข้ากับข้อกำหนดจากมาตรฐานอื่น ๆ เพื่อให้ได้มิติที่กระชับ เหมาะสมกับบริบทของงานด้านการทหาร และช่วยให้กระบวนการประเมินมีความชัดเจนและปฏิบัติได้ง่ายขึ้น ความเชื่อมโยงระหว่างมิติใน MSQA กับ ISO/IEC 25010 และมาตรฐานที่เกี่ยวข้อง อ้างอิงตามตารางที่ 1

MSQA ออกแบบมาเพื่อให้กระบวนการประเมินเป็นระบบ มีความยืดหยุ่น และตรงกับข้อกำหนดเฉพาะของระบบทางทหาร โดยมีเหตุผลหลักของการออกแบบดังนี้

1) ความสามารถในการประเมินแบบแยกส่วนอย่างเป็นระบบ หมายถึง MSQA ออกแบบให้แต่ละมิติมีความเป็นอิสระในการประเมิน ช่วยให้สามารถดำเนินการประเมินแต่ละด้านแยกจากกันได้ตามบริบท เช่น การทดสอบประสิทธิภาพสามารถใช้เครื่องมือเชิงเทคนิคโดยไม่ต้องมีผู้ใช้เข้าร่วม ขณะที่การประเมิน User Interface ต้องอาศัยการทดลองใช้งานจริงกับผู้ปฏิบัติงาน การแยกมิติเช่นนี้ทำให้สามารถใช้ทรัพยากรได้อย่างเหมาะสม ควบคุมกระบวนการทดสอบได้ง่าย และลดความซับซ้อนในการจัดการทดสอบที่ต้องการความแม่นยำสูงภายใต้ข้อจำกัดด้านเวลาและทรัพยากรของภาคการทหาร

ตารางที่ 1 มิติการประเมินของ MSQA และความเกี่ยวพันธ์กับ ISO/IEC25010 และมาตรฐานอื่นๆ

มิติการประเมิน	มิติจาก ISO/IEC 25010	ความสัมพันธ์กับมาตรฐานอื่น
ประสิทธิภาพ (Performance)	- ประสิทธิภาพของระบบ (Performance Efficiency) ความน่าเชื่อถือ (Reliability) - รวมทั้งสองมิติ เนื่องจากในระบบทหาร ความน่าเชื่อถือถือเป็นส่วนหนึ่งของความสามารถในการทำงานอย่างมีประสิทธิภาพ	**MIL-STD-498** (การตรวจสอบสมรรถนะของซอฟต์แวร์) **ISO/IEC 12207** (การบริหารวงจรชีวิตซอฟต์แวร์), **ISO/IEC 15504 (SPICE)** (การปรับปรุงประสิทธิภาพกระบวนการซอฟต์แวร์)
ส่วนติดต่อผู้ใช้ (User Interface)	-ความสามารถในการโต้ตอบ (Interaction Capability) ความเหมาะสมของฟังก์ชัน (Functional Suitability) -เน้นให้ส่วนติดต่อผู้ใช้ตอบสนองความต้องการของผู้ใช้งานอย่างครบถ้วน ถูกต้อง และเหมาะสม รวมถึงง่ายต่อการเรียนรู้และฝึกใช้งาน	ISO/IEC 12207 (การออกแบบซอฟต์แวร์ที่ใช้งานง่าย) MIL-STD-498 (ข้อกำหนดด้านเอกสารและปัจจัยมนุษย์)
การทำงานร่วมกัน (Integration)	-ความเข้ากันได้ (Compatibility) ความเหมาะสมของฟังก์ชัน (Functional Suitability) -เน้นความเข้ากันได้และความเหมาะสมของฟังก์ชัน เพื่อให้ระบบทำงานร่วมกับส่วนอื่นได้อย่างมีประสิทธิภาพ	MIL-STD-1397C (โปรโตคอลการสื่อสารดิจิทัลของกองทัพ) ISO/IEC 12207 (การบริหารจัดการการรวมระบบซอฟต์แวร์) MIL-STD-461 (สามารถทำงานร่วมกับระบบที่มีข้อกำหนดด้าน EMI/EMC ได้อย่างเหมาะสม เช่น ซอฟต์แวร์ที่ควบคุมระบบเรดาร์หรือระบบสื่อสารที่ต้องทำงานในสภาพแวดล้อมที่มีสัญญาณรบกวนสูง)
ความทนทาน (Durability)	-ความน่าเชื่อถือ (Reliability) การบำรุงรักษา (Maintainability) ระบบต้องทำงานได้อย่างถูกต้องและเสถียรในระยะเวลานาน โดยลดโอกาสเกิดข้อผิดพลาดหรือความล้มเหลว และต้องง่ายต่อการบำรุงรักษาเพื่อรักษาประสิทธิภาพและความพร้อมใช้งานอย่างต่อเนื่อง	MIL-STD-882 (มาตรฐานการวิเคราะห์อันตรายและความปลอดภัยของระบบ) ISO/IEC 15504 (SPICE) (มาตรฐานด้านความน่าเชื่อถือของซอฟต์แวร์) MIL-STD-810 (ในบริบทของซอฟต์แวร์ที่ต้องทำงานร่วมกับระบบที่อาจได้รับผลกระทบจากสภาวะแวดล้อม เช่น ระบบในอากาศยานไร้คนขับ (UAV) หรืออุปกรณ์ภาคสนามที่ต้องเผชิญกับอุณหภูมิสุดขั้วและแรงสั่นสะเทือน)
การปฏิบัติตามข้อกำหนด (Compliance)	-ความปลอดภัย (Security) ความปลอดภัยของระบบ (Safety) ความเหมาะสมของฟังก์ชัน (Functional Suitability) -ระบบต้องมีมาตรการป้องกันข้อมูลและการใช้งานที่ผิดพลาด เพื่อป้องกันอันตรายต่อผู้ใช้หรือภารกิจ	ISO/IEC 27001 (มาตรฐานการบริหารความปลอดภัยของข้อมูล) MIL-STD-882 (มาตรฐานความปลอดภัยของระบบในงานทางทหาร)
การติดตั้งและใช้งาน (Deployment)	-ความเข้ากันได้ (Compatibility) ความยืดหยุ่น (Flexibility) -ระบบต้องสามารถติดตั้งและใช้งานได้ง่ายในสภาพแวดล้อมที่หลากหลาย โดยไม่กระทบระบบเดิม และปรับตัวได้ตามข้อจำกัดของพื้นที่หรือภารกิจ	ISO/IEC 12207 (กระบวนการติดตั้งซอฟต์แวร์), MIL-STD-498 (ข้อกำหนดการติดตั้งและตรวจสอบซอฟต์แวร์ในงานทางทหาร)
การบำรุงรักษา (Maintenance)	-การบำรุงรักษา (Maintainability) ความยืดหยุ่น (Flexibility) -ระบบควรตรวจสอบ แก้ไข และอัปเดตได้ง่าย เพื่อรองรับการใช้งานระยะยาว และปรับให้เหมาะกับภารกิจที่เปลี่ยนแปลงได้	ISO/IEC 12207 (การบริหารการบำรุงรักษาซอฟต์แวร์) MIL-STD-498 (การวางแผนและจัดการบำรุงรักษาซอฟต์แวร์เชิงโครงสร้าง) ISO/IEC 15504 (SPICE) (แนวทางการปรับปรุงซอฟต์แวร์อย่างต่อเนื่อง)

