

การสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงโดยการขยายยูเอ็มแอล



นายอิทธิพัทธ์ วงศ์ไชยกุล

ศูนย์วิทยพัทยาการ  
จุฬาลงกรณ์มหาวิทยาลัย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2552

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

SECURITY PATTERNS STRUCTURAL MODEL CONSTRUCTION  
BY EXTENDING UML

Mr. Ittipat Wongchaikul



ศูนย์วิทยทรัพยากร

จุฬาลงกรณ์มหาวิทยาลัย  
A Thesis Submitted in Partial Fulfillment of the Requirements  
for the Degree of Master of Science Program in Software Engineering

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2009

Copyright of Chulalongkorn University

หัวข้อวิทยานิพนธ์

การสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง  
โดยการขยายยูเอ็มแอล

โดย

นายอิทธิพัทธ์ วงศ์ไชยกุล


สาขาวิชา

วิศวกรรมซอฟต์แวร์


อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

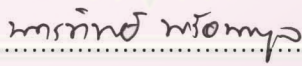
ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล

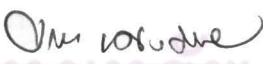
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้หัวข้อวิทยานิพนธ์ฉบับนี้  
เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรบัณฑิต

  
..... คณบดีคณะวิศวกรรมศาสตร์  
(รองศาสตราจารย์ ดร. บุญสม เลิศหิรัญวงศ์)

คณะกรรมการสอบวิทยานิพนธ์

  
..... ประธานกรรมการ  
(รองศาสตราจารย์ ดร. วันชัย รั้วไพบูลย์)

  
..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก  
(ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล)

  
..... กรรมการ  
(อาจารย์ ดร. ยรรยง เต็งอำนาจ)

  
..... กรรมการภายนอกมหาวิทยาลัย  
(อาจารย์ ดร. เฉลิมศักดิ์ เลิศวงศ์เสถียร)

อิทธิพัทธ์ วงศ์ไชยกุล : การสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงโดยการขยายยูเอ็มแอล. (SECURITY PATTERNS STRUCTURAL MODEL CONSTRUCTION BY EXTENDING UML) อ.ที่ปรึกษาวิทยานิพนธ์หลัก : ผศ. นครทิพย์ พร้อมพูล, 147 หน้า.

ในปัจจุบันมีการปรากฏภัยคุกคามที่มากขึ้นและหลากหลายแก่ระบบคอมพิวเตอร์ โดยสิ่งสำคัญที่ทุกองค์กรควรจะต้องตระหนักถึงคือ ความมั่นคงของระบบซอฟต์แวร์ ดังนั้นองค์กรจึงมีความจำเป็นในการนำหลักการทางด้านความมั่นคงมาประยุกต์ใช้ในองค์กร ให้มีความสอดคล้องกับความต้องการและลักษณะของระบบ ซึ่งการนำแบบรูปความมั่นคงเข้ามาประยุกต์ใช้ในการพัฒนาซอฟต์แวร์นั้นเป็นอีกทางเลือกสำหรับแก้ปัญหาความมั่นคงของระบบซอฟต์แวร์ เนื่องจากเป็นกลุ่มของแบบรูปที่อธิบายถึงแนวทางหรือผลเฉลยของปัญหาทางด้านความมั่นคงที่มีการใช้งานอย่างแพร่หลาย

งานวิทยานิพนธ์นี้มีวัตถุประสงค์เพื่อขยายยูเอ็มแอลของแผนภาพคลาสในส่วนของแม่พิมพ์ต้นแบบและป้ายระบุสำหรับแสดงแบบรูปความมั่นคงและปรับปรุงยูเอ็มแอลให้เหมาะสมต่อการนำไปใช้งานในการออกแบบและพัฒนาซอฟต์แวร์ รวมทั้งพัฒนาเครื่องมือสนับสนุนการแสดงโครงสร้างของแบบรูปความมั่นคง ซึ่งส่วนขยายนี้เรียกว่า ยูเอ็มแอลเซคเอสพี-2 ในงานวิทยานิพนธ์นี้ได้วิเคราะห์แบบรูปความมั่นคง โดยครอบคลุมแบบรูปความมั่นคงทั้งหมด 44 แบบรูปจาก 8 กลุ่มแบบรูปความมั่นคง ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง การระบุตัวตนและการพิสูจน์ตัวตน การบันทึกเหตุการณ์ แบบจำลองการควบคุมการเข้าถึง สถาปัตยกรรมการควบคุมการเข้าถึง การควบคุมการเข้าถึงระบบปฏิบัติการ สถาปัตยกรรมไฟร์วอลล์ และการประยุกต์ใช้ความมั่นคงบนอินเทอร์เน็ต การวิเคราะห์โครงสร้างและบริบทของแบบรูปความมั่นคงทำให้ได้ ข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงสำหรับใช้ในการขยายยูเอ็มแอลเพื่อให้สามารถครอบคลุมการแสดงผลข้อมูลของแบบรูปความมั่นคงได้ ซึ่งได้มีการตรวจสอบยูเอ็มแอลเซคเอสพี-2 ให้เป็นไปตามคุณสมบัติมาตรฐานของยูเอ็มแอลโพรไฟล์

ยูเอ็มแอลเซคเอสพี-2 และเครื่องมือที่พัฒนาขึ้นเป็นประโยชน์แก่ผู้พัฒนาระบบให้สามารถเข้าใจโครงสร้างของแบบรูปความมั่นคง ไปประยุกต์ใช้ในการออกแบบและพัฒนาความมั่นคงของระบบได้อย่างมีประสิทธิภาพ

ภาควิชา.....วิศวกรรมคอมพิวเตอร์.....ลายมือชื่อนิสิต.....อิทธิพัทธ์ วงศ์ไชยกุล.....  
 สาขาวิชา.....วิศวกรรมซอฟต์แวร์.....ลายมือชื่ออ.ที่ปรึกษาวิทยานิพนธ์หลัก.....นครทิพย์ พร้อมพูล.....  
 ปีการศึกษา.....2552.....

# # 5070265921 : MAJOR SOFTWARE ENGINEERING

KEYWORDS : UMLSEC / SECURITY PATTERNS / UML PROFILE

ITTIPAT WONGCHAIKUL : SECURITY PATTERNS STRUCTURAL MODEL  
CONSTRUCTION BY EXTENDING UML. THESIS ADVISOR :  
ASST.PROF. NAKORNTHIP PROMPOON, 147 pp.

In present, various kinds of computer threats occur increasingly. An important issue which many enterprises have to consider is security of software system. Thus, organizations have to apply security principles align to their needs and system features. Applying security patterns in software development is a good choice and widely used among security engineers to solve a security problem of software system because they describes solutions in various kinds of security problems and can be applied in many cases.

The objective of this thesis is to extend UML Class diagram, called UMLsec SP-2, for representing the security patterns in order to apply in the software design and development. UML stereotype and tagged value are the two mechanism in expanding UML. In addition, the supporting tool is developed for applying UMLsec SP-2. This thesis covers 44 patterns from 8 security pattern types; Enterprise Security and Risk Management, Identification and Authentication, Accounting, Access Control Model, System Access Control Architecture, Operating System Access Control, Firewall Architecture and Secure Internet Applications. The structure and context of these patterns are analyzed to define pattern structural information and security information for extending UML that follows such patterns. UMLsec SP-2 is validated against the UML profile standard specification.

UMLsec SP-2 and the supporting tool may be beneficial to system developer to understand the security pattern structure and can apply them efficiently in security system design and development.

Department : ..... Computer Engineering .....

Field of Study : ..... Software Engineering .....

Academic Year : ..... 2009 .....

Student's Signature Ittipat Wongchikul

Advisor's Signature Nakornthip Prompoon

## กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วย ความเมตตาและความช่วยเหลืออย่างยิ่งจาก อาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ นครทิพย์ พร้อมพูล อาจารย์ผู้เสียสละเวลาช่วยให้ คำปรึกษา ข้อคิดและคำแนะนำที่มีประโยชน์ต่องานวิจัยและการใช้ชีวิตในสังคม

ขอขอบพระคุณ รองศาสตราจารย์ ดร.วันชัย รั้วไพบูลย์ ประธานกรรมการสอบ วิทยานิพนธ์ อาจารย์ ดร.ยรรยง เต็งอำนาจ และอาจารย์ ดร.เฉลิมศักดิ์ เลิศวงศ์เสถียร กรรมการสอบวิทยานิพนธ์ ที่ได้กรุณาสละเวลาให้คำแนะนำสำหรับโครงร่างวิทยานิพนธ์และ วิทยานิพนธ์ให้มีคุณภาพยิ่งขึ้น

ขอขอบคุณ พี่ตุรกรภากาศ ทุกคนที่ช่วยอำนวยความสะดวกในการทำงานและช่วย ตักเตือนแนะนำสิ่งดีๆ เสมอมา

ขอขอบคุณ เพื่อนๆ พี่ๆ และน้องๆ ที่ผ่านเข้ามาในชีวิตของผู้วิจัยรวมถึงคนใกล้ชิด ของผู้วิจัย ที่ห่วงใย ให้กำลังใจ และให้ความช่วยเหลือในทุกๆ ด้านจนผู้วิจัยสามารถทำ วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วง

ท้ายที่สุด ขอกราบขอบพระคุณบิดา มารดาและสมาชิกในครอบครัวทุกท่าน ที่ให้การ สนับสนุน และให้กำลังใจแก่ผู้วิจัย เสมอมา

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

## สารบัญ

	หน้า
บทคัดย่อภาษาไทย .....	ง
บทคัดย่อภาษาอังกฤษ .....	จ
กิตติกรรมประกาศ .....	ฉ
สารบัญ .....	ช
สารบัญตาราง .....	ฅ
สารบัญภาพ .....	ฉ
บทที่ 1 บทนำ.....	1
1.1 ที่มาและความสำคัญของงานวิจัย.....	1
1.2 วัตถุประสงค์ของงานวิจัย.....	2
1.3 ขอบเขตของงานวิจัย.....	2
1.4 ขั้นตอนของการวิจัย.....	3
1.5 ประโยชน์ที่คาดว่าจะได้รับ.....	3
บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง .....	4
2.1 ทฤษฎีที่เกี่ยวข้อง.....	4
2.1.1 แผนภาพยูเอเอ็มแอล .....	4
2.1.2 ยูเอเอ็มแอลโพรไฟล์.....	8
2.1.3 แบบรูปและแบบรูปความมั่นคง .....	10
2.1.4 วิศวกรรมความมั่นคง.....	11
2.2 งานวิจัยที่เกี่ยวข้อง .....	13
2.2.1 ยูเอเอ็มแอลเซค: ส่วนขยายของยูเอเอ็มแอลเพื่อการพัฒนา ระบบความมั่นคง.....	13
2.2.2 การแสดงแบบรูปการออกแบบในโปรแกรมประยุกต์และส่วนประกอบ... ..	15
2.2.3 เมตาาดาตาและแบบรูปการให้อำนาจ .....	16
2.2.4 การแสดงแบบรูปความมั่นคงโดยการขยายยูเอเอ็มแอลเซค .....	18
บทที่ 3 การวิเคราะห์แบบรูปความมั่นคงและการขยายยูเอเอ็มแอล.....	21
3.1 การศึกษาและกำหนดความต้องการของแบบรูปความมั่นคง .....	23
3.2 การจำลองโครงสร้างของแบบรูปความมั่นคง .....	26
3.3 การปรับปรุงส่วนประกอบทางโครงสร้างของแบบรูปความมั่นคง .....	27
3.4 การวิเคราะห์การแสดงผลแบบรูปความมั่นคง .....	29

3.5 การปรับปรุงยูเอ็มแอลสำหรับแสดงแบบรูปความมั่นคง .....	30
3.5.1 ปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอล .....	31
3.5.2 ปรับปรุงเงื่อนไขบังคับของยูเอ็มแอล.....	34
3.6 การตรวจสอบยูเอ็มแอลเซคเอสพี-2 .....	38
บทที่ 4 การพัฒนาและทดสอบเครื่องมือสนับสนุนสำหรับแสดงแบบรูปความมั่นคง .....	40
4.1 การพัฒนาแบบรูปความมั่นคงในเครื่องมือสนับสนุน .....	41
1) การพัฒนาส่วนกำหนดแบบรูปความมั่นคง .....	43
2) การพัฒนาส่วนช่วยเหลือผู้ใช้งาน .....	44
4.2 การทดสอบเครื่องมือสนับสนุน.....	47
4.3 สภาพแวดล้อมในการพัฒนาเครื่องมือ .....	49
บทที่ 5 การประเมินผลและการวิเคราะห์การแสดงผลแบบรูปความมั่นคง.....	50
5.1 การกำหนดกรณีศึกษาที่ประยุกต์ใช้แบบรูปความมั่นคง .....	50
5.2 การสร้างแผนภาพคลาสตามความต้องการในการแสดงผลแบบรูปความมั่นคง .....	51
5.3 การวิเคราะห์การแสดงผลแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี-2 .....	51
บทที่ 6 สรุปผลการวิจัย .....	54
6.1 บทสรุปของผลงานวิจัย.....	54
6.2 งานวิจัยในอนาคต .....	54
6.3 บทความวิชาการที่ตีพิมพ์ .....	55
รายการอ้างอิง .....	56
ภาคผนวก .....	58
ภาคผนวก ก การศึกษา กำหนดความต้องการ และจำลองโครงสร้าง ของแต่ละแบบรูปความมั่นคง .....	59
ภาคผนวก ข ยูเอ็มแอลเซคเอสพี-2.....	79
ภาคผนวก ค การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแต่ละแบบรูปความมั่นคง .....	92
ภาคผนวก ง กรณีศึกษาที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 สำหรับแสดงแบบรูปความมั่นคง .....	111
ภาคผนวก จ ตัวอย่างการใช้งานเครื่องมือต้นแบบ และผลลัพธ์ที่ได้จากเครื่องมือ.....	121
ภาคผนวก ฉ การเปรียบเทียบการแสดงผลแบบรูปความมั่นคงของยูเอ็มแอล ยูเอ็มแอลเซค ยูเอ็มแอลเซคเอสพีและยูเอ็มแอลเซคเอสพี-2.....	127
ภาคผนวก ช แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพี-2.....	135
ภาคผนวก ซ ผลงานตีพิมพ์ .....	139
ประวัติผู้เขียนวิทยานิพนธ์ .....	147



## สารบัญตาราง

	หน้า
ตารางที่ 2.1 ประเภทของยูเอ็มแอล .....	4
ตารางที่ 2.2 ความหมายของตัวเลขแสดงความสัมพันธ์ .....	8
ตารางที่ 2.3 แม่พิมพ์ต้นแบบของยูเอ็มแอลเซค .....	13
ตารางที่ 2.4 ป้ายระบุของยูเอ็มแอลเซค .....	14
ตารางที่ 3.1 คำอธิบายภาพรวมในการขยายยูเอ็มแอล .....	22
ตารางที่ 3.2 รายการปัญหา บริบท และรายการความต้องการที่ได้จากการสกัดผลเฉลย ของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร .....	26
ตารางที่ 3.3 คลาสของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร .....	27
ตารางที่ 3.4 ตัวอย่างของคุณสมบัติทางด้านความมั่นคงของแต่ละสินทรัพย์ขององค์กร .....	28
ตารางที่ 3.5 องค์กรประกอบทางโครงสร้างที่ปรับปรุงเพิ่มเติม .....	29
ตารางที่ 3.6 การระบุข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการ ความมั่นคงสำหรับสินทรัพย์องค์กร .....	31
ตารางที่ 3.7 แม่พิมพ์ต้นแบบสำหรับระบุงค์ประกอบในแบบจำลอง ของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร .....	32
ตารางที่ 3.8 ป้ายระบุสำหรับระบุงค์ประกอบในแบบจำลองของแบบรูปการระบุ ความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร .....	33
ตารางที่ 3.9 รายการของแม่พิมพ์ต้นแบบและเงื่อนไขบังคับสำหรับแสดง ข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูป การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร .....	36
ตารางที่ 3.10 รายการของป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้าง และข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการ ความมั่นคงสำหรับสินทรัพย์องค์กร .....	37
ตารางที่ 4.1 รายละเอียดของแผนภาพคลาสที่แสดงโครงสร้างของเครื่องมือสนับสนุน .....	43
ตารางที่ 4.2 ตัวอย่างของแผนภาพคลาสที่ได้จากเครื่องมือต้นแบบและเครื่องมือวิสตี้พี เพื่อเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคง .....	48
ตารางที่ 4.3 การเปรียบเทียบความสามารถของเครื่องมือต้นแบบกับเครื่องมือวิสตี้พี .....	48
ตารางที่ 5.1 การเปรียบเทียบการแสดงผลข้อมูลทางโครงสร้างของแบบรูป การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร .....	52
ตารางที่ 5.2 การเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคงของแบบรูป การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร .....	52

ตารางที่ ก.1	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร.....	60
ตารางที่ ก.2	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปการกำหนดมูลค่าสินทรัพย์.....	61
ตารางที่ ก.3	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปการประเมินภัยคุกคาม.....	62
ตารางที่ ก.4	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปการประเมินจุดอ่อน.....	63
ตารางที่ ก.5	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปการกำหนดค่าความเสี่ยง.....	64
ตารางที่ ก.6	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปแนวคิดความมั่นคงองค์กร.....	66
ตารางที่ ก.7	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปบริการความมั่นคงองค์กร.....	67
ตารางที่ ก.8	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปการสื่อสารของผู้มีส่วนองค์กร.....	68
ตารางที่ ก.9	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปความต้องการการระบุและการพิสูจน์ตัวตน.....	69
ตารางที่ ก.10	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปทางเลือกการออกแบบสำหรับการระบุ และการพิสูจน์ตัวตนอัตโนมัติ.....	70
ตารางที่ ก.11	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปการออกแบบและใช้รหัสผ่าน.....	72
ตารางที่ ก.12	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปทางเลือกการออกแบบชีวมิติ.....	73
ตารางที่ ก.13	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง.....	74
ตารางที่ ก.14	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปความต้องการการตรวจสอบ.....	75
ตารางที่ ก.15	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปความต้องการการตรวจสอบหลักฐานและการบันทึก.....	76
ตารางที่ ก.16	รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปความต้องการการป้องกันการบุกรุก.....	77

ตารางที่ ก.17 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้าง ของแบบรูปความต้องการการไม่ถูกปฏิเสธ .....	78
ตารางที่ ข.1 แบบรูปความมั่นคงในแต่ละกลุ่มแบบรูปที่ใช้งานวิทยานิพนธ์ .....	79
ตารางที่ ข.2 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง .....	80
ตารางที่ ข.3 ป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง .....	80
ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง .....	80
ตารางที่ ข.5 ป้ายระบุสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง .....	90
ตารางที่ ค.1 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร .....	93
ตารางที่ ค.2 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป การกำหนดมูลค่าสินทรัพย์ .....	94
ตารางที่ ค.3 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป การประเมินภัยคุกคาม .....	95
ตารางที่ ค.4 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป การประเมินจุดอ่อน .....	96
ตารางที่ ค.5 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป การกำหนดค่าความเสี่ยง .....	97
ตารางที่ ค.6 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป แนวคิดความมั่นคงองค์กร .....	99
ตารางที่ ค.7 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป บริการความมั่นคงองค์กร .....	100
ตารางที่ ค.8 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป การสื่อสารของผู้กับหุ้นส่วนองค์กร .....	101
ตารางที่ ค.9 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป ความต้องการการระบุและการพิสูจน์ตัวตน .....	102
ตารางที่ ค.10 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ .....	103
ตารางที่ ค.11 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป การออกแบบและใช้รหัสผ่าน .....	104
ตารางที่ ค.12 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป ทางเลือกการออกแบบชีวมิติ .....	105
ตารางที่ ค.13 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป ความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง .....	106

ตารางที่ ค.14 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป	
ความต้องการการตรวจสอบ .....	107
ตารางที่ ค.15 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป	
ความต้องการการตรวจสอบหลักฐานและการบันทึก.....	108
ตารางที่ ค.16 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป	
ความต้องการการป้องกันการบุกรุก .....	109
ตารางที่ ค.17 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูป	
ความต้องการการไม่ถูกปฏิเสธ .....	110
ตารางที่ ง.1 รายละเอียดความต้องการในการแสดงข้อมูลทางโครงสร้าง	
และข้อมูลทางความมั่นคงของระบบสั่งซื้อสินค้าออนไลน์ .....	111
ตารางที่ ง.2 แม่พิมพ์ต้นแบบที่กำกับคลาสเพื่อระบุถึงหน้าที่ของคลาส	
ทางด้านความมั่นคงของระบบสั่งซื้อสินค้าออนไลน์.....	115
ตารางที่ ง.3 รายละเอียดความต้องการในการแสดงข้อมูลทางโครงสร้าง	
และข้อมูลทางความมั่นคงของระบบบริการสำหรับการบันทึกเหตุการณ์ .....	117
ตารางที่ ง.4 แม่พิมพ์ต้นแบบที่กำกับคลาสเพื่อระบุถึงหน้าที่ของคลาส	
ทางด้านความมั่นคงของระบบบริการการบันทึกเหตุการณ์.....	119
ตารางที่ ง.5 รายละเอียดความต้องการในการแสดงข้อมูลทางโครงสร้าง	
และข้อมูลทางความมั่นคงของระบบบริการความมั่นคงสำหรับองค์กร.....	120
ตารางที่ ง.6 แม่พิมพ์ต้นแบบที่กำกับคลาสเพื่อระบุถึงหน้าที่ของคลาสทางด้าน	
ความมั่นคงของระบบบริการความมั่นคงสำหรับองค์กร .....	120
ตารางที่ ฉ.1 การเปรียบเทียบการแสดงผลข้อมูลทางโครงสร้างของแบบรูปความมั่นคง.....	127
ตารางที่ ฉ.2 การเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง ...	128

## สารบัญญภาพ

	หน้า
รูปที่ 2.1 ความสัมพันธ์ของคลาส .....	6
รูปที่ 2.2 ความสัมพันธ์แบบเจนเนอรัลไลเซชัน .....	6
รูปที่ 2.3 ความสัมพันธ์แบบดีเฟนเดนซี .....	7
รูปที่ 2.4 ความสัมพันธ์แบบแอสโซซิเอชัน .....	7
รูปที่ 2.5 ความสัมพันธ์แบบแอกกรีเกชัน .....	7
รูปที่ 2.6 ความสัมพันธ์แบบคอมโพสิชัน .....	8
รูปที่ 2.7 ตัวอย่างแม่พิมพ์ต้นแบบและค่าปัยาระบุ .....	9
รูปที่ 2.8 ตัวอย่างเงื่อนไขบังคับ .....	9
รูปที่ 2.9 ขั้นตอนวิธีทางวิศวกรรมความมั่นคง .....	12
รูปที่ 2.10 ยูเอ็มแอลโพรไฟล์และส่วนขยายของยูเอ็มแอลโพรไฟล์ที่เพิ่มขึ้น เพื่อสนับสนุนการใช้แบบรูปการออกแบบ .....	16
รูปที่ 2.11 ความสัมพันธ์ของคลาสในแต่ละระดับของระบบ .....	17
รูปที่ 2.12 ตัวอย่างของแบบรูปการให้อำนาจในการออกแบบคลาส .....	17
รูปที่ 3.1 แผนภาพกิจกรรมแสดงขั้นตอนการดำเนินงานวิจัย .....	21
รูปที่ 3.2 ภาพรวมของการขยายยูเอ็มแอล .....	22
รูปที่ 3.3 แผนภาพคลาสแสดงโครงสร้างแบบรูปการระบุความต้องการ ความมั่นคงสำหรับสินทรัพย์องค์กร .....	26
รูปที่ 3.4 แผนภาพคลาสแสดงโครงสร้างแบบรูปการระบุความต้องการ ความมั่นคงสำหรับสินทรัพย์องค์กรที่ปรับปรุงแล้ว .....	29
รูปที่ 3.5 การลดรูปปัยาระบุที่มีค่าเป็นจริง .....	33
รูปที่ 3.6 การลดรูปปัยาระบุที่มีค่าเป็นเท็จ .....	33
รูปที่ 3.7 แผนภาพคลาสของแบบรูปการระบุความต้องการความมั่นคง สำหรับสินทรัพย์องค์กรที่ใช้ยูเอ็มแอลที่ปรับปรุงเพิ่มเติม .....	38
รูปที่ 4.1 แผนภาพกิจกรรมแสดงขั้นตอนการพัฒนาและทดสอบ เครื่องมือสนับสนุนการแสดงแบบรูปความมั่นคง .....	40
รูปที่ 4.2 หน้าที่การทำงานของเครื่องมือสนับสนุน .....	41
รูปที่ 4.3 โครงสร้างของเครื่องมือสนับสนุน .....	42
รูปที่ 4.4 หน้าต่างแสดงตัวอย่างของส่วนกำหนดองค์ประกอบของแบบรูปความมั่นคง .....	43
รูปที่ 4.5 ตัวอย่างแผนภาพคลาสของแบบรูปการระบุความต้องการ ความมั่นคงสำหรับสินทรัพย์องค์กร .....	44

รูปที่ 4.6 หน้าต่างแสดงตัวอย่างของส่วนช่วยเหลือผู้ใช้งานของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร.....	44
รูปที่ 4.7 แผนภาพกิจกรรมแสดงขั้นตอนการทำงานของเครื่องมือสนับสนุน .....	45
รูปที่ 4.8 แผนภาพคลาสของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรที่เป็นต้นแบบ .....	46
รูปที่ 4.9 แผนภาพคลาสของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรที่สร้างมาจากเครื่องมือสนับสนุน .....	46
รูปที่ 4.10 ส่วนช่วยเหลือผู้ใช้งานของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร .....	47
รูปที่ 5.1 แผนภาพกิจกรรมแสดงขั้นตอนการประเมินผลและการวิเคราะห์การแสดงผลแบบรูปความมั่นคง .....	50
รูปที่ ง.1 แผนภาพคลาสของระบบสั่งซื้อสินค้าออนไลน์ที่ไม่มีการระบุข้อมูลทางความมั่นคง .....	112
รูปที่ ง.2 แผนภาพคลาสของระบบสั่งซื้อสินค้าออนไลน์โดยใช้ยูเอ็มแอลเซคเอสพี-2 .....	114
รูปที่ ง.3 แผนภาพคลาสของระบบบริการการบันทึกเหตุการณ์ที่ไม่มีการระบุข้อมูลทางความมั่นคง .....	116
รูปที่ ง.4 แผนภาพคลาสของระบบบริการการบันทึกเหตุการณ์โดยใช้ยูเอ็มแอลเซคเอสพี-2 .....	118
รูปที่ ง.5 แผนภาพคลาสของระบบบริการความมั่นคงสำหรับองค์กรที่ไม่มีการระบุข้อมูลทางความมั่นคง .....	119
รูปที่ ง.6 แผนภาพคลาสของระบบบริการความมั่นคงสำหรับองค์กรโดยใช้ยูเอ็มแอลเซคเอสพี-2.....	120
รูปที่ จ.1 แบบรูปความมั่นคงในเครื่องมือต้นแบบ .....	121
รูปที่ จ.2 แผนภาพกิจกรรมแสดงการทำงานของเครื่องมือต้นแบบสำหรับแสดงแบบรูปความมั่นคง .....	122
รูปที่ จ.3 ขั้นตอนการเข้าใช้แบบรูปความมั่นคงในโปรแกรมสตาร์ยูเอ็มแอล .....	122
รูปที่ จ.4 หน้าต่างสำหรับเลือกแบบรูปความมั่นคง.....	123
รูปที่ จ.5 หน้าจอหลักแสดงคำอธิบายแบบรูปความมั่นคงที่เลือก .....	123
รูปที่ จ.6 หน้าต่างแสดงรายละเอียดของแบบรูปความมั่นคงที่เลือก .....	124
รูปที่ จ.7 หน้าต่างสำหรับการสร้างหรือเลือกคลาสที่เป็นองค์ประกอบของแบบรูปความมั่นคง .....	124
รูปที่ จ.8 หน้าต่างแสดงคำอธิบายของคลาสที่เลือก.....	125
รูปที่ จ.9 หน้าต่างแสดงการยืนยันการใช้แบบรูปความมั่นคง.....	125

รูปที่ จ.10 ผลลัพธ์จากการใช้แบบรูปการระบุความต้องการความมั่นคง สำหรับสินทรัพย์องค์กรโดยใช้เครื่องมือต้นแบบ .....	126
รูปที่ ช.1 แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพี-2 ของกลุ่มแบบรูป การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง .....	136
รูปที่ ช.2 แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพี-2 ของกลุ่มแบบรูป การระบุตัวตนและการพิสูจน์ตัวตน .....	137
รูปที่ ช.3 แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพี-2 ของกลุ่มแบบรูป การบันทึกเหตุการณ์ .....	138



ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

# บทที่ 1

## บทนำ

### 1.1 ที่มาและความสำคัญของงานวิจัย

ในปัจจุบันความต้องการความมั่นคง (Security Requirements) [1] มีความสำคัญต่อการพัฒนาระบบเป็นอย่างมาก ทั้งนี้เพราะเป็นความต้องการที่เกี่ยวข้องกับจุดอ่อนของระบบ และวิธีป้องกันจุดอ่อนดังกล่าวจากการถูกโจมตี ซึ่งจะช่วยให้ระบบที่พัฒนาขึ้นนั้นมีประสิทธิภาพในการทำงานมากที่สุด ซึ่งเป็นที่มาของแบบรูปความมั่นคง (Security Patterns) [2,3] ที่ถูกเสนอเพื่อช่วยแก้ไขปัญหาการออกแบบความต้องการความมั่นคงของระบบ โดยแบบรูปความมั่นคงจะอธิบายถึงแนวทางหรือผลเฉลยของปัญหาทางด้านความมั่นคงต่างๆ ที่ถูกแก้ปัญหาไว้แล้ว นอกจากนี้ยังสนับสนุนการนำกลับมาใช้ใหม่อีกด้วย โดย D.M. Kienzle และคณะ [4] ได้เสนอแบบรูปความมั่นคงสำหรับการแก้ไขปัญหาการออกแบบความมั่นคงของเว็บไซต์ อีกทั้ง M. Schumacher และคณะ [3] ได้เสนอแบบรูปความมั่นคงสำหรับแก้ไขปัญหาการออกแบบความมั่นคงของระบบทั่วไป

อย่างไรก็ตามการศึกษาและวิเคราะห์แบบรูปความมั่นคงเพื่อนำมาประยุกต์ใช้ในการออกแบบซอฟต์แวร์นั้นทำได้ยาก เนื่องจากผู้พัฒนาต้องศึกษาและทำความเข้าใจโครงสร้างคุณสมบัติ เงื่อนไขบังคับ และผลเฉลยของแบบรูปความมั่นคง ซึ่งหากไม่ศึกษาและวิเคราะห์ให้เข้าใจอย่างถ่องแท้ อาจทำให้เกิดผลเสียต่อระบบตามมากภายหลังได้ เช่น ระบบที่พัฒนาไม่มีความปลอดภัยไม่เพียงพอ ทำให้ผู้โจมตีมองเห็นจุดอ่อนของระบบได้โดยง่าย หรือข้อมูลของระบบถูกขโมยหรือทำลาย เป็นต้น

ยูเอ็มแอลเซค (UMLsec) [5,6] เป็นส่วนขยายของยูเอ็มแอลที่สนับสนุนการแสดงโครงสร้างในรูปของแผนภาพคลาสสำหรับพัฒนาระบบความมั่นคง แต่ยูเอ็มแอลเซคสามารถออกแบบได้ในสภาพแวดล้อมหนึ่งเท่านั้น ซึ่งไม่สอดคล้องตามแบบรูปความมั่นคง อีกทั้งยังมีการแสดงโครงสร้างของแบบรูปความมั่นคงได้ไม่ชัดเจนเท่าที่ควร เช่น ขาดองค์ประกอบที่ระบุโครงสร้างของแบบรูปความมั่นคง ขาดอิสระในการตั้งชื่อคลาสหรือองค์ประกอบอื่น เนื่องจากต้องตั้งชื่อให้สอดคล้องกับหน้าที่ในแบบรูปความมั่นคง เป็นต้น

ดังนั้นงานวิทยานิพนธ์นี้ จึงมีแนวคิดที่จะปรับปรุงยูเอ็มแอล เพื่อช่วยให้ผู้พัฒนาเข้าใจถึงโครงสร้างของแบบรูปความมั่นคงในยูเอ็มแอลได้อย่างชัดเจน อีกทั้งทำให้รู้ว่ามีการดำเนินการ (Operation) หรือคุณลักษณะ (Attribute) ใดที่ต้องจัดเก็บเพื่อตอบสนองการใช้งานในการออกแบบระบบทางด้านความมั่นคง และสอดคล้องกับความต้องการทางด้านความมั่นคงมากที่สุด

โดยผู้วิจัยมุ่งเน้นในการศึกษา วิเคราะห์และขยายยูเอ็มแอลเพื่อแสดงแบบรูปความมั่นคง ซึ่งจะใช้แบบรูปความมั่นคงที่นำเสนอในหนังสือ แบบรูปความมั่นคง การบูรณาการความ



มั่นคงและวิศวกรรมระบบ (Security Patterns: Integrating Security and Systems Engineering) ที่นำเสนอโดย M. Schumacher และคณะ ที่แตกต่างไปจากแบบรูปความมั่นคงที่เกียรติกศักดิ์ ไชยสมบูรณ์ และคณะ [12] ได้ทำได้ จากนั้นทำการปรับปรุงยูเอ็มแอล เพื่อให้มีความเหมาะสมสำหรับนำมาใช้งานในการออกแบบและพัฒนาซอฟต์แวร์ และปรับปรุงส่วนที่มีความซ้ำซ้อนกัน พร้อมทั้งพัฒนาเครื่องมือที่ช่วยสนับสนุนการใช้งานแบบรูปความมั่นคง ซึ่งการออกแบบระบบความมั่นคงโดยใช้แบบรูปความมั่นคงนั้น จะช่วยให้ระบบมีประสิทธิภาพมากยิ่งขึ้น

## 1.2 วัตถุประสงค์ของงานวิจัย

- 1) ขยายยูเอ็มแอลเพื่อรองรับการสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง
- 2) สร้างโปรแกรมเสริม (Plug-in Program) จากโอเพนซอร์ซ (Open Source) โดยนำยูเอ็มแอลเซคเอสพี-2 (UMLsec SP-2) มาประยุกต์ใช้ในการแสดงโครงสร้างของแบบรูปความมั่นคง

## 1.3 ขอบเขตของงานวิจัย

**1.3.1** นำเสนอส่วนขยายของยูเอ็มแอลที่ทำการปรับปรุงเพิ่มเติมจากทั้งยูเอ็มแอล ยูเอ็มแอลเซค และยูเอ็มแอลเซคเอสพี นั้นคือ ยูเอ็มแอลเซคเอสพี-2 ทั้งนี้เพื่อสนับสนุนการแสดงผลแบบรูปความมั่นคง โดยใช้แบบรูปความมั่นคงที่ได้รับการออกแบบและตรวจสอบความถูกต้องแล้ว 3 กลุ่มแบบรูป ดังต่อไปนี้

### 1) การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)

- 1.1) การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Asset)
- 1.2) การกำหนดมูลค่าสินทรัพย์ (Asset Valuation)
- 1.3) การประเมินภัยคุกคาม (Threat Assessment)
- 1.4) การประเมินภาวะเสี่ยง (Vulnerability Assessment)
- 1.5) การกำหนดค่าความเสี่ยง (Risk Determination)
- 1.6) แนวคิดความมั่นคงองค์กร (Enterprise Security Approaches)
- 1.7) บริการความมั่นคงองค์กร (Enterprise Security Services)
- 1.8) การสื่อสารของหุ้นส่วนองค์กร (Enterprise Partner Communication)

### 2) การระบุตัวตนและการพิสูจน์ตัวตน (Identification and Authentication)

- 2.1) ความต้องการการระบุและการพิสูจน์ตัวตน (I&A Requirement)
- 2.2) ทางเลือกการออกแบบสำหรับการระบุตัวตน และการพิสูจน์ตัวตนอัตโนมัติ (Automated I&A Design Alternatives)
- 2.3) การออกแบบและใช้รหัสผ่าน (Password Design and Use)

#### 2.4) ทางเลือกการออกแบบชีวมิติ (Biometrics Design Alternatives)

### 3) การบันทึกเหตุการณ์ (Accounting)

3.1) ความต้องการความมั่นคงในการบันทึกเหตุการณ์ (Security Accounting Requirements)

3.2) ความต้องการการตรวจสอบ (Audit Requirements)

3.3) ความต้องการหลักฐานการตรวจสอบและการบันทึก (Audit Trails and Logging Requirements)

3.4) ความต้องการการป้องกันการบุกรุก (Intrusion Detection Requirements)

3.5) ความต้องการการยอมรับ (Non-Repudiation Requirements)

1.3.2 สร้างโปรแกรมเสริมสำหรับนำยูเอมแอลเซคเอสพี-2 มาประยุกต์ใช้

1.3.3 ทดสอบความถูกต้องของเครื่องมือ โดยใช้แบบรูปความมั่นคงที่ครอบคลุมแบบรูปความมั่นคงในงานวิทยานิพนธ์นี้มาแสดงในแผนภาพยูเอมแอล

#### 1.4 ขั้นตอนของการวิจัย

- 1) ศึกษาแบบรูปความมั่นคงของ M. Schumacher [3] ยูเอมแอลเซค และยูเอมแอลเซคเอสพี
- 2) วิเคราะห์แบบรูปความมั่นคงเพื่อหาโครงสร้างขององค์ประกอบที่สำคัญต่อการออกแบบ
- 3) ออกแบบแบบรูปความมั่นคงโดยใช้ยูเอมแอล ยูเอมแอลเซค และยูเอมแอลเซคเอสพี
- 4) วิเคราะห์การออกแบบแบบรูปความมั่นคงโดยใช้ยูเอมแอล ยูเอมแอลเซค และยูเอมแอลเซคเอสพี
- 5) ปรับปรุงยูเอมแอลเพื่อสนับสนุนการออกแบบแบบรูปความมั่นคงได้อย่างเหมาะสม
- 6) ตรวจสอบยูเอมแอลเซคเอสพี-2
- 7) ศึกษาโอเพนซอร์ซสำหรับสร้างส่วนขยายของยูเอมแอล
- 8) ออกแบบและพัฒนาเครื่องมือสำหรับแสดงแบบรูปความมั่นคง
- 9) สรุปผลการวิจัย
- 10) จัดทำรายงานวิทยานิพนธ์

#### 1.5 ประโยชน์ที่คาดว่าจะได้รับ

- 1) ได้ยูเอมแอลที่ปรับปรุงเพิ่มเติมสำหรับสนับสนุนการแสดงแบบรูปความมั่นคง
- 2) ได้โปรแกรมเสริมสำหรับสนับสนุนการแสดงแบบรูปความมั่นคง
- 3) สนับสนุนการใช้แบบรูปความมั่นคงในการออกแบบได้อย่างมีแบบแผน และมีประสิทธิภาพมากขึ้น
- 4) สามารถนำแบบรูปความมั่นคงดังกล่าว ไปใช้ในกระบวนการต่างๆ ของการพัฒนาซอฟต์แวร์ได้

## บทที่ 2

### ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในบทนี้จะกล่าวถึง ทฤษฎีที่สำคัญสำหรับนำมาสนับสนุนการทำงานวิทยานิพนธ์นี้ รวมถึงงานวิจัยต่างๆ ที่เกี่ยวข้อง โดยมีรายละเอียดดังนี้

#### 2.1 ทฤษฎีที่เกี่ยวข้อง

##### 2.1.1 แผนภาพยูเอ็มแอล (Unified Modeling Language: UML)

แผนภาพยูเอ็มแอล [7,8] เป็นภาษารูปภาพหรือสัญลักษณ์ (Graphical Language) ที่กำหนดมาตรฐานโดยโอเอ็มจี (Object Management Group: OMG) เพื่อใช้อธิบาย แสดง รายละเอียด หรือจำลองระบบ ซึ่งใช้นำเสนอแนวความคิดของการเขียนโปรแกรมเชิงวัตถุ ก่อนนำไปเขียนโปรแกรมจริง

##### 1) ประเภทของแผนภาพยูเอ็มแอล

แผนภาพยูเอ็มแอลสามารถแบ่งออกเป็น 2 กลุ่มหลักๆ ดังตารางที่ 2.1 โดยมี รายละเอียดดังนี้

1.1) แบบจำลองเชิงโครงสร้าง (Structural Model) เป็นแบบจำลองที่แสดงให้เห็นถึงโครงสร้างในส่วนที่ไม่มีการเปลี่ยนแปลงของระบบ

1.2) แบบจำลองเชิงพฤติกรรม (Behavioral Model) เป็นแบบจำลองที่แสดงให้เห็นถึงภาพเชิงกิจกรรมของระบบ อีกทั้งแสดงให้เห็นถึงความสามารถของระบบที่สามารถดำเนินการได้

ตารางที่ 2.1 ประเภทของยูเอ็มแอล [8]

Structural Model	<b>Class Diagram</b>	เป็นแผนภาพที่แสดงแบบจำลองเชิงโครงสร้างของแผนภาพยูเอ็มแอล โดยแสดงให้เห็นถึงอ็อบเจกต์ (Object) หรือคลาส (Class) ในระบบที่มีความสัมพันธ์ต่างๆ ระหว่างคลาส
	<b>Object Diagram</b>	เป็นแผนภาพที่ใช้แสดงกลุ่มของอ็อบเจกต์ และความสัมพันธ์ระหว่างอ็อบเจกต์ ที่เกิดขึ้นในคลาสต่างๆ ของแผนภาพคลาส
	<b>Component Diagram</b>	เป็นแผนภาพที่แสดงถึงโครงสร้างทางกายภาพ (Physical) ของโปรแกรม ประกอบด้วยส่วนประกอบต่างๆ เรียกว่า Component ซึ่งก็คือ ส่วนประกอบย่อยๆ ของซอฟต์แวร์ของระบบงานทั้งหมด
	<b>Deployment Diagram</b>	เป็นแผนภาพที่แสดงโครงสร้างทางด้านฮาร์ดแวร์ของระบบงาน

ตารางที่ 2.1 ประเภทของยูเอ็มแอล [8] (ต่อ)

<b>Behavioral Model</b>	<b>Use Case Diagram</b>	เป็นแผนภาพที่แสดงถึงขั้นตอนการทำงานที่สำคัญของระบบ หรืองานที่ระบบจะต้องทำ เพื่อตอบสนองต่อผู้กระทำ (Actor) ระบบ
	<b>Sequence Diagram</b>	เป็นแผนภาพที่แสดงให้เห็นถึงปฏิสัมพันธ์ (Interaction) หรือการส่งข้อมูลระหว่างคลาสหรืออ็อบเจกต์ตามลำดับเวลา
	<b>Communication Diagram</b>	เป็นแผนภาพที่แสดงให้เห็นถึงปฏิสัมพันธ์ระหว่างอ็อบเจกต์ โดยจะเน้นในส่วนของการแสดงถึงความสัมพันธ์ระหว่างอ็อบเจกต์
	<b>State Machine Diagram</b>	เป็นแผนภาพที่ใช้แสดงสถานะต่างๆ และการเปลี่ยนสถานะของคลาส ตั้งแต่เริ่มต้นการทำงานจนถึงสิ้นสุดการทำงาน
	<b>Activity Diagram</b>	เป็นแผนภาพที่แสดงให้เห็นถึงลำดับการดำเนินกิจกรรม (Activity) จากกิจกรรมหนึ่งไปยังกิจกรรมหนึ่งภายในระบบ

## 2) แผนภาพยูเอ็มแอลที่เกี่ยวข้องกับงานวิจัยนี้

**แผนภาพคลาส (Class Diagram)** เป็นแบบจำลองเชิงโครงสร้าง ที่แสดงถึงโครงสร้างของระบบ อีกทั้งยังแสดงให้เห็นถึงอ็อบเจกต์หรือคลาส ในระบบที่มีความสัมพันธ์ (Relationship) ระหว่างคลาส โดยองค์ประกอบของแผนภาพคลาส จะประกอบไปด้วยส่วนสำคัญต่างๆ ดังต่อไปนี้

**2.1) คลาส** เป็นการอธิบายคุณลักษณะของอ็อบเจกต์หรือคลาส โดยสัญลักษณ์ของคลาสเป็นรูปสี่เหลี่ยม ซึ่งแบ่งออกเป็น 3 ส่วนหลัก ได้แก่ ชื่อคลาส (Class Name) แอททริบิวต์ (Attribute) และโอเปอเรชัน (Operation)

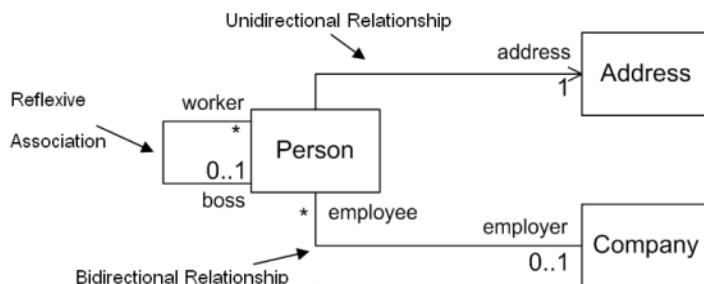
- **ชื่อคลาส** เป็นการบอกชื่อชนิดของคลาส โดยชื่อของแต่ละคลาสจะต้องไม่ซ้ำกัน

- **แอททริบิวต์** แสดงคุณลักษณะของคลาส โดยสามารถระบุความสามารถในการมองเห็น (Visibility) ชนิดของข้อมูล (Data Type) และค่าเริ่มต้นของข้อมูล (Initial Value)

- **โอเปอเรชัน** แสดงถึงการกระทำหรือฟังก์ชันของอ็อบเจกต์ที่คลาสสามารถดำเนินการได้ โดยสามารถระบุความสามารถในการมองเห็น พารามิเตอร์ (Parameter) รวมทั้งชนิดของการคืนค่า (Return Type) ของการดำเนินการ

**2.2) ความสัมพันธ์ระหว่างคลาส** เกิดจากการติดต่อกันของคลาส ซึ่งแสดงด้วยเส้นที่เชื่อมระหว่างคลาส นอกจากนี้ความสัมพันธ์ยังมีทิศทางของเส้นความสัมพันธ์ด้วย ได้แก่ ความสัมพันธ์แบบ 1 ทิศทาง (Unidirectional Relationship) ความสัมพันธ์แบบ 2 ทิศทาง

(Bidirectional Relationship) และเส้นความสัมพันธ์ภายในตัวเอง (Reflexive Association)  
 ดังรูปที่ 2.1

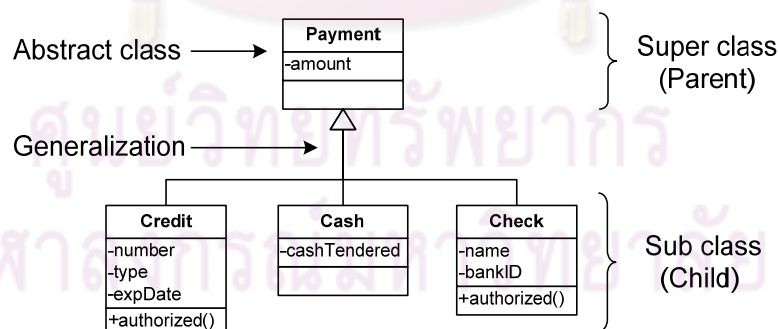


รูปที่ 2.1 ความสัมพันธ์ของคลาส [8]

จากรูปที่ 2.1 แผนภาพคลาสประกอบไปด้วย คลาส Person, Address และ Company โดยที่เส้นความสัมพันธ์ระหว่างคลาส Person กับคลาส Address เป็นแบบทิศทางเดียวโดยมีหัวลูกชี้ไปยังคลาส Address ซึ่งหมายความว่า คลาส Person สามารถเรียกใช้โอเปอเรชันของคลาส Address ได้ แต่คลาส Address ไม่สามารถเรียกใช้โอเปอเรชันของคลาส Person ได้ ส่วนเส้นความสัมพันธ์ระหว่างคลาส Person กับคลาส Company เป็นแบบ 2 ทิศทาง หมายความว่า อ็อบเจกต์ทั้ง 2 คลาสสามารถเรียกใช้งานโอเปอเรชันกันได้ และเส้นความสัมพันธ์ภายในคลาส Person หมายความว่า อ็อบเจกต์ของคลาส Person สามารถเรียกใช้งานโอเปอเรชันของคลาสตัวเองได้

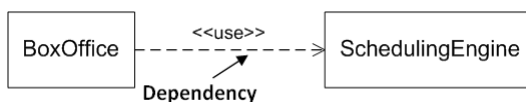
ความสัมพันธ์ระหว่างคลาส แบ่งเป็น 5 ความสัมพันธ์ดังนี้

- **ความสัมพันธ์แบบเจนเนอรัลไลเซชัน (Generalization)** เป็นความสัมพันธ์ที่แสดงการรับทอดคุณลักษณะจากซูเปอร์คลาส (Super Class) ไปยังซับคลาส (Sub Class) โดยที่ซับคลาสสามารถใช้ข้อมูลและโอเปอเรชันในซูเปอร์คลาสได้ ดังรูปที่ 2.2