2) การลดความซ้ำซ้อนของมิติการประเมิน และการส่งเสริมความกระชับของเกณฑ์ หมายถึง MSQA ได้รวมมิติที่เกี่ยวข้องช่วยลดความซับซ้อนในการประเมิน ทำให้ผู้ประเมินสามารถมุ่งเน้นกับประเด็นสำคัญและตัดสินใจได้รวดเร็วขึ้น ซึ่งเหมาะสมกับบริบทที่ต้องการความแม่นยำและเร็วในสถานการณ์ทางทหาร

3) ความสอดคล้องกับบริบทเฉพาะของระบบงานด้านความมั่นคง หมายถึง กรอบการประเมิน MSQA ได้รับการออกแบบให้สะท้อนความต้องการและข้อจำกัดเฉพาะของระบบที่ใช้ในภารกิจด้านความมั่นคง ซึ่งมีลักษณะเฉพาะ

แตกต่างจากระบบพลเรือนทั่วไป โดยระบบทหารจำเป็นต้องมีความน่าเชื่อถือสูง)High Reliability) และความปลอดภัยเชิงข้อมูลและการปฏิบัติขั้นสูง)High-level Security)

4) การเพิ่มมิติการประเมินที่สะท้อนบริบทภาคสนาม หมายถึง MSQA เพิ่มมิติ Deployment ซึ่งไม่รวมอยู่ใน ISO/IEC 25010 แต่ MSQA เพิ่มเข้ามาเพื่อสะท้อนความสำคัญของการติดตั้งและใช้งานในภาคสนามที่มีข้อจำกัดด้านเวลาและทรัพยากร เช่น การติดตั้งระบบในสถานที่ที่ยากลำบาก หรือภายใต้สภาวะวิกฤต

5) การเน้นการใช้งานจริงผ่านมิติของส่วนติดต่อผู้ใช้ หมายถึง ในบริบทของระบบงานด้านความมั่นคง ส่วนติดต่อผู้ใช้ ถือเป็นปัจจัยสำคัญต่อประสิทธิภาพของระบบ เนื่องจากผู้ใช้งานจำนวนมากมิได้มีพื้นฐานด้านเทคโนโลยีสารสนเทศโดยตรง จึงจำเป็นที่ระบบจะต้องออกแบบให้มีความง่ายในการเรียนรู้ และสามารถฝึกใช้งานได้อย่างรวดเร็ว ช่วยลดความเสี่ยงจากข้อผิดพลาด และเพิ่มความมั่นใจในการปฏิบัติงานของผู้ใช้ในสถานการณ์จริง ส่งผลโดยตรงต่อประสิทธิภาพและความปลอดภัยของภารกิจ

กล่าวโดยสรุป การรวมและปรับแต่งมิติของ MSQA ช่วยให้กรอบประเมินนี้มีความเหมาะสมกับลักษณะเฉพาะของซอฟต์แวร์ทางทหาร และทำให้การประเมินเป็นไปอย่างมีประสิทธิภาพและครอบคลุมมากขึ้นในบริบทที่ต้องการความแม่นยำและรวดเร็ว

5. ผลการศึกษา

5.1 กรณีศึกษา

โครงการพัฒนาระบบซอฟแวร์สำหรับการถอดรหัสและแสดงผลข้อมูลเรดาร์ (ASD) ดำเนินการระหว่างปี พ.ศ. 2565 ถึง 2568 เพื่อปรับปรุงส่วนแสดงผลของระบบเรดาร์ให้มีความทันสมัย

โดยมีการเสนอกรอบ MSQA ควบคู่ไปด้วย เพื่อใช้ในการกำกับ ติดตาม และประเมินคุณภาพระบบตลอดวงจรชีวิตของโครงการ และรายละเอียดของการวิจัยพัฒนาระบบ ASD มีดังนี้

ระบบเรดาร์แบบเก่าจำนวนมากประสบปัญหาด้านการบำรุงรักษา เนื่องจากเทคโนโลยีล้าสมัย ขาดแคลนอะไหล่ และมีข้อจำกัดในด้านประสิทธิภาพ โครงการนี้จึงได้รับการพัฒนาขึ้นเพื่อทดแทนส่วนประมวลผลของระบบเรดาร์เดิม โดยออกแบบให้ระบบ ASD แบบใหม่สามารถประมวลผลข้อมูลเรดาร์ได้แบบเรียลไทม์ มีความแม่นยำ ใช้งานง่าย และรองรับการจัดการข้อมูลแผนที่ เพื่อเพิ่มประสิทธิภาพในการรับรู้สถานการณ์ทางอากาศ

เป้าหมายของโครงการคือการพัฒนาระบบ ASD ที่ทันสมัย ใช้งานง่าย และดูแลรักษาง่าย เพื่อทดแทนระบบ ASD รุ่นเก่าในระบบเรดาร์ โดยยังคงสามารถทำงานร่วมกับอุปกรณ์เดิม เช่น เสาอากาศ การพัฒนาระบบดำเนินการภายใต้มาตรฐานทางทหาร และใช้กรอบการประเมินคุณภาพซอฟต์แวร์สมัยใหม่

การประเมินในโครงการนี้มุ่งเน้นเฉพาะส่วนของชุดซอฟต์แวร์ที่ทำหน้าที่ประมวลผลและแสดงผลข้อมูล โดยไม่ครอบคลุมถึงส่วนของฮาร์ดแวร์อื่น ๆ ของระบบเรดาร์ เช่น เสาอากาศ รวมถึงเครือข่ายและระบบการสื่อสาร เนื่องจากระบบใช้โครงสร้างพื้นฐานเครือข่ายอินเทอร์เน็ตที่มีอยู่แล้วในการรับส่งข้อมูล

5.2 การนำไปใช้กับกรณีศึกษา

ในส่วนนี้จะอธิบายรายละเอียดของแต่ละมิติจากกรอบ MSQA ทั้ง 7 ด้าน พร้อมยกตัวอย่างจากกรณีศึกษาการพัฒนาระบบ ASD ซึ่งออกแบบมาโดยมีแนวคิดสำคัญคือ การแยกมิติการประเมินออกจากกันอย่างชัดเจน เพื่อให้สามารถทดสอบและตรวจสอบได้อย่างเป็นอิสระภายใต้บริบทที่แตกต่างกัน

5.2.1 ประสิทธิภาพ (Performance)

คำอธิบายแนวคิด:ประสิทธิภาพในที่นี้หมายถึงความสามารถของระบบในการตอบสนองต่อคำสั่งหรือเหตุการณ์อย่างรวดเร็วแม้ภายใต้ภาระงานที่สูง โดยรวมถึงประสิทธิภาพของการประมวลผลข้อมูล ความเร็วในการแสดงผล การจัดสรรทรัพยากร และความเสถียรของระบบ

วัตถุประสงค์: เพื่อให้มั่นใจว่าระบบสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพภายใต้ข้อจำกัดของเวลา ทรัพยากร และปริมาณข้อมูลที่มาก

บริบทการประเมิน: เน้นการประเมินในเชิงเทคนิค โดยผู้พัฒนาหรือผู้ทดสอบซอฟต์แวร์ โดยใช้การจำลองสถานการณ์ และวิเคราะห์การใช้ทรัพยากรระบบเพื่อวัดความสามารถในการตอบสนองและความเสถียรของระบบ

แนวทางการประเมิน: ทดสอบการประมวลผลข้อมูลแบบเรียลไทม์ภายใต้ภาระงานต่างๆ วิเคราะห์ความเร็วในการโหลดข้อมูลและแสดงผล ตรวจสอบอัตราการใช้ CPU หน่วยความจำ และทรัพยากรอื่นๆ สุดท้ายเปรียบเทียบกับ baseline หรือระบบเดิมที่ใช้งานอยู่

กรณีศึกษาระบบ ASD: การทดสอบภายใต้สถานการณ์ที่มีอากาศยานมากกว่า 200 ลำ ระบบสามารถแสดงผลได้แบบเรียลไทม์ โดยไม่มีอาการหน่วงหรือค้าง นอกจากนี้ ยังได้ดำเนินการทดสอบในรูปแบบต่างๆ ได้แก่

1) Load Test: จำลองการรับข้อมูลจำนวนมากต่อวินาที ระบบยังสามารถรักษาระยะเวลาแสดงผลเฉลี่ยไว้ที่ <200ms
2) Stress Test: เปิดระบบทำงานต่อเนื่อง 72 ชั่วโมงโดยไม่พบอาการล่มหรือ degrade
3) Latency Test: วัดเวลาตอบสนองเมื่อผู้ใช้สั่งงาน พบว่าเวลาเฉลี่ยอยู่ในช่วงที่ยอมรับได้
4) Field User Test: ผู้ใช้งานภาคสนามสามารถปฏิบัติงานตามภารกิจได้สำเร็จในเวลาที่เหมาะสม โดยไม่มีการเรียนรู้ซ้ำ และมีอัตราข้อผิดพลาดต่ำ

ผลจากการทดสอบเหล่านี้สะท้อนว่าระบบสามารถรักษาประสิทธิภาพได้แม้ภายใต้ภาระงานสูง และเหมาะสมกับการใช้งานจริงในสภาพแวดล้อมทางทหารที่มีข้อจำกัดด้านเวลาและความเสถียรของข้อมูล

5.2.2 ส่วนติดต่อผู้ใช้ (User Interface)

คำอธิบายแนวคิด: ส่วนติดต่อผู้ใช้ที่ดีควรมีความชัดเจน ใช้งานง่าย สื่อความหมายตรงไปตรงมา โดยเฉพาะในระบบทหารที่ผู้ใช้มีเวลาเรียนรู้ระบบจำกัด การออกแบบ UI ที่ดีต้องคำนึงถึงการเรียนรู้ที่รวดเร็ว ความถูกต้อง และลดความผิดพลาดจากมนุษย์

วัตถุประสงค์: เพื่อให้ผู้ใช้งานสามารถเข้าใจและใช้งานระบบได้อย่างมีประสิทธิภาพโดยไม่ต้องพึ่งพาผู้เชี่ยวชาญเฉพาะทาง

บริบทการประเมิน: เน้นการประเมินจากผู้ใช้งานจริง โดยใช้การสังเกต การเก็บข้อมูลเชิงพฤติกรรม และแบบสอบถาม เพื่อประเมินความง่ายในการเรียนรู้ ความเข้าใจในการใช้งาน และความพึงพอใจโดยรวม

แนวทางการประเมิน: การทดสอบกับผู้ใช้จริง (user testing) ประเมินเวลาที่ใช้ในการเรียนรู้และใช้งาน วิเคราะห์ความถูกต้องในการใช้งานของผู้ปฏิบัติงาน และตรวจสอบความสม่ำเสมอของการออกแบบ UI

กรณีศึกษาระบบ ASD: อินเทอร์เฟซออกแบบให้ใช้งานได้ง่าย แม้เจ้าหน้าที่ที่ไม่มีความเชี่ยวชาญด้านเทคนิค โดยใช้สีที่มีความหมายและสอดคล้องยุทธวิธี ไอคอนที่สื่อความหมายและเป็นมาตรฐาน และฟอนต์ที่มีขนาดเหมาะสม ในการทดสอบกับผู้ใช้งานจริง ได้ใช้แบบสอบถาม User Experience Questionnaire (UEQ) และการสังเกตพฤติกรรมผู้ใช้ร่วมด้วย พบว่าผู้ใช้งานสามารถเรียนรู้ระบบได้ภายในเวลาอันสั้น)<2 ชั่วโมง(มีอัตราความผิดพลาดต่ำ และสามารถใช้งานต่อเนื่องโดยไม่ต้องพึ่งผู้เชี่ยวชาญ ส่งผลให้ UI ได้รับคะแนนความพึงพอใจสูงทั้งด้านความชัดเจน ความง่ายในการใช้งาน และความน่าเชื่อถือ

5.2.3 การบูรณาการ (Integration)

คำอธิบายแนวคิด: ระบบที่ดีต้องสามารถเชื่อมต่อและทำงานร่วมกับระบบอื่นๆ ที่มีอยู่เดิม เช่น เซนเซอร์ภายนอก ฐานข้อมูล หรือระบบควบคุมอื่น โดยไม่ต้องมีการแก้ไขโค้ดมาก

วัตถุประสงค์: เพื่อให้ระบบสามารถผสานการทำงานกับโครงสร้างพื้นฐานที่มีอยู่แล้ว และลดความยุ่งยากในการติดตั้งหรือแก้ไข

บริบทการประเมิน: เน้นการประเมินโดยผู้พัฒนาร่วมกับตัวแทนจากระบบอื่น โดยการเชื่อมต่อกับระบบภายนอกหรือระบบเดิม วิเคราะห์การไหลของข้อมูล ความถูกต้อง และความเร็วในการสื่อสาร เพื่อยืนยันความสามารถในการทำงานร่วมกัน (interoperability)