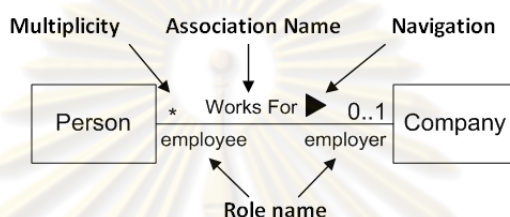
รูปที่ 2.2 ความสัมพันธ์แบบเจนเนอรัลไลเซชัน [8]

- **ความสัมพันธ์แบบดีเพนเดนซี (Dependency)** เป็นความสัมพันธ์ระหว่างคลาสแบบขึ้นแก่กัน โดยมีเส้นประที่มีหัวลูกศรชี้ไปยังคลาสที่ถูกเรียกใช้ หากมีการเปลี่ยนแปลงกับคลาสที่ถูกเรียกใช้ ก็จะส่งผลกระทบต่อคลาสที่ทำการเรียกใช้ได้ ดังรูปที่ 2.3



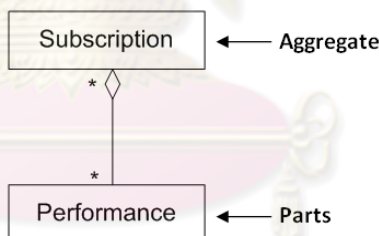
รูปที่ 2.3 ความสัมพันธ์แบบดีเพนเดนซี [8]

- ความสัมพันธ์แบบแอสโซซิเอชัน (**Association**) เป็นการแสดงให้เห็นถึงความสัมพันธ์ระหว่างอ็อบเจกต์ โดยจะแสดงด้วยเส้นที่บ่งเชื่อมต่อบetween คลาสที่มีความสัมพันธ์กัน บนเส้นความสัมพันธ์อาจมีการระบุชื่อความสัมพันธ์ (Association Name) ทิศทางความสัมพันธ์ (Navigation) บทบาท (Role Name) และมัลติพลิซิตี (Multiplicity) เพื่อบอกจำนวนที่เป็นไปได้ของอ็อบเจกต์ของคลาส ดังรูปที่ 2.4



รูปที่ 2.4 ความสัมพันธ์แบบแอสโซซิเอชัน [8]

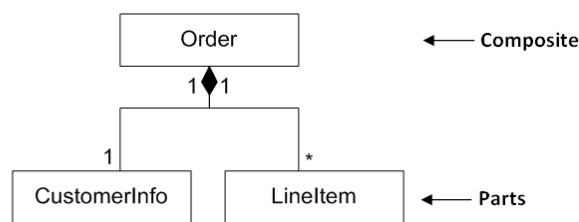
- ความสัมพันธ์แบบแอกกรีเกชัน (**Aggregation**) เป็นความสัมพันธ์ระหว่างคลาสที่มีลักษณะเป็นองค์ประกอบ คือการที่อ็อบเจกต์หนึ่งมีอ็อบเจกต์อื่นๆ เป็นส่วนประกอบ โดยเมื่อลบคลาสหลักทิ้ง คลาสที่เป็นส่วนประกอบก็สามารถคงอยู่ได้ ดังรูปที่ 2.5



รูปที่ 2.5 ความสัมพันธ์แบบแอกกรีเกชัน [8]

จากรูป แผนภาพประกอบด้วยคลาส Subscription และ Performance ที่มีความสัมพันธ์แบบแอกกรีเกชัน โดยอ็อบเจกต์ของคลาส Performance เป็นส่วนประกอบของอ็อบเจกต์ของคลาส Subscription ได้หลายอ็อบเจกต์ และอ็อบเจกต์ของคลาส Subscription สามารถมีอ็อบเจกต์ของคลาส Performance ได้หลายอ็อบเจกต์ เมื่อลบอ็อบเจกต์ของคลาส Subscription ออก อ็อบเจกต์ของคลาส Performance ก็ยังสามารถทำงานได้

- ความสัมพันธ์แบบคอมโพสิชัน (**Composition**) เป็นความสัมพันธ์แบบแอกกรีเกชันที่เข้มงวดขึ้น (Strong) ซึ่งจะมีช่วงชีวิตร่วมกัน โดยช่วงชีวิตของคลาสที่เป็นส่วนประกอบขึ้นอยู่กับคลาสหลัก นั่นคือ เมื่อลบคลาสหลักไป คลาสที่เป็นส่วนประกอบก็จะถูกลบไปด้วย ดังรูปที่ 2.6



รูปที่ 2.6 ความสัมพันธ์แบบคอมโพสิชัน [8]

จากรูป แผนภาพประกอบด้วยคลาส Order คลาส CustomerInfo และคลาส Lineltem ที่มีความสัมพันธ์แบบคอมโพสิชัน โดยอ็อบเจกต์ของคลาส CustomerInfo เป็นส่วนประกอบของ อ็อบเจกต์ของคลาส Order ได้เพียงอ็อบเจกต์เดียวเท่านั้น และอ็อบเจกต์ของคลาส Order มีอ็อบเจกต์ของคลาส CustomerInfo เป็นส่วนประกอบได้เพียงอ็อบเจกต์เดียวเหมือนกัน และอ็อบเจกต์ของคลาส Lineltem เป็นส่วนประกอบของอ็อบเจกต์ของคลาส Order ได้เพียงอ็อบเจกต์เดียวเท่านั้น แต่อ็อบเจกต์ของคลาส Order สามารถมีอ็อบเจกต์ของคลาส Lineltem เป็นส่วนประกอบได้หลายอ็อบเจกต์ และเมื่ออ็อบเจกต์ของคลาส Order ถูกลบไป อ็อบเจกต์ของคลาส CustomerInfo และอ็อบเจกต์ของคลาส Lineltem ก็ถูกลบไปด้วย

### 2.3) มัลติพลิซิติ

ในการพิจารณาความสัมพันธ์ระหว่างคลาส สิ่งที่ต้องคำนึงถึงคือ ค่าที่เป็นไปได้ของจำนวนสมาชิกในคลาสหนึ่งๆ ที่มีความสัมพันธ์กันนั้นเป็นเท่าใด โดยตัวเลขแสดงความสัมพันธ์นี้คือ ค่าของจำนวนสมาชิกของคลาสที่เป็นไปได้ในความสัมพันธ์นั้นๆ ซึ่งทำให้ความสัมพันธ์ระหว่างคลาสมีความชัดเจนมากยิ่งขึ้น โดยใช้ตัวเลขแสดงความสัมพันธ์ต่างๆ ดังตารางที่ 2.2

ตารางที่ 2.2 ความหมายของตัวเลขแสดงความสัมพันธ์ [8]

มัลติพลิซิติ	ความหมาย
-	ไม่ระบุ (unspecified)
1	เพียงหนึ่ง (one)
0..1	ศูนย์หรือหนึ่ง (zero or one)
0..*	ศูนย์หรือมากกว่า (zero or more)
1..*	หนึ่งหรือมากกว่า (one or more)
2..4	กำหนดเป็นช่วง 2 ถึง 4 (specified range)
2,4..10	กำหนด 2, 4 ถึง 10 (specified range)

#### 2.1.2 ยูเอ็มแอลโพรไฟล์ (UML Profiles)

ยูเอ็มแอลโพรไฟล์ [8,9] เป็นองค์ประกอบหนึ่งของแผนภาพยูเอ็มแอล ที่รองรับผู้ใช้ให้สามารถปรับเปลี่ยนหรือกำหนดกฎให้เหมาะสมกับโดเมน (Domain) ที่ต้องการใช้งานได้ โดยมีส่วนประกอบ 3 ส่วนดังนี้

### 1) แม่พิมพ์ต้นแบบ (Stereotype)

แม่พิมพ์ต้นแบบ เป็นชนิดหนึ่งของส่วนประกอบของแบบจำลอง (Model Element) ที่ถูกกำหนดในแบบจำลอง ซึ่งช่วยในการรวมกลุ่มของข้อมูลที่เกี่ยวข้องกันเข้าด้วยกัน แม่พิมพ์ต้นแบบแสดงโดยเครื่องหมาย “<< >>” ล้อมรอบข้อความอักษรซึ่งจะอยู่ภายในหรือใกล้กับสัญลักษณ์ของส่วนประกอบของแบบจำลอง

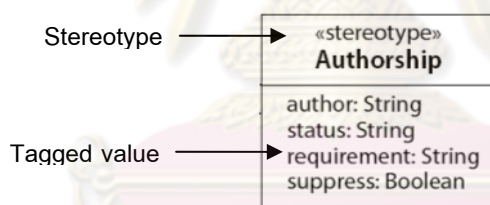
### 2) ค่าป้ายระบุ (Tagged Value)

ค่าป้ายระบุ เป็นข้อมูลเฉพาะในแม่พิมพ์ต้นแบบ ค่าป้ายระบุช่วยกำหนดคุณลักษณะของแม่พิมพ์ต้นแบบ เช่น ค่าป้ายระบุชื่อคลาส แสดงถึงชื่อของคลาสในแม่พิมพ์ต้นแบบ เป็นต้น

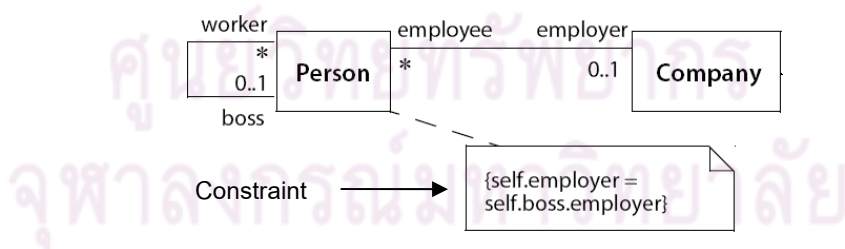
### 3) เงื่อนไขบังคับ (Constraint)

เงื่อนไขบังคับ เป็นข้อบังคับที่จำเป็นต้องพิจารณาเพื่อบอกถึงเงื่อนไขในการใช้งานแม่พิมพ์ต้นแบบหรือค่าป้ายระบุ อีกทั้งเงื่อนไขบังคับยังช่วยกำหนดขอบเขตของการใช้แม่พิมพ์ต้นแบบหรือค่าป้ายระบุ ซึ่งโดยทั่วไปเงื่อนไขบังคับจะถูกเขียนด้วยภาษาโอซีแอล (Object Constraint Language: OCL) ทั้งนี้เพราะภาษาโอซีแอลเป็นภาษามาตรฐานในการระบุข้อบังคับของยูเอ็มแอล

โดยแสดงตัวอย่างแม่พิมพ์ต้นแบบและค่าป้ายระบุ ดังรูปที่ 2.7 และตัวอย่างเงื่อนไขบังคับ ดังรูปที่ 2.8



รูปที่ 2.7 ตัวอย่างแม่พิมพ์ต้นแบบและค่าป้ายระบุ [8]



รูปที่ 2.8 ตัวอย่างเงื่อนไขบังคับ [8]

จากรูปที่ 2.7 คลาส Authorship มีการสร้างแม่พิมพ์ต้นแบบเป็น stereotype และมีการสร้างค่าป้ายระบุ 4 ตัว ได้แก่ ป้ายระบุ author ที่มีชนิดเป็น String, ป้ายระบุ status ที่มีชนิดเป็น String, ป้ายระบุ requirement ที่มีชนิดเป็น String และป้ายระบุ suppress ที่มีชนิดเป็น Boolean และจากรูปที่ 2.8 คลาส Person ในแผนภาพคลาส มีเงื่อนไขบังคับคือ self.employer=self.boss.employer



### 2.1.3 แบบรูปและแบบรูปความมั่นคง (Patterns and Security Patterns)

แบบรูป [2,3] คือปัญหาและผลเฉลยสำหรับปัญหาการออกแบบทั่วไปที่เคยปรากฏในอดีต โดยนำมาแก้ปัญหาที่ปรากฏใหม่ซึ่งมีลักษณะคล้ายกับปัญหาเดิมในแบบรูปนั้น ซึ่งช่วยให้ผู้ใช้สามารถเข้าใจและนำไปใช้ได้โดยไม่ต้องอาศัยความรู้หรือประสบการณ์มากนัก นอกจากนี้แบบรูปยังสนับสนุนความสามารถในการนำกลับมาใช้ใหม่ โดยแบบรูปประกอบด้วย 3 ส่วนหลัก คือ ปัญหา ลักษณะ และผลเฉลย แต่การนำแบบรูปไปใช้นั้น อาจมีองค์ประกอบอื่นเพิ่มเติม เพื่อช่วยให้แบบรูปมีความสมบูรณ์และง่ายต่อการนำไปใช้ เช่น ชื่อแบบรูป (Pattern Name) ฟอर्स (Force) ผลลัพธ์เชิงบริบท (Resulting Context) แบบรูปที่เกี่ยวข้อง (Related Patterns) รวมทั้งองค์ประกอบสนับสนุนที่จะช่วยในการอธิบายผลเฉลยของแบบรูปนั้นๆ เช่น ตัวอย่างการใช้งาน (Example) หรือแผนภาพคลาส เป็นต้น องค์ประกอบเพิ่มเติมเหล่านี้จะขึ้นอยู่กับกรนำแบบรูปไปใช้งาน เพื่อให้สามารถสนับสนุนการใช้งานหรือสามารถทำความเข้าใจกับปัญหาได้ชัดเจนมากยิ่งขึ้น

แบบรูปความมั่นคง [2,3] เป็นแบบรูปที่นำเสนอปัญหาความมั่นคงที่เคยปรากฏในอดีต รวมทั้งผลเฉลยที่พิสูจน์แล้วว่าสามารถแก้ไขปัญหาได้เป็นอย่างดี อีกทั้งยังสามารถประยุกต์ใช้กับการออกแบบโครงสร้างของการแก้ปัญหาความมั่นคงได้อย่างเป็นรูปธรรม เนื่องจากแบบรูปความมั่นคงดังกล่าวได้รวบรวมองค์ความรู้ทางด้านความมั่นคงไว้อย่างมีโครงสร้าง จากผู้ชำนาญการด้านความมั่นคง วิศวกรรมความมั่นคง และวิศวกรรมซอฟต์แวร์ โดยแบบรูปความมั่นคงสามารถแบ่งได้เป็น 3 ประเภท ได้แก่

1) แบบรูปการวิเคราะห์ความมั่นคง (Security Analysis Patterns) เป็นแบบรูปที่แก้ปัญหาการวิเคราะห์ความมั่นคงของระบบ

2) แบบรูปการออกแบบความมั่นคง (Security Design Patterns) เป็นแบบรูปที่แก้ปัญหาการออกแบบโครงสร้างความมั่นคงของระบบ

3) แบบรูปกระบวนการความมั่นคง (Security Process Patterns) เป็นแบบรูปที่แก้ปัญหาการออกแบบความมั่นคงให้กับกระบวนการของระบบ

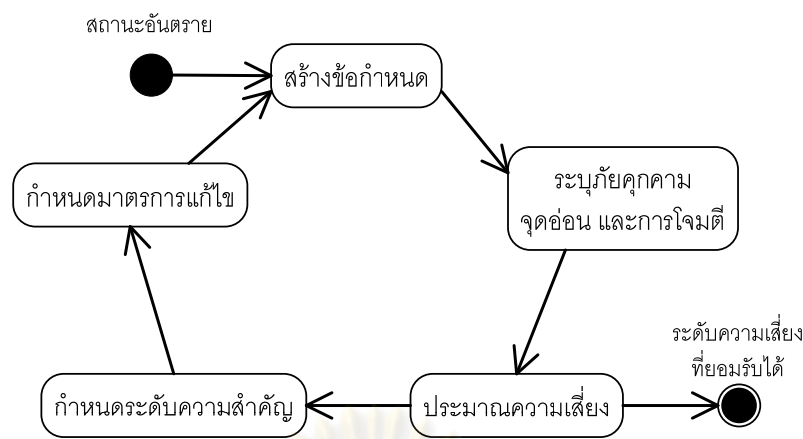
แบบรูปความมั่นคงที่จะนำมาใช้ในงานวิทยานิพนธ์ฉบับนี้ มาจากแบบรูปความมั่นคงของ M.Schumacher และคณะ ที่นำเสนอในหนังสือแบบรูปความมั่นคง การบูรณาการความมั่นคงและวิศวกรรมระบบ (Security Patterns: Integrating Security and Systems Engineering) ซึ่งเป็นแบบรูปที่ได้รับความนิยมและสามารถนำไปประยุกต์ใช้กับการพัฒนาระบบด้านความมั่นคงได้เป็นอย่างดี

องค์ประกอบของแบบรูปความมั่นคงดังกล่าว จะประกอบด้วย 14 องค์ประกอบ ซึ่งในแต่ละแบบรูปความมั่นคงไม่จำเป็นต้องมีองค์ประกอบครบทั้งหมด โดยจะขึ้นอยู่กับความเหมาะสมของการนำไปใช้สำหรับปัญหาด้านความมั่นคงปัญหาใดปัญหาหนึ่ง โดยองค์ประกอบของแบบรูปความมั่นคง มีดังต่อไปนี้

- 1) ชื่อ (Name) เป็นชื่อของแบบรูปความมั่นคง
- 2) ชื่อที่รู้จัก (Also Known As) เป็นชื่ออื่นของแบบรูปความมั่นคง
- 3) ตัวอย่าง (Example) เป็นตัวอย่างที่แสดงถึงปัญหาและความต้องการของแบบรูปความมั่นคง
- 4) บริบท (Context) เป็นสถานการณ์ที่ควรใช้แบบรูปความมั่นคง
- 5) ปัญหา (Problem) เป็นปัญหาที่แบบรูปความมั่นคงต้องแก้ไข
- 6) ผลเฉลย (Solution) เป็นคำตอบภายใต้แบบรูปความมั่นคง
- 7) โครงสร้าง (Structure) เป็นรายละเอียดโครงสร้างของแบบรูปความมั่นคง
- 8) ไคนามิก (Dynamics) เป็นเหตุการณ์ที่อธิบายถึงการทำงานของแบบรูปความมั่นคง
- 9) การทำให้เกิดผล (Implementation) เป็นการแนะนำในการทำให้เกิดผล
- 10) ตัวอย่างการแก้ไข (Example Resolved) เป็นตัวอย่างที่การแก้ไขปัญหาคด้วยแบบรูปความมั่นคง
- 11) รูปแปร (Variants) เป็นคำอธิบายของแบบรูปความมั่นคงที่มีลักษณะแตกต่างหรือพิเศษออกไป
- 12) การนำไปใช้ที่ทราบ (Know Uses) เป็นตัวอย่างของการใช้แบบรูปความมั่นคงในระบบความเป็นจริง
- 13) ผลที่ได้ (Consequence) เป็นประโยชน์ที่ได้จากแบบรูปความมั่นคง
- 14) เห็นได้จาก (See Also) เป็นการอ้างถึงแบบรูปความมั่นคงอื่นที่แก้ไขปัญหาคเดียวกัน

#### 2.1.4 วิศวกรรมความมั่นคง (Security Engineering)

วิศวกรรมความมั่นคง [1] คือ การนำทฤษฎีความมั่นคง (Security Theory) มาใช้ในการปฏิบัติความมั่นคง (Security Practice) ซึ่งจะทำการออกแบบและสร้างระบบให้สามารถป้องกันการบุกรุกหรือโจมตีระบบได้ โดยมีจุดมุ่งหมายเพื่อลดระดับความรุนแรงที่อาจจะเกิดขึ้นกับระบบ หรือเปลี่ยนแปลงสถานะจากอันตรายเป็นสถานะความเสี่ยงที่ยอมรับได้ โดยแสดงกระบวนการวิศวกรรมความมั่นคง ดังรูปที่ 2.9



รูปที่ 2.9 ขั้นตอนวิธีทางวิศวกรรมความมั่นคง [1]

1) **ข้อกำหนด (Specification)** เป็นองค์ประกอบ (Components) และส่วนต่อประสาน (Interface) ทั้งหมดที่ต้องกำหนดให้ครบถ้วนสมบูรณ์ หากไม่ครอบคลุมข้อกำหนดของสถาปัตยกรรมทั้งหมดของระบบ จะก่อให้เกิดช่องโหว่ ภัยอันตราย และการถูกโจมตี ในส่วนที่ไม่ได้ทำการระบุเป็นข้อกำหนดไว้

2) **การระบุภัยคุกคาม จุดอ่อน และการโจมตี (Identification of Threats, Vulnerabilities and Attacks)** เป็นการระบุภัยอันตรายและจุดอ่อนของแต่ละองค์ประกอบ รวมถึงส่วนต่อประสานของระบบที่ได้ระบุไว้แล้ว ซึ่งจะช่วยในการกำหนดรูปแบบการโจมตีที่อาจจะเกิดขึ้นอีกทั้งยังสามารถหาวิธีป้องกันการโจมตีก่อนที่จะเกิดเหตุการณ์นั้นขึ้น

3) **การประมาณความเสี่ยง (Risk Estimation)** องค์ประกอบหรือส่วนต่อประสานของระบบอาจมีความเสี่ยงต่อการถูกโจมตีได้ ดังนั้นจึงต้องทำการพิจารณาความสัมพันธ์ระหว่างข้อกำหนดของภัยคุกคาม จุดอ่อนและรูปแบบการโจมตีเพื่อที่จะประมาณความเสี่ยงที่อาจจะเกิดขึ้น

4) **การกำหนดระดับความสำคัญ (Prioritization)** เป็นขั้นตอนที่สำคัญอย่างมากในการกำหนดมาตรการป้องกัน โดยหากพบว่าองค์ประกอบหรือส่วนต่อประสานใดของระบบมีความเสี่ยงสูง จะต้องให้ความสำคัญไว้เป็นลำดับต้นๆ

5) **มาตรการแก้ไข (Countermeasure)** เป็นวิธีการรับมือกับการโจมตีที่จะเกิดขึ้น โดยทำการจำแนกภัยคุกคาม จุดอ่อนและรูปแบบการโจมตี โดยขึ้นอยู่กับความสำคัญและประเภทของภัยอันตรายด้วย

ในงานวิทยานิพนธ์นี้ได้ใช้แนวคิดของกระบวนการที่จำเป็นในวิศวกรรมความมั่นคงเป็นแนวทางในการแสดงโครงสร้างของแบบรูปความมั่นคงในแผนภาพยูเอ็มแอล เช่น การระบุข้อกำหนดขององค์ประกอบและส่วนต่อประสานโดยใช้ยูเอ็มแอล เป็นต้น

## 2.2 งานวิจัยที่เกี่ยวข้อง

### 2.2.1 ยูเอ็มแอลเซค: ส่วนขยายของยูเอ็มแอลเพื่อการพัฒนากระบวนการความมั่นคง (UMLsec: Extending UML for Secure System Development)

ยูเอ็มแอลเซค [5,6] ได้นำเสนอการสร้างส่วนขยายของยูเอ็มแอลบนพื้นฐานของยูเอ็มแอลโพรไฟล์ สำหรับตอบสนองความต้องการการออกแบบโครงสร้างทางด้านความมั่นคงในการพัฒนาความมั่นคงของระบบ โดยแสดงรายละเอียดของแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลเซคที่สร้างมาจากความต้องการดังกล่าว ดังตารางที่ 2.3 และตารางที่ 2.4 ตามลำดับ

ตารางที่ 2.3 แม่พิมพ์ต้นแบบของยูเอ็มแอลเซค

แม่พิมพ์ต้นแบบ	ป้ายระบุ	ข้อบังคับ	คำอธิบาย
fair exchange	start, stop, adversary	ในระบบย่อย หลังจากเข้าสู่กิจกรรมเริ่มต้นแล้ว จะต้องดำเนินสู่กิจกรรมสิ้นสุดเสมอ	การแลกเปลี่ยนกิจกรรมเริ่มต้นและกิจกรรมสิ้นสุดของระบบย่อย
provable	action, cert, adversary	มีกิจกรรมที่ไม่สามารถถกแย้งได้	การระบุกิจกรรมที่ไม่สามารถถกแย้งได้
rbac	protected, role, right	ผู้ใช้งานถูกควบคุมกิจกรรมให้ เป็นไปตามบทบาทของตน	การควบคุมการเข้าถึงเชิงบทบาทของผู้ใช้งาน
Internet			การเชื่อมโยงผ่านเครือข่าย
encrypted			การเชื่อมโยงที่เข้ารหัสอยู่
LAN			การเชื่อมโยงในเครือข่าย
wire			สายเชื่อมต่อ
smart card			สมาร์ทการ์ด
POS device			อุปกรณ์พีโอเอส
Issuer node			จุดจ่ายข้อมูลที่สำคัญ
secrecy			การรักษาความลับของข้อมูล
integrity			การรักษาความถูกต้องของข้อมูล
high			การรักษาข้อมูลที่สำคัญ
critical	secret, integrity, authenticity, high, fresh		อ็อบเจกต์ที่มีความเสี่ยงต่อการบุกรุก
secure link	adversary	มีการควบคุมความมั่นคงของเส้นเชื่อมตามที่กำหนด	การเชื่อมโยงที่กำหนดความมั่นคง
secure dependency		ใช้ <<call>> และ <<send>> ในการควบคุมความมั่นคงขององค์ประกอบ	การกำหนดความมั่นคงที่สัมพันธ์กับความมั่นคงขององค์ประกอบอื่น
data security	adversary, integrity, authenticity	มีการระบุความลับ ความถูกต้อง ความสมจริง และความสมบูรณ์ของข้อมูล	ข้อมูลที่มีป้องกันภัยคุกคาม
no down-flow		ป้องกันการรั่วไหลของข้อมูล	การป้องกันข้อมูลที่มีระดับความลับต่ำมีผลกระทบต่อข้อมูลที่มีระดับความลับสูง
no up-flow		ป้องกันการรั่วไหลของข้อมูล	การป้องกันข้อมูลที่มีระดับความลับสูงมีผลกระทบต่อข้อมูลที่มีระดับความลับต่ำ

ตารางที่ 2.3 แม่พิมพ์ต้นแบบของยูเอ็มแอลเซค (ต่อ)

แม่พิมพ์ต้นแบบ	ป้ายระบุ	ข้อบังคับ	คำอธิบาย
guarded access		ถ้ามีการเข้าถึงคลาสที่ถูกควบคุม จะต้องมีการตรวจสอบจากอ็อบเจกต์ที่ควบคุมคลาสดังกล่าว	การควบคุมการเข้าถึงโดยใช้อ็อบเจกต์ควบคุม
guarded	guard		อ็อบเจกต์ที่ถูกควบคุม

ตารางที่ 2.4 ป้ายระบุของยูเอ็มแอลเซค

ป้ายระบุ	แม่พิมพ์ต้นแบบ	มัลติพลิซิตี	คำอธิบาย
start	fair exchange	*	กิจกรรมเริ่มต้น
stop	fair exchange	*	กิจกรรมสิ้นสุด
adversary	fair exchange	1	ผู้บุกรุก
action	provable	*	กิจกรรมที่ต้องการพิสูจน์การทำงาน
cert	provable	*	ตัวแปรที่ใช้เป็นใบรับรอง (Certificate) ของกิจกรรมที่ต้องการพิสูจน์การทำงาน
adversary	provable	*	ผู้บุกรุก
protected	rbac	*	กิจกรรมที่ต้องการควบคุม
role	rbac	*	การกำหนดบทบาทให้แก่ผู้แสดง
right	rbac	*	การกำหนดกิจกรรมให้แก่บทบาท
secrecy	critical	*	ตัวแปรที่มีการรักษาความลับของข้อมูล
integrity	critical	*	ตัวแปรที่มีการรักษาความบูรณภาพของข้อมูล
authenticity	critical	*	ตัวแปรที่มีการรักษาความสมจริงของข้อมูล
high	critical	*	การดำเนินการที่มีความสำคัญสูง
fresh	critical	*	ตัวแปรที่มีการใช้ ณ เวลาที่จำเพาะ
adversary	secure links	1	ผู้บุกรุก
adversary	data security	1	ผู้บุกรุก
integrity	data security	*	ตัวแปรที่มีการรักษาความบูรณภาพของข้อมูล
authenticity	data security	*	ตัวแปรที่มีการรักษาความสมจริงของข้อมูล
guard	guarded	1	อ็อบเจกต์ที่ควบคุม

งานวิทยานิพนธ์นี้ได้พิจารณา การนำแม่พิมพ์ต้นแบบ ป้ายระบุและเงื่อนไขบังคับ มาปรับปรุงเพื่อแสดงการออกแบบโดยใช้แบบรูปความมั่นคง ทั้งนี้เพราะยูเอ็มแอลเซคไม่สามารถแสดงแบบรูปความมั่นคงในยูเอ็มแอลได้สมบูรณ์เท่าที่ควร เช่น ขาดองค์ประกอบที่ระบุโครงสร้างของแบบรูปความมั่นคง ขาดอิสระในการตั้งชื่อคลาสหรือองค์ประกอบอื่น เนื่องจากต้องตั้งชื่อให้สอดคล้องกับหน้าที่ในแบบรูปความมั่นคง เป็นต้น ดังนั้นงานวิทยานิพนธ์นี้จึงมีแนวคิดที่จะทำการปรับปรุงยูเอ็มแอล เพื่อแสดงแบบรูปความมั่นคงให้มีความสมบูรณ์มากที่สุด

## 2.2.2 การแสดงแบบรูปการออกแบบในโปรแกรมประยุกต์และส่วนประกอบ (Visualizing Design Patterns in Their Application and Composition)

งานวิจัยนี้ [10] นำเสนอการแสดงแบบรูปการออกแบบในโปรแกรมประยุกต์ โดยใช้แผนภาพคลาส และแผนภาพการสื่อสาร (Communication Diagram) ซึ่งมีการสร้างส่วนขยายของยูเอ็มแอลโพรไฟล์ ดังนี้

1) เมตาโมเดลยูเอ็มแอลโพรไฟล์ (UML Profile Metamodel) ประกอบไปด้วย ยูเอ็มแอลโพรไฟล์พื้นฐาน คือ แม่พิมพ์ต้นแบบ ป้ายระบุ และเงื่อนไขบังคับ

2) ยูเอ็มแอลโพรไฟล์สำหรับแบบรูปการออกแบบ (UML Profile for Design Pattern) เป็นส่วนขยายของยูเอ็มแอลโพรไฟล์ที่สร้างขึ้นมา เพื่อสนับสนุนการใช้แบบรูปการออกแบบ

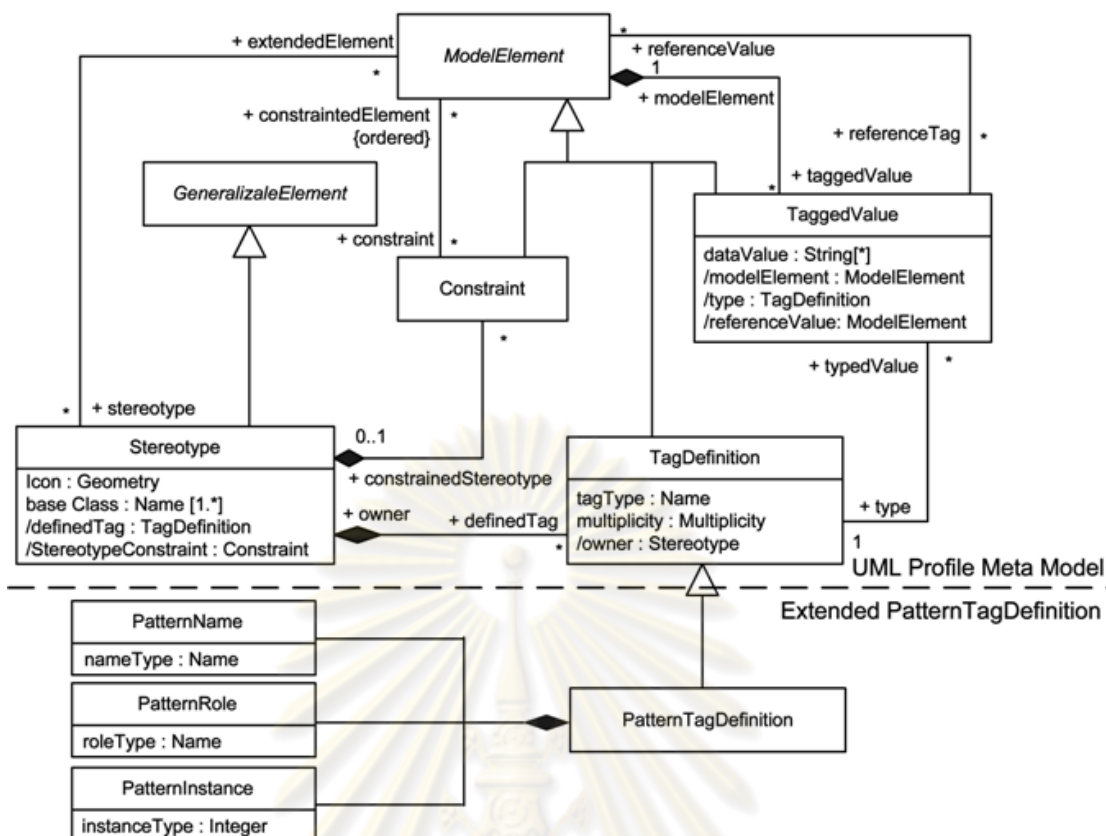
3) ความหมาย (Semantic) เป็นการระบุความหมายที่จะใช้ในยูเอ็มแอลของ แม่พิมพ์ต้นแบบป้ายระบุ และเงื่อนไขบังคับ

4) เงื่อนไขบังคับ (Constraint) เป็นการระบุข้อบังคับที่จะใช้ในยูเอ็มแอลของ แม่พิมพ์ต้นแบบป้ายระบุ และเงื่อนไขบังคับ

5) โครงสร้างจำลอง (Virtual Metamodel) เป็นการระบุรูปแบบการแสดงของ แม่พิมพ์ต้นแบบ ป้ายระบุ และเงื่อนไขบังคับ

ยูเอ็มแอลโพรไฟล์ที่สนับสนุนการใช้แบบรูปการออกแบบ แบ่งเป็นสองส่วนคือ เมตาโมเดลยูเอ็มแอลโพรไฟล์ และบทนิยามป้ายระบุของแบบรูปที่เพิ่มขึ้น (Extended Pattern Tag Definition) ซึ่งงานวิทยานิพนธ์นี้ได้ทำการสร้างบทนิยามป้ายระบุของแบบรูป เพื่อต่อเติม ส่วนสนับสนุนการแสดงแบบรูปการออกแบบ พร้อมทั้งกำหนดความหมาย ข้อบังคับและ โครงสร้างจำลองของบทนิยามป้ายระบุของแบบรูปที่เพิ่มขึ้น เพื่อใช้ในการออกแบบโดยใช้ ยูเอ็มแอล ดังรูปที่ 2.10

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย



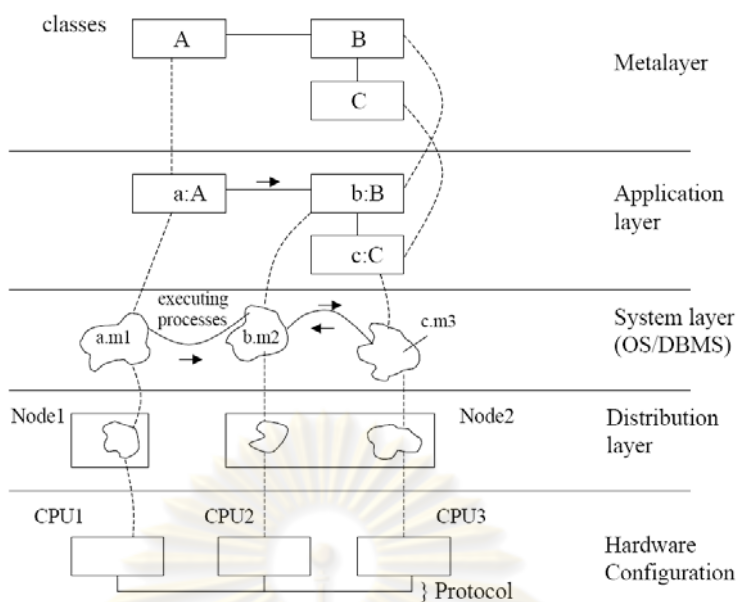
รูปที่ 2.10 ยูเอ็มแอลโพรไฟล์และส่วนขยายของยูเอ็มแอลโพรไฟล์ที่เพิ่มขึ้น  
เพื่อสนับสนุนการใช้แบบรูปการออกแบบ [10]

ในงานวิทยานิพนธ์นี้ ได้นำแนวคิดของรูปแบบการนำเสนอแบบรูปการออกแบบที่แสดงถึงข้อมูลของแบบรูปการออกแบบได้อย่างมีประสิทธิภาพ ซึ่งไม่ทำให้แผนภาพยูเอ็มแอลดูซับซ้อนมากนัก

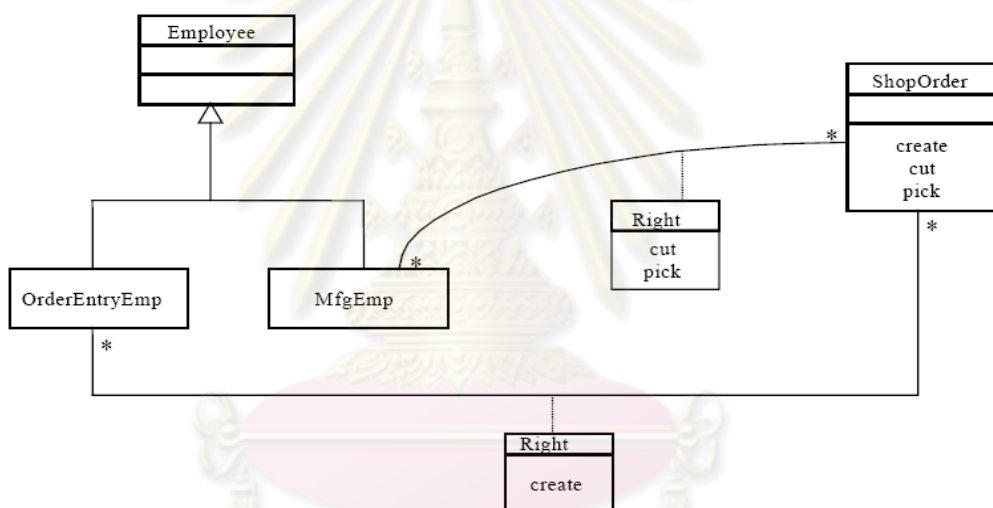
### 2.2.3 เมตาดาตาและแบบรูปการให้อำนาจ

#### (Metadata and Authorization Pattern)

งานวิจัยนี้ได้นำเสนอแบบรูปการให้อำนาจ [11] ในมุมมองของสถาปัตยกรรมชั้นเมตาดาตาของการโปรแกรมเชิงวัตถุ โดยมีการยกตัวอย่างให้เห็นถึงการประยุกต์ใช้มุมมองของสถาปัตยกรรมชั้นเมตาดาตาของแบบรูปการให้อำนาจนี้ โดยมุมมองสถาปัตยกรรมชั้นเมตาดาตานี้ จะช่วยในการควบคุมพฤติกรรม และทิศทางในระดับโปรแกรมประยุกต์ต่อไป โดยแสดงความสัมพันธ์ของคลาสในแต่ละระดับของระบบที่ออกแบบ ดังรูปที่ 2.11 และตัวอย่างของแบบรูปการให้อำนาจ ในแผนภาพคลาสดังรูปที่ 2.12



รูปที่ 2.11 ความสัมพันธ์ของคลาสในแต่ละระดับของระบบ [11]



รูปที่ 2.12 ตัวอย่างของแบบรูปการให้อำนาจในการออกแบบคลาส [11]

จากรูปที่ 2.11 แสดงถึงระดับสถาปัตยกรรมในชั้นต่างๆ จะเห็นได้ว่าในชั้นบนสุดคือ ชั้นของเมตาดาตานั้น จะระบุถึงคลาสต่างๆ ที่มีความสัมพันธ์กัน ต่อมาชั้นของโปรแกรมประยุกต์นั้นจะนำคลาสเหล่านั้นมาใช้ โดยทำการสร้างเป็นอ็อบเจกต์ขึ้นมาสำหรับแต่ละคลาส ต่อมาในชั้นของระบบ เป็นการบริการให้การประมวลต่างๆ สามารถกระทำกันได้ ต่อมาชั้นของการกระจาย จะทำการแยกการประมวลผลและอ็อบเจกต์ต่างๆ ออกไปเป็นโหนด (Node) ซึ่งแต่ละโหนดอาจจะต้องการใช้หน่วยประมวลผลกลางหนึ่งหน่วย หรือมากกว่าก็ได้ อีกทั้งยังมีการเชื่อมโยงกันในระหว่างเครือข่ายโดยการใช้งานโพรโทคอลต่างๆ ในชั้นของโครงแบบฮาร์ดแวร์ และจากรูปที่ 2.12 อ็อบเจกต์ของคลาส OrderEntryEmp สามารถทำการ “create” อ็อบเจกต์ของคลาส ShopOrder และอ็อบเจกต์ของคลาส MfgEmp สามารถทำการ “cut” และ “pick” อ็อบเจกต์ของคลาส ShopOrder ได้



สิ่งที่นำมาพิจารณาใช้ในวิทยานิพนธ์นี้ คือ การสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงนั้น สามารถกระทำได้ในรูปแบบของการใช้แผนภาพคลาส ซึ่งควรมีการพิจารณาถึงสถาปัตยกรรมในชั้นเมตาคลา ซึ่งสามารถออกแบบระบบในระดับที่มีความละเอียดมากยิ่งขึ้นได้ แต่อย่างไรก็ตามจากการแสดงแบบรูปความมั่นคงในแผนภาพยูเอ็มแอลดังกล่าว ไม่ได้ระบุรายละเอียดของแบบรูปความมั่นคงให้ชัดเจน เช่น หน้าที่ของคลาสในแบบรูปความมั่นคง เงื่อนไขบังคับของคลาสในแบบรูปความมั่นคง เป็นต้น ทำให้ไม่สามารถใช้แบบรูปความมั่นคงได้อย่างมีประสิทธิภาพเท่าที่ควร

## 2.2.4 การแสดงแบบรูปความมั่นคงโดยการขยายยูเอ็มแอลเซค (Visualizing Security Patterns by Extending UMLsec)

งานวิจัยนี้ [12] นำเสนอยูเอ็มแอลเซคเอสพี (UMLsec-SP) โดยทำการวิเคราะห์และปรับปรุงยูเอ็มแอลเซคเพื่อสนับสนุนการแสดงผลแบบรูปความมั่นคง ซึ่งจะใช้แบบรูปความมั่นคงที่นำเสนอในหนังสือ แบบรูปความมั่นคง การบูรณาการความมั่นคงและวิศวกรรมระบบ [3] เพื่อสามารถนำมาใช้งานจริงในการออกแบบและพัฒนาซอฟต์แวร์ พร้อมทั้งพัฒนาเครื่องมือที่ช่วยสนับสนุนการใช้แบบรูปความมั่นคง ซึ่งการออกแบบความมั่นคงโดยใช้แบบรูปความมั่นคงนั้นจะช่วยให้การออกแบบความมั่นคงของระบบมีประสิทธิภาพมากยิ่งขึ้น โดยนำแบบรูปความมั่นคงที่ได้รับการออกแบบและตรวจสอบความถูกต้องแล้ว 5 กลุ่มแบบรูปซึ่งมีทั้งหมด 27 แบบรูป โดยมีดังต่อไปนี้

### 1) แบบจำลองควบคุมการเข้าถึง (Access Control Models) ประกอบด้วย

1.1) การให้อำนาจ (Authorization) แบบรูปนี้จะช่วยในการกำหนดว่าใครที่ได้สิทธิ์ในการเข้าถึงทรัพยากรในระบบ ในสภาพแวดล้อมที่ต้องมีการควบคุมการเข้าถึงทรัพยากรของระบบ

1.2) การควบคุมการเข้าถึงเชิงบทบาท (Role-Based Access Control) แบบรูปนี้จะอธิบายการกำหนดสิทธิ์บนพื้นฐานของฟังก์ชันของผู้ใช้ภายใต้สภาพแวดล้อมที่ต้องมีการควบคุมการเข้าถึงทรัพยากร

1.3) ความมั่นคงหลายระดับ (Multilevel Security) แบบรูปนี้จะเป็นการอธิบายว่าจะจัดกลุ่มข้อมูลและการป้องกันข้อมูลอย่างไร เช่น การจัดกลุ่มของผู้ใช้ การจัดกลุ่มของข้อมูล เป็นต้น

1.4) การเฝ้าสังเกตเชิงอ้างอิง (Reference Monitor) แบบรูปนี้จะเป็นการบังคับการประกาศการเข้าถึง โดยเพิ่มความเข้มงวดเมื่อมีการร้องขอการเข้าถึงทรัพยากร

### 2) สถาปัตยกรรมควบคุมการเข้าถึงระบบ (System Access Control Architecture) ประกอบด้วย

2.1) จุดเข้าระบบเดี่ยว (Single Access Point) แบบรูปนี้จะนำเสนอการควบคุมการเข้าถึงของระบบเพียงจุดเดียวเท่านั้น เพื่อให้ง่ายต่อการควบคุม

2.2) จุดตรวจสอบ (Check Point) แบบรูปนี้จะช่วยในการป้องกันการเข้าถึงทรัพยากรที่สำคัญ โดยใช้จุดตรวจสอบในจุดที่มีความสำคัญ

2.3) ช่วงเวลาความมั่นคง (Security Session) แบบรูปนี้จะช่วยในการเก็บข้อมูลเกี่ยวกับการเข้าถึงของผู้ใช้งาน ทำให้ตรวจสอบได้ว่าผู้ใช้งานทำกระบวนการใดบ้าง

2.4) เข้าถึงอย่างเต็มที่ด้วยความผิดพลาด (Full Access with Errors) แบบรูปนี้จะนำเสนอการแสดงช่องทางการเข้าถึงทั้งหมด แต่ถ้าผู้ใช้งานกำลังใช้งานในส่วนที่ไม่มีอำนาจในการเข้าถึง จะเกิดความผิดพลาดแสดงให้เห็น

2.5) การจำกัดการเข้าถึง (Limited Access) แบบรูปนี้จะเสนอการแสดงช่องทางการเข้าถึงที่แตกต่างกันสำหรับผู้ใช้งานที่มีอำนาจในการเข้าถึงต่างกัน

3) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) ประกอบด้วย

3.1) ตัวให้อำนาจ (Authenticator) แบบรูปนี้จะนำเสนอการใช้อ็อบเจกต์ เพื่อยืนยันการให้อำนาจการเข้าถึงของระบบปฏิบัติการ

3.2) ตัวควบคุมการสร้างกระบวนการ (Controlled Process Creator) แบบรูปนี้จะนำเสนอการกำหนดหรืออนุญาตให้เข้าถึงอย่างเหมาะสมของกระบวนการใหม่ที่สร้างขึ้น

3.3) โรงงานควบคุมอ็อบเจกต์ (Controlled Object Factory) แบบรูปนี้จะนำเสนอการระบุความถูกต้องของกระบวนการที่เกี่ยวข้องกับการสร้างอ็อบเจกต์ใหม่

3.4) ฝ้าสังเกตการควบคุมอ็อบเจกต์ (Controlled Object Monitor) แบบรูปนี้จะนำเสนอการฝ้าสังเกตการควบคุมการเข้าถึงของกระบวนการใช้อ็อบเจกต์

3.5) การควบคุมหน่วยเก็บเสมือน (Controlled Virtual Address Space) แบบรูปนี้จะนำเสนอการควบคุมการเข้าถึงของหน่วยเก็บเสมือน (Virtual Address Space)

3.6) ขอบเขตการทำงาน (Execution Domain) แบบรูปนี้จะนำเสนอว่าการกระทำใดต่อระบบจะต้องอยู่ในขอบเขตการทำงาน

3.7) การควบคุมการทำงานสิ่งแวดล้อม (Controlled Execution Environment) แบบรูปนี้จะนำเสนอการควบคุมกระบวนการที่เกิดขึ้นหรือข้าง

3.8) การให้อำนาจในแฟ้ม (File Authorization) แบบรูปนี้จะนำเสนอการเข้าถึงของแฟ้มในระบบปฏิบัติการ

4) สถาปัตยกรรมไฟร์วอลล์ (Firewall Architectures) ประกอบด้วย

4.1) ไฟร์วอลล์สำหรับการกรองแพ็คเก็ต (Packet Filter Firewall) แบบรูปนี้จะนำเสนอการระบุแพ็คเก็ตที่ส่งเข้าออกในระบบเครือข่าย ซึ่งจำแนกตามมุมมองของระดับไอพี (IP Level)

**4.2) ไฟร์วอลล์เชิงตัวแทน (Proxy-Based Firewall)** แบบรูปนี้จะนำเสนอการแทรกแซงระหว่างผู้ร้องขอกับการเข้าถึงทรัพยากร ซึ่งนิยมใช้ในการกรองข้อมูลเข้าออกระบบเครือข่ายโดยอาศัยแอดเดรส (Address)

**4.3) ไฟร์วอลล์เชิงสถานะ (Stateful Firewall)** แบบรูปนี้จะนำเสนอการตรวจสอบข้อมูลเข้าว่าเป็นการเชื่อมต่อไป หรือเป็นการส่งข้อมูลของการเชื่อมต่อเดิมที่มีอยู่

**5) โปรแกรมประยุกต์ทางด้านความมั่นคงบนอินเทอร์เน็ต (Security Internet Applications) ประกอบด้วย**

**5.1) การปิดบังข้อมูล (Information Obscurity)** แบบรูปนี้จะนำเสนอการปิดบังข้อมูลจากการเข้าถึงของกระบวนการที่ไม่พึงประสงค์