แนวทางการประเมิน: การทดสอบเชื่อมต่อกับระบบภายนอก (เช่น เซนเซอร์ ระบบสื่อสาร) วิเคราะห์ความถูกต้องและความเร็วของการแลกเปลี่ยนข้อมูล และตรวจสอบความสามารถในการใช้งานโปรโตคอลมาตรฐาน

กรณีศึกษาระบบ ASD: ASD สามารถเชื่อมต่อกับเสาอากาศและฐานข้อมูลของระบบเดิมผ่านโปรโตคอล ASTERIX โดยไม่ต้องปรับแต่งซอฟต์แวร์เดิม พร้อมแสดงข้อมูลแบบ real-time บนระบบใหม่

นอกจากนี้ ได้ดำเนินการทดสอบการรวมระบบอย่างละเอียดเพื่อประเมินความสามารถในการทำงานร่วมกับระบบเรดาร์ที่มีอยู่จริง โดยครอบคลุมการทดสอบดังนี้

1) การทดสอบความสามารถในการทำงานร่วมกัน (Interoperability Testing): ตรวจสอบว่า ASD สามารถโต้ตอบและรับส่งข้อมูลกับระบบเรดาร์รุ่นเก่าและรุ่นใหม่ได้อย่างราบรื่น
2) การทดสอบการไหลของข้อมูล (Data Flow Testing): จำลองสถานการณ์ข้อมูลเรดาร์ที่หลากหลาย เพื่อตรวจสอบว่า ASD สามารถประมวลผลและแสดงผลข้อมูลได้แบบเรียลไทม์และถูกต้อง
3) การทดสอบการจัดการข้อผิดพลาด (Error Handling Testing): ตรวจสอบว่าระบบสามารถจัดการกับข้อผิดพลาดในการรับ-ส่งข้อมูล เช่น การตัดการเชื่อมต่อ หรือข้อมูลผิดพลาด ได้อย่างเหมาะสมโดยไม่กระทบต่อการปฏิบัติงานหรือทำให้ระบบล่ม

ขั้นตอนการทดสอบเหล่านี้ช่วยยืนยันว่าสามารถรวมระบบเข้ากับโครงสร้างพื้นฐานระบบเรดาร์เดิมได้อย่างมีประสิทธิภาพและเสถียรภาพตามวัตถุประสงค์ของการบูรณาการ

5.2.4 ความทนทาน (Durability)

คำอธิบายแนวคิด: ระบบควรทำงานได้ต่อเนื่องแม้ในสภาวะที่ไม่ปกติ เช่น การเชื่อมต่อขาด โหลดสูง หรือฮาร์ดแวร์มีปัญหา และควรรองรับการซ่อมบำรุงและการอัปเดตได้ง่าย

วัตถุประสงค์: เพื่อให้ระบบสามารถใช้งานในภาคสนามได้อย่างต่อเนื่องและปลอดภัย

บริบทการประเมิน: การประเมินในมิตินี้จำเป็นต้องดำเนินร่วมกับผู้ใช้งานที่มีประสบการณ์ในภาคสนาม เพื่อช่วยระบุเหตุการณ์ผิดปกติหรือสภาพแวดล้อมที่อาจเกิดขึ้นจริง ซึ่งผู้พัฒนาอาจไม่สามารถคาดการณ์ได้ล่วงหน้า ตัวอย่างเช่น การใช้งานในสภาพอากาศที่ร้อนจัดหรือชื้นสูงผิดปกติ การปฏิบัติงานภายใต้การสื่อสารที่มีสัญญาณรบกวน หรือเหตุการณ์ที่ระบบต้องกู้คืนหลังจากเกิดความล้มเหลวเฉียบพลัน มิตินี้จึงมุ่งเน้นการจำลองสถานการณ์วิกฤต การทดสอบความต่อเนื่องของระบบ และการประเมินความสามารถในการฟื้นตัว เพื่อให้มั่นใจว่าระบบสามารถปฏิบัติงานได้อย่างต่อเนื่องและเชื่อถือได้ภายใต้ข้อจำกัดของสภาพแวดล้อมทางทหาร

แนวทางการประเมิน: ทดสอบภายใต้สถานการณ์ผิดปกติ เช่น ตัดไฟ ความล่าช้าในการสื่อสาร ตรวจสอบการทำงานของระบบสำรอง ตรวจสอบความสามารถในการฟื้นฟูอัตโนมัติเมื่อเกิดปัญหา

กรณีศึกษาระบบ ASD: การออกแบบโดยคำนึงถึงความทนทานต่อสภาวะผิดปกติและข้อจำกัดในภาคสนาม โดยมีการดำเนินการทดสอบในสถานการณ์จำลองที่หลากหลายเพื่อประเมินความสามารถในการทำงานอย่างต่อเนื่อง ดังนี้

1) ระบบติดตั้งกลไกตรวจจับความผิดปกติที่สามารถรีสตาร์ทบริการอัตโนมัติเมื่อพบการเชื่อมต่อขัดข้องหรือบริการล่ม ลดการพึ่งพาการ

แทรกแซงจากผู้ใช้

2) ระบบเปิดใช้งานอย่างต่อเนื่องนานกว่า 72 ชั่วโมงในโหมดทำงานจริง เพื่อประเมินความเสถียร พบว่าไม่มีเหตุขัดข้องหรือ downtime ที่กระทบภารกิจ
3) ระบบสามารถทนต่อจำลองสถานการณ์ เช่น ตัดไฟ เครือข่ายล่ม หรืออุปกรณ์บางส่วนล้มเหลว และตรวจสอบว่าระบบสามารถฟื้นฟูการทำงานภายในเวลาไม่เกิน 2 นาทีโดยไม่สูญเสียข้อมูลสำคัญ
4) การทดสอบการทำงานของอุปกรณ์ในสภาพแวดล้อมรุนแรง เช่น อุณหภูมิสูง ความชื้นเกินมาตรฐาน และแรงสั่นสะเทือน พบว่าส่วนประกอบหลักทำงานได้ตามปกติ และสามารถเปลี่ยนอะไหล่สำคัญ (CPU ทั้งเครื่อง หน้าจอ เมาส์ หรือ คีย์บอร์ด) ได้ในเวลาไม่เกิน 5 นาทีโดยไม่ต้องอาศัยทีมซ่อมบำรุง

จากผลการทดสอบข้างต้น แสดงให้เห็นว่า ระบบ ASD สามารถทำงานได้อย่างต่อเนื่อง มีความสามารถในการฟื้นตัวจากความล้มเหลว และรองรับการบำรุงรักษาในบริบทการใช้งานจริงได้อย่างมีประสิทธิภาพตามเป้าหมายด้านความทนทานที่กำหนดไว้ใน MSQA

5.2.5 การปฏิบัติตามข้อกำหนด (Compliance)

คำอธิบายแนวคิด: ระบบต้องสอดคล้องกับมาตรฐานด้านความปลอดภัย ความมั่นคง และข้อกำหนดทางกฎหมาย เช่น MIL-STD ISO/IEC27001 หรือกฎหมายเฉพาะด้าน

วัตถุประสงค์: เพื่อให้แน่ใจว่าระบบสามารถนำไปใช้งานในภารกิจจริงได้ โดยไม่ละเมิดข้อกำหนดหรือกฎหมายใดๆ

บริบทการประเมิน: การประเมินมิตินี้มักดำเนินโดยหน่วยงานที่มีหน้าที่กำกับดูแลหรือผู้มีอำนาจรับรอง เช่น หน่วยรับรองมาตรฐานทางทหาร (เช่น กรมสื่อสารทหาร) หรือเจ้าหน้าที่ด้านความมั่นคงสารสนเทศ โดยใช้กระบวนการตรวจสอบเอกสาร ข้อกำหนดทางเทคนิค และผลการทดสอบระบบ เพื่อประเมินความสอดคล้องกับมาตรฐานและกฎระเบียบเฉพาะด้านของกองทัพ ทั้งนี้การประเมินจะครอบคลุมทั้งด้านฟังก์ชัน การควบคุมความปลอดภัย การจัดการความเสี่ยง และการตรวจสอบย้อนหลัง เพื่อให้มั่นใจว่าระบบสามารถนำไปใช้งานจริงโดยไม่ละเมิดข้อกำหนดหรือกฎหมาย

แนวทางการประเมิน: ทดสอบการทำงานตามข้อกำหนดของแต่ละมาตรฐาน ตรวจสอบระบบควบคุมสิทธิ์ การเข้ารหัส และระบบ log ตรวจสอบเอกสารประกอบที่ยืนยันการทดสอบ

กรณีศึกษาระบบ ASD: การออกแบบให้มีการจำกัดสิทธิ์การเข้าถึงตามระดับ clearance อย่างเข้มงวด เพื่อป้องกันการเข้าถึงข้อมูลหรือฟังก์ชันที่ไม่เหมาะสม และเก็บ log การใช้งานอย่างละเอียดครบถ้วนตามมาตรฐาน MIL-STD-1530 และแนวทางของ ISO/IEC 27001 ซึ่งช่วยให้สามารถตรวจสอบและติดตามกิจกรรมต่าง ๆ ได้อย่างมีประสิทธิภาพ

นอกจากนี้ ระบบยังผ่านการทดสอบความสอดคล้องกับมาตรฐานทางทหารที่สำคัญ อาทิ MIL-STD-810 ที่ครอบคลุมการทดสอบด้านสภาพแวดล้อมต่าง ๆ เช่น ความร้อน ความชื้น และแรงสั่นสะเทือน เพื่อรับประกันว่าระบบสามารถทำงานได้ในสภาวะที่รุนแรงและหลากหลาย รวมถึง MIL-STD-461 ที่ทดสอบด้านการรบกวนทางแม่เหล็กไฟฟ้า เพื่อป้องกันการรบกวนและรักษาความเสถียรของระบบในสนามรบ

ในส่วนของความปลอดภัยทางไซเบอร์ ระบบ ASD ได้ผ่านการทำ penetration testing อย่างเข้มข้น เพื่อประเมินจุดอ่อนและยืนยันว่ากลไกการเข้ารหัสข้อมูล รวมถึงระบบควบคุมสิทธิ์ สามารถป้องกันการโจมตีหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตได้อย่างมีประสิทธิภาพ นอกจากนี้ยังมีการทดสอบระบบ log และ audit trail เพื่อให้มั่นใจว่าสามารถตรวจสอบย้อนหลังได้ในกรณีที่เกิดเหตุการณ์ผิดปกติ

การดำเนินการทดสอบเหล่านี้ช่วยให้มั่นใจว่า ระบบ ASD ไม่เพียงแค่ตอบสนองต่อข้อกำหนดด้านความปลอดภัยและมาตรฐานทางทหารเท่านั้น แต่ยังสามารถ

ปฏิบัติงานในภารกิจจริงได้อย่างมั่นคงและน่าเชื่อถือภายใต้โปรโตคอลของกองทัพ ซึ่งทำให้ระบบได้รับการยอมรับและพร้อมใช้งานในสภาพแวดล้อมที่เข้มงวดและมีความเสี่ยงสูง

5.2.6 การติดตั้งและการใช้งาน (Deployment)

คำอธิบายแนวคิด: ระบบต้องสามารถติดตั้งได้อย่างรวดเร็วในพื้นที่ปฏิบัติการจริง โดยไม่จำเป็นต้องพึ่งพาผู้เชี่ยวชาญ และไม่ส่งผลกระทบต่อระบบที่มีอยู่

วัตถุประสงค์: เพื่อให้ระบบสามารถใช้งานได้ทันทีหลังจากการติดตั้ง แม้ในพื้นที่ที่มีข้อจำกัดเรื่องอุปกรณ์ เวลา หรือทรัพยากรบุคคล

บริบทการประเมิน: เน้นการประเมินโดยให้ผู้ปฏิบัติงานภาคสนาม หรือผู้แทนจากหน่วยงานที่มีหน้าที่บูรณาการระบบ เช่น ฝ่ายสื่อสารหรือฝ่ายโลจิสติกส์ทางทหาร การประเมินจะดำเนินในสภาพแวดล้อมจำลองหรือพื้นที่จริง เพื่อทดสอบความง่ายในการติดตั้ง ความรวดเร็วในการเริ่มใช้งาน และผลกระทบที่อาจเกิดขึ้นกับระบบที่มีอยู่เดิม ทั้งนี้จะพิจารณาด้วยว่าในสถานการณ์เร่งด่วนหรือในพื้นที่ที่มีข้อจำกัดด้านอุปกรณ์และบุคลากร ระบบยังสามารถใช้งานได้อย่างมีประสิทธิภาพหรือไม่

แนวทางการประเมิน: ทดสอบการติดตั้งในสภาพแวดล้อมจำลอง ประเมินเวลาที่ใช้ในการติดตั้งและตรวจสอบเอกสารและคู่มือการติดตั้ง