**5.2) ช่องทางปลอดภัย (Secure Channels)** แบบรูปนี้จะนำเสนอช่องทางในการเข้าถึงระบบที่ปลอดภัย

**5.3) ผู้เป็นหุ้นส่วนที่รู้จัก (Known Partners)** แบบรูปนี้จะนำเสนอการระบุหนทางเฉพาะแก่ผู้เป็นหุ้นส่วนในการเข้าถึงระบบ

**5.4) เขตปลอดการป้องกัน (Demilitarized Zone)** แบบรูปนี้จะนำเสนอการแบ่งแยกอาณาเขตระหว่างการเข้าถึงจากภายนอกและการทำงานภายในระบบ

**5.5) แม่ข่ายตัวแทนการป้องกัน (Protection Reverse Proxy)** แบบรูปนี้จะนำเสนอการใช้แม่ข่ายตัวแทนป้องกันระบบภายในในระดับแอปพลิเคชันโพรโตคอล (Application Protocol)

**5.6) แม่ข่ายตัวแทนการรวบรวม (Integration Reverse Proxy)** แบบรูปนี้จะนำเสนอการใช้แม่ข่ายตัวแทนที่รวบรวมการเข้าถึงแม่ข่ายในระบบทั้งหมด

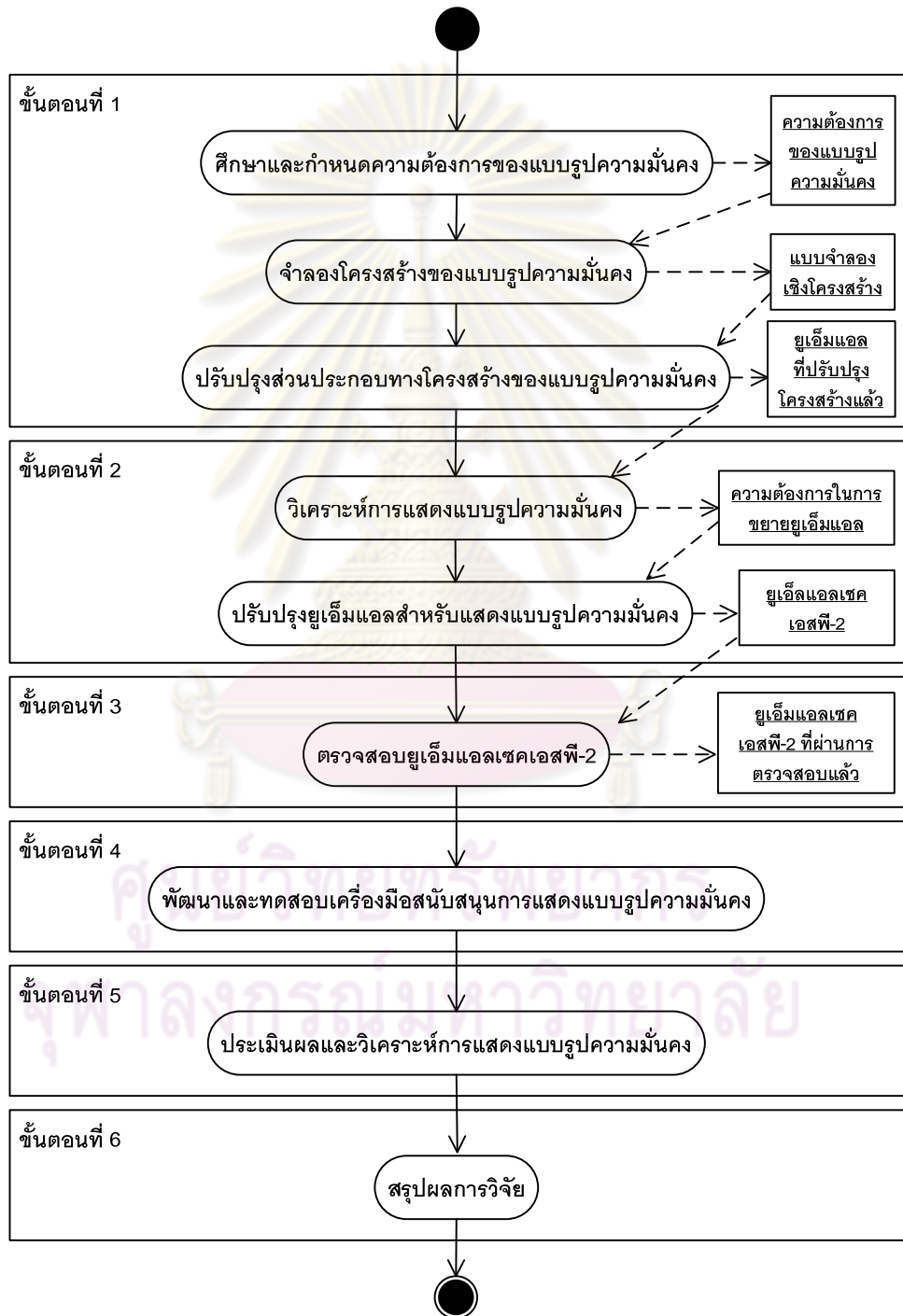
**5.7) ประตูหน้า (Front Door)** แบบรูปนี้จะนำเสนอการใช้ประตูหน้าในการป้องกันการเข้าถึงของผู้ไม่พึงประสงค์จากส่วนหลัง (back-end)

โดยงานวิทยานิพนธ์นี้ได้ใช้แนวคิดของวิเคราะห์และปรับปรุงยูเอมแอลเซคเพื่อแสดงแบบรูปความมั่นคง ซึ่งจะใช้แบบรูปความมั่นคงที่นำเสนอในหนังสือ แบบรูปความมั่นคงการบูรณาการความมั่นคงและวิศวกรรมระบบที่แตกต่างไปจากแบบรูปความมั่นคงที่งานวิจัยนี้ได้ทำไว้ โดยครอบคลุมแบบรูปความมั่นคงทั้งหมด เพื่อช่วยให้การออกแบบความมั่นคงของระบบมีประสิทธิภาพมากยิ่งขึ้น

### บทที่ 3

## การวิเคราะห์แบบรูปความมั่นคงและการขยายยูเอ็มแอล

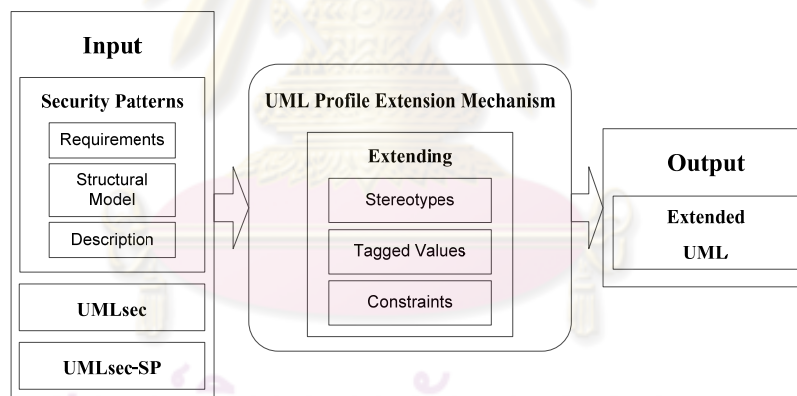
งานวิทยานิพนธ์นี้แบ่งขั้นตอนการดำเนินงานออกเป็น 6 ขั้นตอน โดยแสดงผังแผนภาพกิจกรรม (Activity Diagram) ดังรูปที่ 3.1



รูปที่ 3.1 ผังแผนภาพกิจกรรมแสดงขั้นตอนการดำเนินงานวิจัย

จากรูป ในขั้นตอนที่ 1 เป็นขั้นตอนของการศึกษาและวิเคราะห์แบบรูปความมั่นคง โดยเริ่มจากการศึกษาและกำหนดความต้องการของแบบรูปความมั่นคง เพื่อระบุความต้องการทางด้านความมั่นคงของแบบรูป ต่อมาทำการจำลองโครงสร้างของแบบรูปความมั่นคงจากความต้องการที่ได้ เพื่อแสดงถึงความสัมพันธ์ของแต่ละองค์ประกอบ หลังจากนั้นทำการปรับปรุงส่วนประกอบทางโครงสร้างของแบบรูปความมั่นคง เพื่อให้ครอบคลุมองค์ประกอบทางโครงสร้างที่ปรากฏอยู่ในส่วนประกอบอื่นของแบบรูป ขั้นตอนที่ 2 การขยายยูเอ็มแอล เริ่มต้นด้วยการวิเคราะห์การแสดงแบบรูปความมั่นคง เพื่อระบุความต้องการในการขยายยูเอ็มแอลสำหรับแสดงแบบรูปความมั่นคง หลังจากนั้นทำการปรับปรุงแผนภาพคลาสของยูเอ็มแอลสำหรับแสดงแบบรูปความมั่นคงจากความต้องการในการขยายยูเอ็มแอล ขั้นตอนที่ 3 เป็นการตรวจสอบยูเอ็มแอลเซคเอสพี-2 เพื่อให้มีความสอดคล้องกับข้อกำหนดความต้องการของยูเอ็มแอลโพรไฟล์ [14] สำหรับรายละเอียดในขั้นตอนที่ 4 ขั้นตอน 5 และขั้นตอน 6 ที่เกี่ยวข้องกับการพัฒนาและทดสอบเครื่องมือสนับสนุนการแสดงผลแบบรูปความมั่นคง การประเมินผลและการวิเคราะห์การแสดงผลแบบรูปความมั่นคง และการสรุปผลการวิจัย จะกล่าวถึงต่อไปในบทที่ 4 บทที่ 5 และบทที่ 6 ตามลำดับ

โดยแสดงภาพรวมของการขยายยูเอ็มแอลสำหรับแสดงโครงสร้างของแบบรูปความมั่นคง และคำอธิบายภาพรวมในการขยายยูเอ็มแอล ดังรูปที่ 3.2 และตารางที่ 3.1 ตามลำดับ



รูปที่ 3.2 ภาพรวมของการขยายยูเอ็มแอล

ตารางที่ 3.1 คำอธิบายภาพรวมในการขยายยูเอ็มแอล

ข้อมูลนำเข้า (Input)	1) แบบรูปความมั่นคง (Security Patterns) <ul style="list-style-type: none"> <li>- ความต้องการ (Requirements) ทางด้านความมั่นคง</li> <li>- แบบจำลองเชิงโครงสร้าง (Structural Model) ที่เป็นแผนภาพคลาสจากส่วนประกอบ "Structure" ของแบบรูป</li> <li>- ข้อมูล (Description) ที่ได้จากส่วนประกอบอื่นของแบบรูป</li> </ul> 2) ยูเอ็มแอลโพรไฟล์ของยูเอ็มแอลเซค (UMLsec) 3) ยูเอ็มแอลเซคเอสพี (UMLsec-SP)
กลไกการขยายยูเอ็มแอล (UML Extension Mechanism)	นำข้อมูลจากข้อมูลนำเข้าทั้งหมดมาใช้ในการขยายยูเอ็มแอล ได้แก่ การขยายแม่พิมพ์ต้นแบบ คำป้ายระบุ และเงื่อนไขบังคับ
ผลลัพธ์ (Output)	ยูเอ็มแอลที่ประกอบด้วย แม่พิมพ์ต้นแบบ คำป้ายระบุ และเงื่อนไขบังคับที่ปรับปรุงแล้ว ซึ่งสามารถประยุกต์ใช้ในการออกแบบระบบความมั่นคง

## กลไกการขยายยูเอ็มแอล (UML Extension Mechanism)

ในการพัฒนาระบบซอฟต์แวร์เชิงวัตถุ ภาษาที่ได้รับความนิยมมากในปัจจุบัน คือภาษา ยูเอ็มแอล ทั้งนี้เพราะเป็นภาษาที่สามารถออกแบบระบบได้อย่างหลากหลายมุมมอง แต่อย่างไรก็ตามภาษายูเอ็มแอลก็ยังไม่สามารถออกแบบระบบซอฟต์แวร์บางประเภทได้ เช่น ระบบเรียลไทม์ (Real-time System) หรือแม้กระทั่งการออกแบบความมั่นคงของระบบ (System Security) เป็นต้น ดังนั้นหากต้องการปรับปรุงยูเอ็มแอลให้สามารถออกแบบระบบซอฟต์แวร์ที่มีลักษณะเฉพาะ สามารถทำโดยการปรับปรุงยูเอ็มแอลโพรไฟล์ (UML Profile) โดยการเพิ่มหรือเปลี่ยนแปลงองค์ประกอบต่างๆ ให้อยู่ในโดเมนที่ต้องการได้ โดยการปรับปรุงยูเอ็มแอลโพรไฟล์ มี 2 ขั้นตอน ดังนี้

**1) การปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุ** เป็นการกำหนดองค์ประกอบที่ใช้ระบุประเภทและลักษณะขององค์ประกอบในโดเมนที่ต้องการ โดยมีขั้นตอนดังต่อไปนี้

- 1.1) ระบุความต้องการสำหรับแสดงข้อมูลในแผนภาพยูเอ็มแอล
- 1.2) วิเคราะห์ความต้องการเพื่อหาองค์ประกอบต่างๆ ภายในโดเมนที่ต้องการเพื่อแสดงในแผนภาพยูเอ็มแอล
- 1.3) สร้างแม่พิมพ์ต้นแบบและป้ายระบุให้ตรงกับความต้องการที่กำหนดไว้

**2) การปรับปรุงเงื่อนไขบังคับ** เป็นการระบุข้อบังคับที่ต้องพิจารณาก่อนการใช้งานแม่พิมพ์ต้นแบบ ซึ่งช่วยในการกำหนดขอบเขตของแม่พิมพ์ต้นแบบและป้ายระบุในขั้นตอนของการออกแบบได้ โดยมีขั้นตอนดังนี้

- 2.1) กำหนดข้อบังคับในการใช้งานของแต่ละแม่พิมพ์ต้นแบบที่ปรับปรุงหรือสร้างขึ้น
- 2.2) ระบุนิพจน์ของเงื่อนไขบังคับของแม่พิมพ์ต้นแบบให้อยู่ในภาษาไอซีแอล

ในบทนี้จะกล่าวถึง การศึกษาและกำหนดความต้องการของแบบรูปความมั่นคง การจำลองโครงสร้างของแบบรูปความมั่นคง การปรับปรุงโครงสร้างของแบบรูปความมั่นคง การวิเคราะห์การแสดงผลแบบรูปความมั่นคง การปรับปรุงยูเอ็มแอลสำหรับแสดงแบบรูปความมั่นคง และการตรวจสอบยูเอ็มแอลเซคเอสพี-2 ดังขั้นตอนที่ 1 ขั้นตอนที่ 2 และขั้นตอนที่ 3 ในแผนภาพกิจกรรมข้างต้นตามลำดับ โดยแต่ละขั้นตอนมีรายละเอียดดังนี้

### 3.1 การศึกษาและกำหนดความต้องการของแบบรูปความมั่นคง

จากที่กล่าวในตอนต้นแล้วว่า แบบรูปความมั่นคงที่สามารถแสดงในยูเอ็มแอลได้นั้น มีอยู่ 2 ประเภทคือ แบบรูปการออกแบบความมั่นคงและแบบรูปกระบวนการความมั่นคง เนื่องจากเป็นกลุ่มของแบบรูปความมั่นคงที่มีผลลัพธ์ของการออกแบบเป็นโครงสร้างที่ชัดเจน

งานวิทยานิพนธ์นี้จึงได้เลือกแบบรูปความมั่นคง ที่อยู่ในกลุ่มของแบบรูปการออกแบบความมั่นคงและแบบรูปกระบวนการความมั่นคง เพื่อที่จะทำการศึกษาและวิเคราะห์แบบรูปความมั่นคงนั้น โดยแบบรูปความมั่นคงที่ได้นำมาใช้ในงานวิทยานิพนธ์นี้ ประกอบไปด้วยแบบรูปความมั่นคง 3 กลุ่มแบบรูป ซึ่งมีทั้งหมด 17 แบบรูปความมั่นคง ดังต่อไปนี้

1) การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management) ประกอบด้วยแบบรูปความมั่นคงต่อไปนี้

1.1) การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Asset) แบบรูปนี้นำเสนอการพิจารณาความมั่นคงขององค์กร โดยทำการระบุสินทรัพย์ที่สำคัญขององค์กร เพื่อหาวิธีป้องกันสินทรัพย์ต่างๆ เหล่านั้น

1.2) การกำหนดมูลค่าสินทรัพย์ (Asset Valuation) แบบรูปนี้นำเสนอการกำหนดมูลค่าสินทรัพย์จะช่วยให้สามารถกำหนดความสำคัญของสินทรัพย์ขององค์กรที่เป็นเจ้าของหรือควบคุมอยู่

1.3) การประเมินภัยคุกคาม (Threat Assessment) แบบรูปนี้นำเสนอการกำหนดภัยคุกคาม ความถี่ของภัยคุกคามที่จะเกิดต่อสินทรัพย์ (Threat likelihood) และผลกระทบเมื่อสินทรัพย์ถูกคุกคาม (Threat consequence)

1.4) การประเมินภัยจุดอ่อน (Vulnerability Assessment) แบบรูปนี้นำเสนอการระบุจุดอ่อนของสินทรัพย์ในองค์กร และระดับความรุนแรงเมื่อถูกภัยคุกคามโจมตีจุดอ่อนดังกล่าว (Severity scale)

1.5) การกำหนดค่าความเสี่ยง (Risk Determination) แบบรูปนี้นำเสนอการกำหนดค่าความเสี่ยง โดยใช้ข้อมูลการประเมินมูลค่าสินทรัพย์ ภัยคุกคามและความถี่ที่เกิด ภาวะจุดอ่อนและระดับความรุนแรงมาใช้เป็นข้อมูลนำเข้า เพื่อคำนวณและแสดงระดับความเสี่ยงที่เหมาะสม

1.6) แนวคิดความมั่นคงองค์กร (Enterprise Security Approaches) แบบรูปนี้นำเสนอการกำหนดแนวคิดความมั่นคงให้แก่สินทรัพย์ตามคุณสมบัติของความมั่นคงที่เหมาะสม

1.7) บริการความมั่นคงองค์กร (Enterprise Security Services) แบบรูปนี้ใช้สำหรับแนะนำองค์กรในการเลือกบริการความมั่นคงที่จะนำไปใช้ในการป้องกันสินทรัพย์ ภายหลังจากการกำหนดแนวคิดความมั่นคงสำหรับสินทรัพย์องค์กร

1.8) การสื่อสารของผู้มีส่วนองค์กร (Enterprise Partner Communication) แบบรูปนี้นำเสนอการเตรียมเครื่องมือและบริการต่างๆ สำหรับอำนวยความสะดวกและควบคุมการติดต่อและการแลกเปลี่ยนข้อมูลระหว่างหุ้นส่วนกับองค์กร

2) การระบุตัวตนและการพิสูจน์ตัวตน (Identification and Authentication) ประกอบด้วยแบบรูปความมั่นคงต่อไปนี้

**2.1) ความต้องการการระบุและการพิสูจน์ตัวตน (I&A Requirement)** เป็นแบบรูปสำหรับนำเสนอและสร้างความต้องการพื้นฐานสำหรับการบริการด้านการระบุและพิสูจน์ตัวตน โดยที่การบริการด้านการระบุและพิสูจน์ตัวตนจะเป็นเซตของความพึงพอใจของความต้องการทางด้านการบริการและคุณภาพของบริการ

**2.2) ทางเลือกการออกแบบสำหรับการระบุตัวตน และการพิสูจน์ตัวตนอัตโนมัติ (Automated I&A Design Alternatives)** แบบรูปนี้เป็นแบบรูปที่ช่วยในการกำหนดเทคนิคที่จะใช้กับบริการด้านการระบุและพิสูจน์ตัวตน เพื่อช่วยเลือกเทคนิคที่เหมาะสม โดยมีความสอดคล้องกับความต้องการด้านการระบุและพิสูจน์ตัวตน

**2.3) การออกแบบและการใช้รหัสผ่าน (Password Design and Use)** แบบรูปนี้ใช้ในการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับบริการการระบุและพิสูจน์ตัวตน

**2.4) ทางเลือกการออกแบบชีวมิติ (Biometrics Design Alternatives)** แบบรูปนี้ใช้ในการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการการระบุและพิสูจน์ตัวตนโดยใช้วิธีการทางด้านชีวมิติ

### **3) การบันทึกเหตุการณ์ (Accounting) ประกอบด้วยแบบรูปความมั่นคง ดังต่อไปนี้**

**3.1) ความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง (Security Accounting Requirements)** เป็นแบบรูปสำหรับนำเสนอการสร้างความต้องการในการติดตามความมั่นคงที่เกี่ยวข้องกับเหตุการณ์หรือกิจกรรม เช่น ความเสียหายของทรัพย์สิน หรือพยายามเข้าถึงฐานข้อมูลที่ไม่ได้อนุญาต เป็นต้น และให้ข้อมูลเกี่ยวกับเหตุการณ์เหล่านั้น

**3.2) ความต้องการการตรวจสอบ (Audit Requirements)** แบบรูปนี้นำเสนอการสร้างความต้องการในการวิเคราะห์ข้อมูลต่างๆ ที่ได้บันทึกไว้

**3.3) ความต้องการการตรวจสอบหลักฐานและบันทึก (Audit Trails and Logging Requirements)** แบบรูปนี้นำเสนอการสร้างความต้องการสำหรับการตรวจสอบหลักฐานและการบันทึกต่างๆ เกี่ยวกับเหตุการณ์หรือกิจกรรมที่เกิดขึ้นในองค์กรหรือระบบ

**3.4) ความต้องการการป้องกันการบุกรุก (Intrusion Detection Requirements)** แบบรูปนี้นำเสนอการสร้างความต้องการสำหรับการเฝ้าสังเกตกิจกรรมต่างๆ ที่เกิดขึ้น และการวิเคราะห์กิจกรรมเหล่านั้นเพื่อบอกถึงการละเมิดความมั่นคงขององค์กร

**3.5) ความต้องการการไม่ถูกปฏิเสธ (Non-Repudiation Requirements)** แบบรูปนี้นำเสนอการสร้างความต้องการในการตรวจสอบและรักษาหลักฐานเพื่อให้ผู้มีส่วนร่วมไม่ถูกปฏิเสธจากกิจกรรมใดๆ ของระบบหรือองค์กร



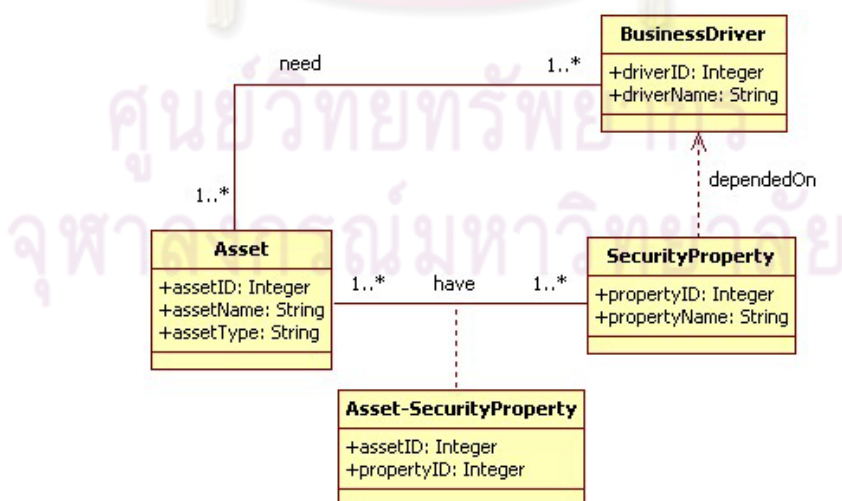
โดยในขั้นตอนการศึกษาและกำหนดความต้องการของแบบรูปความมั่นคงนี้ จะใช้แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร ในกลุ่มการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยงมาเป็นกรณีศึกษา โดยแสดงรายการของปัญหา บริบทของปัญหา และรายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป ดังตารางที่ 3.2

ตารางที่ 3.2 รายการปัญหา บริบท และรายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร [3]

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการกำหนดความมั่นคงให้กับสินทรัพย์ขององค์กร
บริบท	องค์กรต้องการกำหนดความมั่นคงให้กับสินทรัพย์ แต่จะต้องระบุสินทรัพย์และปัจจัยทางด้านธุรกิจเสียก่อน
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>ระบุสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรือ อาคาร เป็นต้น</li> <li>ระบุตัวขับเคลื่อนทางด้านธุรกิจขององค์กรที่เป็นปัจจัยให้เกิดความต้องการของแต่ละสินทรัพย์ เช่น กฎหมาย ระเบียบขององค์กร หุ้นส่วน เป้าหมาย วัตถุประสงค์ กระบวนการทางธุรกิจ สถานที่ที่เกิดกระบวนการทางธุรกิจ เป็นต้น</li> <li>กำหนดความสัมพันธ์ระหว่างสินทรัพย์และตัวขับเคลื่อนทางด้านธุรกิจ เช่น กฎทางด้านความลับของข้อมูลพนักงาน ข้อมูลทางการเงินที่ต้องบอกให้กับหุ้นส่วน เป็นต้น</li> <li>ระบุคุณสมบัติของความมั่นคง ได้แก่ การรักษาความลับ ความสมบูรณ์ สภาพพร้อมใช้งาน และภาวะรับผิดชอบ</li> <li>กำหนดประเภทของสินทรัพย์ โดยพิจารณาจากตัวขับเคลื่อนทางด้านธุรกิจขององค์กร</li> </ol>

### 3.2 การจำลองโครงสร้างของแบบรูปความมั่นคง

ในขั้นตอนการจำลองโครงสร้างของแบบรูปความมั่นคงนั้น จะนำความต้องการของแบบรูปความมั่นคงมาใช้ในการพิจารณา โดยแสดงแผนภาพคลาสที่แสดงโครงสร้าง (Structure) ของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร จากส่วนของ “Structure” ของแบบรูป และคลาสของโครงสร้างแบบรูป ดังรูปที่ 3.3 และตารางที่ 3.3 ตามลำดับ



รูปที่ 3.3 แผนภาพคลาสแสดงโครงสร้างแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

ตารางที่ 3.3 คลาสของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

ชื่อคลาส	คำอธิบาย
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
SecurityProperty	เป็นคลาสของคุณสมบัติทางด้านความมั่นคง
BusinessDriver	เป็นคลาสที่แสดงถึงตัวขับเคลื่อนทางด้านธุรกิจขององค์กร
Asset-SecurityProperty	เป็นคลาสของความสัมพันธ์ระหว่างสินทรัพย์ทางด้านธุรกิจขององค์กรกับคุณสมบัติทางด้านความมั่นคง

โดยรายละเอียดของการศึกษา กำหนดความต้องการ และจำลองโครงสร้างของแต่ละแบบรูปความมั่นคงที่งานวิทยานิพนธ์นี้นำเสนอ แสดงในภาคผนวก ก

### 3.3 การปรับปรุงส่วนประกอบทางโครงสร้างของแบบรูปความมั่นคง

ในขั้นตอนนี้เป็นการนำโครงสร้างของแบบรูปความมั่นคงที่สร้างจากส่วนประกอบทางโครงสร้างจากขั้นตอนที่ 3.2 มาปรับปรุง ทั้งนี้เนื่องจากโครงสร้างที่ได้จากส่วนประกอบดังกล่าวไม่สามารถครอบคลุมองค์ประกอบทางโครงสร้างที่ปรากฏในส่วนประกอบอื่นในแบบรูป ดังนั้นในการปรับปรุงยูเอ็มแอลจึงจำเป็นต้องพิจารณาองค์ประกอบจากส่วนประกอบอื่นของแบบรูปความมั่นคง ได้แก่ Dynamic, Implementation, Solution, Example Resolved และ Variant ทั้งนี้เพื่อให้ยูเอ็มแอลที่ปรับปรุงเพิ่มเติมสามารถแสดงองค์ประกอบของแบบรูปความมั่นคงได้ครบทุกความต้องการภายในแบบรูปความมั่นคง โดยรายละเอียดของแต่ละส่วนประกอบมีดังต่อไปนี้

1) Dynamic แสดงถึงสถานการณ์จำลองที่สามารถนำไปประยุกต์ใช้ได้ ซึ่งจะแสดงถึงพฤติกรรมของแบบรูป โดยจะแสดงลำดับของการดำเนินการ ซึ่งในแบบรูปความมั่นคงนี้ได้อธิบายถึง ขั้นตอนในการแก้ปัญหา ดังนี้ ทำการระบุสินทรัพย์ทางด้านธุรกิจขององค์กรไปพร้อม กับตัวขับเคลื่อนทางด้านธุรกิจขององค์กร ซึ่งจะนำไปสร้างความสัมพันธ์ระหว่างสินทรัพย์ทางด้านธุรกิจขององค์กรกับคุณสมบัติทางด้านความมั่นคง หลังจากนั้นจะทำการกำหนดคุณสมบัติทางด้านความมั่นคง โดยขั้นตอนสุดท้ายจะทำการกำหนดประเภทของสินทรัพย์

2) Implementation แสดงแนวทางในการนำแบบรูปไปใช้งาน โดยเสนอเป็นลำดับขั้นตอนของการนำแบบรูปไปประยุกต์ใช้ในการแก้ไขปัญหา โดยในส่วนของแนวทางในการนำแบบรูปไปใช้งานของแบบรูปความมั่นคงนี้ ได้กล่าวถึงประเภทหรือคุณสมบัติของความมั่นคงว่า มีความสำคัญไม่น้อยไปกว่าการระบุสินทรัพย์ขององค์กร ทั้งนี้เพราะสินทรัพย์หนึ่งๆ อาจจะมีคุณสมบัติทางด้านความมั่นคงมากกว่า 1 คุณสมบัติ ซึ่งคุณสมบัติทางความมั่นคงนี้จะช่วยให้สินทรัพย์มีความปลอดภัยจากความเสี่ยงที่อาจจะเกิดขึ้นได้ โดยแสดงตัวอย่างของคุณสมบัติทางด้านความมั่นคงของแต่ละสินทรัพย์ขององค์กร ดังตารางที่ 3.4

ตารางที่ 3.4 ตัวอย่างของคุณสมบัติทางด้านความมั่นคงของแต่ละสินทรัพย์ขององค์กร

สินทรัพย์ขององค์กร	คุณสมบัติทางด้านความมั่นคง	ตัวขับเคลื่อนทางด้านธุรกิจขององค์กร	รายละเอียด
ข้อมูลส่วนบุคคล (Personnel data)	- การรักษาความลับ - ความสมบูรณ์ - สภาพพร้อมใช้งาน - ภาวะรับผิดชอบ	- กฎหมายความเป็นส่วนตัว - ปัญหาการแข่งขัน	กฎหมายความเป็นส่วนตัวต้องการให้มีการรักษาความลับต่อข้อมูลส่วนบุคคล พนักงานต้องการความมั่นใจว่าจะแก้ไขข้อมูลส่วนตัวได้ และพร้อมใช้งานเวลาเมื่อฝ่ายทรัพยากรบุคคลต้องการ อีกทั้งยังเปลี่ยนแปลงหน้าที่ส่วนบุคคลได้
ข้อมูลทางด้านกฎหมาย (Legal data)	- การรักษาความลับ - ความสมบูรณ์ - ภาวะรับผิดชอบ	- กฎหมาย - ปัญหาการแข่งขัน	องค์กรต้องการให้กฎระเบียบของสัญญา มีการรักษาความลับและ และเมื่อมีการแก้ไขก็ควรจะมีการตรวจสอบสิทธิ์การเข้าถึงเสียก่อน และต้องมีการบันทึกข้อมูลของผู้ที่รับชอบไว้ด้วย
ตึกหรืออาคารต่างๆ (Buildings)	- ความสมบูรณ์ - สภาพพร้อมใช้งาน	- กระบวนการทางธุรกิจ	องค์กรต้องการป้องกันอาคารต่างๆ สำหรับทำงานต่างๆ ที่ไม่มีอำนาจในการดัดแปลงหรือทำลาย และควรอยู่ในสภาพพร้อมใช้งานเสมอ
พนักงาน (Employees)	- สภาพพร้อมใช้งาน - ภาวะรับผิดชอบ	- กระบวนการทำงานของพนักงาน	องค์กรต้องการให้สภาพแวดล้อมมีความปลอดภัยต่อพนักงานเพื่อที่พนักงานเกิดความพร้อมที่จะทำงาน และสร้างความรับผิดชอบในการทำงานของพนักงาน

3) Solution แสดงผลเฉลยของแบบรูป โดยอธิบายขั้นตอนการปฏิบัติในการแก้ปัญหา ซึ่งผู้วิจัยได้ทำการสกัดในส่วนของผลเฉลยของแบบรูปนี้ไปสร้างเป็นรายการความต้องการในขั้นตอนที่ 3.1

4) Example Resolved แสดงตัวอย่างของผลลัพธ์ของการแก้ปัญหา โดยในแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์ขององค์กรนี้ได้แสดงตัวอย่างของผลลัพธ์โดยมีรายละเอียดดังนี้

ในแบบรูปความมั่นคงนี้ได้ใช้พิพธิภัณฑ์มาเป็นองค์กรสำหรับศึกษาการแก้ปัญหา โดยมีการกำหนดประเภทของสินทรัพย์ (Asset Kind) และตัวขับเคลื่อนทางด้านธุรกิจขององค์กร (Business Driver) ดังนี้

- ประเภทของสินทรัพย์ทางด้านธุรกิจขององค์กร มี 2 ประเภทดังนี้ (1) Information assets เช่น ข้อมูลพนักงาน ข้อมูลด้านธุรกิจ ข้อมูลด้านประกันภัย ข้อมูลของสัญญาและแผนธุรกิจ ข้อมูลการวิจัย ข้อมูลด้านโฆษณาและการตลาด เป็นต้น (2) Physical assets เช่น อาคารของพิพธิภัณฑ์ พนักงานของพิพธิภัณฑ์ วัตถุหรือของสะสมต่างๆ และยานพาหนะ เป็นต้น

- ปัจจัยทางด้านธุรกิจขององค์กร มี 2 ประเภทดังนี้ (1) ปัจจัยภายนอกของธุรกิจ เช่น เงื่อนไขของประกันภัย กฎหมายต่างๆ เป้าหมายและกลยุทธ์ เป็นต้น (2) ปัจจัยภายในของธุรกิจ เช่น ข้อมูลของวัตถุ ซึ่งประกอบด้วยที่มาและมูลค่าของวัตถุนั้น แผนการจัดแสดงวัตถุ

ต่าง ๆ แผนผังของอาคาร เงื่อนไขทางด้านงบประมาณ และความสำคัญทางด้านความมั่นคงและการเข้าถึง เป็นต้น

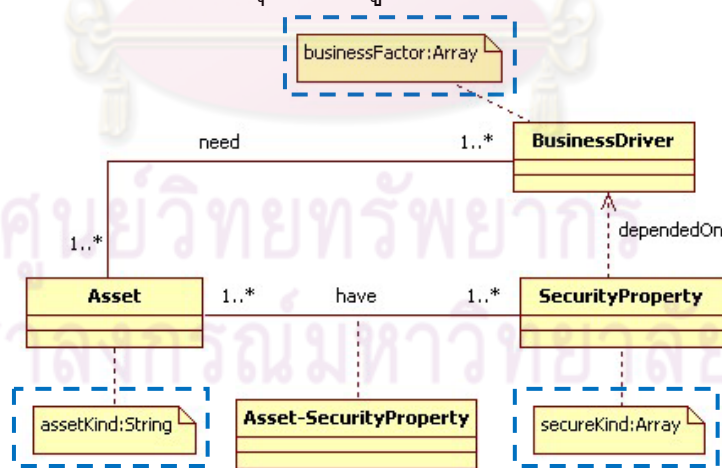
5) Variant แสดงรูปแบบพิเศษของแบบรูปความมั่นคงเพื่อให้เห็นรูปแบบอื่นๆ ของแบบรูป โดยมากจะเป็นการนำประยุกต์ใช้แบบรูปให้เหมาะสมต่อการใช้งาน โดยในส่วนนี้จะไม่ได้กล่าวถึงในแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรที่ยกมาเป็นตัวอย่าง

จากการวิเคราะห์ส่วนประกอบของแบบรูปความมั่นคงดังกล่าว พบว่าสามารถเพิ่มองค์ประกอบทางโครงสร้างได้ดังตารางที่ 3.5

ตารางที่ 3.5 องค์ประกอบทางโครงสร้างที่ปรับปรุงเพิ่มเติม

ส่วนที่ปรับปรุงเพิ่มเติม	ความหมาย	หมายเหตุ
ป้ายระบุ assetKind ของคลาส Asset	คือประเภทของสินทรัพย์ ได้แก่ InformationType และ PhysicalType	ปรับปรุงจากส่วน Example Resolved ทั้งนี้เพราะเป็นคุณสมบัติที่สำคัญของสินทรัพย์ขององค์กร
ป้ายระบุ secureKind ของคลาส securityProperty	คือคุณสมบัติทางด้านความมั่นคงของสินทรัพย์ ได้แก่ การรักษาความลับ ความสมบูรณ์ สภาพพร้อมใช้งาน และภาวะรับผิดชอบ	ปรับปรุงจากส่วน Implementation เพราะเป็นส่วนที่ช่วยให้สินทรัพย์ขององค์กรปลอดภัยจากความเสี่ยงได้
ป้ายระบุ businessFactor ของคลาส businessDriver	คือปัจจัยทางด้านธุรกิจขององค์กร เช่น กฎหมาย ระเบียบขององค์กร หรือเป้าหมาย เป็นต้น	ปรับปรุงจากส่วน Example Resolved เพราะปัจจัยทางด้านธุรกิจมีผลต่อคุณสมบัติทางด้านความมั่นคงและสินทรัพย์ขององค์กร

โดยแสดงแผนภาพคลาสที่แสดงโครงสร้างของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรที่ปรับปรุงแล้ว ดังรูปที่ 3.4



รูปที่ 3.4 แผนภาพคลาสแสดงโครงสร้างแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรที่ปรับปรุงแล้ว

### 3.4 การวิเคราะห์การแสดงผลแบบรูปความมั่นคง

ในขั้นตอนนี้เป็น การนำโครงสร้างของแบบรูปที่ทำการปรับปรุงเพิ่มเติมและข้อมูลของแบบรูปนั้นมาวิเคราะห์การแสดงผลข้อมูลทางโครงสร้างและการแสดงผลข้อมูลทางความมั่นคงของ

แบบรูป เพื่อหาความต้องการในการปรับปรุงยูเอมแอลสำหรับแสดงแบบรูปความมั่นคง ซึ่งในวิทยานิพนธ์นี้จะพิจารณาที่แผนภาพคลาสเพียงอย่างเดียวเท่านั้น ทั้งนี้เพราะเป็นการแสดงข้อมูลในระดับเมตาดาตา ซึ่งเหมาะสมต่อการแสดงโดยใช้แผนภาพคลาส โดยข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงมีรายละเอียดดังนี้

**1) ข้อมูลทางโครงสร้างของแบบรูปความมั่นคง** เป็นข้อมูลที่อธิบายโครงสร้างของแบบรูปความมั่นคง ซึ่งจะช่วยให้ผู้ออกแบบระบบสามารถตรวจสอบและจัดเก็บข้อมูลที่เกี่ยวข้องกับโครงสร้างของแบบรูปได้อย่างถูกต้อง เช่น การกำหนดชื่อแบบรูปความมั่นคงในการออกแบบระบบ จะช่วยให้ทราบว่าโครงสร้างดังกล่าวเป็นไปตามแบบรูปใดบ้าง เป็นต้น ดังนั้นจะเห็นได้ว่าการแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคงเป็นที่จำเป็น ซึ่งถ้าผู้ออกแบบระบบละเลยอาจทำให้เกิดปัญหาต่อการออกแบบทางด้านความมั่นคงของระบบ ดังนี้

1.1) หากต้องการปรับปรุงการออกแบบจะทำได้ยาก เนื่องจากผู้ออกแบบจะไม่สามารถทราบได้ว่าองค์ประกอบในส่วนใด เป็นองค์ประกอบทางด้านโครงสร้างของแบบรูปความมั่นคง ทั้งนี้เพราะไม่มีการระบุองค์ประกอบของแบบจำลอง

1.2) หากผู้ออกแบบระบบไม่ระบุแบบรูปความมั่นคงที่ประยุกต์ใช้ในระบบ อาจทำให้ยากในการสื่อสารกับบุคคลอื่นโดยใช้แบบรูปความมั่นคงของระบบ

1.3) หากผู้ออกแบบระบบจะทำการปรับปรุงการออกแบบความมั่นคงของระบบจากคำแนะนำของแบบรูปความมั่นคงที่ประยุกต์ใช้ในระบบนั้นกระทำได้อาจ ทั้งนี้เพราะไม่สามารถทราบว่ามีมีการประยุกต์ใช้แบบรูปความมั่นคงใดกับระบบบ้าง

จากปัญหาดังที่ได้กล่าวมาข้างต้น จึงมีความจำเป็นที่จะต้องระบุข้อมูลทางโครงสร้างของแบบรูปความมั่นคง เพื่อช่วยให้ผู้ออกแบบระบบสามารถจัดการกับระบบทางด้านความมั่นคงได้ครบถ้วนและสมบูรณ์ อีกทั้งช่วยให้สามารถทำความเข้าใจกับระบบได้ง่ายขึ้นอีกด้วย

**2) ข้อมูลทางความมั่นคงของแบบรูปความมั่นคง** คือข้อมูลทางด้านความมั่นคงที่อยู่ในแบบรูปความมั่นคง ซึ่งในที่นี้จะทำการมุ่งเน้นการแสดงข้อมูลในแผนภาพคลาสเท่านั้น ซึ่งถ้าผู้ออกแบบระบบละเลยอาจทำให้เกิดปัญหาต่อการออกแบบทางด้านความมั่นคงของระบบ ดังนี้

2.1) ผู้ออกแบบระบบจะไม่สามารถทราบได้ว่าองค์ประกอบใดเป็นองค์ประกอบทางด้านความมั่นคงในระบบ จึงทำให้ละเลยการตรวจสอบองค์ประกอบทางด้านความมั่นคงที่สำคัญได้

2.2) ผู้ออกแบบระบบอาจจัดการความมั่นคงของระบบได้ไม่สมบูรณ์ ทั้งนี้เพราะขาดการระบุข้อมูลที่สำคัญทางด้านความมั่นคงของระบบ

จากความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงข้างต้น จะถูกนำมาใช้ในขั้นตอนของการปรับปรุงยูเอมแอลสำหรับแสดงแบบรูปความมั่นคงต่อไป

### 3.5 การปรับปรุงยูเอมแอลสำหรับแสดงแบบรูปความมั่นคง

ภายหลังการวิเคราะห์การแสดงแบบรูปความมั่นคงแล้ว จะได้ความต้องการในการแสดงข้อมูลทางโครงสร้างและการแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงมาใช้ในขั้นตอน

การปรับปรุงยูเอ็มแอล โดยการปรับปรุงยูเอ็มแอลสำหรับแสดงแบบรูปความมั่นคงแบ่งเป็น 2 ขั้นตอน คือ การปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอล และการปรับปรุงเงื่อนไขบังคับของยูเอ็มแอล ดังนี้

### 3.6.1 การปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอล

ในการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลนั้น ก็คือการแก้ไข หรือสร้างแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลขึ้นมาใหม่ โดยมีจุดมุ่งหมายเพื่อให้ยูเอ็มแอลสามารถแสดงรายละเอียดขององค์ประกอบแบบจำลองจากความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ โดยมีขั้นตอนของการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอล ดังนี้

#### 1) ระบุข้อมูลของแบบรูปความมั่นคงที่ต้องการแสดง

ในขั้นตอนนี้จะทำการระบุข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงจากความต้องการของขั้นตอนที่ผ่านมา โดยจะได้ข้อมูลทางโครงสร้างของแบบรูปความมั่นคงได้แก่ (1) ชื่อแบบรูปความมั่นคง (2) ลำดับของแบบรูปความมั่นคงที่ประยุกต์ใช้ในกรณีใช้แบบรูปซ้ำกัน (3) องค์ประกอบแบบจำลองในแบบรูปความมั่นคง และ (4) บทบาทขององค์ประกอบแบบจำลองในแบบรูปความมั่นคง ส่วนข้อมูลทางความมั่นคงของแบบรูปความมั่นคงนั้น ได้จากการนำส่วนของรายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูปความมั่นคงในขั้นตอนที่ 3.1 มาพิจารณาเพื่อหาข้อมูลทางความมั่นคงที่สำคัญของแบบรูปความมั่นคง โดยแสดงรายละเอียดการระบุข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร ดังตารางที่ 3.6

ตารางที่ 3.6 การระบุข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูปความมั่นคง	ข้อมูลทางความมั่นคงของแบบรูปความมั่นคง
1. ระบุสินทรัพย์ทางด้านธุรกิจขององค์กร	- สินทรัพย์ทางด้านธุรกิจขององค์กร
2. ระบุตัวขับเคลื่อนทางด้านธุรกิจขององค์กรที่เป็นปัจจัยให้เกิดความต้องการของแต่ละสินทรัพย์	- ตัวขับเคลื่อนทางด้านธุรกิจขององค์กร
3. กำหนดความสัมพันธ์ระหว่างสินทรัพย์และตัวขับเคลื่อนทางด้านธุรกิจ	- ความสัมพันธ์ระหว่างสินทรัพย์ทางด้านธุรกิจกับตัวขับเคลื่อนทางด้านธุรกิจขององค์กร
4. ระบุคุณสมบัติของความมั่นคง	- คุณสมบัติทางด้านความมั่นคง
5. กำหนดประเภทของสินทรัพย์	- ประเภทของสินทรัพย์

#### 2) ปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุ

หลังจากระบุข้อมูลของแบบรูปความมั่นคงที่ต้องการแสดงแล้ว ในขั้นตอนนี้จะทำการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอลสำหรับแสดงข้อมูลดังกล่าว ซึ่งในการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุนั้น จะช่วยระบุประเภทและลักษณะขององค์ประกอบในแบบจำลอง โดยมีขั้นตอนการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุ ดังนี้

2.1) สร้างแม่พิมพ์ต้นแบบ เพื่อระบุงค์ประกอบในแบบจำลอง โดยจากการพิจารณาข้อมูลของแบบรูปการระบุงค์ความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรที่ต้องการแสดงแล้ว จะทำการสร้างแม่พิมพ์ต้นแบบขึ้นใหม่ ดังตารางที่ 3.7

ตารางที่ 3.7 แม่พิมพ์ต้นแบบสำหรับระบุงค์ประกอบในแบบจำลองของแบบรูปการระบุงค์ความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

แม่พิมพ์ต้นแบบสำหรับระบุงค์ข้อมูลทางโครงสร้างของแบบรูปความมั่นคงดังกล่าว		หมายเหตุ
“spc” (Security Pattern Class)	เป็นแม่พิมพ์ต้นแบบที่ใช้ในการระบุงค์คลาสในแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบสำหรับระบุงค์ข้อมูลทางโครงสร้างของแบบรูปความมั่นคงในส่วนขององค์ประกอบแบบจำลองในแบบรูปความมั่นคง
“spt” (Security Pattern data Type)	เป็นแม่พิมพ์ต้นแบบที่ใช้ในการระบุงค์ชนิดของข้อมูลในแบบรูปความมั่นคง	
“spr” (Security Pattern Relationship)	เป็นแม่พิมพ์ต้นแบบที่ใช้ในการระบุงค์ความสัมพันธ์ระหว่างคลาสในแบบรูปความมั่นคง	
แม่พิมพ์ต้นแบบสำหรับระบุงค์ข้อมูลทางความมั่นคงของแบบรูปความมั่นคงดังกล่าว		
“asset”	เป็นแม่พิมพ์ต้นแบบที่ใช้ระบุงค์คลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร	
“securityProperty”	เป็นแม่พิมพ์ต้นแบบที่ใช้ระบุงค์คุณสมบัติทางความมั่นคง	
“businessDriver”	เป็นแม่พิมพ์ต้นแบบที่ใช้ระบุงค์คลาสที่แสดงถึงตัวขับเคลื่อนทางธุรกิจขององค์กร	

2.2) สร้างป้ายระบุงค์ของแม่พิมพ์ต้นแบบ จากบทนิยามป้ายระบุงค์ [10] สำหรับแสดงข้อมูลทางโครงสร้างที่ระบุงค์ไว้ในขั้นตอนก่อนหน้านี้ เพื่อบอกถึงชื่อแบบรูปความมั่นคง บทบาทขององค์ประกอบแบบจำลองในแบบรูปความมั่นคง และลำดับของแบบรูปความมั่นคงที่ประยุกต์ใช้ในกรณีใช้แบบรูปซ้ำกัน โดยป้ายระบุงค์ของแม่พิมพ์ต้นแบบมีรูปแบบดังนี้

“role@name[instance]”

ทั้งนี้ป้ายระบุงค์ “role@name[instance]” ที่มีค่าเป็นบูลีนในแม่พิมพ์ต้นแบบ “spc” “spt” และ “spr” และแม่พิมพ์ต้นแบบที่ได้จากข้อมูลทางความมั่นคงทั้งหมด โดย “role” เป็นบทบาทขององค์ประกอบดังกล่าวในแบบรูปความมั่นคง “name” เป็นชื่อแบบรูปความมั่นคง และ “instance” เป็นลำดับของแบบรูปความมั่นคงในแผนภาพ ตัวอย่างของชื่อป้ายระบุงค์ขององค์ประกอบในแบบรูปความมั่นคง เช่น “asset@securityNeedsIdentification[1]” เป็นชื่อป้ายระบุงค์ที่แสดงถึงบทบาท “asset” ในแบบรูป “securityNeedsIdentification” ลำดับที่ 1 เป็นต้น โดยค่าของป้ายระบุงค์ดังกล่าวเป็นบูลีน จะมีค่าเป็นจริง เมื่อองค์ประกอบดังกล่าวมีลักษณะตามชื่อป้ายระบุงค์ กล่าวคือ องค์ประกอบดังกล่าวมีบทบาท “role” ในแบบรูป “name” ลำดับที่ “instance” ในแผนภาพ และจะมีค่าเป็นเท็จ เมื่อองค์ประกอบดังกล่าวไม่ได้มีลักษณะตามชื่อป้ายระบุงค์ กล่าวคือ องค์ประกอบดังกล่าวไม่ได้มีบทบาท “role” ในแบบรูป “name” ลำดับที่ “instance” ในแผนภาพ