กรณีศึกษาระบบ ASD: การติดตั้งแบบ container-based deployment ซึ่งหมายถึงการแพ็กเกจระบบและส่วนประกอบทั้งหมดไว้ใน ”กล่อง“ ซอฟต์แวร์ขนาดเล็กที่พร้อมใช้งาน ทำให้การติดตั้งและตั้งค่าระบบเป็นไปอย่างรวดเร็วและง่ายดาย สามารถทำได้ภายในเวลาไม่ถึง30 นาทีบนเครื่องมาตรฐานทั่วไป โดยไม่จำเป็นต้องอาศัยผู้เชี่ยวชาญเฉพาะทางด้านไอทีหรือระบบเครือข่าย นอกจากนี้ ระบบยังออกแบบให้สามารถทำงานร่วมกับระบบเดิมได้อย่างราบรื่นโดยไม่ส่งผลกระทบต่อการปฏิบัติงานปกติในพื้นที่จริง

ในกระบวนการทดสอบการติดตั้งระบบ ASD ได้รับการประเมินในสภาพแวดล้อมจำลองและสภาพแวดล้อมจริง เพื่อวัดระยะเวลาการติดตั้งและตั้งค่า รวมถึงรวบรวมความคิดเห็นจากผู้ใช้งานจริงเกี่ยวกับความชัดเจนของคู่มือการติดตั้ง ความง่ายในการปฏิบัติงาน และปัญหาที่พบระหว่างการติดตั้ง ผลการประเมินชี้ให้เห็นว่า ASD สามารถลดความซับซ้อนของกระบวนการติดตั้งได้อย่างมีนัยสำคัญ และทำให้ระบบพร้อมใช้งานได้อย่างรวดเร็ว แม้ในพื้นที่ที่มีข้อจำกัดเรื่องทรัพยากรบุคคลหรืออุปกรณ์

นอกจากนี้ การใช้แพ็กเกจระบบยังช่วยให้การอัปเดตและบำรุงรักษาระบบในภายหลังเป็นไปอย่างรวดเร็วและไม่รบกวนการทำงานของระบบหลัก ช่วยเพิ่มประสิทธิภาพในการบริหารจัดการระบบในภาคสนามได้อย่างดี

5.2.7. การบำรุงรักษา (Maintenance)

คำอธิบายแนวคิด: ระบบควรออกแบบให้สามารถตรวจสอบ แก้ไข และอัปเดตได้ง่าย เพื่อรองรับการดูแลรักษาระยะยาว และปรับปรุงตามการเปลี่ยนแปลงของภารกิจ

วัตถุประสงค์: เพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่องและทันสมัยตลอดวงจรชีวิต

แนวทางการประเมิน: ตรวจสอบการรองรับการอัปเดตและการย้อนกลับเวอร์ชัน วิเคราะห์เครื่องมือและอินเทอร์เฟซสำหรับผู้ดูแลระบบ และตรวจสอบระบบแจ้งเตือนและบันทึกสถานะ

บริบทการประเมิน: การประเมินมิตินี้มักดำเนินการโดยผู้ดูแลระบบหรือหน่วยสนับสนุนทางเทคนิค เช่น ฝ่ายซ่อมบำรุง โดยอาจใช้การทดสอบในห้องปฏิบัติการหรือการใช้งานจริงในระยะเวลาหนึ่ง เพื่อตรวจสอบความง่ายในการบำรุงรักษา ความรวดเร็วในการแก้ไขปัญหา และผลกระทบที่เกิดขึ้นเมื่อมีการเปลี่ยนส่วนประกอบหรือซอฟต์แวร์ภายใต้ข้อจำกัดของภาคสนาม

กรณีศึกษาระบบ ASD: การออกแบบให้รองรับการบำรุงรักษาได้อย่างมีประสิทธิภาพในระยะยาว โดยมีโมดูล health monitoring สำหรับตรวจสอบสถานะระบบและแจ้งเตือนอัตโนมัติเมื่อพบความผิดปกติ เช่น ความล้มเหลวของเซนเซอร์ การเชื่อมต่อขัดข้อง หรือทรัพยากรระบบไม่เพียงพอ นอกจากนี้ ASD ยังมี

อินเทอร์เฟซสำหรับผู้ดูแลระบบที่สามารถจัดการกับการอัปเดตซอฟต์แวร์ (patch management) และการย้อนกลับเวอร์ชัน (rollback) ได้อย่างสะดวก

จากการทดสอบการบำรุงรักษาในสถานการณ์จำลอง ทีมพัฒนาสามารถอัปเดตซอฟต์แวร์โดยไม่ส่งผลกระทบต่อการทำงานของระบบหลัก และเมื่อจำลองการเปลี่ยนฮาร์ดแวร์หรืออุปกรณ์เชื่อมต่อ ระบบสามารถตรวจจับการเปลี่ยนแปลงและปรับตัวได้โดยไม่ต้องตั้งค่าใหม่ทั้งหมด คู่มือการดูแลระบบมีความชัดเจน ครอบคลุมขั้นตอนการบำรุงรักษา ทั้งในส่วนของซอฟต์แวร์และฮาร์ดแวร์ ช่วยให้เจ้าหน้าที่ที่ไม่ใช่ผู้พัฒนาสามารถดูแลระบบได้อย่างมั่นใจ

5.3 ข้อดีที่ได้รับจากการประยุกต์ใช้กรอบ MSQA

การประยุกต์ใช้กรอบการประเมินคุณภาพซอฟต์แวร์ MSQA กับระบบ ASD ช่วยส่งเสริมการดำเนินโครงการให้มีความเป็นระบบและมีประสิทธิภาพยิ่งขึ้น โดยเริ่มตั้งแต่ขั้นตอนการวางแผนที่มีเป้าหมายชัดเจน MSQA ช่วยให้สามารถระบุคุณลักษณะด้านคุณภาพที่สำคัญ เช่น ความทนทาน การบำรุงรักษา และความสามารถในการทำงานร่วมกับระบบอื่น ซึ่งเป็นข้อมูลพื้นฐานในการกำหนดเกณฑ์และแนวทางการทดสอบตั้งแต่ระยะแรกของการพัฒนา ทั้งยังมีการจัดทำเอกสารเกณฑ์การประเมินในแต่ละมิติเพื่อใช้ประกอบการหารือกับหน่วยผู้ใช้งาน ทำให้สามารถลดระยะเวลาในการกำหนดข้อกำหนดระบบ เมื่อเปรียบเทียบกับโครงการพัฒนาอื่นก่อนหน้า

กรอบ MSQA ยังช่วยลดความเสี่ยงในการดำเนินโครงการด้วยแนวทางการประเมินที่มีโครงสร้างชัดเจน โดยสามารถระบุจุดอ่อนหรือความไม่สอดคล้องได้ตั้งแต่ต้น ตัวอย่างเช่น การตรวจพบปัญหาด้านการบูรณาการระบบ (integration) ในช่วงต้นของโครงการ ทำให้สามารถวางแผนเปลี่ยนสายสัญญาณเดิมให้สามารถทำงานร่วมกับคอมพิวเตอร์สมัยใหม่ได้อย่างเหมาะสม ส่งผลให้ต้องมีการปรับแผนด้านการเชื่อมต่อและการแปลงหัวต่อใหม่ตั้งแต่ระยะแรก