จากความสัมพันธ์ระหว่างสินทรัพย์ทางด้านธุรกิจกับตัวขับเคลื่อนทางด้านธุรกิจขององค์กร และประเภทของสินทรัพย์ที่เป็นข้อมูลทางความมั่นคงของแบบรูปความมั่นคง

และแผนภาพคลาสที่แสดงโครงสร้างแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรที่ปรับปรุงแล้วนั้น สามารถสร้างป้ายระบุได้ดังตารางที่ 3.8

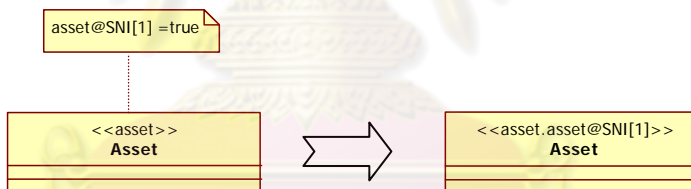
ตารางที่ 3.8 ป้ายระบุสำหรับระบุองค์ประกอบในแบบจำลองของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

ข้อมูลของแบบรูปความมั่นคง	ป้ายระบุ	แม่พิมพ์ต้นแบบ
ความสัมพันธ์ระหว่างสินทรัพย์ทางด้านธุรกิจกับตัวขับเคลื่อนทางด้านธุรกิจขององค์กร	asset-securityProperty@ securityNeedsIdentification	spc
ประเภทของสินทรัพย์	assetKind	asset
คุณสมบัติด้านความมั่นคงของสินทรัพย์	secureKind	securityProperty
ปัจจัยทางด้านธุรกิจขององค์กร	businessFactor	businessDriver

### 3) กำหนดรูปแบบของแม่พิมพ์ต้นแบบและค่าป้ายระบุ

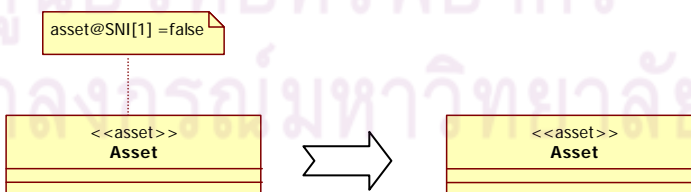
หลังจากทำการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุของแบบรูปความมั่นคงแล้ว ต่อมาจะทำการกำหนดรูปแบบของแม่พิมพ์ต้นแบบและค่าป้ายระบุนั้น ทั้งนี้เพื่อลดความซับซ้อนของแผนภาพที่เกิดจากการระบุข้อมูลของแบบรูปความมั่นคง อีกทั้งทำให้เข้าใจความหมายของแผนภาพได้ง่ายอีกด้วย โดยมีรายละเอียดดังนี้

3.1) ถ้าค่าของป้ายระบุจากบทนิยามป้ายระบุเป็น “จริง” ผู้ออกแบบสามารถลดรูปให้เหลือเพียงการระบุชื่อป้ายระบุเท่านั้น โดยการระบุชื่อป้ายระบุไว้ในเครื่องหมาย “<<” และ “>>” ของแม่พิมพ์ต้นแบบและคั่นด้วยเครื่องหมาย “.” ดังตัวอย่างในรูปที่ 3.5



รูปที่ 3.5 การลดรูปป้ายระบุที่มีค่าเป็นจริง

3.2) ถ้าค่าของป้ายระบุจากบทนิยามป้ายระบุเป็น “เท็จ” ผู้ออกแบบระบบไม่จำเป็นต้องระบุชื่อและค่าของป้ายระบุดังกล่าว ดังตัวอย่างในรูปที่ 3.6



รูปที่ 3.6 การลดรูปป้ายระบุที่มีค่าเป็นเท็จ

โดยจากรูปทั้ง 2 ป้ายระบุจะมีค่าเป็นจริงเมื่อ asset มาจากแบบรูป SNI และมีค่าเป็นเท็จเมื่อ asset ไม่ได้มาจากแบบรูป SNI ซึ่งจากการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุในขั้นตอนข้างต้น ผลลัพธ์คือ ได้แม่พิมพ์ต้นแบบและป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง แต่อย่างไรก็ตามการนำแม่พิมพ์



ต้นแบบมาประยุกต์ใช้นั้น จะต้องระบุข้อบังคับที่ต้องพิจารณาก่อนการใช้งานเสียก่อน โดยมีรายละเอียดดังหัวข้อต่อไป

### 3.6.2 ปรับปรุงเงื่อนไขบังคับของยูเอ็มแอล

หลังจากได้แม่พิมพ์ต้นแบบและป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงแล้ว ขั้นตอนนี้จะทำการปรับปรุงเงื่อนไขบังคับของแม่พิมพ์ต้นแบบที่ได้สำหรับพิจารณาก่อนการนำไปประยุกต์ใช้ ทั้งนี้เพื่อลดความผิดพลาดในการใช้งานแม่พิมพ์ต้นแบบดังกล่าว โดยมีรายละเอียดของการปรับปรุงเงื่อนไขบังคับดังนี้

1) ระบุข้อบังคับในการใช้งานของแต่ละแม่พิมพ์ต้นแบบ โดยในที่นี้ขอยกตัวอย่างแม่พิมพ์ต้นแบบ “spc” เป็นตัวอย่างในการปรับปรุงเงื่อนไขบังคับ ทั้งนี้เนื่องจากแม่พิมพ์ต้นแบบดังกล่าวแสดงองค์ประกอบหลักทางโครงสร้างของแบบรูปความมั่นคง โดยมีเงื่อนไขบังคับในการใช้งานแม่พิมพ์ต้นแบบ “spc” ดังนี้

1.1) ค่าป้ายระบุของแม่พิมพ์ต้นแบบไม่สามารถเป็นค่าว่างได้

1.2) ค่าป้ายระบุที่แสดงลำดับของแบบรูปความมั่นคงในแม่พิมพ์ต้นแบบสามารถเป็นค่าว่างได้ ถ้าแบบรูปดังกล่าวไม่ซ้ำกันในแผนภาพคลาส

1.3) ค่าป้ายระบุที่แสดงลำดับของแบบรูปความมั่นคงในแม่พิมพ์ต้นแบบไม่สามารถเป็นค่าว่างได้ ถ้าแบบรูปความมั่นคงดังกล่าวซ้ำกันในแผนภาพคลาส

2) ระบุนิพจน์ตามเงื่อนไขบังคับในการใช้งานแม่พิมพ์ต้นแบบ ให้เป็นนิพจน์ในภาษาไอซีแอล โดยแม่พิมพ์ต้นแบบ “spc” จะได้นิพจน์ที่ระบุเงื่อนไขบังคับในการใช้งาน คือ

2.1) นิพจน์ “ค่าป้ายระบุของแม่พิมพ์ต้นแบบไม่สามารถเป็นค่าว่างได้” จะมีนิพจน์ในรูปของภาษาไอซีแอล คือ

```
self.taggedValue.dataValue.name -> notEmpty
```

2.2) นิพจน์ “ค่าป้ายระบุที่แสดงลำดับของแบบรูปความมั่นคงในแม่พิมพ์ต้นแบบสามารถเป็นค่าว่างได้ ถ้าแบบรูปดังกล่าวไม่ซ้ำกันในแผนภาพคลาส” จะมีนิพจน์ในรูปของภาษาไอซีแอล คือ

```
self.taggedValue.name->forall(v1, v2:name | v1.name <> v2.name)
```

```
implies (v1.instance->isEmpty and v2.instance->isEmpty)
```

2.3) นิพจน์ “ค่าป้ายระบุที่แสดงลำดับของแบบรูปความมั่นคงในแม่พิมพ์ต้นแบบไม่สามารถเป็นค่าว่างได้ ถ้าแบบรูปความมั่นคงดังกล่าวซ้ำกันในแผนภาพคลาส” จะมีนิพจน์ในรูปของภาษาไอซีแอล คือ

```
self.taggedValue.name->exist(v1, v2:name | v1.name = v2.name) implies
```

```
(v1.instance->notEmpty and v2.instance->notEmpty and v1.instance <> v2.instance)
```

จากกระบวนการในการปรับปรุงยูเอ็มแอลสำหรับแสดงแบบรูปความมั่นคงดังกล่าวข้างต้นจะได้ ยูเอ็มแอลเซคเอสพี-2 (UMLsec SP-2) โดยประกอบด้วยรายการของแม่พิมพ์ต้นแบบ และป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปดังตารางที่ 3.9 และ 3.10 ตามลำดับ โดยรายการของแม่พิมพ์ต้นแบบ ประกอบด้วย ชื่อแบบรูปความมั่นคง คำอธิบายของแบบรูปความมั่นคง แม่พิมพ์ต้นแบบ คลาสพื้นฐาน (Base class) ที่ใช้แม่พิมพ์ต้นแบบ ป้ายระบุที่ใช้ในแม่พิมพ์ต้นแบบ เงื่อนไขบังคับของแม่พิมพ์ต้นแบบ และคำอธิบายของแม่พิมพ์ต้นแบบ ส่วนรายการของป้ายระบุ ประกอบไปด้วย ชื่อแบบรูปความมั่นคง ป้ายระบุ แม่พิมพ์ต้นแบบที่ใช้ ค่าของป้ายระบุ ตัวอย่างค่าของป้ายระบุ มัลติพลิซิติที่คำอธิบายของป้ายระบุ และแผนภาพคลาสของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรที่ใช้ยูเอ็มแอลเซคเอสพี-2 แสดงดังรูปที่ 3.7



ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

ตารางที่ 3.9 รายการของแม่พิมพ์ต้นแบบและเงื่อนไขบังคับสำหรับแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

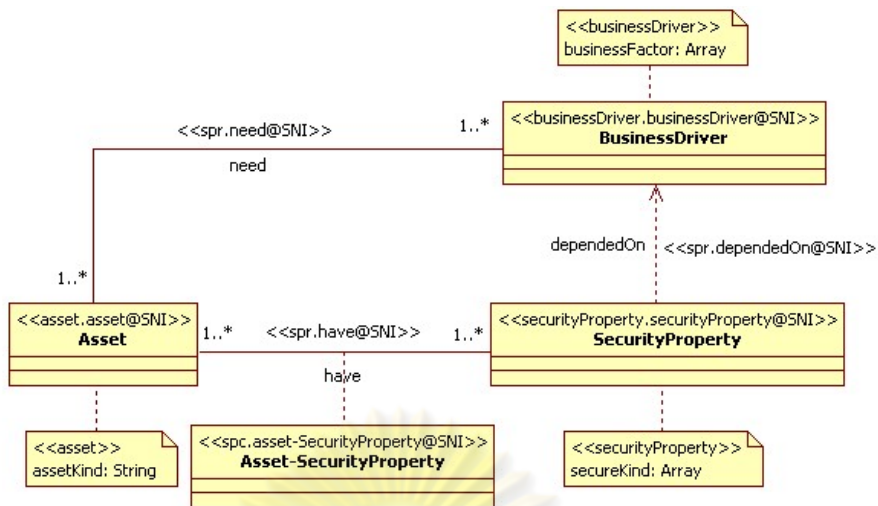
แม่พิมพ์ต้นแบบและเงื่อนไขบังคับสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร						
แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	คำอธิบาย	เงื่อนไขบังคับ		
spc (Security Pattern Class)	Class	"role@name[instance]"	คลาสที่เป็นองค์ประกอบภายในแบบรูปความมั่นคง	1> self.taggedValue.dataValue.name -> notEmpty 2> self.taggedValue.name -> forall(v1, v2:name   v1.name <> v2.name)		
spt (Security Pattern data Type)	Class	"role@name[instance]"	คลาสที่เป็นแบบชนิดข้อมูลภายในแบบรูปความมั่นคง	implies (v1.instance -> isEmpty and v2.instance -> isEmpty) 3> self.taggedValue.name -> exists(v1, v2:name   v1.name = v2.name)		
spr (Security Pattern Relationship)	Relationship	"role@name[instance]"	ความสัมพันธ์ระหว่างคลาสที่เป็นองค์ประกอบภายในแบบรูปความมั่นคง	implies (v1.instance -> notEmpty and v2.instance -> notEmpty and v1.instance <> v2.instance)		
แม่พิมพ์ต้นแบบและเงื่อนไขบังคับสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร						
แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	คำอธิบาย	เงื่อนไขบังคับ
การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Asset)	เป็นแบบรูปที่เสนอการพิจารณาความมั่นคงขององค์กร โดยทำการระบุสินทรัพย์ที่สำคัญขององค์กร เพื่อหาวิธีป้องกันสินทรัพย์ต่างๆ เหล่านั้น	asset	Class	assetKind และ "role@name[instance]"	สินทรัพย์ทางด้านธุรกิจขององค์กร	1> self.taggedValue -> forall(tv tv.name ="assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)
		securityProperty	Class	secureKind และ "role@name[instance]"	คุณสมบัติทางด้านความมั่นคง	1> self.taggedValue -> forall(tv tv.name ="secureKind") implies (tv.dataValue = Confidentiality or tv.dataValue = Integrity or tv.dataValue = Availability or tv.dataValue = Accountaability)
		businessDriver	Class	businessFactor และ "role@name[instance]"	ตัวขับเคลื่อนทางด้านธุรกิจขององค์กร	1> self.taggedValue -> forall(tv tv.name ="businessFactor") implies (tv.dataValue -> isEmpty)

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

ตารางที่ 3.10 รายการของป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

รายการของป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร					
ป้ายระบุ	แม่พิมพ์ต้นแบบ	ค่าของป้ายระบุ	ตัวอย่างค่าของป้ายระบุ	มัลติพลิซิติ	คำอธิบาย
"role@name[instance]"	แม่พิมพ์ต้นแบบที่สร้างทั้งหมด	บูลีนแสดงลักษณะองค์ประกอบดังกล่าวในแบบรูป	true หรือ false	*	ระบุว่า องค์ประกอบดังกล่าวมีบทบาท "role" ในแบบรูป "name" ลำดับที่ "instance" ในแผนภาพหรือไม่
รายการของป้ายระบุสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร					
แบบรูปความมั่นคง	ป้ายระบุ	แม่พิมพ์ต้นแบบ	ตัวอย่างค่าของป้ายระบุ	มัลติพลิซิติ	คำอธิบาย
การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Asset)	assetKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	secureKind	securityProperty	Confidentiality, Integrity, Availability, Accountaability	*	คุณสมบัติด้านความมั่นคงของสินทรัพย์
	businessFactor	businessDriver	Laws, Goals, Business processes, etc.	*	ปัจจัยทางด้านธุรกิจขององค์กร

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย



รูปที่ 3.7 แผนภาพคลาสของแบบรูปการระบุความต้องการความมั่นคง สำหรับสินทรัพย์องค์กรที่ใช้ยูเอ็มแอลเซคเอสพี-2

จากรูปที่ 3.7 แสดงการนำยูเอ็มแอลเซคเอสพี-2 มาใช้ในการแสดงข้อมูลทางโครงสร้าง และข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร โดยแม่พิมพ์ต้นแบบ “<<asset.asset@SNI>>” ที่กำกับอยู่ในคลาส “Asset” เพื่อระบุว่า คลาสดังกล่าวเป็นสินทรัพย์ขององค์กรและเป็นองค์ประกอบในแบบรูป แม่พิมพ์ต้นแบบ “<<securityProperty.securityProperty@SNI>>” กำกับที่คลาส “SecurityProperty” เพื่อระบุว่า คลาสดังกล่าว เป็นคุณสมบัติทางด้านความมั่นคงและเป็นองค์ประกอบในแบบรูป แม่พิมพ์ ต้นแบบ “<<spc.asset-SecurityProperty@SNI>>” กำกับที่คลาส “aset-SecurityProperty” เพื่อระบุว่า คลาสดังกล่าวเป็นความสัมพันธ์ระหว่างสินทรัพย์ทางด้านธุรกิจขององค์กรกับ สินทรัพย์ทางด้านธุรกิจขององค์กร และเป็นองค์ประกอบในแบบรูป แม่พิมพ์ต้นแบบ “<<businessDriver.businessDriver@SNI>>” กำกับที่คลาส “BusinessDriver” เพื่อระบุว่า คลาสดังกล่าวเป็นตัวขับเคลื่อนทางด้านธุรกิจขององค์กรและเป็นองค์ประกอบในแบบรูป

### 3.6 การตรวจสอบยูเอ็มแอลเซคเอสพี-2

ในการตรวจสอบยูเอ็มแอลเซคเอสพี-2 นั้นจะพิจารณาจากข้อกำหนดความต้องการของ ยูเอ็มแอลโพรไฟล์ (UML Profile Specification) ตามที่ [14] ได้กล่าวไว้ โดยยูเอ็มแอลเซค เอสพี-2 จะต้องมีความสอดคล้องกับข้อกำหนดความต้องการดังนี้

- 1) เป็นขอบเขตของยูเอ็มแอลเมตาโมเดล (UML Metamodel)

จากบทนิยามป้ายระบุแบบรูป ที่มีชื่อแบบรูป บทบาทในแบบรูป และลำดับของแบบรูป เป็นองค์ประกอบซึ่งใช้สำหรับกำหนดชื่อป้ายระบุ โดยมีรูปแบบคือ “role@name[instance]” ซึ่งยูเอ็มแอลเซคเอสพี-2 นั้น มาจากการขยายยูเอ็มแอลที่เป็นกลไกภายในของยูเอ็มแอลเมตา โมเดล ดังนั้นยูเอ็มแอลที่ปรับปรุงเพิ่มเติมจึงเป็นขอบเขตของยูเอ็มแอลเมตาโมเดล

2) มีกฎการควบคุมรูปแบบการใช้งาน (Well-Formedness Rules) ขององค์ประกอบ

ยูเอ็มแอลเซคเอสพี-2 นั้นได้กำหนดเงื่อนไขบังคับในการควบคุมรูปแบบการใช้งานของแม่พิมพ์ต้นแบบซึ่งอยู่ในรูปของภาษาโอซีแอล เช่น เงื่อนไขบังคับที่ว่า “ค่าของป้ายระบุของแม่พิมพ์ต้นแบบไม่สามารถเป็นค่าว่างได้” เป็นต้น ดังนั้นยูเอ็มแอลเซคเอสพี-2 จึงมีกฎการควบคุมรูปแบบการใช้งาน

3) ใช้ระบุองค์ประกอบที่นอกเหนือจากองค์ประกอบมาตรฐานของยูเอ็มแอล

จากที่กล่าวในตอนต้นว่า แม่พิมพ์ต้นแบบและป้ายระบุของยูเอ็มแอล ไม่สามารถแสดงรายละเอียดขององค์ประกอบแบบจำลองสำหรับแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ ดังนั้นงานวิทยานิพนธ์นี้จึงการปรับปรุงแม่พิมพ์ต้นแบบและป้ายระบุเพื่อรองรับการแสดงผลดังกล่าว

4) มีการกำหนดความหมายของแต่ละองค์ประกอบ

ยูเอ็มแอลเซคเอสพี-2 นั้นได้อธิบายความหมายของแต่ละองค์ประกอบในรายการของแม่พิมพ์ต้นแบบและรายการของป้ายระบุ เช่น แม่พิมพ์ต้นแบบ asset หมายถึง สินทรัพย์ทางด้านธุรกิจขององค์กร หรือ แม่พิมพ์ต้นแบบ businessDriver ที่หมายถึง ปัจจัยทางด้านธุรกิจขององค์กร เป็นต้น

5) มีการกำหนดองค์ประกอบแบบจำลองที่ใช้ในองค์ประกอบที่ได้สร้างไว้

ยูเอ็มแอลเซคเอสพี-2 นั้นได้กำหนดคลาสพื้นฐานของแต่ละแม่พิมพ์ต้นแบบที่แสดงถึงประเภทขององค์ประกอบแบบจำลอง เช่น แม่พิมพ์ต้นแบบ asset มีคลาสพื้นฐานคือ Class หรือแม่พิมพ์ต้นแบบ spr มีคลาสพื้นฐานคือ Relationship เป็นต้น

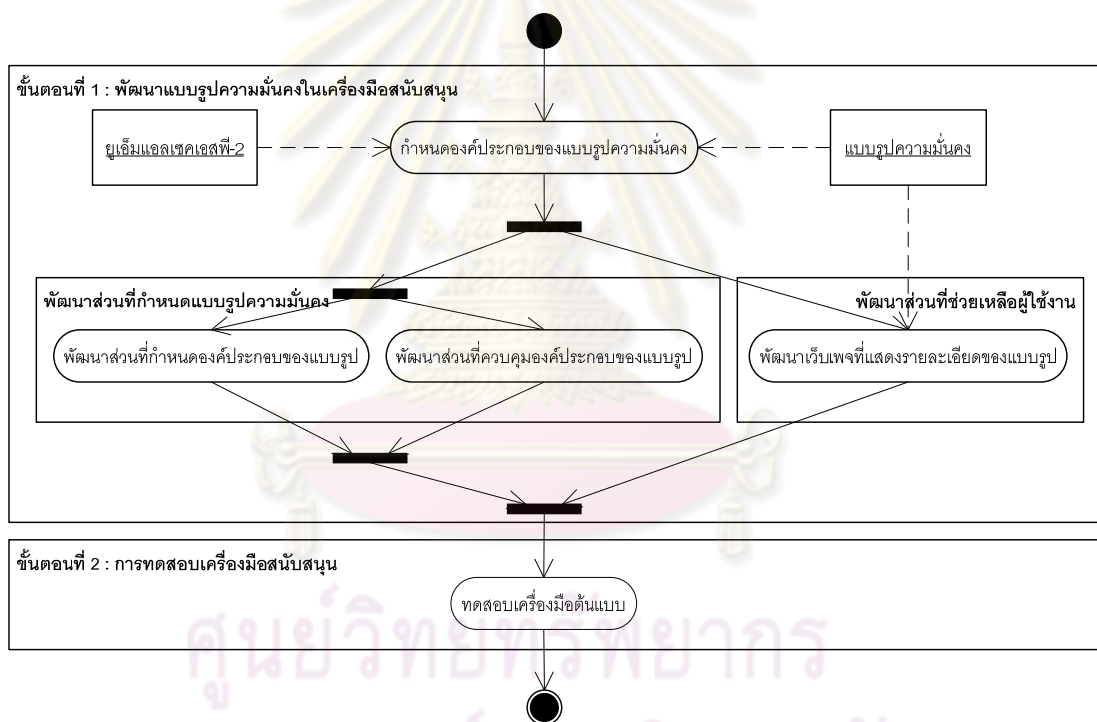
จากการวิเคราะห์ข้อกำหนดความต้องการของยูเอ็มแอลโพรไฟล์ที่ได้กล่าวมาในข้างต้น โดยการทวนสอบยูเอ็มแอลเซคเอสพี-2 พบว่า ยูเอ็มแอลเซคเอสพี-2 มีข้อมูลและลักษณะพื้นฐานต่างๆ ไม่แตกต่างจากยูเอ็มแอลโพรไฟล์ ดังนั้นยูเอ็มแอลเซคเอสพี-2 จึงมีความสอดคล้องกับข้อกำหนดความต้องการ

โดยแสดงรายละเอียดของยูเอ็มแอลเซคเอสพี-2 ของแบบรูปความมั่นคงที่อยู่ในขอบเขตของงานวิทยานิพนธ์ ในภาคผนวก ข ส่วนในภาคผนวก ค แสดงการประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแต่ละแบบรูปความมั่นคง และในภาคผนวก ง แสดงกรณีศึกษาเพื่อประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 สำหรับแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง

## บทที่ 4

### การพัฒนาและทดสอบเครื่องมือสนับสนุน การแสดงผลแบบรูปความมั่นคง

หลังจากการปรับปรุงยูเอ็มแอลเพื่อแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงแล้วผลลัพธ์คือ ได้ยูเอ็มแอลที่ปรับปรุงเพิ่มเติมแล้ว ซึ่งก็คือ ยูเอ็มแอลเซคเอสพี-2 แต่การนำยูเอ็มแอลเซคเอสพี-2 ไปประยุกต์ใช้นั้นควรมีเครื่องมือสนับสนุนการใช้งานเพื่อให้ง่ายต่อการประยุกต์ใช้ ดังนั้นในงานวิทยานิพนธ์นี้จึงได้พัฒนาเครื่องมือสนับสนุนการแสดงผลแบบรูปความมั่นคงที่อยู่บนพื้นฐานของยูเอ็มแอลเซคเอสพี-2 เพื่อเพิ่มความสะดวกกับผู้ใช้งานในการนำยูเอ็มแอลเซคเอสพี-2 ไปประยุกต์ใช้ โดยมีขั้นตอนหลักๆ ดังแผนภาพกิจกรรม ดังรูปที่ 4.1



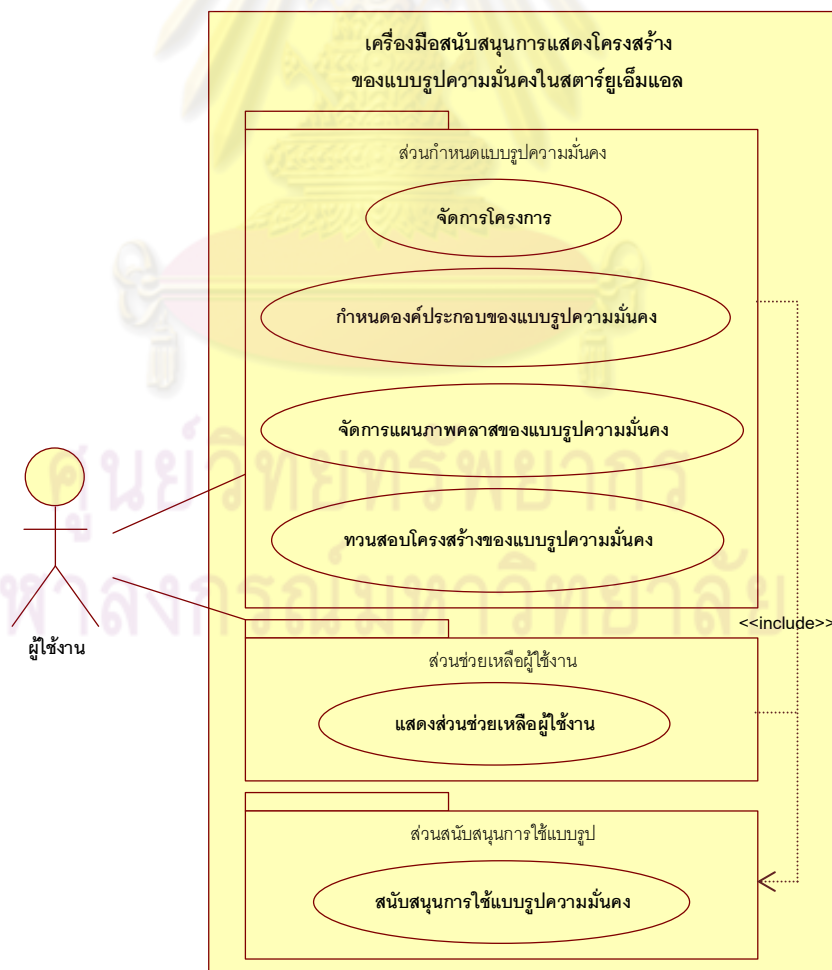
รูปที่ 4.1 แผนภาพกิจกรรมแสดงขั้นตอนการพัฒนา  
และทดสอบเครื่องมือสนับสนุนการแสดงผลแบบรูปความมั่นคง

จากรูป ขั้นตอนที่ 1 เป็นขั้นตอนการพัฒนาแบบรูปความมั่นคงในเครื่องมือสนับสนุน ซึ่งมีการพัฒนาในส่วนกำหนดแบบรูปความมั่นคง และการพัฒนาส่วนช่วยเหลือผู้ใช้งาน หลังจากพัฒนาเครื่องมือสนับสนุนแล้วขั้นตอนต่อมาคือ การทดสอบเครื่องมือสนับสนุน ซึ่งจะแสดงในขั้นตอนที่ 2 โดยมีรายละเอียดของแต่ละขั้นตอน ดังนี้

#### 4.1 การพัฒนาแบบรูปความมั่นคงในเครื่องมือสนับสนุน

ในงานวิทยานิพนธ์นี้ผู้วิจัยแนวคิดที่จะพัฒนาเครื่องมือต้นแบบ โดยการพัฒนาส่วนเพิ่มเติมจากเครื่องมือที่ใช้ในการเขียนยูเอ็มแอลที่เป็นซอฟต์แวร์โอเพนซอร์ส (Open Source Software) ซึ่งเป็นซอฟต์แวร์ที่ผู้พัฒนาสามารถนำซอสโค้ด (Source Code) ไปปรับเปลี่ยนตามความต้องการได้ โดยในการพัฒนาเครื่องมือสนับสนุนการแสดงผลแบบรูปความมั่นคงนี้ ผู้วิจัยได้นำสตาร์ยูเอ็มแอล (StarUML) มาใช้ในการพัฒนา ทั้งนี้เนื่องจากสตาร์ยูเอ็มแอลมีความยืดหยุ่น และสามารถขยายความสามารถของโปรแกรมได้ โดยการสร้างส่วนขยายของโปรแกรมเพื่อเสริมความสามารถในส่วนที่ต้องการ อีกทั้งมีฟังก์ชันที่ช่วยในการพัฒนาส่วนต่อเติมของโปรแกรม นั่นคือ โอเพนเอพีไอ (Open API)

โดยงานวิจัยนี้มีแนวคิดที่จะปรับปรุงส่วนสนับสนุนการใช้แบบรูปในการออกแบบ โดยการเพิ่มแผนภาพคลาสที่แสดงโครงสร้างของแต่ละแบบรูปความมั่นคง ซึ่งใช้ยูเอ็มแอลเซคเอสพี-2 และเพิ่มเติมส่วนที่อธิบายการใช้งานแบบรูปความมั่นคงเพื่อช่วยให้ผู้ใช้งานเข้าใจแบบรูปความมั่นคงได้ดียิ่งขึ้น โดยแสดงแผนภาพการติดต่อกันระหว่างผู้ใช้งาน (Actors) กับฟังก์ชันงานต่างๆ ในเครื่องมือสนับสนุน ดังรูปที่ 4.2 และแสดงโครงสร้างของเครื่องมือสนับสนุน ดังรูปที่ 4.3 ซึ่งมีรายละเอียดดังนี้

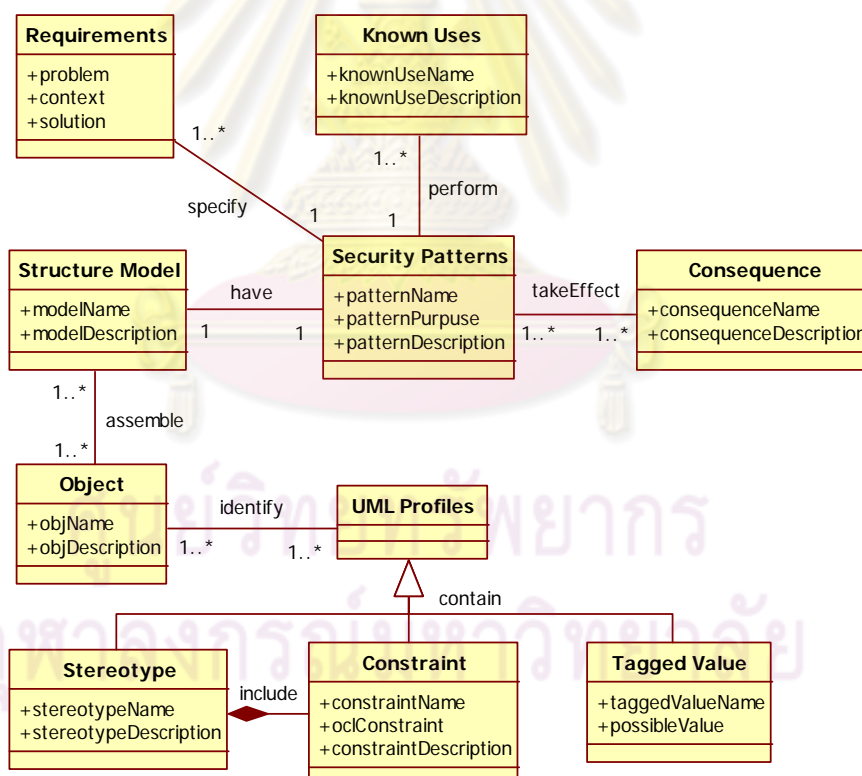


รูปที่ 4.2 หน้าี่การทำงานของเครื่องมือสนับสนุน



จากรูป หน้าี่การทำงานของเครื่องมือสนับสนุน ประกอบไปด้วย 6 ฟังก์ชันงาน ซึ่งมีรายละเอียด ดังนี้

- ส่วนจัดการโครงการ เป็นส่วนของการสร้างโครงการจากโปรแกรม
- ส่วนกำหนดองค์ประกอบของแบบรูปความมั่นคง เป็นส่วนของการระบุองค์ประกอบต่างๆ ของแบบรูปความมั่นคง
- ส่วนจัดการแผนภาพคลาสของแบบรูปความมั่นคง เป็นส่วนของการสร้างแผนภาพคลาสเพื่อแสดงแบบรูปความมั่นคง
- ส่วนทวนสอบโครงสร้างของแบบรูปความมั่นคง เป็นส่วนของการตรวจสอบความถูกต้องของแผนภาพที่สร้างขึ้นโดยผู้ใช้งาน โดยเป็นไปตามข้อกำหนดความต้องการของยูเอ็มแอลโพรไฟล์
- ส่วนแสดงส่วนช่วยเหลือผู้ใช้งาน เป็นส่วนของการแสดงรายละเอียดต่างๆ ของแบบรูปความมั่นคงเพื่อช่วยผู้ใช้งานเข้าใจแบบรูปความมั่นคงนั้นๆ
- ส่วนสนับสนุนการใช้แบบรูปความมั่นคง เป็นส่วนของการออกแบบโครงสร้างของแบบรูปความมั่นคง และรายละเอียดต่างๆ ของแบบรูปความมั่นคง



รูปที่ 4.3 โครงสร้างของเครื่องมือสนับสนุน

จากแผนภาพคลาสที่แสดงโครงสร้างของเครื่องมือสนับสนุน ประกอบด้วย 9 คลาส โดยมีรายละเอียดดังตารางที่ 4.1

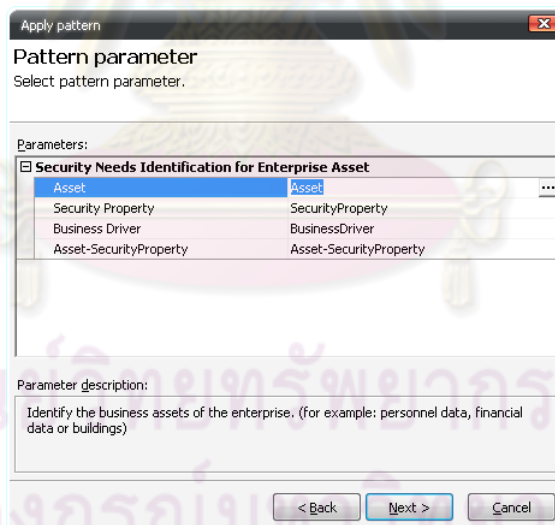
ตารางที่ 4.1 รายละเอียดของแผนภาพคลาสที่แสดงโครงสร้างของเครื่องมือสนับสนุน

คลาส	คำอธิบาย
Security Patterns	เป็นคลาสของแบบรูปความมั่นคง
Known Uses	เป็นคลาสของการประยุกต์ใช้แบบรูปความมั่นคง
Consequence	เป็นคลาสของประโยชน์ที่จะได้รับเมื่อประยุกต์ใช้แบบรูป
Requirements	เป็นคลาสของความต้องการทางด้านความมั่นคง
Structure Model	เป็นคลาสของแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง
Object	เป็นคลาสของอ็อบเจกต์ในแบบรูปความมั่นคง
UML Profiles	เป็นคลาสของยูเอ็มแอลโพรไฟล์
Stereotype	เป็นคลาสของแม่พิมพ์ต้นแบบ
Constraint	เป็นคลาสของเงื่อนไขบังคับ

โดยมีขั้นตอนของการพัฒนาแบบรูปความมั่นคง ดังนี้

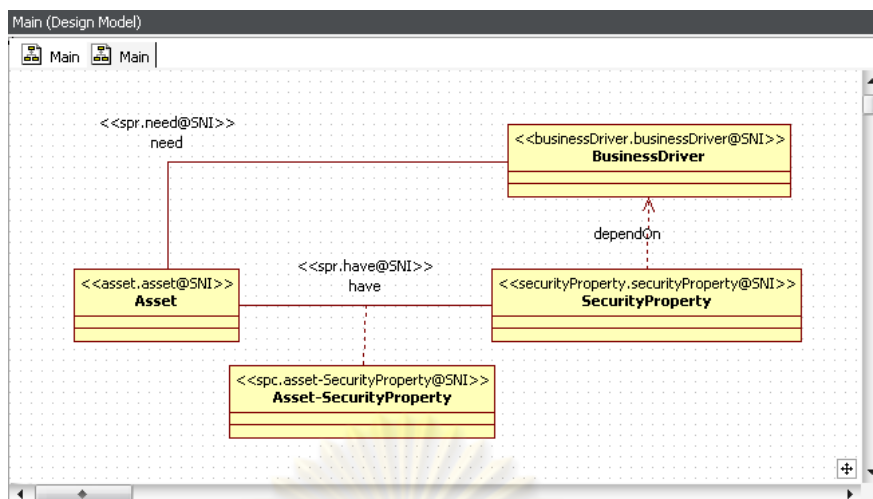
### 1) การพัฒนาส่วนกำหนดแบบรูปความมั่นคง มีการพัฒนา 2 ส่วนดังนี้

1.1) ส่วนกำหนดองค์ประกอบของแบบรูปความมั่นคง โดยในส่วนนี้จะเป็นการพัฒนาโดยใช้ภาษาเอกซ์เอ็มแอล (eXtensible Markup Language: XML) และทำการระบุองค์ประกอบต่างๆ ของแบบรูปความมั่นคง โดยแสดงหน้าต่างตัวอย่างของส่วนกำหนดองค์ประกอบของแบบรูปความมั่นคง ดังรูปที่ 4.4



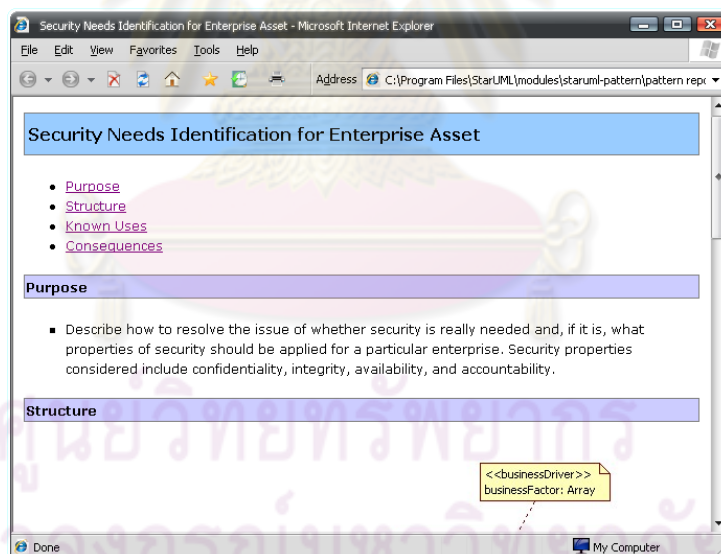
รูปที่ 4.4 หน้าต่างแสดงตัวอย่างของส่วนกำหนดองค์ประกอบของแบบรูปความมั่นคง

1.2) ส่วนควบคุมองค์ประกอบของแบบรูปความมั่นคง ในส่วนนี้จะนำโอเพนเอพีไอของสตาร์ยูเอ็มแอลมาพัฒนาร่วมกับภาษาจาวาสคริปต์ (JavaScript) และทำการกำหนดแม่พิมพ์ต้นแบบ ป้ายระบุ และเงื่อนไขบังคับโดยใช้ยูเอ็มแอลที่ปรับปรุงเพิ่มเติมในแต่ละองค์ประกอบของแบบรูปความมั่นคง ซึ่งจะได้ผลลัพธ์คือ โครงสร้างของแบบรูปความมั่นคงในรูปของแผนภาพคลาสของยูเอ็มแอล โดยแสดงตัวอย่างแผนภาพคลาสของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร ดังรูปที่ 4.5



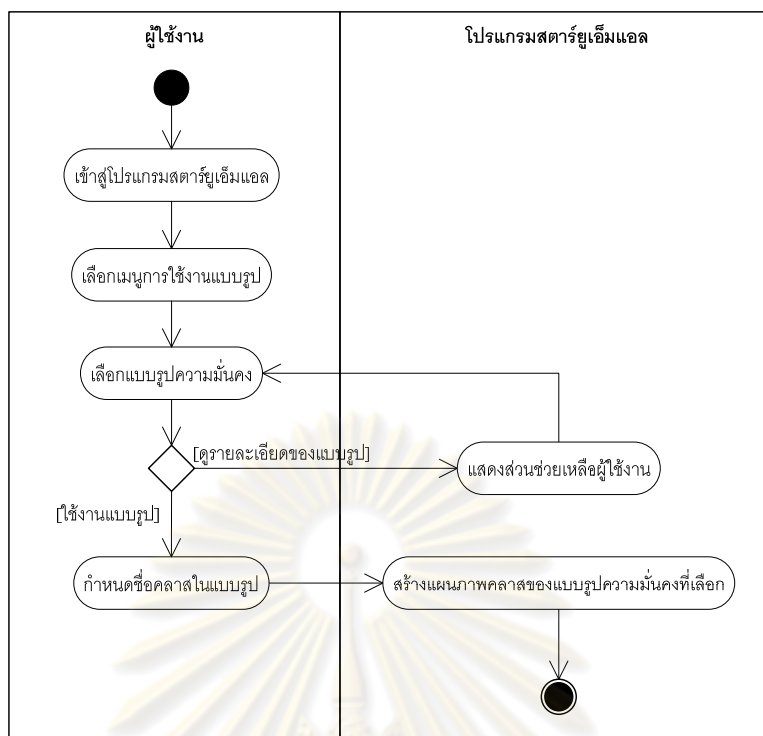
รูปที่ 4.5 ตัวอย่างแผนภาพคลาสของแบบรูปการระบุความต้องการ  
ความมั่นคงสำหรับสินทรัพย์องค์กร

2) การพัฒนาส่วนช่วยเหลือผู้ใช้งาน การพัฒนาในส่วนช่วยเหลือผู้ใช้งานนี้จะนำภาษาเอชทีเอ็มแอล (Hyper Text Markup Language: HTML) มาใช้ โดยจะแสดงรายละเอียดต่างๆ ของแบบรูปความมั่นคงที่ผู้ใช้เลือก โดยแสดงตัวอย่างหน้าต่างของส่วนช่วยเหลือผู้ใช้งาน ของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร ดังรูปที่ 4.6



รูปที่ 4.6 หน้าต่างของส่วนช่วยเหลือผู้ใช้งานของแบบรูปการระบุ  
ความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

หลังจากพัฒนาแบบรูปความมั่นคงในเครื่องมือสนับสนุนแล้ว จะได้เครื่องมือสนับสนุนการแสดงผลแบบรูปความมั่นคง ซึ่งประกอบด้วยการทำงาน 2 ส่วนด้วยกัน คือ ส่วนสร้างแผนภาพคลาสของแบบรูปความมั่นคง และส่วนแสดงส่วนช่วยเหลือผู้ใช้งาน โดยแสดงรายละเอียดของการทำงานของเครื่องมือสนับสนุน ดังรูปที่ 4.7

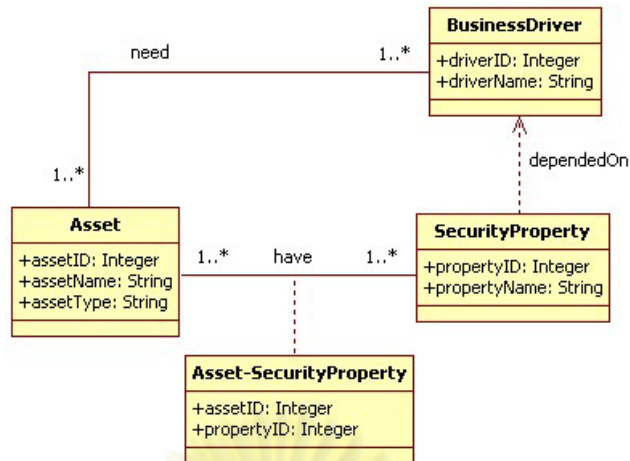


รูปที่ 4.7 แผนภาพกิจกรรมแสดงขั้นตอนการทำงานของเครื่องมือสับสนุ่น

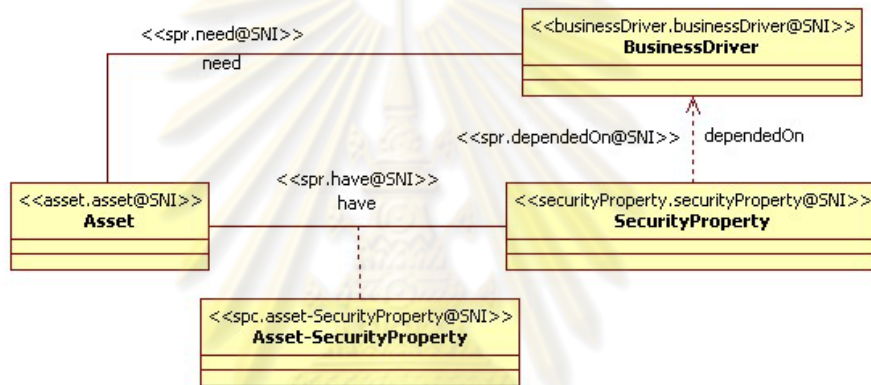
โดยแสดงรายละเอียดของขั้นตอนการทำงานของเครื่องมือสับสนุ่นดังนี้

### 1) ส่วนสร้างแผนภาพคลาสของแบบรูปความมั่นคง

ในส่วนของการสร้างแผนภาพคลาสของแบบรูปความมั่นคง เป็นส่วนสำคัญ ของเครื่องมือสับสนุ่น ซึ่งจะช่วยในการกำหนดโครงสร้างของแผนภาพคลาสของแบบรูปความมั่นคง โดยที่ผู้ใช้งานจะเป็นคนเลือกแบบรูปความมั่นคงที่ต้องการนำไปประยุกต์ใช้ อีกทั้งยังสามารถสร้างองค์ประกอบของแบบรูปขึ้นมาใหม่ หรือเลือกองค์ประกอบที่มีในแผนภาพที่ผู้ใช้เลือกได้ หลังจากนั้นเครื่องมือสับสนุ่นจะทำการสร้างองค์ประกอบของแบบรูปความมั่นคง โดยใช้ยูเอ็มแอลที่ปรับปรุงเพิ่มเติม ในการแสดงแบบรูปความมั่นคงในรูปของแผนภาพคลาส โดยแสดงตัวอย่างของแผนภาพคลาสของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรที่เป็นต้นแบบ และแผนภาพคลาสของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร ที่สร้างมาจากส่วนสนุ่นการใช้แบบรูปความมั่นคง ดังรูปที่ 4.8 และรูปที่ 4.9 ตามลำดับ



รูปที่ 4.8 แผนภาพคลาสของแบบรูปการระบุความต้องการ  
ความมั่นคงสำหรับสินทรัพย์องค์กรที่เป็นต้นแบบ

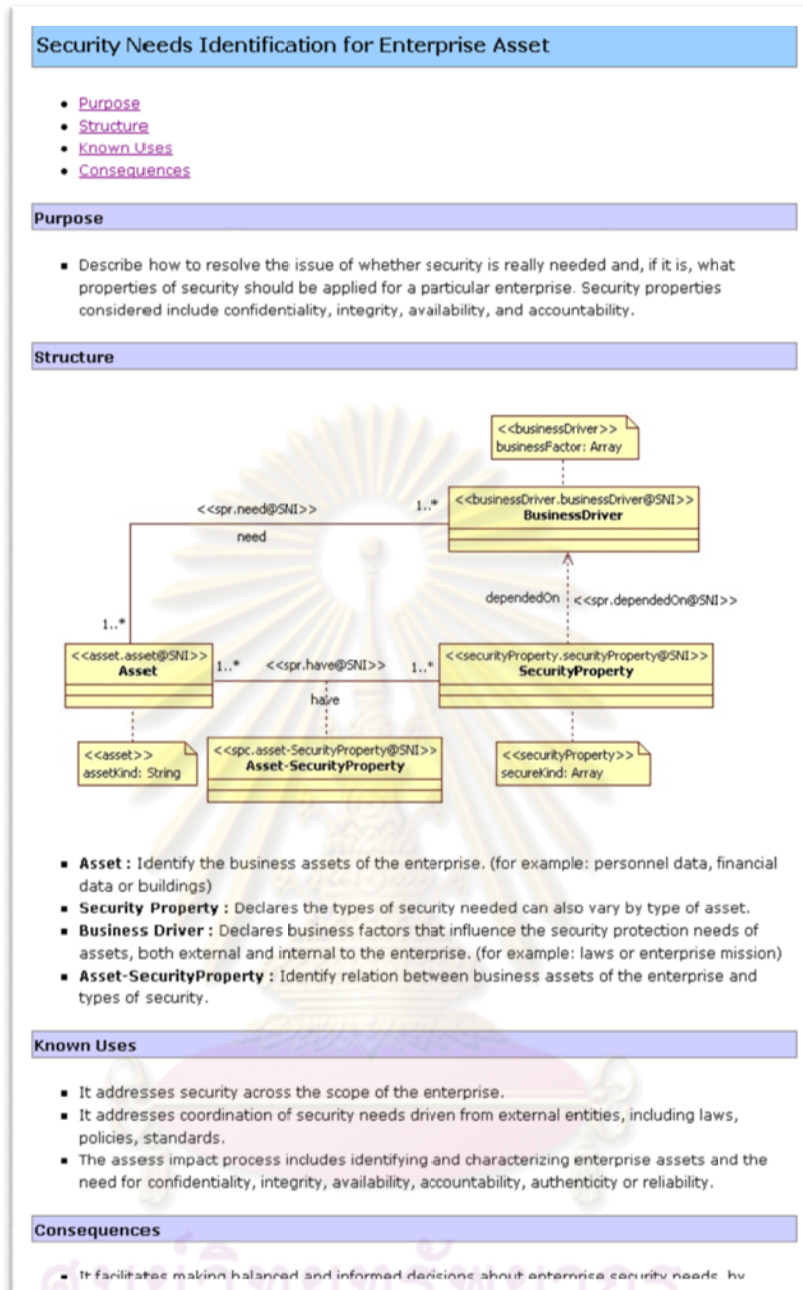


รูปที่ 4.9 แผนภาพคลาสของแบบรูปการระบุความต้องการความมั่นคง  
สำหรับสินทรัพย์องค์กรที่สร้างมาจากเครื่องมือสนับสนุน

โดยในแต่ละองค์ประกอบของแบบรูป ที่สร้างมาจากเครื่องมือสนับสนุนนี้ แสดงให้เห็นถึงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรโดยใช้ยูเอ็มแอลที่ปรับปรุงเพิ่มเติม

## 2) ส่วนช่วยเหลือผู้ใช้งาน

ในส่วนช่วยเหลือผู้ใช้งานนี้ เป็นส่วนของการช่วยเหลือผู้ใช้งานโดยจะแสดงข้อมูลและรายละเอียดต่าง ๆ ของแบบรูปความมั่นคงที่ผู้ใช้เลือก ซึ่งจะช่วยให้ผู้ใช้งานเข้าใจในแบบรูปความมั่นคงที่เลือกได้เป็นอย่างดี โดยส่วนช่วยเหลือผู้ใช้งานนี้จะประกอบไปด้วย จุดประสงค์ในการใช้แบบรูปความมั่นคง (Purpose) โครงสร้างของแบบรูปความมั่นคง (Structure) ตัวอย่างของการประยุกต์ใช้แบบรูปความมั่นคง (Known Uses) และประโยชน์ที่จะได้รับ (Consequence) โดยในที่นี้ขอยกตัวอย่างของส่วนช่วยเหลือผู้ใช้งานของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร ดังรูปที่ 4.10



รูปที่ 4.10 ส่วนช่วยเหลือผู้ใช้งานของแบบรูปการระบุความต้องการ  
ความมั่นคงสำหรับสินทรัพย์องค์กร

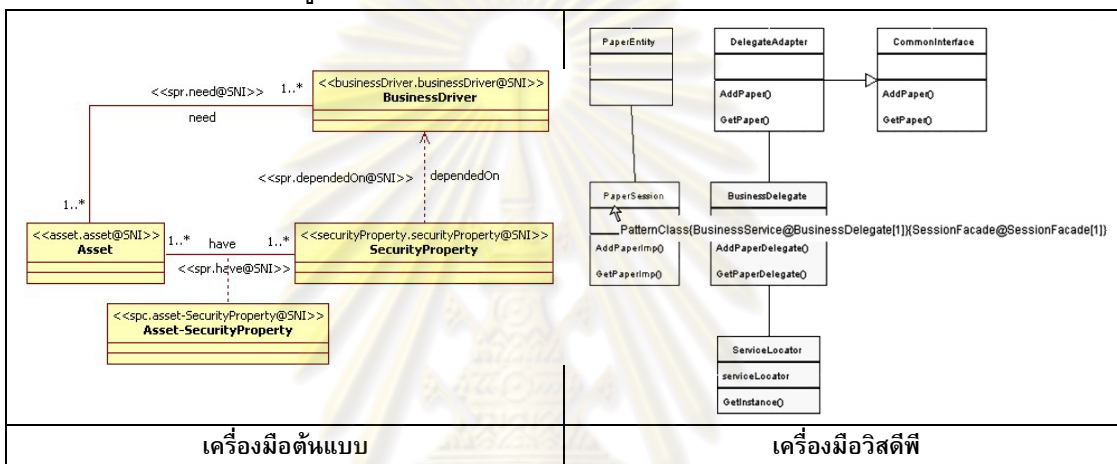
โดยแสดงรายละเอียดการใช้งานเครื่องมือสนับสนุนและผลลัพธ์ที่ได้จากเครื่องมือสนับสนุนในภาคผนวก จ

#### 4.2 การทดสอบเครื่องมือสนับสนุน

หลังจากพัฒนาเครื่องมือต้นแบบสำหรับสนับสนุนการแสดงแบบรูปความมั่นคงแล้ว ในขั้นตอนนี้จะทำการตรวจสอบเครื่องมือสนับสนุน ว่ามีความสามารถที่ตรงกับความต้องการในการแสดงข้อมูลต่าง ๆ ของแบบรูปความมั่นคงหรือไม่ อีกทั้งยังเปรียบเทียบความสามารถของเครื่องมือต้นแบบที่พัฒนาขึ้นกับเครื่องมือเครื่องมือสำหรับแสดงข้อมูลทางโครงสร้างของ

แบบรูปการออกแบบ โดยในที่นี่จะนำเครื่องมือที่ชื่อ วิสตีพี (Visualize Design Pattern: VisDP) มาเปรียบเทียบ ซึ่งเป็นเครื่องมือที่เป็นส่วนเสริมของเครื่องมือสำหรับเขียนเขียนแผนภาพยูเอ็มแอล เช่น แรชันแนลโรส (Rational Rose) เป็นต้น ทั้งนี้เพราะเครื่องมือวิสตีพีสามารถสร้างแบบรูปการออกแบบที่แสดงให้เห็นถึงข้อมูลต่างๆ ได้เป็นอย่างดี โดยแสดงตัวอย่างของแผนภาพคลาสที่ได้จากเครื่องมือต้นแบบและเครื่องมือวิสตีพีเพื่อเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคง ดังตารางที่ 4.2 และแสดงการเปรียบเทียบความสามารถของเครื่องมือต้นแบบกับเครื่องมือวิสตีพี ดังตารางที่ 4.3

ตารางที่ 4.2 ตัวอย่างของแผนภาพคลาสที่ได้จากเครื่องมือต้นแบบและเครื่องมือวิสตีพีเพื่อเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคง



ตารางที่ 4.3 การเปรียบเทียบความสามารถของเครื่องมือต้นแบบกับเครื่องมือวิสตีพี

ฟังก์ชันการทำงาน	เครื่องมือต้นแบบ	เครื่องมือวิสตีพี
- การกำหนดข้อมูลและองค์ประกอบของแบบรูปความมั่นคง	เครื่องมือช่วยกำหนดบางส่วน	ผู้ใช้งานกำหนดเองทั้งหมด
- การตรวจสอบข้อมูลและองค์ประกอบของแบบรูปความมั่นคง	เครื่องมือช่วยตรวจสอบบางส่วน	ผู้ใช้งานตรวจสอบเองทั้งหมด
- การแสดงข้อมูลและองค์ประกอบของแบบรูปความมั่นคง	ข้อความ	ข้อความแบบพลวัต

จากการวิเคราะห์การแสดงผลการเปรียบเทียบความสามารถของเครื่องมือต้นแบบกับเครื่องมือวิสตีพีพบว่า ในเครื่องมือวิสตีพี ผู้ใช้งานจะต้องทำการกำหนดและตรวจสอบข้อมูลและองค์ประกอบของแบบรูปเองทั้งหมด ซึ่งอาจจะเกิดความผิดพลาดได้ง่าย ซึ่งเครื่องมือต้นแบบนี้สามารถลดหน้าที่ของผู้ใช้งานลงได้ โดยจะช่วยกำหนดและตรวจสอบข้อมูลและองค์ประกอบของแบบรูปให้ในบางส่วน ได้แก่ แม่พิมพ์ต้นแบบ ป้ายระบุ เงื่อนไขบังคับ และองค์ประกอบของแบบรูปความมั่นคง ซึ่งสามารถลดความผิดพลาดที่จะเกิดจากผู้ใช้งานได้

อย่างไรก็ตามเครื่องมือต้นแบบนี้ ยังมีการแสดงข้อมูลและองค์ประกอบของแบบรูปความมั่นคงเป็นแบบข้อมูลธรรมดา ซึ่งทำให้แผนภาพคลาสที่แสดงข้อมูลทางโครงสร้างและ

ข้อมูลทางความมั่นคงของแบบรูปความมั่นคงมีความซับซ้อน ทั้งนี้เพราะจำนวนตัวอักษรในแผนภาพที่เพิ่มมากขึ้น ซึ่งต่างจากการแสดงข้อความแบบพลวัตในเครื่องมือวิสตี้พี โดยจะแสดงข้อความก็ต่อเมื่อผู้ใช้งานเลือกชี้ที่องค์ประกอบนั้นๆ ซึ่งสามารถลดจำนวนของตัวอักษรในแผนภาพได้ โดยผู้วิจัยจะใช้เป็นแนวทางในการปรับปรุงเครื่องมือต้นแบบต่อไป

#### 4.3 สภาพแวดล้อมในการพัฒนาเครื่องมือ

ในการพัฒนาเครื่องมือต้นแบบนั้น ผู้วิจัยได้ทำการพัฒนาภายใต้สภาพแวดล้อม ดังนี้

##### 1) สภาพแวดล้อมทางด้านฮาร์ดแวร์ (Hardware)

1.1) โน้ตบุ๊กคอมพิวเตอร์ ซึ่งมีหน่วยประมวลผลอินเทลคอร์ทูดูโอ (Intel Core2 Duo) ความเร็ว 2.10 กิกะเฮิรซ์ (GHz)

1.2) หน่วยความจำหลัก DDR2 ขนาด 3.50 กิกะไบต์ (GB)

1.3) ฮาร์ดดิสก์ความเร็ว 5,400 รอบ/วินาที ขนาด 250 กิกะไบต์

##### 2) สภาพแวดล้อมทางด้านซอฟต์แวร์ (Software)

2.1) ระบบปฏิบัติการไมโครซอฟท์วินโดวส์เอ็กซ์พี เซอร์วิสแพ็ค 3 (Microsoft Windows XP Service Pack 3)

2.2) สตาร์ยูเอ็มแอล เวอร์ชัน 5.0.2.1570 ในการพัฒนาเครื่องมือต้นแบบ

2.3) โน้ตแพชพลัสพลัส เวอร์ชัน 3.9 (Notepad++ Ver.39) สำหรับพัฒนาเครื่องมือในส่วนของการตัดโค้ดทั้งหมด เช่น ส่วนช่วยเหลือผู้ใช้งานที่ใช้ภาษาเอชทีเอ็มแอล ส่วนกำหนดองค์ประกอบของแบบรูปความมั่นคงที่ใช้ภาษาเอกซ์เอ็มแอล และส่วนควบคุมองค์ประกอบของแบบรูปความมั่นคงที่ใช้ภาษาจาวาสคริปต์ เป็นต้น

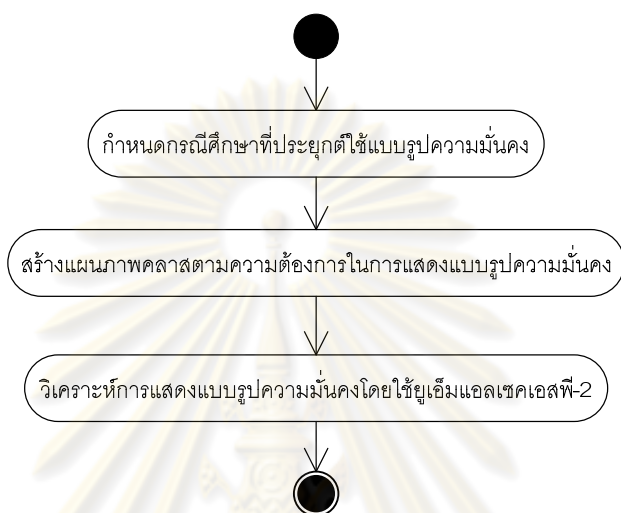
ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย



## บทที่ 5

### การประเมินผลและการวิเคราะห์การแสดงผลแบบรูปความมั่นคง

ในบทนี้จะกล่าวถึง การประเมินผลการแสดงผลแบบรูปความมั่นคงและการวิเคราะห์การแสดงผลแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี-2 ซึ่งมีขั้นตอนดังรูปที่ 5.1



รูปที่ 5.1 แผนภาพกิจกรรมแสดงขั้นตอนการประเมินผลและการวิเคราะห์การแสดงผลแบบรูปความมั่นคง

ในขั้นตอนการประเมินผลการแสดงผลแบบรูปความมั่นคงและการวิเคราะห์การแสดงผลแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี-2 ซึ่งประกอบไปด้วย การกำหนดกรณีศึกษาที่ประยุกต์ใช้ในแบบรูปความมั่นคง การสร้างแผนภาพคลาสตามความต้องการในการแสดงผลแบบรูปความมั่นคง และการวิเคราะห์การแสดงผลแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี-2 โดยมีรายละเอียดของแต่ละขั้นตอนดังนี้

#### 5.1 การกำหนดกรณีศึกษาที่ประยุกต์ใช้แบบรูปความมั่นคง

กรณีศึกษาที่นำมาใช้ในการประเมินผลซึ่งมีการประยุกต์ใช้แบบรูปความมั่นคงที่นำเสนอภายใต้ขอบเขตของงานวิทยานิพนธ์นี้ได้แก่

1) ระบบสั่งซื้อสินค้าออนไลน์ (Online Shopping System) เป็นระบบสำหรับสั่งซื้อสินค้าต่างๆ ผ่านอินเทอร์เน็ต โดยผู้ที่ใช้งานจะต้องทำการลงทะเบียนเพื่อเข้าสู่ระบบเสียก่อน ซึ่งจะต้องตั้งรหัสผ่านให้ตรงกับนโยบายทางด้านรหัสผ่านของระบบ โดยมีระบบการตรวจสอบความถูกต้องของข้อมูลผู้ใช้ อีกทั้งยังมีการระบุภัยคุกคาม ความเสี่ยงของสินค้าที่อาจจะเกิดความสูญเสียทางธุรกิจ ความน่าจะเป็นที่จะเกิดเหตุการณ์ที่เสี่ยงอันตรายขึ้น รวมไปถึงต้นเหตุของภัยคุกคาม โดยสามารถประยุกต์ใช้แบบรูปความมั่นคงในกลุ่มการจัดการความมั่นคงองค์กร และการจัดการความเสี่ยง และกลุ่มการระบุตัวตนและการพิสูจน์ตัวตนได้

2) ระบบบริการสำหรับการบันทึกเหตุการณ์ (Accounting Service System) คือระบบที่ให้บริการสำหรับบันทึกเหตุการณ์ทางด้านความมั่นคงของระบบ ได้แก่ บริการการตรวจสอบเหตุการณ์ทางด้านความมั่นคง บริการการตรวจสอบหลักฐานและการบันทึก บริการการป้องกันการบุกรุก และบริการการไม่ถูกปฏิเสธ ซึ่งจะต้องระบุขอบเขตของบริการ ความต้องการในการบันทึกเหตุการณ์ ปัจจัยที่เกี่ยวข้อง และบทบาทของผู้มีส่วนเกี่ยวข้อง โดยสามารถประยุกต์ใช้แบบรูปความมั่นคงในกลุ่มการบันทึกเหตุการณ์ได้

3) ระบบบริการความมั่นคงสำหรับองค์กร (Business Security Services System) คือระบบที่แนะนำองค์กรในการเลือกบริการความมั่นคง เช่น บริการการระบุและยืนยันตัวตน หรือบริการการควบคุมการเข้าถึง เป็นต้น เพื่อนำไปใช้ในการป้องกันสินทรัพย์ขององค์กรจากความเสียหายที่อาจจะเกิดขึ้น ทั้งนี้บริการความมั่นคงจะต้องมีความสอดคล้องกับแนวคิดทางด้านความมั่นคงขององค์กร โดยสามารถประยุกต์ใช้แบบรูปแนวคิดความมั่นคงองค์กร และแบบรูปบริการความมั่นคงองค์กรได้

โดยในที่นี้ขอแสดงรายละเอียดของการประเมินผลในแต่ละกรณีศึกษา ดังภาคผนวก ง

## 5.2 การสร้างแผนภาพคลาสตามความต้องการในการแสดงแบบรูปความมั่นคง

ในการสร้างแผนภาพคลาสของแบบรูปความมั่นคงนี้ จะเป็นการสร้างแผนภาพคลาสโดยใช้ยูเอ็มแอล ยูเอ็มแอลเซค ยูเอ็มแอลเซคเอสพี และยูเอ็มแอลเซคเอสพี-2 ของกรณีศึกษาที่นำมาใช้ในการประเมินผล ซึ่งจะแสดงรายละเอียดของแผนภาพคลาสของกรณีศึกษาในภาคผนวก ง

จากการวิเคราะห์ระบบที่นำมาเป็นกรณีศึกษาสำหรับประยุกต์ใช้แบบรูปความมั่นคงนั้น พบว่าระบบที่นำมาเป็นกรณีศึกษาทุกระบบ ได้แก่ ระบบสั่งซื้อสินค้าออนไลน์ ระบบบริการสำหรับการบันทึกเหตุการณ์ ไม่สามารถสร้างแผนภาพคลาสโดยใช้ยูเอ็มแอล และยูเอ็มแอลเซคได้ เนื่องจากไม่สามารถรองรับการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงที่ถูกประยุกต์ใช้ในกรณีศึกษาที่กล่าวมาได้ อีกทั้งยูเอ็มแอลเซคเอสพีก็สามารถแสดงข้อมูลได้เพียงบางส่วนเท่านั้น

## 5.3 การวิเคราะห์การแสดงผลแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี-2

วัตถุประสงค์ประสงค์ของงานวิทยานิพนธ์นี้คือ การขยายยูเอ็มแอลเพื่อรองรับการสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง ดังนั้นในขั้นตอนนี้จะทำการวิเคราะห์การแสดงผลข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแต่ละแบบรูปความมั่นคงที่อยู่ในขอบเขตของงานวิทยานิพนธ์ โดยทำการวิเคราะห์แผนภาพทั้ง 4 ลักษณะ คือ 1) แผนภาพคลาสจากยูเอ็มแอล 2) แผนภาพคลาสจากยูเอ็มแอลเซค 3) แผนภาพคลาสจากยูเอ็มแอลเซคเอสพี และ 4) แผนภาพคลาสจากยูเอ็มแอลเซคเอสพี-2 เพื่อเปรียบเทียบความสามารถของการแสดงผลข้อมูลดังกล่าว ซึ่งแบ่งเป็นการเปรียบเทียบการแสดงผลข้อมูลทางโครงสร้างของแบบรูปความมั่นคง และการเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง

โดยในที่นี่จะแสดงตัวอย่างการเปรียบเทียบการแสดงผลข้อมูลทางโครงสร้างและการแสดงข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร ดังตารางที่ 5.1 และตารางที่ 5.2 ตามลำดับดังนี้

ตารางที่ 5.1 การเปรียบเทียบการแสดงผลข้อมูลทางโครงสร้างของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

ยูเอ็มแอล	ไม่สามารถแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง ดังนี้ 1. องค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป 2. แบบรูปที่ใช้งาน 3. ลำดับของแบบรูปในแผนภาพ 4. บทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป
ยูเอ็มแอลเซค	ไม่สามารถแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคงได้เช่นเดียวกับการแสดงผลข้อมูลทางโครงสร้างของยูเอ็มแอล
ยูเอ็มแอลเซคเอสพี	สามารถแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง ดังนี้ 1. ใช้แม่พิมพ์ต้นแบบ spc spt และ spr ในการแสดงองค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป 2. ใช้ป้ายระบุ "role@name[instance]" แสดงบทบาทขององค์ประกอบในแบบรูป แบบรูปที่ใช้งาน และลำดับของแบบรูป
ยูเอ็มแอลเซคเอสพี-2	แสดงผลข้อมูลทางโครงสร้างของแบบรูปความมั่นคงเช่นเดียวกับการแสดงผลข้อมูลทางโครงสร้างของยูเอ็มแอลเซคเอสพี

ตารางที่ 5.2 การเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

ยูเอ็มแอล	ไม่ได้แสดงผลข้อมูลทางความมั่นคงในแผนภาพ คือ 1. สินทรัพย์ทางด้านธุรกิจขององค์กร 2. คุณสมบัติทางด้านความมั่นคง 3. ปัจจัยทางด้านธุรกิจขององค์กร
ยูเอ็มแอลเซค	ไม่สามารถแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล
ยูเอ็มแอลเซคเอสพี	ไม่สามารถแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล
ยูเอ็มแอลเซคเอสพี-2	แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสินทรัพย์ทางด้านธุรกิจขององค์กร 2. ใช้แม่พิมพ์ต้นแบบ "securityProperty" แสดงคุณสมบัติทางด้านความมั่นคง 3. ใช้แม่พิมพ์ต้นแบบ "businessDriver" แสดงปัจจัยทางด้านธุรกิจขององค์กร

จากการเปรียบเทียบการแสดงผลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กรของแผนภาพคลาส โดยใช้ ยูเอ็มแอล ยูเอ็มแอลเซค ยูเอ็มแอลเซคเอสพี และยูเอ็มแอลเซคเอสพี-2 พบว่า แผนภาพคลาสจากยูเอ็มแอล ยูเอ็มแอลเซค และยูเอ็มแอลเซคเอสพีไม่สามารถแสดงผลทางความมั่นคงของแบบรูปความมั่นคงได้ เนื่องจากแผนภาพทั้ง 3 ลักษณะนั้นไม่สามารถรองรับการแสดงผลข้อมูลทางความมั่นคงของแบบรูปดังกล่าวได้ ซึ่งต่างจากแผนภาพคลาสที่ใช้ยูเอ็มแอลเซคเอสพี-2 ที่สามารถแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้อย่างครบถ้วนสมบูรณ์ ซึ่งตรงกับความต้องการของแบบรูปความมั่นคง

โดยแสดงการเปรียบเทียบการแสดงผลทางโครงสร้าง และการแสดงผลข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคงในภาคผนวก จ และแสดงแผนภาพคลาสที่เกิดจากการบูรณาการแบบรูปความมั่นคงในแต่ละกลุ่มแบบรูปความมั่นคงในภาคผนวก ช



ศูนย์วิทยพัชกร  
จุฬาลงกรณ์มหาวิทยาลัย

## บทที่ 6

### สรุปผลการวิจัย

#### 6.1 บทสรุปของผลงานวิจัย

งานวิทยานิพนธ์นี้ได้ทำการศึกษา วิเคราะห์ และปรับปรุงยูเอเอ็มแอลเพื่อแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคง ซึ่งอยู่ในรูปของแผนภาพยูเอเอ็มแอล โดยครอบคลุมแบบรูปความมั่นคงทั้งหมดที่นำเสนอโดย M. Schumacher และคณะ [3] ซึ่งประกอบด้วย 8 กลุ่มแบบรูปความมั่นคง ได้แก่ การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง การระบุตัวตนและการพิสูจน์ตัวตน การบันทึกเหตุการณ์ แบบจำลองการควบคุมการเข้าถึง สถาปัตยกรรมการควบคุมการเข้าถึงระบบ การควบคุมการเข้าถึงระบบปฏิบัติการ สถาปัตยกรรมไฟร์วอลล์ และการประยุกต์ใช้ความมั่นคงบนอินเทอร์เน็ต ซึ่งเป็นแบบรูปที่อธิบายถึงแนวทางในการแก้ปัญหาทางด้านความมั่นคงของระบบ

ยูเอเอ็มแอลที่ปรับปรุงเพิ่มเติมที่ได้จากแบบรูปความมั่นคงในขอบเขตงานวิจัยนี้ เรียกว่า ยูเอเอ็มแอลเซคเอสพี-2 ซึ่งประกอบด้วย 47 แม่พิมพ์ต้นแบบและ 12 ป้ายระบุจาก 3 กลุ่มแบบรูปความมั่นคง โดยยูเอเอ็มแอลเซคเอสพี-2 นี้มีการตรวจสอบความถูกต้องเพื่อให้เป็นไปตามคุณสมบัติมาตรฐานของยูเอเอ็มแอลโพรไฟล์

อีกทั้งยังได้พัฒนาเครื่องมือสนับสนุนแสดงโครงสร้างของแบบรูปความมั่นคงในรูปของแผนภาพคลาสที่อยู่บนพื้นฐานของยูเอเอ็มแอลเซคเอสพี-2 เพื่อช่วยให้ผู้ใช้งานสามารถนำแบบรูปความมั่นคงไปประยุกต์ใช้ในกระบวนการต่างๆ ของการพัฒนาซอฟต์แวร์ได้อย่างมีแบบแผนและมีประสิทธิภาพมากขึ้น โดยเครื่องมือมีความสามารถได้ดังนี้ สามารถระบุองค์ประกอบต่างๆ ของแบบรูปความมั่นคง ออกแบบโครงสร้างเพื่อแสดงแบบรูปความมั่นคงตามที่ใช้ต้องการโดยแสดงในรูปของแผนภาพคลาส และช่วยแสดงรายละเอียดต่างๆ ของแบบรูปความมั่นคง ซึ่งจะช่วยให้ผู้ใช้งานเข้าใจในแบบรูปความมั่นคงที่เลือกได้เป็นอย่างดี

ผลลัพธ์ของงานวิทยานิพนธ์นี้คือ ยูเอเอ็มแอลเซคเอสพี-2 ที่รองรับการสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง และเครื่องมือสนับสนุนการใช้งานแบบรูปความมั่นคงบนพื้นฐานของยูเอเอ็มแอลเซคเอสพี-2 ซึ่งสนับสนุนผู้พัฒนาระบบความมั่นคงให้สามารถเข้าใจโครงสร้างของแบบรูปความมั่นคง อีกทั้งยังสามารถนำผลลัพธ์ที่แสดงในรูปแบบของแผนภาพคลาสไปประยุกต์ใช้ในการออกแบบความมั่นคงของระบบได้เป็นอย่างดีมีประสิทธิภาพ

#### 6.2 งานวิจัยในอนาคต

งานวิทยานิพนธ์นี้ได้ทำการปรับปรุงยูเอเอ็มแอลโดยการขยายยูเอเอ็มแอลเพื่อแสดงแบบรูปความมั่นคงในรูปของแผนภาพคลาส ซึ่งสนับสนุนการแสดงผลแบบรูปความมั่นคงทั้งหมดที่นำเสนอโดย M. Schumacher และคณะ [3] ดังนั้นหากมีการแสดงลำดับการดำเนินกิจกรรมในรูปของแผนภาพกิจกรรมในแต่ละแบบรูปความมั่นคง จะช่วยทำให้ง่ายและลดข้อผิดพลาด

ของขั้นตอนการออกแบบความมั่นคงของระบบได้ นอกจากนี้การปรับปรุงยูเอ็มแอล หรือการ แสดงแผนภาพคลาสให้มีความละเอียดมากยิ่งขึ้นเพื่อช่วยให้ผู้ใช้งานสามารถเข้าใจโครงสร้าง ของแบบรูปความมั่นคง ก็เป็นสิ่งที่ท้าทายเช่นกัน เนื่องจากอาจทำให้แผนภาพคลาส มีความซับซ้อนเพิ่มมากขึ้น อีกทั้งการที่มีแบบรูปความมั่นคงเป็นจำนวนมาก ดังนั้นการสร้าง การแสดงแบบรูปความมั่นคงเป็นลำดับชั้นของความสัมพันธ์ในแต่ละมุมมอง เช่น มุมมองของ กลุ่มแบบรูป หรือมุมมองของสินทรัพย์ว่าต้องการกำหนดให้อะไรเป็นสินทรัพย์ขององค์กร โดยเฉพาะ เป็นต้น ซึ่งจะช่วยให้เกิดความง่ายในการออกแบบระบบมากยิ่งขึ้น เนื่องจากมีการ ระบุมุมมองที่ต้องการโดยเฉพาะ

### 6.3 บทความวิชาการที่ตีพิมพ์

ในงานวิทยานิพนธ์นี้ ผู้วิจัยและคณะผู้วิจัยได้ส่งผลงานวิชาการในการประชุมวิชาการ ในประเทศ คือ บทความวิชาการเรื่อง “การสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความ มั่นคงโดยการขยายยูเอ็มแอล (Security Patterns Structural Model Construction by Extending UML)” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการทาง วิทยาการคอมพิวเตอร์และวิศวกรรมคอมพิวเตอร์แห่งชาติ ครั้งที่ 13 (The 13th National Computer Science and Engineering Conference: NCSEC 2009)” ระหว่างวันที่ 4 – 6 พฤศจิกายน 2552 ณ โรงแรมมณเฑียรริเวอร์ไซด์ กรุงเทพฯ โดยแสดงในภาคผนวก ซ

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

## รายการอ้างอิง

- [1] M. Schumacher. Security Engineering with Patterns. Berlin Heidelberg: Springer-Verlag, 2002
- [2] B. Blakley, C. Heath and members of The Open Group Security Forum, Security Design Patterns. United Kingdom: The Open Group U.K., April 2004.
- [3] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann and P. Sommerlad. Security Patterns: Integrating Security and Systems Engineering. United Kingdom: John Wiley & Sons, 2005.
- [4] D.M. Kienzle, M.C. Elder, D. Tyree and J. Edwards-Hewitt. Security Patterns Repository Version 1.0, [Computer file]. Available from: <http://www.scrypt.net/~celer/securitypatterns> [2009, March 27].
- [5] J. Jürjens. UMLsec: Extending UML for Secure Systems Development. Berlin Heidelberg: Springer-Verlag, 2002.
- [6] J. Jürjens. Secure Systems Development with UML. Berlin Heidelberg: Springer-Verlag, 2003.
- [7] G. Booch, J. Rumbaugh, I. Jacobson. The Unified Modeling Language User Guide. United State of America: Addison-Wesley, 1999.
- [8] G. Booch, J. Rumbaugh, I. Jacobson. The Unified Modeling Language Reference Manual. 2nd ed. United State of America: Addison-Wesley, 2004.
- [9] K. Hamilton and R. Miles. Learning UML 2.0. United State of America: O'Reilly, 2006.
- [10] J. Dong, S. Yang and K. Zhang. Visualizing Design Patterns in Their Applications and Composition. IEEE Transactions on software engineering, 33(7) (2007): 433-453.
- [11] E.B. Fernandez. Metadata and authorization patterns. Florida: Florida Atlantic University, Report TR-CSE-00-16, 2000.
- [12] เกียรติศักดิ์ ไชยสมบูรณ์. การแสดงผลแบบรูปความมั่นคงโดยการขยายยูเอ็มแอลเซค. วิทยานิพนธ์ปริญญาโทมหาบัณฑิต, ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2551.
- [13] Object Management Group. UML Standard Elements [Computer file]. Available from: <http://www.omg.org> [2009, March 27].
- [14] Object Management Group. UML Profile Specifications [Computer file]. Available from: <http://www.omg.org> [2009, March 27].

[15] Dong, J. VisDP: A Web Service for Visualizing Design Pattern on Demand

[Computer program]. Available from <http://www.utdallas.edu/~jdong/VisDP> [2009, March 27].



ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย





ภาคผนวก

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

ภาคผนวก ก  
การศึกษา กำหนดความต้องการ  
และจำลองโครงสร้างของแต่ละแบบรูปความมั่นคง

ในการศึกษา กำหนดความต้องการ และจำลองโครงสร้างของแต่ละแบบรูปความมั่นคง จะแบ่งตามกลุ่มของแบบรูปความมั่นคงซึ่งประกอบด้วย 17 แบบรูปความมั่นคง จาก 3 กลุ่ม แบบรูป โดยแสดงรายการของปัญหา บริบทของปัญหา ผลเฉลยของปัญหา และการจำลอง โครงสร้างของแบบรูปความมั่นคงของแต่ละแบบรูปความมั่นคง ดังนี้



ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

## ข.1 การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)

### 1) การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Asset)

เป็นแบบรูปเริ่มต้นสำหรับการพิจารณาความมั่นคงขององค์กร โดยทำการระบุสินทรัพย์ที่สำคัญขององค์กร เพื่อหาวิธีป้องกันสินทรัพย์ต่างๆ เหล่านั้น ซึ่งจะช่วยให้เข้าใจถึงความต้องการทางด้านความมั่นคงที่จำเป็นต้องมีในองค์กร เพื่อที่จะนำคุณสมบัติทางด้านความมั่นคงมาประยุกต์ใช้ โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร ดังตารางที่ ก.1

ตารางที่ ก.1 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการกำหนดความมั่นคงให้กับสินทรัพย์ขององค์กร
บริบท	องค์กรต้องการกำหนดความมั่นคงให้กับสินทรัพย์ แต่จะต้องระบุสินทรัพย์และปัจจัยทางด้านธุรกิจเสียก่อน
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>ระบุสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรือ อาคาร เป็นต้น</li> <li>ระบุตัวขับเคลื่อนทางด้านธุรกิจขององค์กรที่เป็นปัจจัยให้เกิดความต้องการของแต่ละสินทรัพย์ เช่น กฎหมาย ระเบียบขององค์กร หุ่นยนต์ เป้าหมาย วัตถุประสงค์ กระบวนการทางธุรกิจ สถานที่ที่เกิดกระบวนการทางธุรกิจ เป็นต้น</li> <li>กำหนดความสัมพันธ์ระหว่างสินทรัพย์และตัวขับเคลื่อนทางด้านธุรกิจ เช่น กฎทางด้านความปลอดภัยของข้อมูลพนักงาน ข้อมูลทางการเงินที่ต้องบอกให้กับหุ้นส่วน เป็นต้น</li> <li>ระบุคุณสมบัติของความมั่นคง ได้แก่ การรักษาความลับ ความสมบูรณ์ สภาพพร้อมใช้งาน และภาวะรับมือข้อบกพร่อง</li> <li>กำหนดประเภทของสินทรัพย์ โดยพิจารณาจากตัวขับเคลื่อนทางด้านธุรกิจขององค์กร</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร</b>	
<pre> classDiagram     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     class SecurityProperty {         +propertyID: Integer         +propertyName: String     }     class BusinessDriver {         +driverID: Integer         +driverName: String     }     class Asset_SecurityProperty {         +assetID: Integer         +propertyID: Integer     }     Asset "1..*" -- "1..*" SecurityProperty : have     BusinessDriver "1..*" -- "1..*" Asset : need     SecurityProperty "1..*" -- "1..*" Asset_SecurityProperty : have     BusinessDriver ..&gt; SecurityProperty : dependedOn     </pre>	
ชื่อคลาส	คำอธิบาย
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
SecurityProperty	เป็นคลาสของคุณสมบัติทางด้านความมั่นคง
BusinessDriver	เป็นคลาสที่แสดงถึงตัวขับเคลื่อนทางด้านธุรกิจขององค์กร
Asset-SecurityProperty	เป็นคลาสของความสัมพันธ์ระหว่างสินทรัพย์ทางด้านธุรกิจขององค์กรกับคุณสมบัติทางด้านความมั่นคง

## 2) การกำหนดมูลค่าสินทรัพย์ (Asset Valuation)

การกำหนดมูลค่าสินทรัพย์จะช่วยให้สามารถกำหนดความสำคัญของสินทรัพย์ขององค์กรที่เป็นเจ้าของและควบคุมอยู่ เพื่อระบุว่าเมื่อเกิดความสูญเสียสินทรัพย์จะส่งผลกระทบต่อองค์กรในด้านใดบ้าง ซึ่งอาจจะช่วยลดค่าใช้จ่ายที่สูง เช่น ค่าปรับหรือค่าใช้จ่าย ให้น้อยลงได้จากการสูญเสียส่วนแบ่งการตลาดและความเชื่อถือจากลูกค้า โดยมูลค่าสินทรัพย์จะได้รับการพิจารณาผลกระทบในด้านต่างๆ ได้แก่ ด้านความต้องการความมั่นคง ด้านเศรษฐกิจ และด้านธุรกิจ โดยแสดงรายการปัญหา บริษัท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการกำหนดมูลค่าสินทรัพย์ ดังตารางที่ ก.2

ตารางที่ ก.2 รายการปัญหา บริษัท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการกำหนดมูลค่าสินทรัพย์

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการกำหนดมูลค่าของสินทรัพย์ต่างๆขององค์กร
บริษัท	องค์กรต้องการกำหนดมูลค่าของสินทรัพย์ เพื่อนำไปใช้ในกระบวนการประเมินความเสี่ยง
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>1. กำหนดค่าความมั่นคง (Security value) ของสินทรัพย์องค์กร</li> <li>2. กำหนดค่าทางการเงิน (Financial value) ของสินทรัพย์ เช่น ค่าใช้จ่ายต่างๆ เป็นต้น</li> <li>3. กำหนดค่าของผลกระทบทางธุรกิจ (Business impact value) ของสินทรัพย์องค์กร เช่น การเสียลูกค้าหรือส่วนแบ่งการตลาด เป็นต้น</li> <li>4. สร้างตารางการประเมินสินทรัพย์และกำหนดค่าโดยรวม (Overall value) ของสินทรัพย์</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างแบบรูปการกำหนดมูลค่าสินทรัพย์</b>	
<pre> classDiagram     class Asset {         +assetID: Integer         +assetName: String         +assetType     }     class AssetValue {         +securityValue: Integer         +securityDescription: String         +financialValue: Integer         +financialDescription: String         +businessValue: Integer         +businessDescription: String         +overAllValue: Integer         +overAllDescription: String         +calculateOverAllValue()     }     Asset "1..*" -- "1..1" AssetValue : include     </pre>	
ชื่อคลาส	คำอธิบาย
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
AssetValue	เป็นคลาสของมูลค่าของสินทรัพย์องค์กร

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

### 3) การประเมินภัยคุกคาม (Threat Assessment)

ภัยคุกคามเป็นความน่าจะเป็นหรือความเป็นไปได้ที่จะเกิดเหตุการณ์ที่เสี่ยงอันตรายขึ้น ซึ่งสามารถส่งผลกระทบต่อทุกๆ สินทรัพย์หรือหรือทุกๆ สิ่งภายในองค์กรได้ ดังนั้นแบบรูปนี้จึงนำเสนอการกำหนดภัยคุกคาม ความถี่ของภัยคุกคามที่จะเกิดต่อสินทรัพย์ และผลกระทบเมื่อสินทรัพย์ถูกคุกคาม โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการประเมินภัยคุกคาม ดังตารางที่ ก.3

ตารางที่ ก.3 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการประเมินภัยคุกคาม

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการระบุภัยคุกคามที่จะเกิดขึ้นกับสินทรัพย์
บริบท	เมื่อมีการกำหนดสินทรัพย์แล้ว จะต้องระบุเหตุการณ์ที่เป็นภัยต่อสินทรัพย์
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	1. ระบุภัยคุกคาม ประกอบด้วย <ol style="list-style-type: none"> <li>1) ต้นเหตุที่ทำให้เกิดภัยคุกคาม เช่น พนักงาน หรือแฮกเกอร์ เป็นต้น</li> <li>2) ภัยคุกคามที่จะเกิดขึ้น เช่น ไฟไหม้ หรืออีเมลขยะ เป็นต้น</li> <li>3) ผลที่จะตามมาเมื่อภัยคุกคามนั้นเกิดขึ้น เช่น ระบบล่ม หรือข้อมูลสูญหาย เป็นต้น</li> </ol> 2. สร้างตารางภัยคุกคาม 3. ระบุระดับความถี่ที่จะเกิดภัยคุกคามขึ้น เช่น 1-6 หรือ 1-10 เป็นต้น 4. ระบุความถี่ที่แต่ละภัยคุกคามจะเกิดขึ้น เช่น 6 (Extreme) หรือ 2 (Low) เป็นต้น
<b>แผนภาพคลาสแสดงโครงสร้างแบบรูปการประเมินภัยคุกคาม</b>	
<pre> classDiagram     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     class Threat {         +threatID: Integer         +threatName: String         +threatDescription: String     }     class ThreatSource {         +threatSourceID: Integer         +threatSourceName: String     }     class ThreatConsequence {         +threatConsequenceID: Integer         +threatConsequenceName: String     }     class ThreatLikelihood {         +threatLikelihoodID: Integer         +threatLikelihoodName: String         +threatLikelihoodValue: Integer     }     Asset "1..*" -- "1..*" Threat : include     Threat "1..*" -- "1..*" ThreatSource : cause     Threat "1..*" -- "1..*" ThreatConsequence : takeEffect     Threat "1..*" -- "1..*" ThreatLikelihood           </pre>	
ชื่อคลาส	คำอธิบาย
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
Threat	เป็นคลาสของภัยคุกคามที่อาจจะเกิดขึ้นกับสินทรัพย์ขององค์กร
ThreatSource	เป็นคลาสของต้นเหตุที่ทำให้เกิดภัยคุกคาม
ThreatConsequence	เป็นคลาสของผลที่จะตามมาเมื่อเกิดภัยคุกคามขึ้น
ThreatLikelihood	เป็นคลาสของความน่าจะเป็นที่อาจจะเกิดเหตุการณ์ที่เสี่ยงอันตราย

จุฬาลงกรณ์มหาวิทยาลัย

#### 4) การประเมินจุดอ่อน (Vulnerability Assessment)

จุดอ่อนหรือภาวะไม่มั่นคง เป็นจุดที่จะถูกนำไปใช้โดยภัยคุกคาม (Threat) การประเมินภาวะเสี่ยง คือการระบุถึงจุดอ่อนของสินทรัพย์ในองค์กร และระดับความรุนแรงที่จะเกิดขึ้นเมื่อถูกภัยคุกคามโจมตีจุดอ่อนดังกล่าว (Security scale) โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการประเมินจุดอ่อน ดังตารางที่ ก.4

ตารางที่ ก.4 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการประเมินจุดอ่อน

รายการ	รายละเอียด
ปัญหา	ทำอย่างไรจึงจะกำหนดจุดอ่อนของสินทรัพย์ และระดับความรุนแรงเมื่อเกิดภัยคุกคามโจมตี
บริบท	องค์กรต้องการกำหนดจุดอ่อนที่ภัยคุกคามใช้โจมตี
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>รวบรวมข้อมูลของภัยคุกคาม</li> <li>ระบุจุดอ่อนที่อาจเกิดขึ้น เช่น ระบบแจ้งเตือนล้มเหลว หรือความไม่สมบูรณ์ของข้อมูลสำรอง เป็นต้น</li> <li>สร้างตารางความสัมพันธ์ระหว่างจุดอ่อนและภัยคุกคาม เช่น การเกิดไฟไหม้ เกิดจากระบบแจ้งเตือนล้มเหลวหรือเกิดจากระบบดับเพลิงล้มเหลว เป็นต้น</li> <li>กำหนดระดับความรุนแรง เช่น 4 (High) 1 (Negligible) เป็นต้น</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปการประเมินจุดอ่อน</b>	
<pre> classDiagram     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     class Threat {         +threatID: Integer         +threatAction: String         +threatDescription: String     }     class SeverityScale {         +severityScaleID: Integer         +severityScaleName: String         +severityScaleNumber: Integer         +severityScaleDescription: String     }     class Vulnerability {         +vulnerabilityID: Integer         +vulnerabilityName: String         +setVulnerability()     }     Asset "1..*" -- "1..*" Threat : include     Threat "1..*" -- "1..*" Vulnerability : contain     SeverityScale "1..1" -- "1..*" Vulnerability : specify     </pre>	
ชื่อคลาส	คำอธิบาย
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
Threat	เป็นคลาสของภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร
Vulnerability	เป็นคลาสของจุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง
SeverityScale	เป็นคลาสของระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตี

### 5) การกำหนดค่าความเสี่ยง (Risk Determination)

เป็นขั้นตอนสุดท้ายของกระบวนการประเมินความเสี่ยง โดยนำข้อมูลที่ได้จากการกำหนดมูลค่าสินทรัพย์ การประเมินภัยคุกคามและภาวะเสี่ยง มาเป็นข้อมูลนำเข้า เพื่อคำนวณและแสดงผลระดับความเสี่ยง ช่วยทำให้องค์กรทราบถึงความเสี่ยงของสินทรัพย์และจัดลำดับความสำคัญของสินทรัพย์ได้ โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการกำหนดค่าความเสี่ยง ดังตารางที่ ก.5

ตารางที่ ก.5 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการกำหนดค่าความเสี่ยง

รายการ	รายละเอียด
ปัญหา	องค์กรจะกำหนดค่าความเสี่ยงให้กับสินทรัพย์ได้อย่างไร
บริบท	องค์กรต้องการกำหนดค่าความเสี่ยงให้กับสินทรัพย์และประเมินค่าความสำคัญของแต่ละสินทรัพย์ในองค์กร
รายการความ ต้องการที่ได้จาก การสกัดผลเฉลย ของแบบรูป	<ol style="list-style-type: none"> <li>รวบรวมผลลัพธ์จากการกำหนดมูลค่าสินทรัพย์ การประเมินภัยคุกคาม และการประเมินจุดอ่อน</li> <li>กำหนดความสัมพันธ์ระหว่างจุดอ่อน และภัยคุกคามแต่ละสินทรัพย์เข้าด้วยกัน เช่น ไฟไหม้พีซีพีทภัณฑ์ เกิดจากระบบแจ้งเตือนเสียงหรือระบบรับไฟไหม้ล้มเหลว เป็นต้น</li> <li>คำนวณค่าความเสี่ยงตามสูตร  <math display="block">\text{ค่าความเสี่ยง} = \sum_{i=1}^n (\text{ThreatLikelihood}_i \times \text{VulnerabilitySeverityScale}_i) \times \text{AssetValue}</math> </li> <li>แสดงผลลัพธ์ความเสี่ยง ว่าอยู่ในช่วงไหน เช่น เล็กน้อย รุนแรง เป็นต้น</li> </ol>
แผนภาพคลาสแสดงโครงสร้างของแบบรูปการกำหนดค่าความเสี่ยง	
ชื่อคลาส	คำอธิบาย
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
Risk	เป็นคลาสของความเสี่ยงของแต่ละสินทรัพย์
RiskScale	เป็นคลาสรายละเอียดของความเสี่ยงนั้นๆ
Threat	เป็นคลาสของภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร
Vulnerability	เป็นคลาสของจุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง
SeverityScale	เป็นคลาสของระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตี

ตารางที่ ก.5 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูป  
การกำหนดค่าความเสี่ยง (ต่อ)

ชื่อคลาส	คำอธิบาย
ThreatSource	เป็นคลาสของต้นเหตุที่ทำให้เกิดภัยคุกคาม
ThreatLikelihood	เป็นคลาสของความน่าจะเป็นที่อาจเกิดเหตุการณ์ที่เสี่ยงอันตราย
ThreatConsequence	เป็นคลาสของผลที่จะตามมาเมื่อเกิดภัยคุกคามขึ้น
AssetValue	เป็นคลาสของมูลค่าของสินทรัพย์องค์กร



ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย



## 6) แนวคิดความมั่นคงองค์กร (Enterprise Security Approaches)

แบบรูปนี้แนะนำการเลือกแนวคิดทางด้านความมั่นคง คุณสมบัติความมั่นคงที่เหมาะสม และระดับความเสี่ยงของสินทรัพย์ที่พิจารณา โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปแนวคิดความมั่นคงองค์กร ดังตารางที่ ก.6

ตารางที่ ก.6 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปแนวคิดความมั่นคงองค์กร