ด้านการสื่อสารและการตรวจสอบย้อนกลับ MSQA ช่วยให้การประสานงานระหว่างทีมพัฒนาและผู้ใช้งานภาคสนามมีความราบรื่นมากยิ่งขึ้น เนื่องจากมีเกณฑ์ที่ชัดเจนในการประเมินคุณภาพ ช่วยให้การออกแบบระบบตอบสนองต่อสภาพแวดล้อมและข้อกำหนดภารกิจได้อย่างเหมาะสม อีกทั้งการใช้แบบฟอร์มตรวจสอบ (checklist) และเอกสารบันทึกผลตามกรอบ MSQA ยังช่วยให้สามารถติดตามสถานะของแต่ละมิติการทดสอบได้อย่างโปร่งใส และสามารถตรวจสอบย้อนหลังได้โดยสะดวก

นอกจากนี้ MSQA ยังเอื้อต่อการทดสอบที่ครอบคลุมและสามารถวัดผลได้จริงในสภาพแวดล้อมการใช้งานที่หลากหลาย โดยการทดสอบในแต่ละมิติได้รวม การรองรับภาระงานสูง (Stress Test) การทำงานต่อเนื่องเมื่อเกิดความล้มเหลว (Failover Test) การใช้งานของผู้ใช้ (Usability Test) และความสอดคล้องตามข้อกำหนดหรือมาตรฐาน (Compliance Test) ช่วยให้สามารถประเมินระบบได้อย่างรอบด้านและลึกซึ้ง สอดคล้องกับข้อจำกัดและลักษณะเฉพาะของบริบทภาคสนามอย่างแท้จริง

5.4 ข้อสังเกตเบื้องต้น

จากการประยุกต์ใช้กรอบการประเมินคุณภาพซอฟต์แวร์ MSQA ในโครงการพัฒนาระบบซอฟต์แวร์ทางทหาร พบว่ากรอบดังกล่าวสามารถสนับสนุนการดำเนินงานได้อย่างเป็นระบบ โดยเฉพาะในบริบทที่มีข้อจำกัดด้านเวลา ทรัพยากร และบุคลากร อย่างไรก็ตาม การประเมินภาคสนามสะท้อนข้อจำกัดบางประการที่ควรนำไปพิจารณาเพื่อปรับปรุงกรอบ MSQA ให้เหมาะสมกับการใช้งานจริงมากยิ่งขึ้น อาทิ มิติบางด้าน เช่น Deployment และ Durability อาจต้องมีแนวทางการประเมินที่ยืดหยุ่นมากขึ้น เพื่อให้สามารถรองรับเทคโนโลยีใหม่หรือระบบเฉพาะทางที่ไม่สอดคล้องกับแนวทางการประเมินแบบเดิมได้อย่างมีประสิทธิภาพ อีกทั้งการประเมินในกรณีศึกษาครอบคลุมเฉพาะซอฟต์แวร์ เนื่องจากฮาร์ดแวร์ยังคงมีความหลากหลายตามบริบทการใช้งานจริง ซึ่งทำให้การกำหนดเกณฑ์การประเมินในบางด้าน เช่น ความทนทาน

ของอุปกรณ์ หรือการติดตั้งเฉพาะรุ่น ไม่สามารถกำหนดเป็นมาตรฐานกลางได้อย่างเหมาะสม

นอกจากนี้ การขาดช่องทางสำหรับให้ผู้ใช้งานหรือผู้ปฏิบัติงานภาคสนามสะท้อนข้อจำกัดหรือสภาพการณ์จริงกลับเข้าสู่กระบวนการประเมิน อาจส่งผลให้ผลการประเมินขาดความครอบคลุมต่อบริบทเฉพาะของการใช้งาน ขณะที่ความสำเร็จของกระบวนการประเมินยังคงขึ้นอยู่กับระดับความร่วมมือระหว่างผู้พัฒนา ผู้ประเมิน และผู้ใช้งานปลายทาง ซึ่งการส่งเสริมให้เกิดการมีส่วนร่วมของทุกฝ่ายตั้งแต่เริ่มต้นจนถึงสิ้นสุดกระบวนการจะช่วยให้การประเมินมีประสิทธิภาพและสะท้อนข้อเท็จจริงของการใช้งานได้ชัดเจนยิ่งขึ้น

ข้อสังเกตเหล่านี้สามารถใช้เป็นแนวทางปรับปรุง MSQA ให้มีความยืดหยุ่นสูงขึ้น และรองรับความหลากหลายของบริบทการใช้งานจริงกับต้นแบบระบบซอฟต์แวร์ได้ดียิ่งขึ้นในอนาคต

6. สรุปผลและอภิปรายผล

บทความนี้ได้นำเสนอกรอบการประเมินคุณภาพซอฟต์แวร์ MSQA ที่ออกแบบให้เหมาะสมกับระบบซอฟต์แวร์ในบริบททางทหาร โดยผสานแนวคิดจากมาตรฐาน ISO/IEC 25010 และมาตรฐานที่เกี่ยวข้อง เพื่อให้ครอบคลุมประเด็นสำคัญทั้งด้านความปลอดภัย ความทนทาน การบำรุงรักษา และความสามารถในการติดตั้งใช้งานจริง

กรอบ MSQA ช่วยให้สามารถประเมินได้อย่างเป็นระบบ มีความยืดหยุ่นต่อบริบทเฉพาะ และรองรับความต้องการเฉพาะด้านของระบบทางทหาร กรณีศึกษาที่นำเสนอแสดงให้เห็นถึงศักยภาพของ MSQA ในการสนับสนุนการพัฒนาและทดสอบระบบจริงได้อย่างมีประสิทธิภาพ โดยจากการทดลองใช้ MSQA กับระบบแสดงผลเรดาร์ พบว่าระบบสามารถผ่านเกณฑ์การประเมินทั้ง 7 มิติ เช่น ประสิทธิภาพการทำงานที่ตอบสนองภารกิจในสภาพแวดล้อมจริง ความสามารถในการบูรณาการกับระบบเดิม และความทนทานต่อสภาพแวดล้อมที่ท้าทาย การประเมินช่วยให้ทีมพัฒนาวางแผนเชิงระบบและจัดลำดับความสำคัญของคุณภาพตั้งแต่ระยะแรก ลดความเสี่ยงและเวลาการแก้ไขซ้ำ นอกจากนี้ MSQA ยังส่งเสริมการสื่อสารที่มีประสิทธิภาพระหว่างผู้พัฒนาและผู้ใช้งาน ทำให้การรับมอบและตรวจสอบระบบเป็นไปอย่างราบรื่น

ผลลัพธ์เหล่านี้สะท้อนว่ากรอบ MSQA สามารถนำไปประยุกต์ใช้ในองค์กรที่มีข้อจำกัดด้านทรัพยากร ความเสี่ยงสูง และต้องการการควบคุมคุณภาพอย่างเป็นระบบและโปร่งใสตลอดวงจรชีวิตของระบบ ซึ่งทำให้ MSQA เป็นแนวทางที่มีศักยภาพในการต่อยอดและใช้งานในภาคส่วนอื่นที่มีข้อกำหนดเข้มงวด เช่น ระบบทางทหาร หรือระบบสำคัญเชิงยุทธศาสตร์

7. ข้อจำกัดและข้อเสนอแนะ

แม้ว่ากรอบการประเมิน MSQA จะได้รับการออกแบบให้ครอบคลุมประเด็นสำคัญของซอฟต์แวร์ทางการทหาร และมีความยืดหยุ่นในการประยุกต์ใช้กับบริบทที่หลากหลาย แต่อย่างไรก็ตาม จากการดำเนินการวิจัยในครั้งนี้ยังพบข้อจำกัดบางประการที่ควรพิจารณาเพิ่มเติม ดังนี้

1) การประเมินกรอบ MSQA ในงานวิจัยนี้ดำเนินการเฉพาะกับระบบแสดงผลข้อมูลเรดาร์เพียงระบบเดียว คือ ระบบ ASD ซึ่งแม้จะเป็นระบบที่มีการใช้งานจริงในภาคสนาม แต่ยังไม่สามารถสะท้อนความหลากหลายหรือความซับซ้อนของซอฟต์แวร์ทางการทหารประเภทอื่น เช่น ระบบควบคุมอาวุธ ระบบสื่อสาร หรือระบบสนับสนุนการตัดสินใจ
2) ระบบทางทหารบางประเภทอาจมีลักษณะเฉพาะที่แตกต่างจากระบบ ASD เช่น ระบบที่ต้องทำงานร่วมกับฮาร์ดแวร์เฉพาะทาง หรือระบบควบคุมที่มีข้อกำหนดด้านความปลอดภัยและความมั่นคงในระดับสูง ซึ่งระบบเหล่านี้อาจต้องการเกณฑ์หรือวิธีการประเมินที่มีความเฉพาะเจาะจงมากกว่าที่ระบุไว้ในกรอบ MSQA
3) การใช้งานกรอบ MSQA อย่างมีประสิทธิภาพจำเป็นต้องอาศัยความเข้าใจร่วมกันจากผู้มีส่วนเกี่ยวข้อง เช่น วิศวกร ผู้ประเมิน และผู้ใช้งานปลายทาง จึงอาจต้องมีการจัดทำคู่มือแนวทางการใช้งานที่ชัดเจน รวมถึงการฝึกอบรม

เพื่อสร้างความตระหนักรู้และส่งเสริมการยอมรับ

จากข้อจำกัดที่พบเหล่านี้ จึงควรมีการพัฒนาและปรับปรุง MSQA ให้สามารถตอบสนองความต้องการของระบบเฉพาะทางได้มากขึ้น รวมถึงสนับสนุนการใช้งานในสถานการณ์จริงที่มีข้อจำกัดแตกต่างกัน เพื่อให้กรอบนี้สามารถใช้เป็นเครื่องมือในการประเมินคุณภาพซอฟต์แวร์ทางการทหารได้อย่างครบถ้วนและยั่งยืนในระยะยาว

8. กิตติกรรมประกาศ

งานวิจัยนี้ได้รับทุนสนับสนุนจาก สำนักงานการวิจัยแห่งชาติ (วช.) รหัสโครงการ N23A671094

9. บรรณานุกรม

[1] Toropin, K. (2022, September 20). *Sailors' medical discharges halted for almost a week due to computer glitch.* Military.com. Retrieved from http://www.military.com/daily-news/2022/09/20/sailors-medical-discharges-halted-almost-week-due-computer-glitch.html on March 10, 2025

[2] Cluley, G. (2023, April 18). *Army helicopter crash blamed on skipped software patch.* Bitdefender. Retrieved from http://www.bitdefender.com/en-us/blog/hotforseciruty/army-helocopter-crash-blamed-on-skipped-software-patch on March 10, 2025

[3] International Organization for Standardization. (2011). *ISO/IEC 25010:2011 - Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Quality model.* Retrieved from http://cdn.Standards.iten.ai/ samples/35733/2ca18b477b7845a5b8cae39d6de0c098/ISO-IEC-25010-2011.pdf

[4] International Organization for Standardization. (n.d.). *ISO/IEC 25010.* Retrieved from http://iso25000.com/index.php/en/iso-25000-standards/iso-25010 on March 10, 2025

[5] Department of Defense. (1994). *MIL-STD-498: Software development and documentation.* Retrieved from http://apps.dtic.mil/sti/pdfs/ADA282003.pdf on March 10, 2025

[6] Department of Defense. (2000). *MIL-STD-882: System safety.*

[7] Department of Defense. (1999). *MIL-STD-1397C: Digital communication protocols for military systems.* Retrieved from http://everyspec.com/MIL-STD/MIL-STD-1300-1399/MIL_STD_1397C_554/ on March 10, 2025

[8] International Organization for Standardization. (2017). *ISO/IEC/IEEE 12207: Systems and software engineering – Software life cycle processes.* Retrieved from http://ieeexplore.ieee.org/document/8100771 on March 10, 2025

[9] International Organization for Standardization. (2003). *ISO/IEC 15504: Information technology – Process assessment.* Retrieved from https://www.iso.org/standard/63712.html on March 10, 2025

[10] International Organization for Standardization. (2013). *ISO/IEC 27001: Information security management systems – Requirements.* Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en on March 10, 2025

[11] International Organization for Standardization. (2011). *ISO/IEC 29110: Systems and software engineering.* Retrieved from https://www.iso.org/standard/85337.html on March 10, 2025

[12] Department of Defense. (2019). *MIL-STD-810: Environmental testing.* Retrieved from https://ebindustries.com/wp-content/uploads/2021/11/MIL-STD-810.pdf on March 10, 2025

[13] Department of Defense. (2015). *MIL-STD-461: Requirements for the control of electromagnetic interference characteristics of subsystems and equipment.* Retrieved from https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=35789 on March 10, 2025

[14] Wagner, S., Felderer, M., & Fernández, D. M. (2017). Quality requirements in industrial practice – an empirical study. Requirements Engineering, 22(3), 331–355.

[15] Alnanih, R., Ormandjieva, O., & Radhakrishnan, T. (2014). A Systematic Approach for Evaluating Software Quality Using ISO/IEC 25010. Procedia Computer Science, 37, 337–344.