รายการ	รายละเอียด
ปัญหา	องค์กรจะกำหนดแนวคิดความมั่นคงให้แก่สินทรัพย์ได้อย่างไร
บริบท	สินทรัพย์ต้องการการป้องกัน โดยองค์กรจะต้องมีความเข้าใจความเสี่ยงต่างๆ
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>รวบรวมข้อมูลที่เป็นของสินทรัพย์องค์กร</li> <li>รวบรวมข้อมูลค่าความเสี่ยงของสินทรัพย์</li> <li>เลือกแนวคิดความมั่นคงให้เหมาะสมกับสินทรัพย์ ได้แก่ การป้องกัน (Prevention) การตรวจหา (Detection) และ การตอบสนอง (Response)</li> <li>ทวนสอบแนวคิดของแต่ละสินทรัพย์ เมื่อมีสถานการณ์เปลี่ยนแปลง เช่น เกิดการเปลี่ยนแปลงทางด้านกระบวนการธุรกิจ เป็นต้น</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปแนวคิดความมั่นคงองค์กร</b>	
<pre> classDiagram     class SecurityProperty {         +propertyID: Integer         +propertyName: String     }     class Risk {         +assetRiskID: Integer         +assetRiskValue: Integer         +calculateRiskValue()     }     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     class SecurityApproach {         +approachID: Integer         +approachName: String         +approachDescription: String         +setApproach()     }     class Prevention {         +preventionID: Integer         +preventionName: String         +businessPriority: String     }     class Detection {         +detectionID: Integer         +detectionName: String         +businessPriority: String     }     class Response {         +responseID: Integer         +responseName: String         +businessPriority: String     }     SecurityProperty "1..*" -- "1..*" Asset : have     Risk "1..1" -- "1..1" Asset : include     Asset "1..*" -- "1..*" SecurityApproach : include     SecurityApproach "1..*" -- "1..*" Prevention : include     SecurityApproach "1..*" -- "1..*" Detection : include     SecurityApproach "1..*" -- "1..*" Response : include </pre>	
ชื่อคลาส	คำอธิบาย
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
Risk	เป็นคลาสของความเสี่ยงของสินทรัพย์องค์กร
SecurityProperty	เป็นคลาสของคุณสมบัติความมั่นคง
SecurityApproach	เป็นคลาสของแนวคิดความมั่นคง
Prevention	เป็นคลาสของแนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย
Detection	เป็นคลาสของแนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย
Response	เป็นคลาสของแนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย

## 7) บริการความมั่นคงองค์กร (Enterprise Security Services)

แบบรูปนี้ใช้สำหรับแนะนำองค์กรในการเลือกบริการความมั่นคงที่จะนำไปใช้ในการป้องกันสินทรัพย์ ภายหลังจากการกำหนดแนวคิดความมั่นคงสำหรับสินทรัพย์องค์กร ตัวอย่างเช่น บริการการระบุและยืนยันตัวตน หรือบริการการควบคุมการเข้าถึง เป็นต้น โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปบริการความมั่นคงองค์กร ดังตารางที่ ก.7

ตารางที่ ก.7 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปบริการความมั่นคงองค์กร

รายการ	รายละเอียด
ปัญหา	องค์กรจะกำหนดบริการความมั่นคงของสินทรัพย์ในองค์กรได้อย่างไร
บริบท	สินทรัพย์ต้องการการบริการความมั่นคง โดยพิจารณาจากแนวคิดความมั่นคง
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>รวบรวมข้อมูลที่สำคัญ เช่น ประเภทของสินทรัพย์ คุณสมบัติความมั่นคง แนวคิดความมั่นคงองค์กร เป็นต้น</li> <li>กำหนดบริการความมั่นคงสำหรับสินทรัพย์ เช่น Access control หรือ Accounting เป็นต้น และแนวคิดความมั่นคง ได้แก่ การป้องกัน การค้นหา และการตอบสนอง</li> <li>ทวนสอบบริการความมั่นคงอย่างสม่ำเสมอ เมื่อมีสถานการณ์เปลี่ยนแปลง</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปบริการความมั่นคงองค์กร</b>	
<pre> classDiagram     class SecurityProperty {         +propertyID: Integer         +propertyName: String     }     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     class SecurityService {         +serviceID: Integer         +serviceName: String         +setService()     }     class SecurityApproach {         +approachID: Integer         +approachName: String         +setApproach()     }     class Prevention {         +preventionID: Integer         +preventionName: String         +businessPriority: String     }     class Detection {         +detectionID: Integer         +detectionName: String         +businessPriority: String     }     class Response {         +responseID: Integer         +responseName: String         +businessPriority: String     }      SecurityProperty "1..*" -- "1..*" Asset : have     Asset "1..*" -- "1..*" SecurityApproach : include     SecurityService "1..*" -.-&gt; "1..*" SecurityApproach : dependedOn     SecurityApproach "1..*" -- "1..*" Prevention : include     SecurityApproach "1..*" -- "1..*" Detection : include     SecurityApproach "1..*" -- "1..*" Response : include     SecurityApproach "1..*" -- "1..*" SecurityApproach : include </pre>	
ชื่อคลาส	คำอธิบาย
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
SecurityProperty	เป็นคลาสของคุณสมบัติความมั่นคง
SecurityApproach	เป็นคลาสของแนวคิดความมั่นคง
SecurityService	เป็นคลาสของบริการความมั่นคงสำหรับสินทรัพย์ในองค์กร
Prevention	เป็นคลาสของแนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย
Detection	เป็นคลาสของแนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย
Response	เป็นคลาสของแนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย

## 8) การสื่อสารของผู้มีส่วนองค์กร (Enterprise Partner Communication)

เมื่อองค์กรมีการติดต่อกับองค์กรภายนอก จะต้องมีการเตรียมเครื่องมือและบริการต่างๆ ไว้อำนวยความสะดวก, ควบคุมการติดต่อ และการแลกเปลี่ยนข้อมูล แต่การดำเนินการดังกล่าวจะต้องเลือกบริการความมั่นคงที่เหมาะสมสำหรับการจัดการสิทธิ์การเข้าถึง รวมถึงการป้องกันข้อมูลไม่ให้ถูกเข้าถึงจากผู้ที่ไม่ได้รับสิทธิ์ โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการสื่อสารของผู้มีส่วนองค์กร ดังตารางที่ ก.8

ตารางที่ ก.8 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการสื่อสารของผู้มีส่วนองค์กร

รายการ	รายละเอียด
ปัญหา	เมื่อมีการติดต่อกับองค์กรภายนอก องค์กรจะป้องกันระบบและข้อมูลขององค์กรได้อย่างไร
บริบท	องค์กรต้องการกำหนดสิทธิ์ในการเข้าถึงสำหรับองค์กรภายนอก โดยพิจารณาจากกฎต่างๆ ในองค์กร
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>ระบุข้อมูลและบริการต่างๆ ที่ต้องแลกเปลี่ยนระหว่างองค์กร จากนั้นระบุความต้องการความมั่นคงของข้อมูลดังกล่าว</li> <li>ตรวจสอบองค์กรภายนอก โดยพิจารณาจากความต้องการความมั่นคงของข้อมูลและนโยบายขององค์กร</li> <li>ระบุและป้องกันช่องทางการติดต่อ <ol style="list-style-type: none"> <li>ระบุช่องทางการติดต่อ เช่น โปรโตคอล หรืออุปกรณ์ฮาร์ดแวร์ เป็นต้น</li> <li>แยกช่องทางขององค์กรภายนอกออกจากช่องทางปกติ</li> <li>ระบุการจัดการของ Port และ Portal</li> <li>ระบุการควบคุมการเข้าถึง</li> </ol> </li> <li>กำหนดวิธีดำเนินการที่ใช้ในช่องทางการติดต่อ เช่น On-demand Transfer หรือ Real-time Information Exchange เป็นต้น</li> <li>ดำเนินกิจกรรมการสิ้นสุด ตามข้อตกลงที่ได้รับไว้ เช่น การถอนสิทธิ์ เป็นต้น</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปการสื่อสารของผู้มีส่วนองค์กร</b>	
<pre> classDiagram     class CommunicationChannel {         +channelID: Integer         +channelName: String         +channelType: String         +channelDescription: String         +setCommunicationChannel()     }     class SecurityProperty {         +propertyID: Integer         +propertyName: String     }     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     class ExchangeMethod {         +exchangeMethodID: Integer         +exchangeMethodName: String         +setExchangeMethod()     }     class ServiceTermination {         +serviceTerminationID: Integer         +serviceTerminationName: String         +serviceTerminationDescription: String         +setServiceTermination()     }     class EnterprisePartner {         +partnerID: Integer         +partnerName: String         +partnerType: String         +partnerAddress: String         +setPermission()     }     class Role {         +roleID: Integer         +roleName: String     }     class IAService {         +I&amp;AID: Integer         +I&amp;AName: String         +I&amp;ADescription: String         +setService()     }      CommunicationChannel "1..*" -- "1..*" SecurityProperty : have     CommunicationChannel "1..*" -- "1..*" Asset : identify     Asset "1..*" -- "1..*" IAService : authenticate     Asset "1..*" -- "1..*" Role : access     ServiceTermination "1..*" -- "1..*" EnterprisePartner : perform     EnterprisePartner "1..*" -- "1..*" Role : memberOf     Role "1..*" -- "1..*" IAService : use     </pre>	
ชื่อคลาส	คำอธิบาย
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
SecurityProperty	เป็นคลาสของคุณสมบัติความมั่นคง
Role	เป็นคลาสของบทบาทของผู้มีส่วนเกี่ยวข้อง
I&AService	เป็นคลาสของบริการที่ตอบสนองความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
EnterprisePartner	เป็นคลาสขององค์กรภายนอก
CommunicationChannel	เป็นคลาสของช่องทางการติดต่อกับองค์กรภายนอก
ExchangeMethod	เป็นคลาสของวิธีดำเนินการที่ใช้ในช่องทางการติดต่อ
ServiceTermination	เป็นคลาสของกิจกรรมการสิ้นสุด

## ข.2 การระบุตัวตนและการพิสูจน์ตัวตน (Identification and Authentication)

### 1) ความต้องการการระบุและการพิสูจน์ตัวตน (I&A Requirement)

เป็นแบบรูปสำหรับนำเสนอและสร้างความต้องการพื้นฐานสำหรับการบริการด้านการระบุและพิสูจน์ตัวตน โดยที่การบริการด้านการระบุและพิสูจน์ตัวตนจะเป็นเซตของความพึงพอใจของความต้องการทางด้านการบริการและคุณภาพของบริการ โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการระบุและการพิสูจน์ตัวตน ดังตารางที่ ก.9

ตารางที่ ก.9 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการระบุและการพิสูจน์ตัวตน

รายการ	รายละเอียด
ปัญหา	องค์กรจะกำหนดความต้องการในการระบุและพิสูจน์ตัวตนอย่างไร
บริบท	องค์กรต้องการระบุความต้องการสำหรับใช้บริการการระบุและพิสูจน์ตัวตนในการเข้าถึงระบบ
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>กำหนดขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน เช่น ความต้องการในการระบุและพิสูจน์ตัวตนสำหรับการทำการในเวลาทำการและเวลานอกเวลาทำการ</li> <li>ระบุปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการ เช่น เงื่อนไขบังคับขององค์กร ประสิทธิภาพของผู้ใช้ หรือ ความถี่ในการใช้งาน เป็นต้น</li> <li>ระบุความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตนสำหรับขอบเขตเป้าหมาย เช่น เวลาและ effort ที่น้อยลง หรือ ป้องกัน I&amp;A assets เป็นต้น</li> <li>กำหนดความสัมพันธ์ระหว่างปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการ และความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปความต้องการการระบุและการพิสูจน์ตัวตน</b>	
<pre> classDiagram     class DomainFactor {         +factorID: Integer         +factorName: String         +factorDescription: String     }     class I&amp;ARequirement {         +requirementID: Integer         +requirementName: String         +requirementDescription: String         +setI&amp;ARequirement()     }     class I&amp;ADomain {         +domainID: Integer         +domainName: String         +domainDescription: String     }     class DomainFactorRequirement {         +domainFactorRequirementID: Integer         +domainFactorRequirementName: String         +setDomainFactorRequirement()     }     class I&amp;AService {         +I&amp;AID: Integer         +I&amp;AName: String         +I&amp;ADescription: String         +setI&amp;AService()     }     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     DomainFactor "1..*" -- "1..*" I&amp;ARequirement : haveEffect     I&amp;ADomain "1..*" -- "1..*" I&amp;ARequirement : specify     DomainFactorRequirement ..&gt; I&amp;ARequirement : dependedOn     I&amp;AService "1..*" -- "1..*" Asset : use     </pre>	
ชื่อคลาส	คำอธิบาย
I&A Domain	เป็นคลาสของขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน
DomainFactor	เป็นคลาสของปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการ
I&ARequirement	เป็นคลาสของความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
DomainFactorRequirement	เป็นความสัมพันธ์ระหว่างปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการและความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
I&AService	เป็นคลาสของบริการที่ตอบสนองความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กรที่ถูกนำไปใช้ในการบริการ

## 2) ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ

### (Automated I&A Design Alternatives)

แบบรูปนี้เป็นแบบรูปที่ช่วยในการกำหนดเทคนิคที่จะใช้กับบริการด้านการระบุและพิสูจน์ตัวตน เพื่อช่วยเลือกเทคนิคที่เหมาะสม โดยมีความสอดคล้องกับความต้องการด้านการระบุและพิสูจน์ตัวตน โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ ดังตารางที่ ก.10

ตารางที่ ก.10 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ

รายการ	รายละเอียด
ปัญหา	จะเลือกใช้เทคนิคในการระบุและพิสูจน์ตัวตนให้เหมาะสมกับความต้องการจากแบบรูปความต้องการการระบุและการพิสูจน์ตัวตนได้อย่างไร
บริบท	องค์กรต้องการกำหนดเทคนิคการระบุ และพิสูจน์ตัวตนให้เหมาะสมกับความต้องการจากแบบรูปความต้องการการระบุและการพิสูจน์ตัวตน
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>รวบรวมข้อมูลที่เป็นต่อสำหรับการระบุเทคนิคที่เหมาะสม                     <ol style="list-style-type: none"> <li>ขอบเขตในการใช้บริการ เช่น เฉพาะเวลากลางคืน หรือวันสุดสัปดาห์ เป็นต้น</li> <li>ความต้องการของการใช้บริการ เช่น ใช้เวลาและความพยายามที่น้อยที่สุด เป็นต้น</li> <li>บริการการระบุและพิสูจน์ตัวตน</li> </ol> </li> <li>ระบุเทคนิคในการระบุและพิสูจน์ตัวตน เช่น Biometrics หรือ Unregistered Users เป็นต้น โดยให้เหมาะสมกับความต้องการการให้บริการ</li> <li>เปรียบเทียบในแต่ละเทคนิคที่เหมาะสมกับความต้องการ เช่น ความต้องการในการใช้งานง่าย วิธี Biometrics จะมีความพึงพอใจสูง ส่วนวิธี Unregistered User จะมีความพึงพอใจในระดับปานกลาง เป็นต้น</li> <li>ในแต่ละความต้องการ หากใช้เทคนิคเดียวไม่เพียงพอ สามารถใช้เทคนิคอื่นเข้ามาช่วยได้</li> </ol>
แผนภาพคลาสแสดงโครงสร้างของแบบรูปทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ	
ชื่อคลาส	คำอธิบาย
I&A Domain	เป็นคลาสของขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน
DomainFactor	เป็นคลาสของปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการ
I&ARequirement	เป็นคลาสของความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน

ตารางที่ ก.10 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูป  
ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ (ต่อ)

ชื่อคลาส	คำอธิบาย
DomainFactorRequirement	เป็นคลาสของความสัมพันธ์ระหว่างปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการและความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
I&AService	เป็นคลาสของบริการที่ตอบสนองความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กรที่นำไปใช้ในการบริการ
I&ATechnique	เป็นคลาสของเทคนิคในการระบุและพิสูจน์ตัวตน
ลาส I&ATechniqueProfile	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตนและเทคนิคในการระบุและพิสูจน์ตัวตน



ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

### 3) การออกแบบและใช้รหัสผ่าน (Password Design and Use)

แบบรูปนี้ใช้ในการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการ การระบุและพิสูจน์ตัวตน โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของ โครงสร้างของแบบรูปการออกแบบและใช้รหัสผ่าน ดังตารางที่ ก.11

ตารางที่ ก.11 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปการออกแบบและใช้รหัสผ่าน

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการสร้าง จัดการ และใช้งานรหัสผ่านได้อย่างปลอดภัย
บริบท	องค์กรต้องการกำหนดคุณลักษณะของรหัสผ่านที่จะใช้
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>1. กำหนดตัวอักษรที่จะใช้ในรหัสผ่าน</li> <li>2. กำหนดความยาวของรหัสผ่าน</li> <li>3. กำหนดที่มาของรหัสผ่าน</li> <li>4. กำหนดอายุการใช้งานของรหัสผ่าน</li> <li>5. กำหนดบุคคลที่มีสิทธิ์ในการใช้งานรหัสผ่าน</li> <li>6. กำหนดวิธีการในการกรอกรหัสผ่าน</li> <li>7. กำหนดระยะเวลาของการพิสูจน์ตัวตนโดยใช้รหัสผ่าน</li> <li>8. กำหนดวิธีการในการส่งรหัสผ่านให้ผู้ใช้งาน</li> <li>9. กำหนดวิธีการในการจัดเก็บรหัสผ่าน</li> <li>10. กำหนดวิธีการในการถ่ายโอนรหัสผ่าน เพื่อใช้ในการตรวจสอบ</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปการออกแบบและใช้รหัสผ่าน</b>	
<pre> classDiagram     class I&amp;ATechnique {         +techniqueID: Integer         +techniqueName: String     }     class Password {         +passwordID: Integer         +passwordName: String         +passwordDescription: String         +composition: String         +lengthRange: String         +source: String         +lifetime: String         +ownership: String         +entry: String         +authenticationPeriod: String         +distribution: String         +storage: String         +transmission: String     }     class PasswordPolicy {         +passwordPolicyID: Integer         +passwordPolicyName: String         +passwordPolicyDescription: String         +setPasswordPolicy()     }     PasswordPolicy ..&gt; I&amp;ATechnique : dependedOn     I&amp;ATechnique o-- Password : contain     </pre>	
ชื่อคลาส	คำอธิบาย
I&ATechnique	เป็นคลาสของเทคนิคในการระบุและพิสูจน์ตัวตน
PasswordPolicy	เป็นคลาสของนโยบายทางด้านรหัสผ่าน
Password	เป็นคลาสที่เก็บข้อมูลของรหัสผ่านต่างๆ

#### 4) ทางเลือกการออกแบบชีวมิติ (Biometrics Design Alternatives)

แบบรูปนี้ใช้ในการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการ การระบุและพิสูจน์ตัวตน โดยใช้วิธีการทางด้านชีวมิติ โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปทางเลือกการออกแบบชีวมิติ ดังตารางที่ ก.12

ตารางที่ ก.12 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูป ทางเลือกการออกแบบชีวมิติ

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการเลือกใช้ชีวมิติให้มีความเหมาะสมกับความต้องการในการระบุและพิสูจน์ตัวตน
บริบท	องค์กรต้องการกำหนดการออกแบบทางชีวมิติที่จะใช้
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>1. ทบทวนการออกแบบทางชีวมิติที่เป็นไปได้ทั้งหมดตามแต่ละปัจจัย เช่น ความง่ายในการใช้งาน ความปลอดภัย และความสะดวกรวดเร็ว เป็นต้น</li> <li>2. เลือกการออกแบบทางชีวมิติที่เหมาะสม เช่น Face recognition, Finger image และ Iris scan เป็นต้น</li> </ol>
แผนภาพคลาสแสดงโครงสร้างของแบบรูปทางเลือกการออกแบบชีวมิติ	
<pre> classDiagram     class I&amp;ATechnique {         +techniqueID: Integer         +techniqueName: String     }     class BiometricMechanism {         +biometricMechanismID: Integer         +biometricMechanismName: String         +biometricMechanismDescription: String         +setBiometricMechanism()     }     class I&amp;ATechniqueFactor {         +techniqueFactorID: Integer         +techniqueFactorName: String         +techniqueFactorDescription: String     }     class BiometricCharacteristic {         +biometricCharacteristicID: Integer         +biometricCharacteristicName: String     }     I&amp;ATechnique "1" -- "*" BiometricMechanism : contain     BiometricMechanism "1..*" -- "1..*" I&amp;ATechniqueFactor : haveEffect     BiometricCharacteristic "1" -- "1" I&amp;ATechniqueFactor     </pre>	
ชื่อคลาส	คำอธิบาย
I&ATechnique	เป็นคลาสของเทคนิคในการระบุและพิสูจน์ตัวตน
I&ATechniqueFactor	เป็นคลาสของปัจจัยในการออกแบบทางชีวมิติ
BiometricMechanism	เป็นคลาสของโครงสร้างของชีวมิติ
BiometricCharacteristic	เป็นคลาสของคุณลักษณะของชีวมิติ



### ข.3 การบันทึกเหตุการณ์ (Accounting)

#### 1) ความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง (Security Accounting Requirements)

เป็นแบบรูปสำหรับนำเสนอการสร้างความต้องการในการติดตามความมั่นคงที่เกี่ยวข้องกับเหตุการณ์หรือกิจกรรม เช่น ความเสียหายของทรัพย์สิน หรือพยายามเข้าถึงฐานข้อมูลที่ไม่ได้อนุญาต เป็นต้น และให้ข้อมูลเกี่ยวกับเหตุการณ์เหล่านั้น โดยใช้วิธีการทางด้านชีวิตมิติ โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของรูปความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง ดังตารางที่ ก.13

ตารางที่ ก.13 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการกำหนดความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง เพื่อให้แต่ละความต้องการไม่เกิดความขัดแย้งกัน
บริบท	องค์กรต้องการระบุความต้องการสำหรับใช้บริการการบันทึกเหตุการณ์ทางด้านความมั่นคงของระบบ
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>กำหนดขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น กลุ่มผู้ใช้งาน หรือกิจกรรมที่เกี่ยวข้อง เป็นต้น</li> <li>กำหนดปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น ระเบียบองค์กร หรือความรับผิดชอบ เป็นต้น</li> <li>กำหนดความต้องการสำหรับการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น ข้อมูลของเหตุการณ์ต่างๆ หรือข้อมูลของผู้ที่อยู่ในกิจกรรมต่างๆ เป็นต้น</li> <li>ระบุความสำคัญของแต่ละความต้องการ ได้แก่ High Medium Low</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง</b>	
<pre> classDiagram     class AccountingDomain {         +accountingDomainID: Integer         +accountingDomainName: String         +accountingDomainDescription: String     }     class AccountingFactorRequirement {         +accountingFactorRequirementID: Integer         +accountingFactorRequirementName: String         +setDomainFactorRequirement()     }     class AccountingFactor {         +accountingFactorID: Integer         +accountingFactorName: String         +accountingFactorDescription: String         +accountingFactorPriority: String     }     class AccountingRequirement {         +accountingReqID: Integer         +accountingReqName: String         +accountingReqDescription: String         +setAccountingRequirement()     }     class Role {         +roleID: Integer         +roleName: String         +setRole()     }     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     class AccountingService {         +accountingServiceID: Integer         +accountingServiceName: String         +accountingServiceDescription: String         +setAccountingServiceService()     }     AccountingDomain "1..*" -- "1..*" AccountingFactorRequirement : specify     AccountingFactorRequirement "1..*" -- "1..*" AccountingFactor : haveEffect     AccountingFactor "1..*" -- "1..*" Role : accsee     Role "1..*" -- "1..*" Asset : use     Asset "1..*" -- "1..*" AccountingService : use     AccountingRequirement "1..*" -- "1..*" AccountingService : dependedOn     </pre>	
ชื่อคลาส	คำอธิบาย
AccountingService	เป็นคลาสของบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingRequirement	เป็นคลาสของความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingFactor	เป็นคลาสของปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingFactorRequirement	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingDomain	เป็นคลาสของขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
Role	เป็นคลาสของบทบาทของผู้มีส่วนเกี่ยวข้อง

## 2) ความต้องการการตรวจสอบ (Audit Requirements)

แบบรูปนี้นำเสนอการสร้างความต้องการในการวิเคราะห์ข้อมูลต่างๆ ที่ได้บันทึกไว้ โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการตรวจสอบ ดังตารางที่ ก.14

ตารางที่ ก.14 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการตรวจสอบ

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการวิเคราะห์ข้อมูลต่างๆ ที่ได้บันทึกไว้
บริบท	องค์กรจะต้องมีความเข้าใจเหตุการณ์ทางด้านความมั่นคงต่างๆ ที่ได้บันทึกไว้
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>กำหนดขอบเขตสำหรับบริการการตรวจสอบ เช่น กลุ่มของผู้ใช้งาน หรือกิจกรรมที่เกี่ยวข้อง เป็นต้น</li> <li>ระบุปัจจัยที่มีผลต่อความต้องการการตรวจสอบ เช่น ระเบียบภายในองค์กร หรือความรับผิดชอบ เป็นต้น</li> <li>ระบุความต้องการการตรวจสอบสำหรับขอบเขตที่ได้กำหนดไว้ เช่น ข้อมูลของผู้ที่กระทำกิจกรรมกับกิจกรรมนั้นๆ เป็นต้น</li> <li>กำหนดความสำคัญของแต่ละความต้องการ ได้แก่ High Medium Low</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปความต้องการการตรวจสอบ</b>	
<pre> classDiagram     class AccountingDomain {         +accountingDomainID: Integer         +accountingDomainName: String         +accountingDomainDescription: String     }     class AccountingFactorRequirement {         +accountingFactorRequirementID: Integer         +accountingFactorRequirementName: String         +setDomainFactorRequirement()     }     class AccountingFactor {         +accountingFactorID: Integer         +accountingFactorName: String         +accountingFactorDescription: String         +accountingFactorPriority: String     }     class AccountingRequirement {         +accountingReqID: Integer         +accountingReqName: String         +accountingReqDescription: String         +setAccountingReqRequirement()     }     class Role {         +roleID: Integer         +roleName: String         +setRole()     }     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     class AccountingService {         +accountingServiceID: Integer         +accountingServiceName: String         +accountingServiceDescription: String         +setAccountingServiceService()     }     class AuditService {         +auditServiceID: Integer         +auditServiceName: String         +auditServiceDescription: String     }     AccountingDomain "1..*" -- "1..*" AccountingFactorRequirement : specify     AccountingFactorRequirement .. AccountingFactor     AccountingFactor "1..*" -- "1..*" AccountingRequirement : haveEffect     AccountingRequirement .. AccountingService : dependedOn     Role "1..*" -- "1..*" Asset : accsee     Asset "1..*" -- "1..*" AccountingService : use     AccountingService &lt; -- AuditService : type             </pre>	
ชื่อคลาส	คำอธิบาย
AccountingService	เป็นคลาสของบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AuditService	เป็นคลาสของบริการการตรวจสอบเหตุการณ์ทางด้านความมั่นคง
AccountingRequirement	เป็นคลาสของความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingFactor	เป็นคลาสของปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingFactorRequirement	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingDomain	เป็นคลาสของขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
Asset	เป็นคลาสของสินทรัพย์ทางด้านการบัญชีขององค์กร
Role	เป็นคลาสของบทบาทของผู้มีส่วนเกี่ยวข้อง

### 3) ความต้องการการตรวจสอบหลักฐานและการบันทึก (Audit Trails and Logging Requirements)

แบบรูปนี้นำเสนอการสร้างความต้องการสำหรับการตรวจสอบหลักฐานและการบันทึกต่าง ๆ เกี่ยวกับเหตุการณ์หรือกิจกรรมที่เกิดขึ้นในองค์กรหรือระบบ โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการตรวจสอบหลักฐานและการบันทึก ดังตารางที่ ก.15

ตารางที่ ก.15 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการตรวจสอบหลักฐานและการบันทึก

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการตรวจสอบหลักฐานที่ได้ทำการบันทึกไว้ในระบบ
บริบท	องค์กรจะต้องมีความเข้าใจในความต้องการการตรวจสอบเพื่อทำการตรวจสอบหลักฐานทางด้านความมั่นคง
รายการความต้องการที่ได้จากการสกัด	1. กำหนดขอบเขตสำหรับบริการการตรวจสอบหลักฐานและการบันทึก เช่น กลุ่มของผู้ใช้งาน หรือกิจกรรมที่เกี่ยวข้อง เป็นต้น
ผลเฉลยของแบบรูป	2. ระบุปัจจัยที่มีผลต่อความต้องการการตรวจสอบหลักฐานและการบันทึก เช่น ระเบียบภายในองค์กร หรือความรับผิดชอบ เป็นต้น 3. ระบุความต้องการการตรวจสอบสำหรับขอบเขตที่กำหนดไว้ เช่น สามารถให้บริการได้เมื่อมีความต้องการที่จะใช้ได้ เป็นต้น 4. กำหนดความสำคัญของแต่ละความต้องการ ได้แก่ High Medium Low
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปความต้องการการตรวจสอบหลักฐานและการบันทึก</b>	
<pre> classDiagram     class AccountingDomain {         +accountingDomainID: Integer         +accountingDomainName: String         +accountingDomainDescription: String     }     class AccountingFactorRequirement {         +accountingFactorRequirementID: Integer         +accountingFactorRequirementName: String         +setDomainFactorRequirement()     }     class AccountingFactor {         +accountingFactorID: Integer         +accountingFactorName: String         +accountingFactorDescription: String         +accountingFactorPriority: String     }     class AccountingRequirement {         +accountingReqID: Integer         +accountingReqName: String         +accountingReqDescription: String         +setAccountingRequirement()     }     class Role {         +roleID: Integer         +roleName: String         +setRole()     }     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     class AccountingService {         +accountingServiceID: Integer         +accountingServiceName: String         +accountingServiceDescription: String         +setAccountingServiceService()     }     class ATLSERVICE {         +AT&amp;LServiceID: Integer         +AT&amp;LServiceName: String         +AT&amp;LServiceDescription: String     }     AccountingDomain "1..*" -- "1..*" AccountingFactorRequirement : specify     AccountingFactorRequirement .. AccountingFactor : haveEffect     AccountingFactorRequirement .. AccountingRequirement : haveEffect     AccountingRequirement .. AccountingService : dependedOn     AccountingService &lt; -- ATLSERVICE : type     Role "1..*" -- "1..*" Asset : accsee     Asset "1..*" -- "1..*" AccountingService : use     </pre>	
ชื่อคลาส	คำอธิบาย
AccountingService	เป็นคลาสของบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AT&LService	เป็นคลาสของบริการการตรวจสอบหลักฐานและการบันทึก
AccountingRequirement	เป็นคลาสของความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingFactor	เป็นคลาสของปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingFactorRequirement	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingDomain	เป็นคลาสของขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
Role	เป็นคลาสของบทบาทของผู้มีส่วนเกี่ยวข้อง

#### 4) ความต้องการการป้องกันการบุกรุก (Intrusion Detection Requirements)

แบบรูปนี้นำเสนอการสร้างความต้องการสำหรับการเฝ้าสังเกตกิจกรรมต่างๆ ที่เกิดขึ้น และการวิเคราะห์กิจกรรมเหล่านั้นเพื่อบอกถึงการละเมิดความมั่นคงขององค์กร โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการป้องกันการบุกรุก ดังตารางที่ ก.16

ตารางที่ ก.16 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการป้องกันการบุกรุก

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการที่จะป้องกันระบบและเครือข่ายจากผู้บุกรุก
บริบท	องค์กรจะต้องมีความเข้าใจถึงความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>กำหนดขอบเขตสำหรับบริการการป้องกันการบุกรุก เช่น กลุ่มของผู้ใช้งาน หรือกิจกรรมที่เกี่ยวข้อง เป็นต้น</li> <li>ระบุปัจจัยที่มีผลต่อความต้องการการป้องกันการบุกรุก เช่น ระเบียบภายในองค์กร หรือความรับผิดชอบ เป็นต้น</li> <li>ระบุความต้องการการป้องกันการบุกรุกสำหรับขอบเขตที่กำหนดไว้ เช่น ป้องกันกิจกรรมที่อาจก่อให้เกิดการบุกรุก เป็นต้น</li> <li>กำหนดความสำคัญของแต่ละความต้องการ ได้แก่ High Medium Low</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปความต้องการการป้องกันการบุกรุก</b>	
<pre> classDiagram     class AccountingDomain {         +accountingDomainID: Integer         +accountingDomainName: String         +accountingDomainDescription: String     }     class AccountingFactorRequirement {         +accountingFactorRequirementID: Integer         +accountingFactorRequirementName: String         +setDomainFactorRequirement()     }     class AccountingFactor {         +accountingFactorID: Integer         +accountingFactorName: String         +accountingFactorDescription: String         +accountingFactorPriority: String     }     class AccountingRequirement {         +accountingReqID: Integer         +accountingReqName: String         +accountingReqDescription: String         +setAccountingRequirement()     }     class Role {         +roleID: Integer         +roleName: String         +setRole()     }     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }     class AccountingService {         +accountingServiceID: Integer         +accountingServiceName: String         +accountingServiceDescription: String         +setAccountingServiceService()     }     class IDSService {         +IDSServiceID: Integer         +IDSServiceName: String         +IDSServiceDescription: String     }     AccountingDomain "1..*" -- "1..*" AccountingFactorRequirement : specify     AccountingFactorRequirement .. AccountingFactor     AccountingFactor "1..*" -- "1..*" AccountingRequirement : haveEffect     AccountingRequirement .. AccountingService : dependedOn     Role "1..*" -- "1..*" Asset : accsee     Asset "1..*" -- "1..*" AccountingService : use     AccountingService &lt; -- IDSService : type     </pre>	
ชื่อคลาส	คำอธิบาย
AccountingService	เป็นคลาสของบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
IDSService	เป็นคลาสของบริการการป้องกันการบุกรุก
AccountingRequirement	เป็นคลาสของความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingFactor	เป็นคลาสของปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingFactorRequirement	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingDomain	เป็นคลาสของขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
Asset	เป็นคลาสของสินทรัพย์ทางธุรกิจขององค์กร
Role	เป็นคลาสของบทบาทของผู้มีส่วนเกี่ยวข้อง

## 5) ความต้องการการไม่ถูกปฏิเสธ (Non-Repudiation Requirements)

แบบรูปนี้นำเสนอการสร้างความต้องการในการตรวจสอบและรักษาหลักฐานเพื่อให้ผู้มีส่วนร่วมไม่ถูกปฏิเสธจากกิจกรรมใดๆ ของระบบหรือองค์กร โดยแสดงรายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการไม่ถูกปฏิเสธ ดังตารางที่ ก.17

ตารางที่ ก.17 รายการปัญหา บริบท ผลเฉลย โครงสร้าง และคลาสของโครงสร้างของแบบรูปความต้องการการไม่ถูกปฏิเสธ

รายการ	รายละเอียด
ปัญหา	องค์กรจะกำหนดบริการของการไม่ถูกปฏิเสธได้อย่างไร
บริบท	องค์กรจะต้องมีความเข้าใจถึงความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง และวางแผนการทำงานเพื่อที่จะไม่ถูกปฏิเสธ
รายการความต้องการที่ได้จากการสกัดผลเฉลยของแบบรูป	<ol style="list-style-type: none"> <li>กำหนดขอบเขตสำหรับบริการการไม่ถูกปฏิเสธ เช่น กลุ่มของผู้ใช้งาน หรือกิจกรรมที่เกี่ยวข้อง เป็นต้น</li> <li>ระบุปัจจัยที่มีผลต่อความต้องการการไม่ถูกปฏิเสธ เช่น ระเบียบภายในองค์กร หรือความรับผิดชอบ เป็นต้น</li> <li>ระบุความต้องการการไม่ถูกปฏิเสธสำหรับขอบเขตที่กำหนดไว้ เช่น ระยะเวลาในการระบุและพิสูจน์ตัวตน เป็นต้น</li> <li>กำหนดความสำคัญของแต่ละความต้องการ ได้แก่ High Medium Low</li> </ol>
<b>แผนภาพคลาสแสดงโครงสร้างของแบบรูปความต้องการการไม่ถูกปฏิเสธ</b>	
<pre> classDiagram     class AccountingDomain {         +accountingDomainID: Integer         +accountingDomainName: String         +accountingDomainDescription: String     }     class AccountingFactorRequirement {         +accountingFactorRequirementID: Integer         +accountingFactorRequirementName: String         +setDomainFactorRequirement()     }     class AccountingFactor {         +accountingFactorID: Integer         +accountingFactorName: String         +accountingFactorDescription: String         +accountingFactorPriority: String     }     class AccountingRequirement {         +accountingReqID: Integer         +accountingReqName: String         +accountingReqDescription: String         +setAccountingRequirement()     }     class AccountingService {         +accountingServiceID: Integer         +accountingServiceName: String         +accountingServiceDescription: String         +setAccountingServiceService()     }     class NonRepudiationService {         +nonRepudiationServiceID: Integer         +nonRepudiationServiceName: String         +nonRepudiationServiceDescription: String     }     class Role {         +roleID: Integer         +roleName: String         +setRole()     }     class Asset {         +assetID: Integer         +assetName: String         +assetType: String     }      AccountingDomain "1..*" -- "1..*" AccountingFactorRequirement : specify     AccountingFactorRequirement "1..*" -- "1..*" AccountingFactor : haveEffect     AccountingFactorRequirement "1..*" -- "1..*" AccountingRequirement : haveEffect     AccountingRequirement "1..*" .. &gt; AccountingService : dependedOn     AccountingService "1..*" -- &gt; NonRepudiationService : type     Role "1..*" -- "1..*" Asset : accsee     Asset "1..*" -- "1..*" AccountingService : use     </pre>	
ชื่อคลาส	คำอธิบาย
AccountingService	เป็นคลาสของบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
NonRepudiationService	เป็นคลาสของบริการการไม่ถูกปฏิเสธ
AccountingRequirement	เป็นคลาสของความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingFactor	เป็นคลาสของปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingFactorRequirement	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
AccountingDomain	เป็นคลาสของขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
Asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร
Role	เป็นคลาสของบทบาทของผู้มีส่วนเกี่ยวข้อง

## ภาคผนวก ข

### ยูเอ็มแอลเซคเอสพี-2

ยูเอ็มแอลเซคเอสพี-2 ที่ได้จากแบบรูปความมั่นคงในขอบเขตงานวิจัยนี้ ประกอบด้วย 47 แม่พิมพ์ต้นแบบและ 12 ป้ายระบุจาก 17 แบบรูปความมั่นคง จาก 3 กลุ่มแบบรูปความมั่นคง ซึ่งสามารถจำแนกตามกลุ่มของแบบรูปความมั่นคงได้ดังตารางที่ ข.1

ตารางที่ ข.1 แบบรูปความมั่นคงในแต่ละกลุ่มแบบรูปที่ใช้งานวิทยานิพนธ์

<b>กลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง</b>	<ol style="list-style-type: none"> <li>1) การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร</li> <li>2) การกำหนดมูลค่าสินทรัพย์</li> <li>3) การประเมินภัยคุกคาม</li> <li>4) การประเมินจุดอ่อน</li> <li>5) การกำหนดค่าความเสี่ยง</li> <li>6) แนวคิดความมั่นคงองค์กร</li> <li>7) บริการความมั่นคงองค์กร</li> <li>8) การสื่อสารของผู้กับหุ้นส่วนองค์กร</li> </ol>
<b>กลุ่มแบบรูปการระบุตัวตนและการพิสูจน์ตัวตน</b>	<ol style="list-style-type: none"> <li>1) ความต้องการการระบุและการพิสูจน์ตัวตน</li> <li>2) ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ</li> <li>3) การออกแบบและใช้รหัสผ่าน</li> <li>4) ทางเลือกการออกแบบชีวมิติ</li> </ol>
<b>กลุ่มแบบรูปการบันทึกเหตุการณ์</b>	<ol style="list-style-type: none"> <li>1) ความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง</li> <li>2) ความต้องการการตรวจสอบ</li> <li>3) ความต้องการการตรวจสอบหลักฐานและการบันทึก</li> <li>4) ความต้องการการป้องกันการบุกรุก</li> <li>5) ความต้องการการไม่ถูกปฏิเสธ</li> </ol>

โดยรายละเอียดของแต่ละแม่พิมพ์ต้นแบบ ประกอบไปด้วย ชื่อแบบรูปความมั่นคง คำอธิบายของแบบรูปความมั่นคง ชื่อแม่พิมพ์ต้นแบบ คลาสพื้นฐาน ป้ายระบุที่ใช้อธิบายแม่พิมพ์ต้นแบบ เงื่อนไขบังคับที่จำเป็นต้องพิจารณา คำอธิบายของแม่พิมพ์ต้นแบบ และในรายละเอียดของแต่ละป้ายระบุ ประกอบไปด้วย ชื่อแบบรูปความมั่นคง ชื่อป้ายระบุ แม่พิมพ์ต้นแบบที่ใช้ป้ายระบุ ตัวอย่างค่าของป้ายระบุ มัลติพลิซิทีของป้ายระบุ คำอธิบายของป้ายระบุ โดยมีรายละเอียดดังต่อไปนี้

ตารางที่ ข.2 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง

แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	คำอธิบาย	เงื่อนไขบังคับ
spc (Security Pattern Class)	Class	"role@name[instance]"	คลาสที่เป็นองค์ประกอบภายในแบบรูปความมั่นคง	1> self.taggedValue.dataValue.name -> notEmpty 2> self.taggedValue.name -> forall(v1, v2:name   v1.name <> v2.name)
spt (Security Pattern data Type)	Class	"role@name[instance]"	คลาสที่เป็นแบบชนิดข้อมูลภายในแบบรูปความมั่นคง	implies (v1.instance -> isEmpty and v2.instance -> isEmpty) 3> self.taggedValue.name -> exists(v1, v2:name   v1.name = v2.name)
spr (Security Pattern Relationship)	Relationship	"role@name[instance]"	ความสัมพันธ์ระหว่างคลาสที่เป็นองค์ประกอบภายในแบบรูปความมั่นคง	implies (v1.instance -> notEmpty and v2.instance -> notEmpty and v1.instance <> v2.instance)

ตารางที่ ข.3 ป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปความมั่นคง

ป้ายระบุ	แม่พิมพ์ต้นแบบ	ค่าของป้ายระบุ	ตัวอย่างค่าของป้ายระบุ	มัลติพลิซิตี	คำอธิบาย
"role@name[instance]"	แม่พิมพ์ต้นแบบที่สร้างทั้งหมด	บูลีนแสดงลักษณะองค์ประกอบดังกล่าวในแบบรูป	true หรือ false	*	ระบุว่า องค์ประกอบดังกล่าวมีบทบาท "role" ในแบบรูป "name" ลำดับที่ "instance" ในแผนภาพหรือไม่

ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Asset)	เป็นแบบรูปที่เสนอการพิจารณาความมั่นคงขององค์กร โดยทำการระบุสินทรัพย์ที่สำคัญขององค์กร เพื่อหาวิธีป้องกันสินทรัพย์ต่างๆ เหล่านั้น	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name ="assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		securityProperty	Class	secureKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name ="secureKind") implies (tv.dataValue = Confidentiality or tv.dataValue = Integrity or tv.dataValue = Availability or tv.dataValue = Accountability)	คุณสมบัติทางด้านความมั่นคง
		businessDriver	Class	businessFactor และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name ="businessFactor") implies (tv.dataValue -> isEmpty)	ตัวขับเคลื่อนทางด้านธุรกิจขององค์กร

ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
การกำหนดมูลค่าสินทรัพย์ (Asset Valuation)	เป็นแบบรูปที่เสนอการกำหนดมูลค่าสินทรัพย์จะช่วยให้สามารถกำหนดความสำคัญของสินทรัพย์ขององค์กรที่เป็นเจ้าของหรือควบคุมอยู่	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name ="assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		assetValue	Class	overAllValue และ "role@name[instance]"	1> self.taggedValue -> select(tv tv.name ="overAllValue").dataValue.oclsTypeOf(Integer); 2> self.taggedValue -> forall(tv tv.name ="overAllValue") implies (tv.dataValue >= 1 and tv.dataValue <= 6)	มูลค่าของสินทรัพย์ทางด้านธุรกิจขององค์กร
		securityValue	Class	"role@name[instance]"		มูลค่าความมั่นคงของสินทรัพย์องค์กร
		financialValue	Class	"role@name[instance]"		มูลค่าทางการเงินของสินทรัพย์องค์กร
		businessValue	Class	"role@name[instance]"		มูลค่าผลกระทบทางธุรกิจของสินทรัพย์องค์กร
การประเมินภัยคุกคาม (Threat Assessment)	เป็นแบบรูปที่นำเสนอการกำหนดภัยคุกคาม ความถี่ของภัยคุกคามที่จะเกิดต่อสินทรัพย์ และผลกระทบเมื่อสินทรัพย์ถูกคุกคาม	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name ="assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		threat	Class	operation และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "operation") implies (tv.dataValue -> isEmpty)	ภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร
		threatConsequence	Class	effect และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "effect") implies (tv.dataValue -> isEmpty)	ผลที่จะตามมาเมื่อเกิดภัยคุกคามขึ้น
		threatSource	Class	source และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "source") implies (tv.dataValue -> isEmpty)	ต้นเหตุที่ทำให้เกิดภัยคุกคาม
		threatLikelihood	Class	rating และ "role@name[instance]"	1> self.taggedValue -> select(tv tv.name ="overAllValue").dataValue.oclsTypeOf(Integer); 2> self.taggedValue -> forall(tv tv.name = "rating") implies (tv.dataValue -> isEmpty)	ความน่าจะเป็นที่อาจเกิดเหตุการณ์ที่เสี่ยงอันตราย



ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
การประเมินภาวะเสี่ยง (Vulnerability Assessment)	เป็นแบบรูปที่นำเสนอการระบุถึงจุดอ่อนของสินทรัพย์ในองค์กร และระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตีจุดอ่อนดังกล่าว	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name ="assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		threat	Class	operation และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "operation") implies (tv.dataValue -> isNotEmpty)	ภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร
		vulnerability	Class	weakness และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "weakness") implies (tv.dataValue -> isNotEmpty)	จุดอ่อนของสินทรัพย์ในองค์กรที่ทำให้เกิดภาวะเสี่ยง
		severityScale	Class	"role@name[instance]"		ระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตี
การกำหนดค่าความเสี่ยง (Risk Determination)	เป็นแบบรูปที่นำเสนอการกำหนดค่าความเสี่ยง เพื่อคำนวณและแสดงระดับความเสี่ยงที่เหมาะสม	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name ="assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		threat	Class	operation และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "operation") implies (tv.dataValue -> isNotEmpty)	ภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร
		threatConsequence	Class	effect และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "effect") implies (tv.dataValue -> isNotEmpty)	ผลที่จะตามมาเมื่อเกิดภัยคุกคามขึ้น
		threatSource	Class	source และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "source") implies (tv.dataValue -> isNotEmpty)	ต้นเหตุที่ทำให้เกิดภัยคุกคาม
		threatLikelihood	Class	rating และ "role@name[instance]"	1> self.taggedValue -> select(tv tv.name ="overAllValue").dataValue.ocIsTypeOf(Integer); 2> self.taggedValue -> forall(tv tv.name = "rating") implies (tv.dataValue -> isNotEmpty)	ความน่าจะเป็นที่อาจเกิดเหตุการณ์ที่เสี่ยงอันตราย
		vulnerability	Class	weakness และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "weakness") implies (tv.dataValue -> isNotEmpty)	จุดอ่อนของสินทรัพย์ในองค์กรที่ทำให้เกิดภาวะเสี่ยง
		severityScale	Class	"role@name[instance]"		ระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตี

ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
		assetValue	Class	overAllValue และ "role@name[instance]"	1> self.taggedValue -> select(tv tv.name ="overAllValue").dataValue.ocllsTypeOf(Integer); 2> self.taggedValue -> forall(tv tv.name ="overAllValue") implies (tv.dataValue >= 1 and tv.dataValue <= 6)	มูลค่าของสินทรัพย์ทางด้านธุรกิจของ องค์กร
		securityValue	Class	"role@name[instance]"		มูลค่าความมั่นคงของสินทรัพย์องค์กร
		financialValue	Class	"role@name[instance]"		มูลค่าทางการเงินของสินทรัพย์องค์กร
		businessValue	Class	"role@name[instance]"		มูลค่าผลกระทบทางธุรกิจของสินทรัพย์ องค์กร
		risk	Class	"role@name[instance]"		ความเสี่ยงของสินทรัพย์
		riskScale	Class	"role@name[instance]"		รายละเอียดของแต่ละความเสี่ยง
แนวคิดความมั่นคงองค์กร (Enterprise Security Approaches)	เป็นแบบรูปที่นำเสนอการกำหนด แนวคิดความมั่นคงให้แก่สินทรัพย์ของ องค์กร	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name ="assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		risk	Class	"role@name[instance]"		ความเสี่ยงของสินทรัพย์
		securityApproach	Class	"role@name[instance]"		แนวคิดความมั่นคงขององค์กร
		businessPriority	Class	"role@name[instance]"		ความสำคัญทางธุรกิจของแนวคิดความ มั่นคงขององค์กร
		prevention	Class	"role@name[instance]"		แนวคิดความมั่นคงสำหรับการป้องกัน เหตุการณ์ที่เสี่ยงอันตราย
		detection	Class	"role@name[instance]"		เป็นคลาสของแนวคิดความมั่นคงสำหรับ การค้นหาเหตุการณ์ที่เสี่ยงอันตราย
response	Class	"role@name[instance]"		เป็นคลาสของแนวคิดความมั่นคงสำหรับ การตอบสนองเหตุการณ์ที่เสี่ยงอันตราย		

ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
บริการความมั่นคงองค์กร (Enterprise Security Services)	เป็นแบบรูปสำหรับแนะนำองค์กรในการเลือกบริการความมั่นคงที่จะนำไปใช้ในการป้องกันสินทรัพย์	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv.name = "assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		securityProperty	Class	secureKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv.name = "secureKind") implies (tv.dataValue = Confidentiality or tv.dataValue = Integrity or tv.dataValue = Availability or tv.dataValue = Accountaability)	คุณสมบัติทางด้านความมั่นคง
		securityApproach	Class	"role@name[instance]"		แนวคิดความมั่นคงขององค์กร
		prevention	Class	"role@name[instance]"		แนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย
		detection	Class	"role@name[instance]"		เป็นคลาสของแนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย
		response	Class	"role@name[instance]"		เป็นคลาสของแนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย
		securityService	Class	"role@name[instance]"		บริการความมั่นคงสำหรับสินทรัพย์องค์กร
การสื่อสารของผู้มีส่วนองค์กร (Enterprise Partner Communication)	เป็นแบบรูปที่นำเสนอการเตรียมเครื่องมือและบริการต่างๆ สำหรับอำนวยความสะดวกและควบคุมการติดต่อและการแลกเปลี่ยนข้อมูลระหว่างผู้ส่วนกับองค์กร	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv.name = "assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		channel	Class	connectionChannel และ "role@name[instance]"	1> self.taggedValue -> forall(tv.name = "connectionChannel") implies (tv.dataValue -> isEmpty)	ช่องทางการติดต่อกับองค์กรภายนอก
		exchangeMethod	Class	"role@name[instance]"		วิธีดำเนินการที่ใช้ในช่องทางการติดต่อ
		serviceTermination	Class	"role@name[instance]"		กิจกรรมการสิ้นสุด
		*client	Class	"role@name[instance]"		ผู้ใช้งานจากภายนอกระบบ
		*role	Class	"role@name[instance]"		บทบาทของผู้ใช้ระบบ
		I&AService	Class	"role@name[instance]"		บริการที่ตอบสนองความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
*monitored	Relationship	monitor และ "role@name[instance]"	1> self.taggedValue -> forall(tv.name = "monitor") implies (tv.dataValue -> isEmpty)	การเชื่อมโยงที่มีการตรวจสอบการเข้าถึงระบบ		

\* คือการนำยูเอ็มแอลเซคเอสพีมาประยุกต์ใช้

ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
ความต้องการการระบุและการพิสูจน์ตัวตน (I&A Requirement)	เป็นแบบรูปที่นำเสนอและสร้างความต้องการพื้นฐานสำหรับการบริการด้านการระบุและพิสูจน์ตัวตน	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		I&AService	Class	"role@name[instance]"		บริการที่ตอบสนองความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
		I&ARequirement	Class	requirement และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "requirement") implies (tv.dataValue -> isEmpty)	ความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
		I&ADomain	Class	"role@name[instance]"		ขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน
		domainFactor	Class	"role@name[instance]"		ปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการ
ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ (Automated I&A Design Alternatives)	เป็นแบบรูปที่นำเสนอการกำหนดเทคนิคที่จะใช้กับบริการด้านการระบุและพิสูจน์ตัวตน	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		I&AService	Class	"role@name[instance]"		บริการที่ตอบสนองความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
		I&ARequirement	Class	requirement และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "requirement") implies (tv.dataValue -> isEmpty)	ความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน
		I&ADomain	Class	"role@name[instance]"		ขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน
		domainFactor	Class	"role@name[instance]"		ปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการ
		I&ATechnique	Class	technique และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "technique") implies (tv.dataValue -> isEmpty)	เทคนิคในการระบุและพิสูจน์ตัวตน
การออกแบบและใช้รหัสผ่าน (Password Design and Use)	เป็นแบบรูปที่นำเสนอการออกแบบการสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการการระบุและพิสูจน์ตัวตน	I&ATechnique	Class	technique และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "technique") implies (tv.dataValue -> isEmpty)	เทคนิคในการระบุและพิสูจน์ตัวตน
		password	Class	"role@name[instance]"		ที่เก็บข้อมูลของรหัสผ่านต่างๆ
		passwordPolicy	Class	policy และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "policy") implies (tv.dataValue -> isEmpty)	นโยบายทางด้านรหัสผ่าน

ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
		ownership	Class	"role@name[instance]"		บุคคลที่มีสิทธิ์ในการใช้งานรหัสผ่าน
		entry	Class	"role@name[instance]"		วิธีการในการกรอกรหัสผ่าน
		distribution	Class	"role@name[instance]"		วิธีการส่งรหัสผ่านให้ผู้ใช้งาน
		storage	Class	"role@name[instance]"		วิธีการจัดเก็บรหัสผ่าน
		transmission	Class	"role@name[instance]"		วิธีการถ่ายโอนรหัสผ่าน เพื่อใช้ในการตรวจสอบ
ทางเลือกการออกแบบชีวมิติ (Biometrics Design Alternatives)	เป็นแบบรูปที่นำเสนอการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่าน โดยใช้วิธีการทางด้านชีวมิติ	I&ATechnique	Class	technique และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "technique") implies (tv.dataValue -> isEmpty)	เทคนิคในการระบุและพิสูจน์ตัวตน
		biometricMechanism	Class	"role@name[instance]"		โครงสร้างของชีวมิติ
		biometricCharacteristic	Class	"role@name[instance]"		คุณลักษณะของชีวมิติ
		biometricFactor	Class	"role@name[instance]"		ปัจจัยในการออกแบบทางชีวมิติ
ความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง (Security Accounting Requirements)	เป็นแบบรูปสำหรับนำเสนอการสร้างความต้องการในการติดตามความมั่นคงที่เกี่ยวข้องกับเหตุการณ์หรือกิจกรรม	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		*role	Class	"role@name[instance]"		บทบาทของผู้ใช้ระบบ
		accountingRequirement	Class	"role@name[instance]"		ความต้องการสำหรับในการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingDomain	Class	"role@name[instance]"		ขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingFactor	Class	"role@name[instance]"		ปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingService	Class	"role@name[instance]"		บริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		*monitored	Relationship	monitor และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "monitor") implies (tv.dataValue -> isEmpty)	การเชื่อมโยงที่มีการตรวจสอบการเข้าถึงระบบ

\* คือการนำยูเอมแอลเซคเอสที่มาประยุกต์ใช้

ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
ความต้องการการตรวจสอบ (Audit Requirements)	แบบรูปนี้นำเสนอการสร้างความต้องการในการวิเคราะห์ข้อมูลต่างๆ ที่ได้บันทึกไว้	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		*role	Class	"role@name[instance]"		บทบาทของผู้ใช้ในระบบ
		accountingRequirement	Class	"role@name[instance]"		ความต้องการสำหรับการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountginDomain	Class	"role@name[instance]"		ขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingFactor	Class	"role@name[instance]"		ปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingService	Class	"role@name[instance]"		บริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		audit	Class	"role@name[instance]"		เป็นคลาสของบริการการตรวจสอบ
*monitored	Relationship	monitor และ "role@name[instance]"		1> self.taggedValue -> forall(tv tv.name = "monitor") implies (tv.dataValue -> isEmpty)	การเชื่อมโยงที่มีการตรวจสอบการเข้าถึงระบบ	
ความต้องการการตรวจสอบหลักฐานและการบันทึก (Audit Trails and Logging Requirements)	เป็นแบบรูปที่เสนอการสร้างความต้องการสำหรับการตรวจสอบหลักฐานและการบันทึกต่างๆ เกี่ยวกับเหตุการณ์หรือกิจกรรมที่เกิดขึ้นในองค์กรหรือระบบ	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		*role	Class	"role@name[instance]"		บทบาทของผู้ใช้ในระบบ
		accountingRequirement	Class	"role@name[instance]"		ความต้องการสำหรับการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountginDomain	Class	"role@name[instance]"		ขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingFactor	Class	"role@name[instance]"		ปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingService	Class	"role@name[instance]"		บริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		AT&L	Class	"role@name[instance]"		เป็นคลาสของบริการการตรวจสอบหลักฐานและการบันทึก

\* คือการนำยูเอ็มแอลเซตเอสพีมาประยุกต์ใช้

ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
		*monitored	Relationship	monitor และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "monitor") implies (tv.dataValue -> isNotEmpty)	การเชื่อมโยงที่มีการตรวจสอบการเข้าถึงระบบ
ความต้องการการป้องกันการบุกรุก (Intrusion Detection Requirements)	เป็นแบบรูปที่เสนอการสร้างความต้องการสำหรับการเฝ้าสังเกตกิจกรรมต่างๆ ที่เกิดขึ้น และการวิเคราะห์กิจกรรมเหล่านั้นเพื่อบอกถึงการละเมิดความมั่นคงขององค์กร	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		*role	Class	"role@name[instance]"		บทบาทของผู้ใช้ระบบ
		accountingRequirement	Class	"role@name[instance]"		ความต้องการสำหรับในการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountginDomain	Class	"role@name[instance]"		ขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingFactor	Class	"role@name[instance]"		ปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingService	Class	"role@name[instance]"		บริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		IDS	Class	"role@name[instance]"		เป็นคลาสของบริการการป้องกันการบุกรุก
		*monitored	Relationship	monitor และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "monitor") implies (tv.dataValue -> isNotEmpty)	การเชื่อมโยงที่มีการตรวจสอบการเข้าถึงระบบ
ความต้องการการไม่ถูกปฏิเสธ (Non-Repudiation Requirements)	เป็นแบบรูปที่เสนอการสร้างความต้องการในการตรวจสอบและรักษาหลักฐานเพื่อให้ผู้มีส่วนร่วมไม่ถูกปฏิเสธจากกิจกรรมใดๆ ขององค์กร	asset	Class	assetKind และ "role@name[instance]"	1> self.taggedValue -> forall(tv tv.name = "assetKind") implies (tv.dataValue = Information or tv.dataValue = Physical)	สินทรัพย์ทางด้านธุรกิจขององค์กร
		*role	Class	"role@name[instance]"		บทบาทของผู้ใช้ระบบ
		accountingRequirement	Class	"role@name[instance]"		ความต้องการสำหรับในการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountginDomain	Class	"role@name[instance]"		ขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingFactor	Class	"role@name[instance]"		ปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
		accountingService	Class	"role@name[instance]"		บริการการบันทึกเหตุการณ์ทางด้านความมั่นคง

\* คือการนำยูเอ็มแอลเซคเอสพีมาประยุกต์ใช้

ตารางที่ ข.4 แม่พิมพ์ต้นแบบสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	คำอธิบายของแบบรูปความมั่นคง	แม่พิมพ์ต้นแบบ	คลาสพื้นฐาน	ป้ายระบุ	เงื่อนไขบังคับ	คำอธิบาย
		nonRepudiation	Class	"role@name[instance]"		เป็นคลาสของบริการการไม่ถูกปฏิเสธ
		*monitored	Relationship	monitor และ "role@name[instance]"	1 > self.taggedValue -> forall(tv tv.name = "monitor") implies (tv.dataValue -> isEmpty)	การเชื่อมโยงที่มีการตรวจสอบการเข้าถึงระบบ

\* คือการนำยูเอ็มแอลเซตเอสพีมาประยุกต์ใช้

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย



ตารางที่ ข.5 ป้ายระบุสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง

แบบรูปความมั่นคง	ป้ายระบุ	แม่พิมพ์ต้นแบบ	ตัวอย่างค่าของป้ายระบุ	มัลติพลิซิติ	คำอธิบาย
การระบุความต้องการความมั่นคงสำหรับ สินทรัพย์องค์กร (Security Needs Identification for Enterprise Asset)	assettKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	secureKind	securityProperty	Confidentiality, Integrity, Availability, Accountaability	*	คุณสมบัติด้านความมั่นคงของสินทรัพย์
	businessFactor	businessDriver	Laws, Goals, Business processes, etc.	*	ปัจจัยทางด้านธุรกิจขององค์กร
การกำหนดมูลค่าสินทรัพย์ (Asset Valuation)	assettKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	overAllValue	assetValue	ค่าของสินทรัพย์องค์กร	1	มูลค่าของสินทรัพย์องค์กร
การประเมินภัยคุกคาม (Threat Assessment)	assettKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	action	threat	Data entry errors, Accidental damage to vehicles, etc.	*	ภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร
	source	threatSource	Hackers, Terrorists, Internal threat, etc.	*	ต้นเหตุที่ทำให้เกิดภัยคุกคาม
	effect	threatConsequence	incapacitation, corruption, exposure of informational assets, etc.	*	ผลที่จะตามมาเมื่อเกิดภัยคุกคามขึ้น
การประเมินภาวะเสี่ยง (Vulnerability Assessment)	assettKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	action	threat	Data entry errors, Accidental damage to vehicles, etc.	*	ภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร
	weakness	vulnerability	Lack of protection, Carelessness of employees, etc.	*	จุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง
	rating	threatLikelihood	1, 2, 3, 4, etc.	1	ความน่าจะเป็นที่อาจเกิดเหตุการณ์ที่เสี่ยงอันตราย
การกำหนดค่าความเสี่ยง (Risk Determination)	assettKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	overAllValue	assetValue	ค่าของสินทรัพย์องค์กร	1	มูลค่าของสินทรัพย์องค์กร
	action	threat	Data entry errors, Accidental damage to vehicles, etc.	*	ภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร
	source	threatSource	Hackers, Terrorists, Internal threat, etc.	*	ต้นเหตุที่ทำให้เกิดภัยคุกคาม
	effect	threatConsequence	incapacitation, corruption, exposure of informational assets, etc.	*	ผลที่จะตามมาเมื่อเกิดภัยคุกคามขึ้น
	rating	threatLikelihood	1, 2, 3, 4, etc.	1	ความน่าจะเป็นที่อาจเกิดเหตุการณ์ที่เสี่ยงอันตราย
	weakness	vulnerability	Lack of protection, Carelessness of employees, etc.	*	จุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง
แนวคิดความมั่นคงองค์กร (Enterprise Security Approaches)	assettKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	secureKind	securityProperty	Confidentiality, Integrity, Availability, Accountaability	*	คุณสมบัติด้านความมั่นคงของสินทรัพย์
บริการความมั่นคงองค์กร (Enterprise Security Services)	assettKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	secureKind	securityProperty	Confidentiality, Integrity, Availability, Accountaability	*	คุณสมบัติด้านความมั่นคงของสินทรัพย์

จุฬาลงกรณ์มหาวิทยาลัย

ตารางที่ ข.5 ป้ายระบุสำหรับแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ป้ายระบุ	แม่พิมพ์ต้นแบบ	ตัวอย่างค่าของป้ายระบุ	มัลติพลิซิติ	คำอธิบาย
การสื่อสารของผู้มีส่วนองค์กร (Enterprise Partner Communication)	assessKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	secureKind	securityProperty	Confidentiality, Integrity, Availability, Accountaability	*	คุณสมบัติด้านความมั่นคงของสินทรัพย์
	connectionChannel	channel	Protocal (VANs, HTTPS, etc.), Hardware devices (servers, firewalls, etc.), Communication lines (dedicated, public)	*	ช่องทางการติดต่อกับองค์กรภายนอก
	*monitor	*monitored	-	*	ชื่ออ็อบเจกต์ที่เป็นผู้ตรวจสอบการเข้าถึงระบบ
ความต้องการการระบุและการพิสูจน์ตัวตน (I&A Requirement)	assessKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	requirement	I&ARequirement	Minimize costs, Protect I&A assets, etc.	*	บริการที่ตอบสนองความต้องการในการใช้บริการ การระบุและพิสูจน์ตัวตน
ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ ตัวตนอัตโนมัติ (Automated I&A Design Alternatives)	assessKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	requirement	I&ARequirement	Minimize costs, Protect I&A assets, etc.	*	บริการที่ตอบสนองความต้องการในการใช้บริการ การระบุและพิสูจน์ตัวตน
	technique:	I&ATechnique	Biometrics, Hardware Token, etc	*	เทคนิคในการระบุและพิสูจน์ตัวตน
การออกแบบและใช้รหัสผ่าน (Password Design and Use)	policy	posswordPolicy	ความยาวรหัสผ่านอย่างน้อย 8 ตัวอักษร	*	นโยบายทางด้านรหัสผ่าน
	technique:	I&ATechnique	Biometrics, Hardware Token, etc	*	เทคนิคในการระบุและพิสูจน์ตัวตน
ทางเลือกการออกแบบชีวมิติ (Biometrics Design Alternatives)	technique:	I&ATechnique	Biometrics, Hardware Token, etc	*	เทคนิคในการระบุและพิสูจน์ตัวตน
ความต้องการการบันทึกเหตุการณ์ทางด้านความ มั่นคง (Security Accounting Requirements)	assessKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	*monitor	*monitored	-	*	ชื่ออ็อบเจกต์ที่เป็นผู้ตรวจสอบการเข้าถึงระบบ
ความต้องการการตรวจสอบ (Audit Requirements)	assessKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	*monitor	*monitored	-	*	ชื่ออ็อบเจกต์ที่เป็นผู้ตรวจสอบการเข้าถึงระบบ
ความต้องการการตรวจสอบหลักฐานและการบันทึก (Audit Trails and Logging Requirements)	assessKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	*monitor	*monitored	-	*	ชื่ออ็อบเจกต์ที่เป็นผู้ตรวจสอบการเข้าถึงระบบ
ความต้องการการป้องกันการบุกรุก (Intrusion Detection Requirements)	assessKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	* monitor	*monitored	-	*	ชื่ออ็อบเจกต์ที่เป็นผู้ตรวจสอบการเข้าถึงระบบ
ความต้องการการไม่ถูกปฏิเสธ (Non-Repudiation Requirements)	assessKind	asset	Information Type, PhysicalType	1	ชนิดของสินทรัพย์
	*monitor	*monitored	-	*	ชื่ออ็อบเจกต์ที่เป็นผู้ตรวจสอบการเข้าถึงระบบ

\* คือการนำยูเอมแอลเซคเอสพีมาประยุกต์ใช้

## ภาคผนวก ค

### การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแต่ละแบบรูปความมั่นคง

การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแต่ละแบบรูปความมั่นคง เป็นอธิบายโครงสร้างเบื้องต้นของแต่ละแบบรูปความมั่นคง อีกทั้งยังแสดงถึงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงอีกด้วย โดยการประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแต่ละแบบรูปความมั่นคง ส่วนประกอบดังนี้

- ชื่อแบบรูปความมั่นคง
- ชื่อกลุ่มแบบรูปความมั่นคง
- คำอธิบายของแบบรูปความมั่นคง
- แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2
- องค์กรประกอบแบบจำลองภายในแบบรูปความมั่นคง
- ยูเอ็มแอลเซคเอสพี-2 ที่ประยุกต์ใช้
- คำอธิบายของแต่ละองค์กรประกอบแบบจำลอง

โดยมีรายละเอียดของแต่ละแบบรูปความมั่นคง ดังต่อไปนี้

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

ตารางที่ ค.1 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร

ชื่อแบบรูปความมั่นคง	การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Asset)	
กลุ่มแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)	
คำอธิบาย	เป็นแบบรูปที่เสนอการพิจารณาความมั่นคงขององค์กร โดยทำการระบุสินทรัพย์ที่สำคัญขององค์กร เพื่อหาวิธีป้องกันสินทรัพย์ต่างๆ เหล่านั้น	
<b>แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2</b>		
<pre> classDiagram     class Asset {         &lt;&lt;asset@SNI&gt;&gt;     }     class SecurityProperty {         &lt;&lt;securityProperty@SNI&gt;&gt;     }     class BusinessDriver {         &lt;&lt;businessDriver&gt;&gt;         businessFactor: Array     }     class Asset_SecurityProperty {         &lt;&lt;spc.asset-SecurityProperty@SNI&gt;&gt;     }     class AssetKind {         &lt;&lt;asset&gt;&gt;         assetKind: String     }     class SecureKind {         &lt;&lt;securityProperty&gt;&gt;         secureKind: Array     }      Asset "1..*" -- "1..*" BusinessDriver : need     SecurityProperty "1..*" -- "1..*" Asset : have     SecurityProperty "1..*" -- "1..*" BusinessDriver : dependOn     Asset_SecurityProperty "1..*" -- "1..*" Asset : have     Asset_SecurityProperty "1..*" -- "1..*" SecurityProperty : have     AssetKind ..&gt; Asset : assetKind: String     SecureKind ..&gt; SecurityProperty : secureKind: Array     </pre>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว อาคาร เป็นต้น
คลาส "SecurityProperty"	securityProperty	เป็นคลาสของคุณสมบัติทางด้านความมั่นคง ได้แก่ การรักษาความลับ ความสมบูรณ์ สภาพพร้อมใช้งาน และภาวะรับผิดชอบ
คลาส "BusinessDriver"	businessDriver	เป็นคลาสที่แสดงถึงตัวขับเคลื่อนทางด้านธุรกิจขององค์กร เช่น กฎหมาย ระเบียบขององค์กร หุ้นส่วน เป้าหมาย วัตถุประสงค์ กระบวนการทางธุรกิจ สถานที่ที่เกิดกระบวนการทางธุรกิจ เป็นต้น
คลาส "Asset-SecurityProperty"	spc	เป็นคลาสของความสัมพันธ์ระหว่างสินทรัพย์ทางด้านธุรกิจขององค์กรกับสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น กฎทางด้านความลับของข้อมูลพนักงาน ข้อมูลทางการเงินที่ต้องบอกให้กับหุ้นส่วน เป็นต้น

ตารางที่ ค.2 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปการกำหนดมูลค่าสินทรัพย์

ชื่อแบบรูปความมั่นคง	การกำหนดมูลค่าสินทรัพย์ (Asset Valuation)	
กลุ่มแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)	
คำอธิบาย	เป็นแบบรูปที่เสนอการกำหนดมูลค่าสินทรัพย์จะช่วยให้สามารถกำหนดความสำคัญของสินทรัพย์ขององค์กรที่เป็นเจ้าของหรือควบคุมอยู่	
<b>แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2</b>		
<pre> classDiagram     class Asset {         assetKind: String     }     class AssetValue {         overAllValue: Integer         securityValue: securityValue@assetValuation         financialValue: financialValue@assetValuation         businessValue: businessValue@assetValuation     }     Asset "1..*" -- "1..1" AssetValue : include     </pre>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "AssetValue"	assetValue	เป็นคลาสของมูลค่าของสินทรัพย์ เช่น 6 (Extreme) 4 (High) 1 (Negligible) เป็นต้น
คุณลักษณะ "securityValue" ของคลาส "AssetValue"	securityValue	เป็นมูลค่าความมั่นคงของสินทรัพย์องค์กร
คุณลักษณะ "financialValue" ของคลาส "AssetValue"	financialValue	เป็นมูลค่าทางการเงินขององค์กร เช่น ค่าใช้จ่ายต่างๆ เป็นต้น
คุณลักษณะ "businessValue" ของคลาส "AssetValue"	businessValue	เป็นมูลค่าผลกระทบทางธุรกิจขององค์กร เช่น การเสียลูกค้า หรือส่วนแบ่งการตลาด เป็นต้น

ตารางที่ ค.3 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปการประเมินภัยคุกคาม

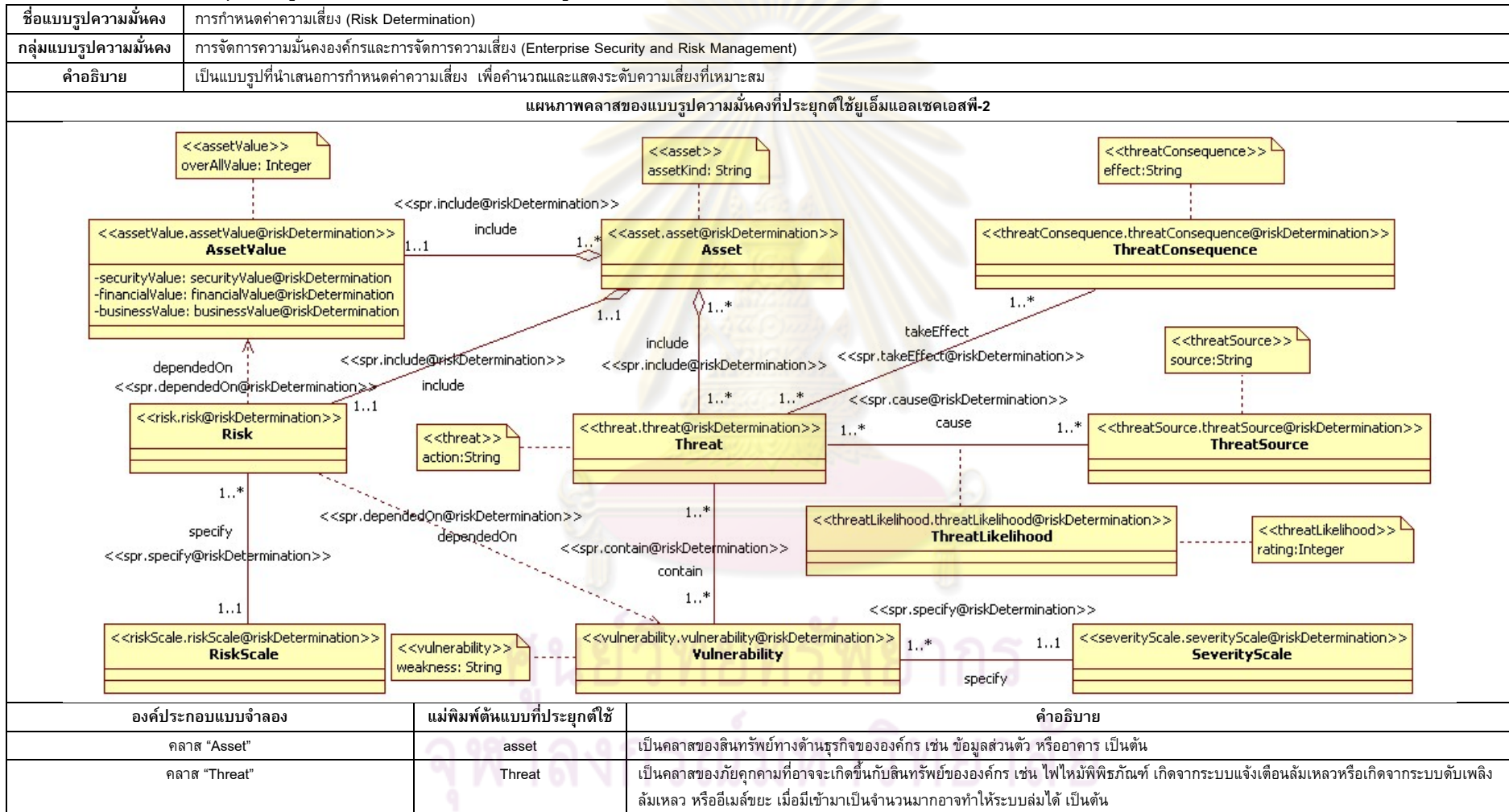
ชื่อแบบรูปความมั่นคง	การประเมินภัยคุกคาม (Threat Assessment)	
กลุ่มแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)	
คำอธิบาย	เป็นแบบรูปที่นำเสนอการกำหนดภัยคุกคาม ความถี่ของภัยคุกคามที่เกิดต่อสินทรัพย์ และผลกระทบเมื่อสินทรัพย์ถูกคุกคาม	
<b>แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2</b>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "Threat"	threat	เป็นคลาสของภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร เช่น ไฟไหม้พิศภักดิ์ เกิดจากระบบแจ้งเตือนล้มเหลวหรือเกิดจากระบบดับเพลิงล้มเหลว หรืออีเมลขยะ เมื่อมีเข้ามาเป็นจำนวนมากอาจทำให้ระบบล่มได้ เป็นต้น
คลาส "ThreatSource"	threatSource	เป็นคลาสของต้นเหตุที่ทำให้เกิดภัยคุกคาม เช่น พนักงาน หรือแฮกเกอร์ เป็นต้น
คลาส "ThreatLikelihood"	threatLikelihood	เป็นคลาสของความน่าจะเป็นที่อาจเกิดเหตุการณ์ที่เสี่ยงอันตราย เช่น 6 (Extreme) หรือ 2 (Low) เป็นต้น
คลาส "threatConsequence"	threatConsequence	เป็นคลาสของผลของภัยคุกคามนั้น เช่น ระบบล่ม หรือข้อมูลสูญหาย เป็นต้น

จุฬาลงกรณ์มหาวิทยาลัย

ตารางที่ ค.4 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปการประเมินจุดอ่อน

ชื่อแบบรูปความมั่นคง	การประเมินจุดอ่อน (Vulnerability Assessment)	
กลุ่มแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)	
คำอธิบาย	เป็นแบบรูปที่นำเสนอการระบุถึงจุดอ่อนของสินทรัพย์ในองค์กร และระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตีจุดอ่อนดังกล่าว	
<b>แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2</b>		
<pre> classDiagram     class Asset {         assetKind:String     }     class Threat {         action:String     }     class SeverityScale {         severityScale@vulnerabilityAssessment     }     class Vulnerability {         weakness:String     }     Asset "1..*" -- "1..*" Threat : include     Threat "1..*" -- "1..*" Vulnerability : contain     SeverityScale "1..1" -- "1..*" Vulnerability : specify     </pre>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "Threat"	threat	เป็นคลาสของภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร เช่น ไฟไหม้พีพีทริกเกอร์ เกิดจากระบบแจ้งเตือนล้มเหลวหรือเกิดจากระบบดับเพลิงล้มเหลว หรืออีเมลขยะ เมื่อมีเข้ามาเป็นจำนวนมากอาจทำให้ระบบล่มได้ เป็นต้น
คลาส "Vulnerability"	vulnerability	เป็นคลาสของจุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง เช่น ระบบแจ้งเตือนล้มเหลว หรือความไม่สมบูรณ์ของข้อมูลสำรอง เป็นต้น
คลาส "SeverityScale"	severityScale	เป็นคลาสของระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตี เช่น 4 (High) 1 (Negligible) เป็นต้น

ตารางที่ ค.5 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปการกำหนดค่าความเสี่ยง





ตารางที่ ค.5 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปการกำหนดค่าความเสี่ยง (ต่อ)

องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Vulnerability"	vulnerability	เป็นคลาสของจุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง เช่น ระบบแจ้งเตือนล้มเหลว หรือความไม่สมบูรณ์ของข้อมูลสำรอง เป็นต้น
คลาส "SeverityScale"	severityScale	เป็นคลาสของระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตี เช่น 4 (High) 1 (Negligible) เป็นต้น
คลาส "ThreatSource"	threatSource	เป็นคลาสของต้นเหตุที่ทำให้เกิดภัยคุกคาม เช่น พนักงาน หรือแฮคเกอร์ เป็นต้น
คลาส "ThreatLikelihood"	threatLikelihood	เป็นคลาสของความน่าจะเป็นที่อาจเกิดเหตุการณ์ที่เสี่ยงอันตราย เช่น 6 (Extreme) 2 (Low) เป็นต้น
คลาส "threatConsequence" ของคลาส	threatConsequence	เป็นคลาสของผลของภัยคุกคามนั้น เช่น ระบบล่ม หรือข้อมูลสูญหาย เป็นต้น
คลาส "Risk"	risk	เป็นคลาสของความเสี่ยงของสินทรัพย์
คลาส "RiskScale"	riskScale	เป็นคลาสระดับของความเสี่ยง เช่น Extreme Medium Low เป็นต้น
คลาส "AssetValue"	assetValue	เป็นคลาสของมูลค่าของสินทรัพย์ เช่น 6 (Extreme) 4 (High) 1 (Negligible) เป็นต้น
คุณลักษณะ "securityValue" ของคลาส "AssetValue"	securityValue	เป็นมูลค่าความมั่นคงของสินทรัพย์องค์กร
คุณลักษณะ "financialValue" ของคลาส "AssetValue"	financialValue	เป็นมูลค่าทางการเงินขององค์กร เช่น ค่าใช้จ่ายต่างๆ เป็นต้น
คุณลักษณะ "businessValue" ของคลาส "AssetValue"	businessValue	เป็นมูลค่าผลกระทบทางธุรกิจขององค์กร เช่น การเสียลูกค้า หรือส่วนแบ่งการตลาด เป็นต้น

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

ตารางที่ ค.6 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปแนวคิดความมั่นคงองค์กร

ชื่อแบบรูปความมั่นคง	แนวคิดความมั่นคงองค์กร (Enterprise Security Approaches)	
กลุ่มแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)	
คำอธิบาย	เป็นแบบรูปที่นำเสนอการกำหนดแนวคิดความมั่นคงให้แก่สินทรัพย์ขององค์กร	
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2		
<pre> classDiagram     class Risk["&lt;&lt;risk.risk@ESA&gt;&gt;\nRisk"]     class Prevention["&lt;&lt;prevention.securityApproach@ESA&gt;&gt;\nPrevention"]     class Detection["&lt;&lt;detection.securityApproach@ESA&gt;&gt;\nDetection"]     class Response["&lt;&lt;response.securityApproach@ESA&gt;&gt;\nResponse"]     class Asset["&lt;&lt;asset.asset@ESA&gt;&gt;\nAsset"]     class SecurityProperty["&lt;&lt;securityProperty.securityProperty@ESA&gt;&gt;\nSecurityProperty"]     class SecurityApproach["&lt;&lt;securityApproach.securityApproach@ESA&gt;&gt;\nSecurityApproach"]      Risk "1..1" -- "1..1" Asset : include &lt;&lt;spr.include@ESA&gt;&gt;     Prevention "1..*" -- "1..*" SecurityApproach : include &lt;&lt;spr.include@ESA&gt;&gt;     Detection "1..*" -- "1..*" SecurityApproach : include &lt;&lt;spr.include@ESA&gt;&gt;     Response "1..*" -- "1..*" SecurityApproach : include &lt;&lt;spr.include@ESA&gt;&gt;     Asset "1..*" -- "1..*" SecurityApproach : include &lt;&lt;spr.include@ESA&gt;&gt;     Asset "1..*" -- "1..*" SecurityProperty : have &lt;&lt;spr.have@ESA&gt;&gt;     </pre> <p>UML Class Diagram illustrating the relationships between Enterprise Security Approaches (ESA) and related concepts:</p> <ul style="list-style-type: none"> <li><b>Risk</b> (1..1) includes <b>Asset</b> (1..1) via <code>&lt;&lt;spr.include@ESA&gt;&gt;</code>.</li> <li><b>Prevention</b> (1..*), <b>Detection</b> (1..*), and <b>Response</b> (1..*) all include <b>SecurityApproach</b> (1..*) via <code>&lt;&lt;spr.include@ESA&gt;&gt;</code>.</li> <li><b>Asset</b> (1..*) includes <b>SecurityApproach</b> (1..*) via <code>&lt;&lt;spr.include@ESA&gt;&gt;</code>.</li> <li><b>Asset</b> (1..*) has <b>SecurityProperty</b> (1..*) via <code>&lt;&lt;spr.have@ESA&gt;&gt;</code>.</li> </ul> <p>Annotations:</p> <ul style="list-style-type: none"> <li><code>&lt;&lt;asset&gt;&gt;</code> assetKind: String</li> <li><code>&lt;&lt;securityProperty&gt;&gt;</code> secureKind: Array</li> </ul>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "Risk"	risk	เป็นคลาสของความเสี่ยงของสินทรัพย์
คลาส "SecurityProperty"	securityProperty	เป็นคลาสของคุณสมบัติความมั่นคง ได้แก่ การรักษาความลับ ความสมบูรณ์ สภาพพร้อมใช้งาน และภาวะรับผิดชอบ
คลาส "SecurityApproach"	securityApproach	เป็นคลาสของแนวคิดความมั่นคง ได้แก่ การป้องกัน การค้นหา และการตอบสนอง
คลาส "Prevention"	prevention	เป็นคลาสของแนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย เช่น การโจมตีระบบ เป็นต้น
คลาส "Detection"	detection	เป็นคลาสของแนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย เช่น เครื่องตรวจจับความเคลื่อนไหว เป็นต้น
คลาส "Response"	response	เป็นคลาสของแนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย เช่น ปิดระบบ ฟืนฟูหรือซ่อมแซมสินทรัพย์ขององค์กร เป็นต้น

ตารางที่ ค.7 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปบริการความมั่นคงองค์กร

ชื่อแบบรูปความมั่นคง	บริการความมั่นคงองค์กร (Enterprise Security Services)	
กลุ่มแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)	
คำอธิบาย	เป็นแบบรูปสำหรับแนะนำองค์กรในการเลือกบริการความมั่นคงที่จะนำไปใช้ในการป้องกันสินทรัพย์	
<b>แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2</b>		
<pre> classDiagram     class SecurityProperty["&lt;&lt;securityProperty.securityProperty@ESS&gt;&gt; SecurityProperty"]     class Asset["&lt;&lt;asset.asset@ESS&gt;&gt; Asset"]     class SecurityService["&lt;&lt;securityService.securityService@ESS&gt;&gt; SecurityService"]     class SecurityApproach["&lt;&lt;securityApproach.securityApproach@ESS&gt;&gt; SecurityApproach"]     class Prevention["&lt;&lt;prevention.securityApproach@ESS&gt;&gt; Prevention"]     class Detection["&lt;&lt;detection.securityApproach@ESS&gt;&gt; Detection"]     class Response["&lt;&lt;response.securityApproach@ESS&gt;&gt; Response"]      SecurityProperty "1..*" -- "1..*" SecurityApproach : have &lt;&lt;spr.have@ESS&gt;&gt;     SecurityProperty "1..*" -- "1..*" Asset     Asset "1..*" -- "1..*" SecurityService : protect &lt;&lt;spr.protect@ESS&gt;&gt;     Asset "1..*" -- "1..*" SecurityApproach : include &lt;&lt;spr.include@ESS&gt;&gt;     SecurityService "1..*" -- "1..*" SecurityApproach : dependedOn &lt;&lt;spr.dependedOn@ESS&gt;&gt;     SecurityApproach "1..*" -- "1..*" Prevention : include &lt;&lt;spr.include@ESS&gt;&gt;     SecurityApproach "1..*" -- "1..*" Detection : include &lt;&lt;spr.include@ESS&gt;&gt;     SecurityApproach "1..*" -- "1..*" Response : include &lt;&lt;spr.include@ESS&gt;&gt;     </pre>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "SecurityProperty"	securityProperty	เป็นคลาสของคุณสมบัติความมั่นคง ได้แก่ การรักษาความลับ ความสมบูรณ์ สภาพพร้อมใช้งาน และภาวะรับผิดชอบ
คลาส "SecurityApproach"	securityApproach	เป็นคลาสของแนวคิดความมั่นคง ได้แก่ การป้องกัน การค้นหา และการตอบสนอง
คลาส "SecurityService"	securityService	เป็นคลาสของบริการความมั่นคงสำหรับสินทรัพย์ในองค์กร เช่น Access control หรือ Accounting เป็นต้น
คลาส "Prevention"	prevention	เป็นคลาสของแนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย เช่น การโจมตีระบบ เป็นต้น
คลาส "Detection"	detection	เป็นคลาสของแนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย เช่น เครื่องตรวจจับความเคลื่อนไหว เป็นต้น
คลาส "Response"	response	เป็นคลาสของแนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย เช่น ปัดระบบ ฟืนฟูหรือซ่อมแซมสินทรัพย์ขององค์กร เป็นต้น

ตารางที่ ค.8 การประยุกต์ใช้เอ็มแอลเซคเอสพี-2 ในแบบรูปการสื่อสารของผู้กับหุ้นส่วนองค์กร

ชื่อแบบรูปความมั่นคง	การสื่อสารของผู้กับหุ้นส่วนองค์กร (Enterprise Partner Communication)	
กลุ่มแบบรูปความมั่นคง	การจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)	
คำอธิบาย	เป็นแบบรูปที่นำเสนอการเตรียมเครื่องมือและบริการต่างๆ สำหรับอำนวยความสะดวกและความปลอดภัยติดต่อและการแลกเปลี่ยนข้อมูลระหว่างหุ้นส่วนกับองค์กร	
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้เอ็มแอลเซคเอสพี-2		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "SecurityProperty"	securityProperty	เป็นคลาสของคุณสมบัติความมั่นคง ได้แก่ การรักษาความลับ ความสมบูรณ์ สภาพพร้อมใช้งาน และภาวะรับผิดชอบ
คลาส "Role"	* role	เป็นคลาสของบทบาทของผู้ใช้ระบบเช่น บทบาทของผู้บริการระบบ หรือลูกค้า เป็นต้น
คลาส "I&AService"	I&AService	เป็นคลาสของบริการการระบุและพิสูจน์ตัวตนในการเข้าถึงสินทรัพย์ขององค์กร
คลาส "EnterprisePartner"	* client	เป็นคลาสของผู้ใช้งานจากภายนอกระบบ
คลาส "ServiceTermination"	serviceTermination	เป็นคลาสของกิจกรรมการสิ้นสุด เช่น การถอนสิทธิ์ เป็นต้น
คลาส "CommunicationChannel"	channel	เป็นคลาสของช่องทางการติดต่อกับองค์กรภายนอก เช่น โพรโตคอล หรืออุปกรณ์ฮาร์ดแวร์ เป็นต้น
คลาส "ExchangeMethod"	exchangeMethod	เป็นคลาสของวิธีดำเนินการที่ใช้ในช่องทางการติดต่อ เช่น On-demand Transfer หรือ Real-time Information Exchange เป็นต้น

\* คือการนำเอ็มแอลเซคเอสพีมาประยุกต์ใช้

ตารางที่ ค.9 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปความต้องการการระบุและการพิสูจน์ตัวตน

ชื่อแบบรูปความมั่นคง	ความต้องการการระบุและการพิสูจน์ตัวตน (I&A Requirement)	
กลุ่มแบบรูปความมั่นคง	การระบุตัวตนและการพิสูจน์ตัวตน (Identification and Authentication)	
คำอธิบาย	เป็นแบบรูปที่นำเสนอและสร้างความต้องการพื้นฐานสำหรับการบริการด้านการระบุและพิสูจน์ตัวตน	
<b>แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2</b>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "I&AService"	I&AService	เป็นคลาสของบริการการระบุและพิสูจน์ตัวตนในการเข้าถึงสินทรัพย์ขององค์กร
คลาส "I&ARequirement"	I&ARequirement	เป็นคลาสของความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน เช่น ใช้เวลาและความพยายามที่น้อยที่สุด เป็นต้น
คลาส "DomainFactor"	domainFactor	เป็นคลาสของปัจจัยที่มีผลกระทบต่อการกำหนดความต้องการ เช่น ประสบการณ์ของผู้ใช้ หรือความถี่ในการใช้งาน เป็นต้น
คลาส "DomainFactorRequirement"	spc	เป็นความสัมพันธ์ระหว่างปัจจัยที่มีผลกระทบต่อการกำหนดความต้องการ และความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน เช่น การใช้เวลาและความพยายามที่น้อยที่สุด จะขึ้นอยู่กับ ความถี่ในการใช้งานหรือลักษณะเฉพาะของผู้ใช้งาน เป็นต้น
คลาส "I&ADomain"	I&ADomain	เป็นคลาสของขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน เช่น เฉพาะเวลากลางคืน หรือวันสุดสัปดาห์ เป็นต้น



ตารางที่ ค.11 การประยุกต์ใช้เอ็มแอลเซคเอสพี-2 ในแบบรูปการออกแบบและใช้รหัสผ่าน

ชื่อแบบรูปความมั่นคง	การออกแบบและใช้รหัสผ่าน (Password Design and Use)	
กลุ่มแบบรูปความมั่นคง	การระบุตัวตนและการพิสูจน์ตัวตน (Identification and Authentication)	
คำอธิบาย	เป็นแบบรูปที่นำเสนอการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่านสำหรับการบริการการระบุและพิสูจน์ตัวตน	
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้เอ็มแอลเซคเอสพี-2		
<pre> classDiagram     class IATechnique {         &lt;&lt;I&amp;ATechnique&gt;&gt;         technique: String     }     class PasswordPolicy {         &lt;&lt;passwordPolicy.passwordPolicy@passwordDesignAndUse&gt;&gt;     }     class Password {         &lt;&lt;password.password@passwordDesignAndUse&gt;&gt;         +ownership: ownership@passwordDesignAndUse         +entry: entry@passwordDesignAndUse         +distribution: distribution@passwordDesignAndUse         +storage: storage@passwordDesignAndUse         +transmission: transmission@passwordDesignAndUse     }     PasswordPolicy ..&gt; IATechnique : dependOn     PasswordPolicy ..&gt; PasswordPolicy : policy: String     PasswordPolicy ..&gt; Password : contain     </pre>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "I&ATechnique"	I&ATechnique	เป็นคลาสของเทคนิคในการระบุและพิสูจน์ตัวตน เช่น Biometrics หรือ Unregistered Users เป็นต้น
คลาส "Password"	password	เป็นคลาสที่เก็บข้อมูลของรหัสผ่านต่างๆ เช่น เป็นรหัสผ่านส่วนบุคคล เป็นต้น
คลาส "PasswordPolicy"	passwordPolicy	เป็นคลาสของนโยบายทางด้านรหัสผ่าน เช่น ความยาวของรหัสผ่านอย่างน้อย 8 ตัวอักษร เป็นต้น

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

ตารางที่ ค.12 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปทางเลือกการออกแบบชีวมิติ

ชื่อแบบรูปความมั่นคง	ทางเลือกการออกแบบชีวมิติ (Biometrics Design Alternatives)	
กลุ่มแบบรูปความมั่นคง	การระบุตัวตนและการพิสูจน์ตัวตน (Identification and Authentication)	
คำอธิบาย	เป็นแบบรูปที่นำเสนอการออกแบบ การสร้าง และการจัดการการใช้รหัสผ่าน โดยใช้วิธีการทางด้านชีวมิติ	
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2		
<pre> classDiagram     class IATechnique {         &lt;&lt;I&amp;ATechnique.I&amp;ATechnique@BDA&gt;&gt;         technique: String     }     class BiometricMechanism {         &lt;&lt;biometricMechanism.biometricMechanism@BDA&gt;&gt;     }     class BiometricFactor {         &lt;&lt;biometricFactor.biometricFactor@BDA&gt;&gt;     }     class BiometricCharacteristic {         &lt;&lt;biometricCharacteristic.biometricCharacteristic@BDA&gt;&gt;     }     IATechnique &lt; -- BiometricMechanism     IATechnique o-- BiometricMechanism : contain &lt;&lt;spr.contain@BDA&gt;&gt;     BiometricMechanism -- BiometricFactor : 1..* haveEffect &lt;&lt;spr.haveEffect@BDA&gt;&gt;     BiometricFactor -- BiometricCharacteristic : 1..* haveEffect     </pre>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "I&ATechnique"	I&ATechnique	เป็นคลาสของเทคนิคในการระบุและพิสูจน์ตัวตน เช่น Biometrics หรือ Unregistered Users เป็นต้น
คลาส "BiometricFactor"	biometricFactor	เป็นคลาสของปัจจัยในการออกแบบทางชีวมิติ เช่น ความง่ายในการใช้งาน ความปลอดภัย หรือความถูกต้อง เป็นต้น
คลาส "BiometricMechanism"	biometricMechanism	เป็นคลาสของวิธีการทางด้านชีวมิติ เช่น การตรวจสอบเสียง เป็นต้น
คลาส "BiometricCharacteristic"	biometricCharacteristic	เป็นคลาสของคุณลักษณะของชีวมิติ เช่น ความง่ายในการใช้งาน เมื่อใช้เสียงในการระบุและพิสูจน์ตัวตนจะมีความง่ายในการใช้งานสูง แต่เมื่อใช้จดจำใบหน้าในการระบุและพิสูจน์ตัวตนจะมีความง่ายในการใช้งานต่ำ

จุฬาลงกรณ์มหาวิทยาลัย



ตารางที่ ค.13 การประยุกต์ใช้เอ็มแอลเซคเอสพี-2 ในแบบรูปความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง

ชื่อแบบรูปความมั่นคง	ความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง (Security Accounting Requirements)	
กลุ่มแบบรูปความมั่นคง	การบันทึกเหตุการณ์ (Accounting)	
คำอธิบาย	เป็นแบบรูปสำหรับนำเสนอการสร้างความต้องการในการติดตามความมั่นคงที่เกี่ยวข้องกับเหตุการณ์หรือกิจกรรม	
แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้เอ็มแอลเซคเอสพี-2		
<pre> classDiagram     class AccountingDomain["&lt;&lt;accountingDomain,accountingDomain@SAR&gt;&gt; AccountingDomain"]     class AccountingFactorRequirement["&lt;&lt;SPC,accountingFactorRequirement@SAR&gt;&gt; AccountingFactorRequirement"]     class AccountingFactor["&lt;&lt;accountingFactor,accountingFactor@SAR&gt;&gt; AccountingFactor"]     class AccountingRequirement["&lt;&lt;accountingRequirement,accountingRequirement@SAR&gt;&gt; AccountingRequirement"]     class Role["&lt;&lt;role,role@SAR&gt;&gt; Role"]     class Asset["&lt;&lt;asset,asset@SAR&gt;&gt; Asset"]     class AccountingService["&lt;&lt;accountingService,accountingService@SAR&gt;&gt; AccountingService"]      AccountingDomain "1..*" -- "1..*" AccountingFactorRequirement : specify &lt;&lt;spr.specify@SAR&gt;&gt;     AccountingFactorRequirement "1..*" -- "1..*" AccountingFactor : haveEffect &lt;&lt;spr.haveEffect@SAR&gt;&gt;     AccountingFactorRequirement "1..*" -- "1..*" AccountingRequirement : haveEffect &lt;&lt;spr.haveEffect@SAR&gt;&gt;     AccountingRequirement "1..*" -- "1..*" AccountingService : use &lt;&lt;spr.use@SAR&gt;&gt;     Role "1..*" -- "1..*" Asset : access &lt;&lt;monitored.access@SAR&gt;&gt;     Role "1..*" -- "1..*" AccountingService : use &lt;&lt;spr.use@SAR&gt;&gt;     Asset "1..*" -- "1..*" AccountingService : use &lt;&lt;spr.use@SAR&gt;&gt;      note for AccountingFactorRequirement "monitor: Array"     note for Asset "assetKing: String"     </pre>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "Role"	* role	เป็นคลาสของบทบาทของผู้ใช้ในระบบ เช่น บทบาทของผู้บริการระบบ หรือลูกค้า เป็นต้น
คลาส "AccountingRequirement"	accountingRequirement	เป็นคลาสของความต้อการสำหรับการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น ข้อมูลของเหตุการณ์ หรือข้อมูลของผู้ที่อยู่ในกิจกรรม เป็นต้น
คลาส "AccountingDomain"	accountingDomain	เป็นคลาสของขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น กลุ่มของพนักงาน หรือกิจกรรมที่เกี่ยวข้อง เป็นต้น
คลาส "AccountingFactor"	accountingFactor	เป็นคลาสของปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น ระเบียบภายในองค์กร หรือความรับผิดชอบ เป็นต้น
คลาส "AccountingFactorRequirement"	spc	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
คลาส "SecurityAccountingService"	accountingService	เป็นคลาสของบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง

\* คือการนำเอ็มแอลเซคเอสพีมาประยุกต์ใช้

ตารางที่ ค.14 การประยุกต์ใช้เอ็มแอลเซคเอสพี-2 ในแบบรูปความต้องการการตรวจสอบ

ชื่อแบบรูปความมั่นคง	ความต้องการการตรวจสอบ (Audit Requirements)	
กลุ่มแบบรูปความมั่นคง	การบันทึกเหตุการณ์ (Accounting)	
คำอธิบาย	แบบรูปนี้นำเสนอการสร้างความต้องการในการวิเคราะห์ข้อมูลต่างๆ ที่บันทึกไว้	
<b>แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้เอ็มแอลเซคเอสพี-2</b>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "Role"	* role	เป็นคลาสของบทบาทของผู้ใช้ในระบบเช่น บทบาทของผู้บริการระบบ หรือลูกค้า เป็นต้น
คลาส "AccountingRequirement"	accountingRequirement	เป็นคลาสของความต้องการการตรวจสอบสำหรับขอบเขตที่กำหนดไว้ เช่น ข้อมูลของผู้ที่กระทำกิจกรรมกับกิจกรรมอื่นๆ เป็นต้น
คลาส "AccountingDomain"	accountingDomain	เป็นคลาสของขอบเขตสำหรับบริการการตรวจสอบ เช่น กลุ่มของผู้ใช้งาน หรือกิจกรรมที่เกี่ยวข้อง เป็นต้น
คลาส "AccountingFactor"	accountingFactor	เป็นคลาสของปัจจัยที่มีผลต่อความต้องการการตรวจสอบ เช่น ระเบียบภายในองค์กร หรือความรับผิดชอบ เป็นต้น
คลาส "AccountingFactorRequirement"	spc	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
คลาส "SecurityAccountingService"	accountingService	เป็นคลาสของบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
คลาส "AuditService"	audit	เป็นคลาสของบริการการตรวจสอบ

\* คือการนำเอ็มแอลเซคเอสพีมาประยุกต์ใช้

ตารางที่ ค.15 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปความต้องการการตรวจสอบหลักฐานและการบันทึก

ชื่อแบบรูปความมั่นคง	ความต้องการการตรวจสอบหลักฐานและการบันทึก (Audit Trails and Logging Requirements)	
กลุ่มแบบรูปความมั่นคง	การบันทึกเหตุการณ์ (Accounting)	
คำอธิบาย	เป็นแบบรูปที่เสนอการสร้างความต้องการสำหรับการตรวจสอบหลักฐานและการบันทึกต่างๆ เกี่ยวกับเหตุการณ์หรือกิจกรรมที่เกิดขึ้นในองค์กรหรือระบบ	
<b>แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2</b>		
<pre> classDiagram     class AccountingDomain["&lt;&lt;accountingDomain, accountingDomain@AT&amp;L&gt;&gt;"]     class AccountingFactorRequirement["&lt;&lt;SPC, accountingFactorRequirement@AT&amp;L&gt;&gt;"]     class AccountingFactor["&lt;&lt;accountingFactor, accountingFactor@AT&amp;L&gt;&gt;"]     class AccountingRequirement["&lt;&lt;accountingRequirement, accountingRequirement@AT&amp;L&gt;&gt;"]     class AccountingService["&lt;&lt;accountingService, accountingService@AT&amp;L&gt;&gt;"]     class Role["&lt;&lt;role, role@AT&amp;L&gt;&gt;"]     class Asset["&lt;&lt;asset, asset@AT&amp;L&gt;&gt;"]     class ATLServices["&lt;&lt;AT&amp;L, accountingService@AT&amp;L&gt;&gt;"]      AccountingDomain "1..*" -- "1..*" AccountingFactorRequirement : specify &lt;&lt;spr, specify@AT&amp;L&gt;&gt;     AccountingFactorRequirement .. AccountingFactor     AccountingFactor "1..*" -- "1..*" AccountingRequirement : haveEffect &lt;&lt;spr, haveEffect@AT&amp;L&gt;&gt;     AccountingRequirement .. AccountingService : dependedOn &lt;&lt;spr, dependedOn@AT&amp;L&gt;&gt;     AccountingService .. ATLServices : type &lt;&lt;spr, type@AT&amp;L&gt;&gt;     Role "1..*" -- "1..*" Asset : access &lt;&lt;monitored, access@AT&amp;L&gt;&gt;     Asset "1..*" -- "1..*" AccountingService : use &lt;&lt;spr, use@AT&amp;L&gt;&gt;     </pre>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "Role"	* role	เป็นคลาสของบทบาทของผู้ใช้ในระบบเช่น บทบาทของผู้บริการระบบ หรือลูกค้า เป็นต้น
คลาส "AccountingRequirement"	accountingRequirement	เป็นคลาสของความต้องการสำหรับการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น ข้อมูลของเหตุการณ์ หรือข้อมูลของผู้ที่อยู่ในกิจกรรม เป็นต้น
คลาส "AccountingDomain"	accountingDomain	เป็นคลาสของขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น กลุ่มของผู้ใช้งาน หรือกิจกรรมที่เกี่ยวข้อง เป็นต้น
คลาส "AccountingFactor"	accountingFactor	เป็นคลาสของปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น ระเบียบภายในองค์กร หรือความรับผิดชอบ เป็นต้น
คลาส "AccountingFactorRequirement"	spc	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
คลาส "SecurityAccountingService"	accountingService	เป็นคลาสของบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
คลาส "AT&LService"	AT&L	เป็นคลาสของบริการการตรวจสอบหลักฐานและการบันทึก

\* คือการนำยูเอ็มแอลเซคเอสพีมาประยุกต์ใช้

ตารางที่ ค.16 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปความต้องการการป้องกันการบุกรุก

ชื่อแบบรูปความมั่นคง	ความต้องการการป้องกันการบุกรุก (Intrusion Detection Requirements)	
กลุ่มแบบรูปความมั่นคง	การบันทึกเหตุการณ์ (Accounting)	
คำอธิบาย	เป็นแบบรูปที่เสนอการสร้างความต้องการสำหรับการเฝ้าสังเกตกิจกรรมต่างๆ ที่เกิดขึ้น และการวิเคราะห์กิจกรรมเหล่านั้นเพื่อป้องกันความมั่นคงขององค์กร	
<b>แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2</b>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "Role"	* role	เป็นคลาสของบทบาทของผู้ใช้ในระบบเช่น บทบาทของผู้บริหารระบบ หรือลูกค้า เป็นต้น
คลาส "AccountingRequirement"	accountingRequirement	เป็นคลาสของความต้องการสำหรับการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น ข้อมูลของเหตุการณ์ หรือข้อมูลของผู้ที่อยู่ในกิจกรรม เป็นต้น
คลาส "AccountingDomain"	accountingDomain	เป็นคลาสของขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น กลุ่มของพนักงาน หรือกิจกรรมที่เกี่ยวข้อง เป็นต้น
คลาส "AccountingFactor"	accountingFactor	เป็นคลาสของปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น ระเบียบภายในองค์กร หรือความรับผิดชอบ เป็นต้น
คลาส "AccountingFactorRequirement"	spc	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
คลาส "SecurityAccountingService"	accountingService	เป็นคลาสของบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
คลาส "IDSService"	IDS	เป็นคลาสของบริการการป้องกันการบุกรุก

\* คือการนำยูเอ็มแอลเซคเอสพีมาประยุกต์ใช้

ตารางที่ ค.17 การประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2 ในแบบรูปความต้องการการไม่ถูกปฏิเสธ

ชื่อแบบรูปความมั่นคง	ความต้องการการไม่ถูกปฏิเสธ (Non-Repudiation Requirements)	
กลุ่มแบบรูปความมั่นคง	การบันทึกเหตุการณ์ (Accounting)	
คำอธิบาย	เป็นแบบรูปนี้เสนอการสร้างความต้องการในการตรวจสอบและรักษาหลักฐานเพื่อให้ผู้มีส่วนร่วมไม่ถูกปฏิเสธจากกิจกรรมใดๆ ของระบบหรือองค์กร	
<b>แผนภาพคลาสของแบบรูปความมั่นคงที่ประยุกต์ใช้ยูเอ็มแอลเซคเอสพี-2</b>		
องค์ประกอบแบบจำลอง	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้	คำอธิบาย
คลาส "Asset"	asset	เป็นคลาสของสินทรัพย์ทางด้านธุรกิจขององค์กร เช่น ข้อมูลส่วนตัว หรืออาคาร เป็นต้น
คลาส "Role"	* role	เป็นคลาสของบทบาทของผู้ใช้ในระบบเช่น บทบาทของผู้บริการระบบ หรือลูกค้า เป็นต้น
คลาส "AccountingRequirement"	accountingRequirement	เป็นคลาสของความต้อการสำหรับการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น ข้อมูลของเหตุการณ์ หรือข้อมูลของผู้ที่อยู่ในกิจกรรม เป็นต้น
คลาส "AccountingDomain"	accountingDomain	เป็นคลาสของขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น กลุ่มของใช้งาน หรือกิจกรรมที่เกี่ยวข้อง เป็นต้น
คลาส "AccountingFactor"	accountingFactor	เป็นคลาสของปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง เช่น ระเบียบภายในองค์กร หรือความรับผิดชอบ เป็นต้น
คลาส "AccountingFactorRequirement"	spc	เป็นคลาสของความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง
คลาส "SecurityAccountingService"	accountingService	เป็นคลาสของบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง
คลาส "NonRepudiationService"	nonRepudiation	เป็นคลาสของบริการการไม่ถูกปฏิเสธ

\* คือการนำยูเอ็มแอลเซคเอสพีมาประยุกต์ใช้

## ภาคผนวก ง

### กรณีศึกษาที่ประยุกต์ใช้ยูเอเอ็มแอลเซคเอสพี-2

#### สำหรับแสดงแบบรูปความมั่นคง

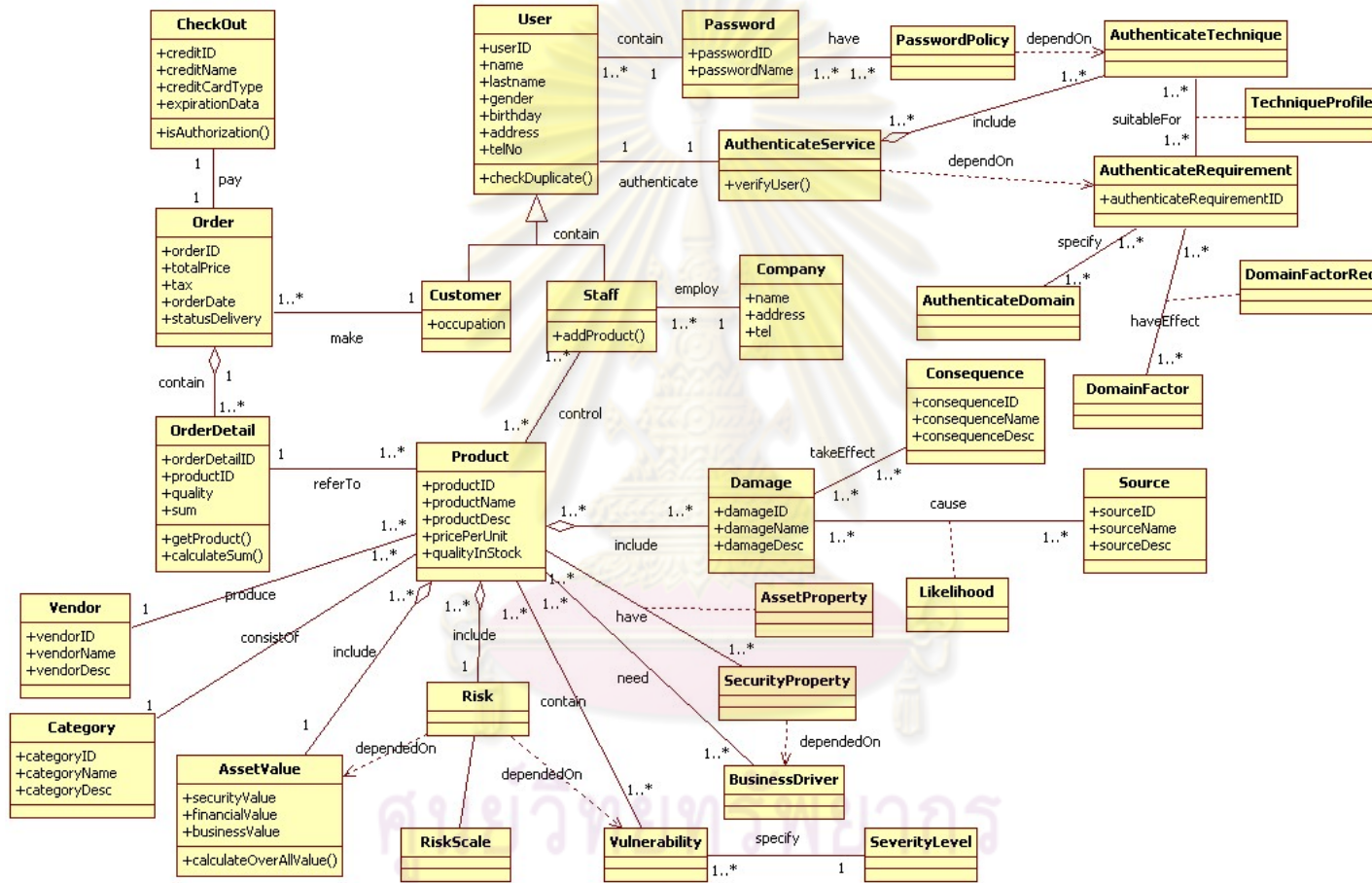
#### กรณีศึกษาที่ 1: ระบบสั่งซื้อสินค้าออนไลน์ (Online Shopping System)

ระบบสั่งซื้อสินค้าออนไลน์ คือระบบสำหรับสั่งซื้อสินค้าต่างๆ ผ่านอินเทอร์เน็ต โดยในการใช้งานระบบนั้นผู้ใช้งานจะต้องทำการลงทะเบียนเพื่อเข้าสู่ระบบเสียก่อน ซึ่งรหัสผ่านสำหรับเข้าระบบนั้น จะขึ้นอยู่กับนโยบายที่องค์กรได้กำหนดไว้จึงจะสามารถเข้าใช้งานระบบได้ โดยมีระบบตรวจสอบความถูกต้องของข้อมูลผู้ใช้งาน อีกทั้งยังมีการระบุภัยคุกคาม ความเสี่ยงของสินค้า ความน่าจะเป็นที่อาจจะเกิดขึ้น รวมไปถึงต้นเหตุของภัยคุกคาม โดยแสดงแผนภาพคลาสของระบบสั่งซื้อสินค้าออนไลน์ที่ไม่มีการระบุข้อมูลทางความมั่นคง ดังรูปที่ ง.1

จากการศึกษาและวิเคราะห์โครงสร้างของระบบพบว่า ระบบสั่งซื้อสินค้าออนไลน์นี้มีความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคง ดังตารางที่ ง.1

ตารางที่ ง.1 รายละเอียดความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของระบบสั่งซื้อสินค้าออนไลน์

ข้อมูลทางโครงสร้างของแบบรูป	ข้อมูลทางความมั่นคงของแบบรูป
1) ข้อมูลที่ระบุองค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป	1) สินค้าขององค์กร (Product)
2) ข้อมูลที่ระบุแบบรูปที่ใช้งาน	2) ตัวขับเคลื่อนทางด้านธุรกิจขององค์กร (BusinessDriver)
3) ข้อมูลที่ระบุลำดับของแบบรูป	3) คุณสมบัติทางด้านความมั่นคง (SecurityProperty)
4) ข้อมูลที่ระบุบทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป	4) ความสัมพันธ์ระหว่างสินทรัพย์กับคุณสมบัติความมั่นคง (AssetProperty)
	5) มูลค่าของสินทรัพย์ขององค์กร (AssetValue)
	6) ภัยคุกคามที่อาจจะเกิดขึ้นกับสินทรัพย์ขององค์กร (Damage)
	7) ผลที่จะตามมาเมื่อเกิดภัยคุกคามขึ้น (Consequence)
	8) ต้นเหตุที่ทำให้เกิดภัยคุกคาม (Source)
	9) ความน่าจะเป็นที่อาจจะเกิดเหตุการณ์ที่เสี่ยงอันตราย (Likelihood)
	10) ความเสี่ยงของแต่ละสินทรัพย์ (Risk)
	11) รายละเอียดของความเสี่ยง (RiskScale)
	12) จุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง (Vulnerability)
	13) ระดับความรุนแรงที่อาจจะเกิดขึ้น (SeverityLevel)
	14) ผู้จำหน่าย (Vendor)
	15) บทบาทของผู้ใช้ระบบ (User) ซึ่งแบ่งเป็น 2 ประเภท คือ ลูกค้า (Customer) และพนักงาน (Staff)
	16) บริการที่ตอบสนองความต้องการบริการการระบุและพิสูจน์ตัวตน (AuthenticateService)
	17) ความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน (AuthenticateRequirement)
	18) เทคนิคในการระบุและพิสูจน์ตัวตน (AuthenticateTechnique)
	19) ความสัมพันธ์ระหว่างความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตนกับเทคนิคในการระบุและพิสูจน์ตัวตน (TechniqueProfile)
	20) ขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน (AuthenticateDomain)
	21) ปัจจัยที่มีผลกระทบต่อความต้องการ (DomainFactor)
	22) ความสัมพันธ์ระหว่างปัจจัยที่มีผลกระทบต่อความต้องการกับความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน (DomainFactorReq)
	23) ที่เก็บข้อมูลของรหัสผ่านต่างๆ (Password)
	24) นโยบายทางด้านรหัสผ่าน (PasswordPolicy)



รูปที่ ง.1 แผนภาพคลาสของระบบสั่งซื้อสินค้าออนไลน์ที่ไม่มีการระบุข้อมูลทางความมั่นคง

ในการวิเคราะห์ระบบและความต้องการของระบบ พบว่าในระบบการสั่งซื้อสินค้าออนไลน์นี้ จะเน้นความสำคัญให้กับสินค้าขององค์กร โดยจะกำหนดให้เป็นสินทรัพย์ทางด้านธุรกิจขององค์กร ทั้งนี้เพราะเป็นระบบสั่งซื้อสินค้า ถ้าเกิดเหตุการณ์ทางด้านความมั่นคงขึ้นกับสินค้า ระบบจะไม่สามารถดำเนินธุรกิจขององค์กรต่อไปได้

จากความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของระบบสั่งซื้อสินค้าออนไลน์นี้ พบว่าไม่สามารถสร้างแผนภาพคลาสโดยใช้ยูเอ็มแอล และยูเอ็มแอลเซคได้ เนื่องจากยูเอ็มแอลทั้ง 2 ลักษณะไม่สามารถรองรับการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคง แต่ยูเอ็มแอลเซคเอสพีสามารถรองรับการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงได้เพียงบางส่วนเท่านั้น แต่ในขณะที่เดียวกันยูเอ็มแอลเซคเอสพี-2 สามารถรองรับการแสดงข้อมูลดังกล่าวได้ โดยมีการประยุกต์ใช้กลุ่มแบบรูปการจัดการความมั่นคง องค์กรและการจัดการความเสี่ยง ได้แก่ แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร แบบรูปการกำหนดมูลค่าสินทรัพย์ แบบรูปการประเมินภัยคุกคาม แบบรูปการประเมินจุดอ่อน แบบรูปการกำหนดค่าความเสี่ยง และแบบรูปการสื่อสารของผู้กับหุ้นส่วนองค์กร และกลุ่มแบบรูปการระบุตัวตนและการพิสูจน์ตัวตน ได้แก่ แบบรูปความต้องการการระบุและการพิสูจน์ตัวตน แบบรูปทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตน อัตโนมัติ และแบบรูปการออกแบบและใช้รหัสผ่าน โดยแสดงแผนภาพคลาสของระบบเพื่อแสดงข้อมูลดังกล่าว โดยใช้ยูเอ็มแอลเซคเอสพี-2 ดังรูปที่ ง.2 และแสดงแม่พิมพ์ต้นแบบที่กำกับคลาสเพื่อระบุถึงหน้าที่ของคลาสทางด้านความมั่นคง ดังตารางที่ ง.2

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย





ตารางที่ ง.2 แม่พิมพ์ต้นแบบที่กำกับคลาสเพื่อระบุถึงหน้าที่ของคลาสทางด้านความมั่นคงของระบบสั่งซื้อสินค้าออนไลน์

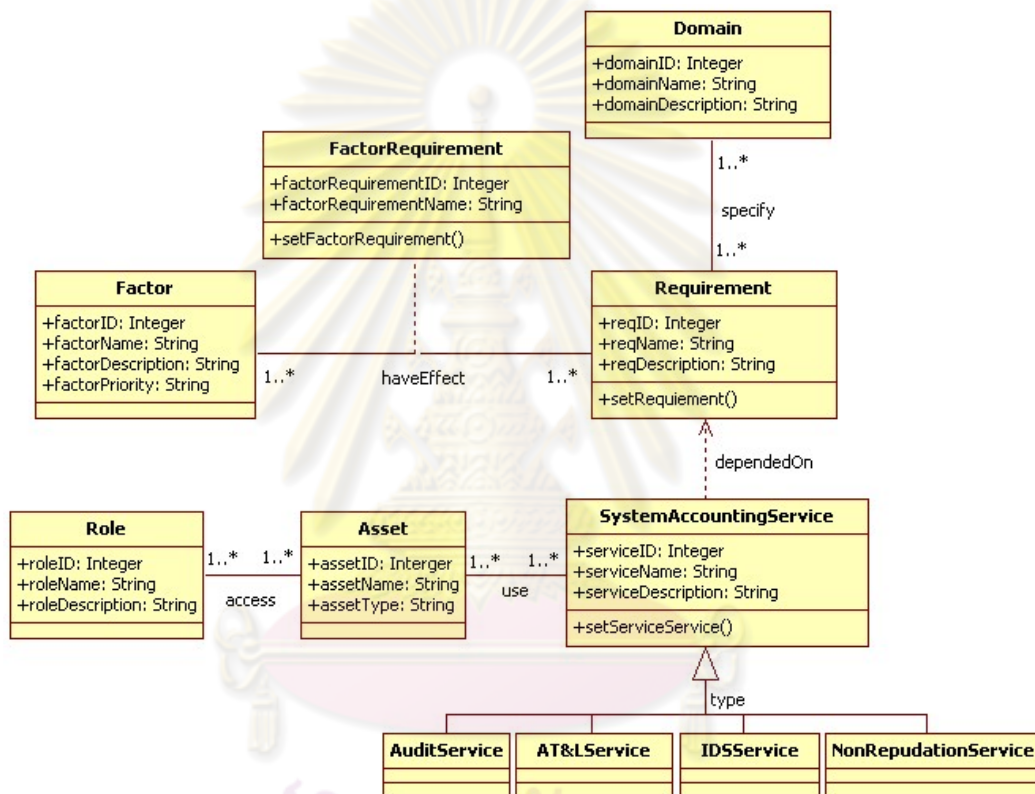
คลาส	หน้าที่ของคลาส	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้
Product	สินค้าขององค์กร	asset
BusinessDriver	ตัวขับเคลื่อนทางด้านธุรกิจขององค์กร	businessDriver
SecurityProperty	คุณสมบัติทางด้านความมั่นคง	securityProperty
AssetProperty	ความสัมพันธ์ระหว่างสินทรัพย์กับคุณสมบัติความมั่นคง	SPC
AssetValue	มูลค่าของสินทรัพย์ขององค์กร	assetValue
Damage	ภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร	threat
Consequence	ผลที่จะตามมาเมื่อเกิดภัยคุกคามขึ้น	threatConsequence
Source	ต้นเหตุที่ทำให้เกิดภัยคุกคาม	threatSource
Likelihood	ความน่าจะเป็นที่จะเหตุการณ์ที่เสี่ยงอันตราย	threatLikelihood
Risk	ความเสี่ยงของแต่ละสินทรัพย์	risk
RiskScale	รายละเอียดของความเสี่ยง	riskScale
Vulnerability	จุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง	vulnerability
SeverityLevel	ระดับความรุนแรงที่อาจเกิดขึ้น	SeverityScale
Vendor	ผู้ใช้งานจากภายนอกระบบ	* client
User	บทบาทของผู้เข้าใช้ทรัพยากรของระบบ	* role
AuthenticateService	บริการที่ตอบสนองความต้องการบริการการระบุและพิสูจน์ตัวตน	I&AService
AuthenticateRequirement	ความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน	I&ARequirement
AuthenticateTechnique	เทคนิคในการระบุและพิสูจน์ตัวตน	I&ATechnique
TechniqueProfile	ความสัมพันธ์ระหว่างความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตนกับเทคนิคในการระบุและพิสูจน์ตัวตน	SPC
AuthenticateDomain	ขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน	I&ADomain
DomainFactor	ปัจจัยที่มีผลกระทบต่อความต้องการ	domainFactor
DomainFactorReq	ความสัมพันธ์ระหว่างปัจจัยที่มีผลกระทบต่อความต้องการกับความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน	SPC
Password	ที่เก็บข้อมูลของรหัสผ่านต่างๆ	password
PasswordPolicy	นโยบายทางด้านรหัสผ่าน	passwordPolicy

\* คือการนำยูเอ็มแอลเซตเอสพีมาประยุกต์ใช้

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

**กรณีศึกษาที่ 2: ระบบบริการการบันทึกเหตุการณ์ (Accounting Service System)**

ระบบบริการการบันทึกเหตุการณ์ เป็นระบบที่ให้บริการสำหรับบันทึกเหตุการณ์ทางด้านความมั่นคงของระบบ ได้แก่ บริการการตรวจสอบเหตุการณ์ทางด้านความมั่นคง บริการการตรวจสอบหลักฐานและการบันทึก บริการการป้องกันการบุกรุก และบริการการไม่ถูกปฏิเสธ ที่อยู่ภายใต้ขอบเขตของบริการ ความต้องการในการบันทึกเหตุการณ์ ปัจจัยที่เกี่ยวข้อง และบทบาทของผู้มีส่วนเกี่ยวข้อง ซึ่งจะช่วยป้องกันความเสียหาย หรือการบุกรุกที่จะเกิดกับสินทรัพย์องค์กร โดยแสดงแผนภาพคลาสของระบบบริการการบันทึกเหตุการณ์ที่ไม่มีการระบุข้อมูลทางความมั่นคง ดังรูปที่ ง.3



รูปที่ ง.3 แผนภาพคลาสของระบบบริการการบันทึกเหตุการณ์ที่ไม่มีการระบุข้อมูลทางความมั่นคง

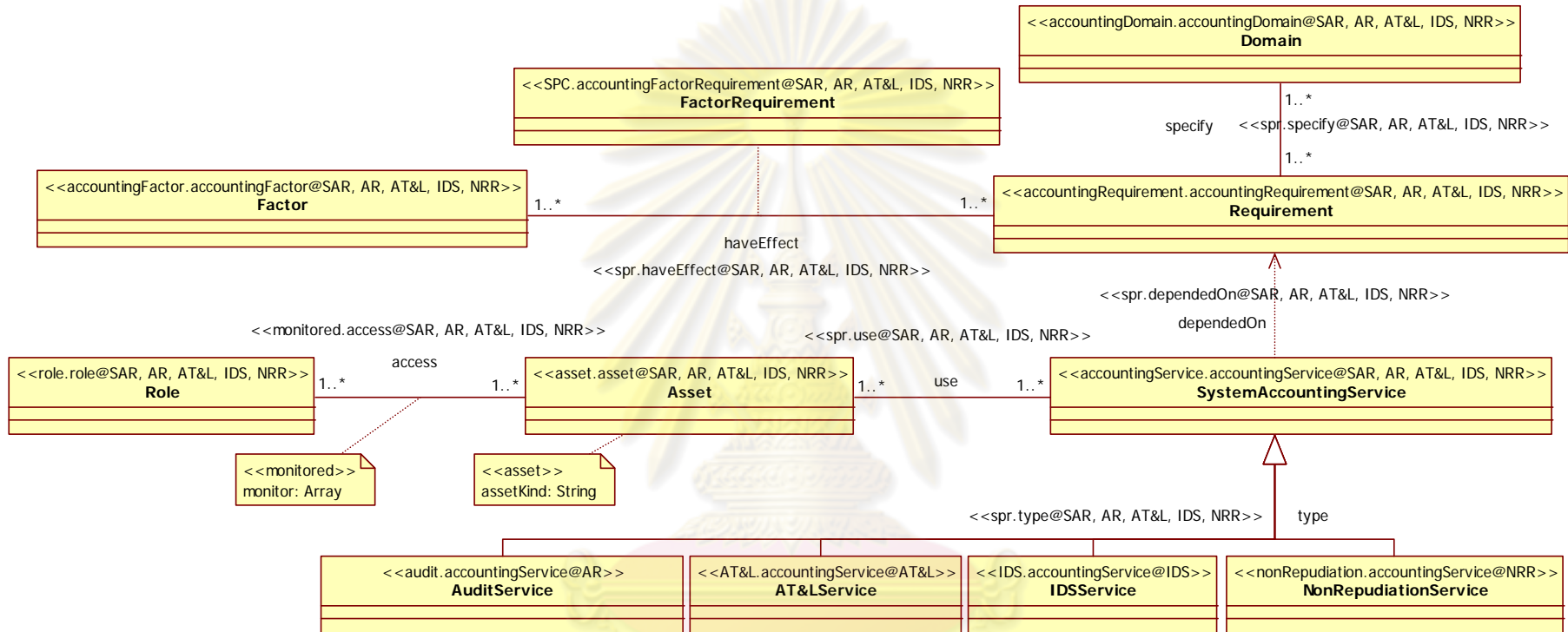
จากการศึกษาและวิเคราะห์โครงสร้างของระบบพบว่า ระบบบริการการบันทึกเหตุการณ์นี้ มีความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคง ดังตารางที่ ง.3

ตารางที่ ง.3 รายละเอียดความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของระบบบริการสำหรับการบันทึกเหตุการณ์

ข้อมูลทางโครงสร้างของแบบรูป	ข้อมูลทางความมั่นคงของแบบรูป
1) ข้อมูลที่ระบุองค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป 2) ข้อมูลที่ระบุแบบรูปที่ใช้งาน 3) ข้อมูลที่ระบุลำดับของแบบรูป 4) ข้อมูลที่ระบุบทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป	1) บริการการบันทึกเหตุการณ์ทางด้านความมั่นคง (SystemAccountingService) 2) ความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง (Requirement) 3) ปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง (Factor) 4) ความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง (FactorRequirement) 5) ขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง (Domain) 6) สินทรัพย์ทางด้านธุรกิจขององค์กร (Asset) 7) บทบาทของผู้มีส่วนเกี่ยวข้อง (Role) 8) บริการการตรวจสอบเหตุการณ์ทางด้านความมั่นคง (AuditService) 9) บริการการตรวจสอบหลักฐานและการบันทึก (AT&LService) 10) บริการการป้องกันการบุกรุก (IDService) 11) บริการการไม่ถูกปฏิเสธ (NonRepudiationService)

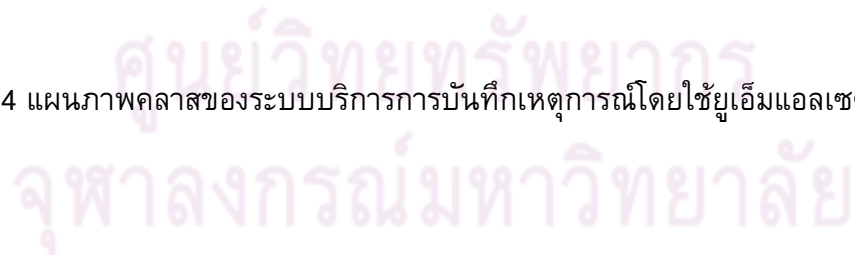
จากความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของระบบบริการสำหรับการบันทึกเหตุการณ์นี้ พบว่าไม่สามารถสร้างแผนภาพคลาสโดยใช้ยูเอ็มแอลและยูเอ็มแอลเซคได้ เนื่องจากยูเอ็มแอลทั้ง 2 ลักษณะไม่สามารถรองรับการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคง แต่ยูเอ็มแอลเซคเอสพีสามารถรองรับการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงได้เพียงบางส่วนเท่านั้น แต่ในขณะเดียวกันยูเอ็มแอลเซคเอสพี-2 สามารถรองรับการแสดงข้อมูลดังกล่าวได้ โดยมีการประยุกต์ใช้กลุ่มแบบรูปการบันทึกเหตุการณ์ ได้แก่ แบบรูปความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง แบบรูปความต้องการการตรวจสอบ แบบรูปความต้องการการตรวจสอบหลักฐานและการบันทึก แบบรูปความต้องการการป้องกันการบุกรุก และแบบรูปความต้องการการไม่ถูกปฏิเสธ โดยแสดงแผนภาพคลาสของระบบเพื่อแสดงข้อมูลดังกล่าว โดยใช้ยูเอ็มแอลเซคเอสพี-2 ดังรูปที่ ง.4 และแสดงแม่พิมพ์ต้นแบบที่กำกับคลาสเพื่อระบุถึงหน้าที่ของคลาสทางด้านความมั่นคง ดังตารางที่ ง.4

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย



SAR : Security Accounting Requirements  
 AR : Audit Requirements  
 AT&L : Audit Trails and Logging Requirements  
 IDS : Intrusion Detection Requirements  
 NRR : Non-Repudiation Requirements

รูปที่ ง.4 แผนภาพคลาสของระบบบริการการบันทึกเหตุการณ์โดยใช้ยูเอ็มแอลเซคเอสพี-2



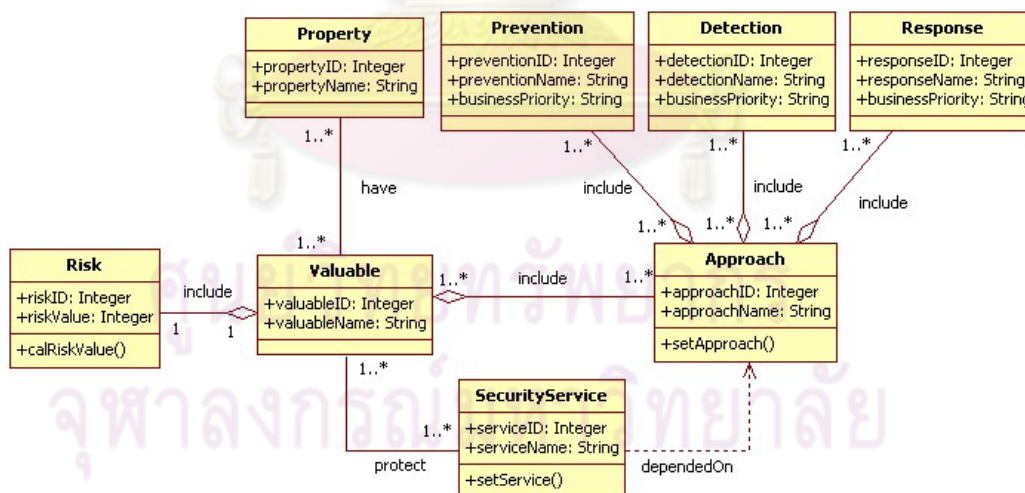
ตารางที่ ง.4 แม่พิมพ์ต้นแบบที่กำกับคลาสเพื่อระบุถึงหน้าที่ของคลาสทางด้านความมั่นคงของระบบบริการการบันทึกเหตุการณ์

คลาส	หน้าที่ของคลาส	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้
SystemAccountingService	บริการการบันทึกเหตุการณ์ทางด้านความมั่นคง	accountingService
Requirement	ความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง	accountingRequirement
Factor	ปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง	accountingFactor
FactorRequirement	ความสัมพันธ์ระหว่างความต้องการและปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง	spc
Domain	ขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง	accountingDomain
Asset	สินทรัพย์ทางด้านธุรกิจขององค์กร	asset
Role	บทบาทของผู้ใช้ทรัพยากรของระบบ	* role
AuditService	บริการการตรวจสอบเหตุการณ์ทางด้านความมั่นคง	audit
AT&LService	บริการการตรวจสอบหลักฐานและการบันทึก	AT&L
IDSService	บริการการป้องกันการบุกรุก	IDS
NonRepudiationService	บริการการไม่ถูกปฏิเสธ	nonRepudiation

\* คือการนำยูเอ็มแอลเซตเอสพีมาประยุกต์ใช้

### กรณีศึกษาที่ 3: ระบบบริการความมั่นคงสำหรับองค์กร (Business Security Services System)

ระบบบริการความมั่นคงสำหรับองค์กร คือระบบที่แนะนำองค์กรในการเลือกบริการความมั่นคง เช่น บริการการระบุและยืนยันตัวตน หรือบริการการควบคุมการเข้าถึง เป็นต้น เพื่อนำไปใช้ในการป้องกันสินทรัพย์ขององค์กรจากความเสี่ยงที่อาจเกิดขึ้น ทั้งนี้บริการความมั่นคงจะต้องมีความสอดคล้องกับแนวคิดทางด้านความมั่นคงขององค์กร โดยแสดงแผนภาพคลาสของระบบบริการความมั่นคงสำหรับองค์กรที่ไม่มีการระบุข้อมูลทางความมั่นคง ดังรูป ง.5



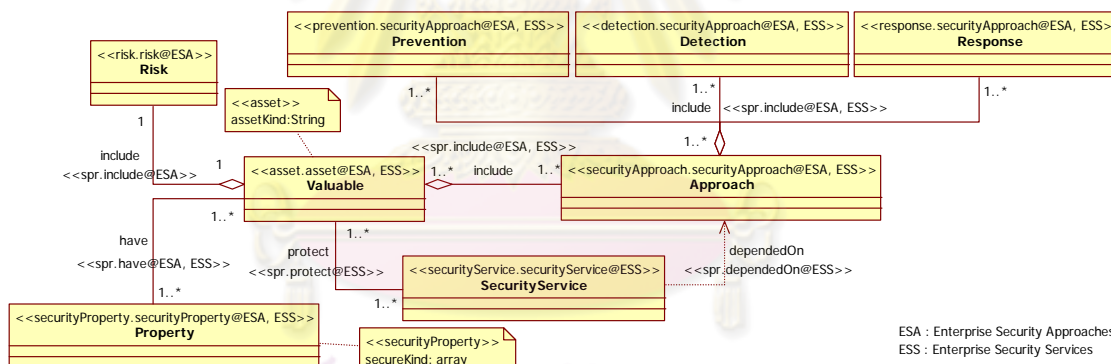
รูปที่ ง.5 แผนภาพคลาสของระบบบริการความมั่นคงสำหรับองค์กรที่ไม่มีการระบุข้อมูลทางความมั่นคง

จากการศึกษาและวิเคราะห์โครงสร้างของระบบพบว่า ระบบบริการความมั่นคงสำหรับองค์กรนี้ มีความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคง ดังตารางที่ ง.5

ตารางที่ ง.5 รายละเอียดความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของระบบบริการความมั่นคงสำหรับองค์กร

ข้อมูลทางโครงสร้างของแบบรูป	ข้อมูลทางความมั่นคงของแบบรูป
1) ข้อมูลที่ระบุองค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป	1) สินทรัพย์ทางด้านธุรกิจขององค์กร (Valuable)
2) ข้อมูลที่ระบุแบบรูปที่ใช้งาน	2) ความเสี่ยงของสินทรัพย์ (Risk)
3) ข้อมูลที่ระบุลำดับของแบบรูป	3) คุณสมบัติความมั่นคง (Property)
4) ข้อมูลที่ระบุบทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป	4) แนวคิดความมั่นคง (Approach)
	5) แนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย (Prevention)
	6) แนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย (Detection)
	7) แนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย (Response)
	8) บริการความมั่นคงสำหรับสินทรัพย์ในองค์กร (SecurityService)

จากความต้องการในการแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของระบบบริการความมั่นคงสำหรับองค์กรนี้ พบว่าไม่สามารถสร้างแผนภาพคลาสโดยใช้ยูเอ็มแอล ยูเอ็มแอลเซค และยูเอ็มแอลเซคเอสพีได้ เนื่องจากยูเอ็มแอลทั้ง 3 ลักษณะไม่สามารถรองรับการแสดงผลข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคง แต่ในขณะเดียวกันยูเอ็มแอลเซคเอสพี-2 สามารถรองรับการแสดงผลข้อมูลดังกล่าวได้ โดยมีการประยุกต์ใช้กลุ่มแบบรูปแนวคิดความมั่นคงองค์กร และแบบรูปบริการความมั่นคงองค์กรโดยแสดงแผนภาพคลาสของระบบ เพื่อแสดงผลข้อมูลดังกล่าวโดยใช้ยูเอ็มแอลเซคเอสพี-2 ดังรูปที่ ง.6 และแสดงแม่พิมพ์ต้นแบบที่กำกับคลาสเพื่อระบุถึงหน้าที่ของคลาสทางด้านความมั่นคง ดังตารางที่ ง.6



รูปที่ ง.6 แผนภาพคลาสของระบบบริการความมั่นคงสำหรับองค์กร โดยใช้ยูเอ็มแอลเซคเอสพี-2

ตารางที่ ง.6 แม่พิมพ์ต้นแบบที่กำกับคลาสเพื่อระบุถึงหน้าที่ของคลาสทางด้านความมั่นคงของระบบบริการความมั่นคงสำหรับองค์กร

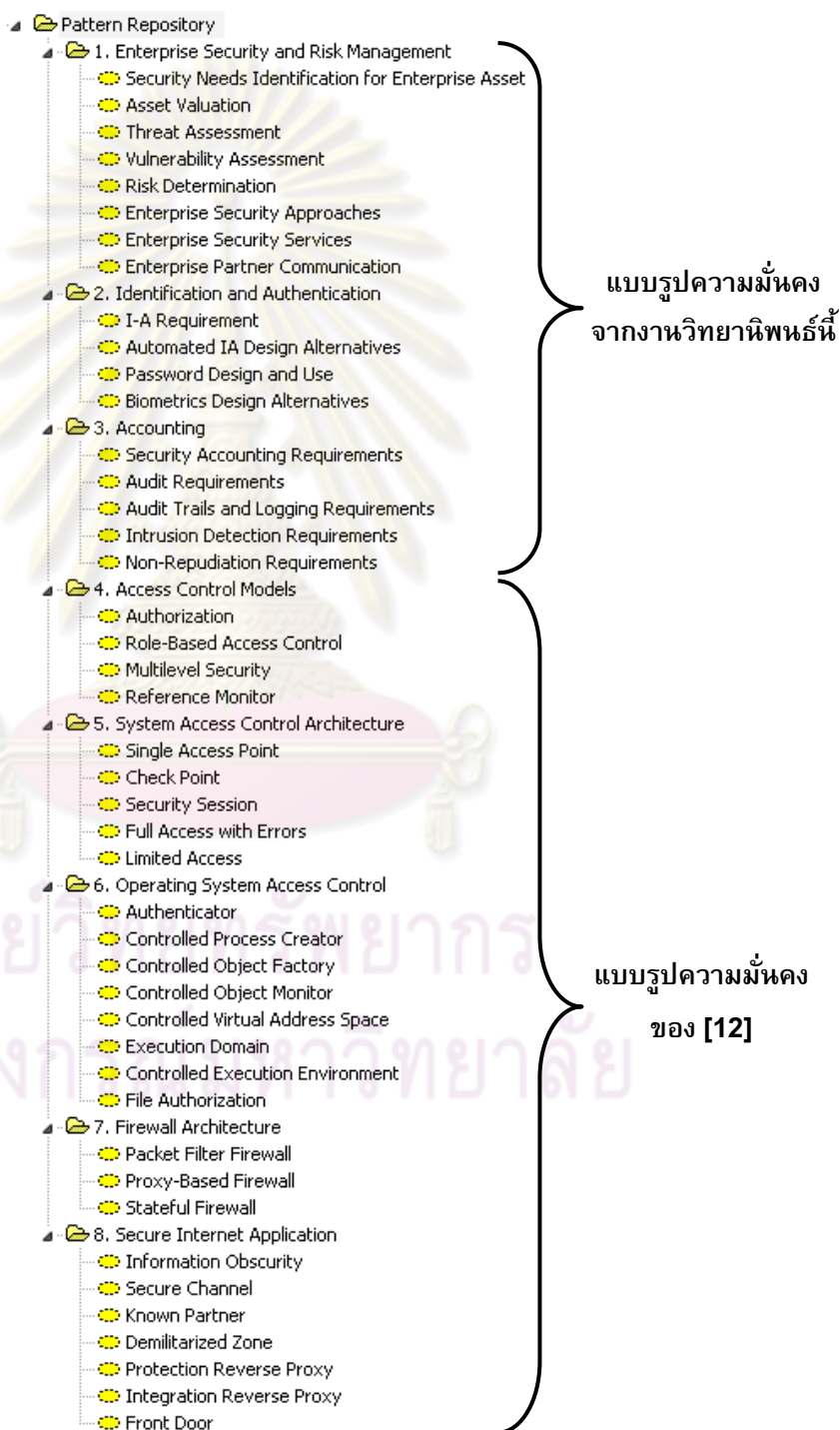
คลาส	หน้าที่ของคลาส	แม่พิมพ์ต้นแบบที่ประยุกต์ใช้
Valuable	สินทรัพย์ทางด้านธุรกิจขององค์กร	asset
Risk	ความเสี่ยงของสินทรัพย์	risk
Property	คุณสมบัติความมั่นคง	securityProperty
Approach	แนวคิดความมั่นคง	securityApproach
Prevention	แนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย	prevention
Detection	แนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย	detection
Response	แนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย	response
SecurityService	บริการความมั่นคงสำหรับสินทรัพย์ในองค์กร	securityService

## ภาคผนวก จ

### ตัวอย่างการใช้งานเครื่องมือต้นแบบและผลลัพธ์ที่ได้จากเครื่องมือ

#### จ.1 ขอบเขตของแบบรูปความมั่นคงในเครื่องมือต้นแบบ

ขอบเขตของแบบรูปความมั่นคงในเครื่องมือต้นแบบนี้ จะเป็นไปตามขอบเขตงานวิจัยรวมทั้งหมด 8 กลุ่มแบบรูปความมั่นคง ซึ่งประกอบไปด้วย 44 แบบรูปความมั่นคง ดังรูปที่ จ.1

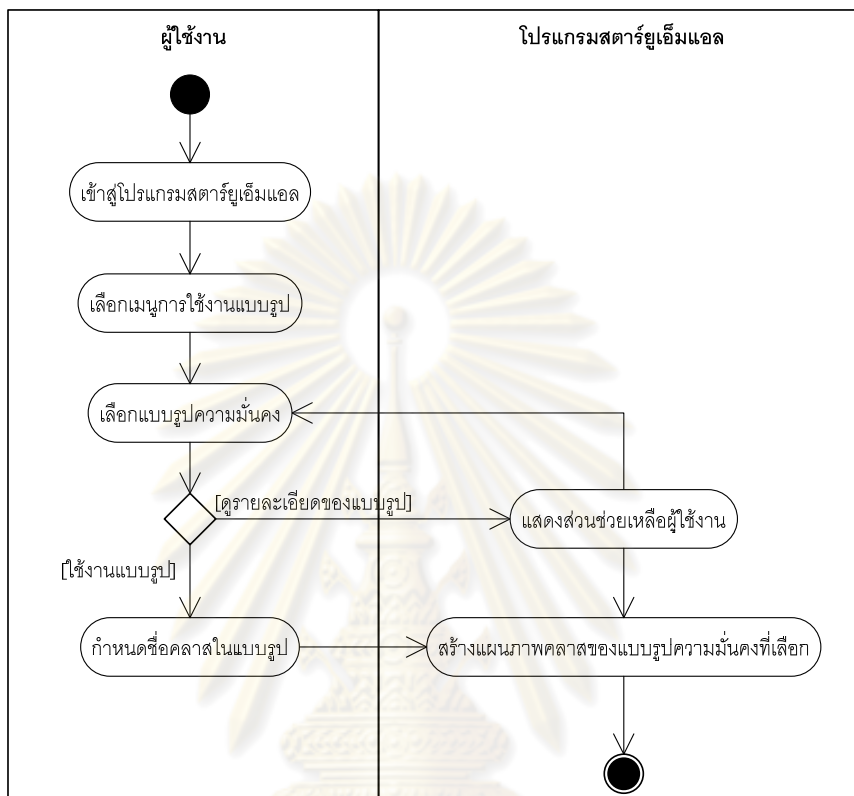


รูปที่ จ.1 แบบรูปความมั่นคงในเครื่องมือต้นแบบ



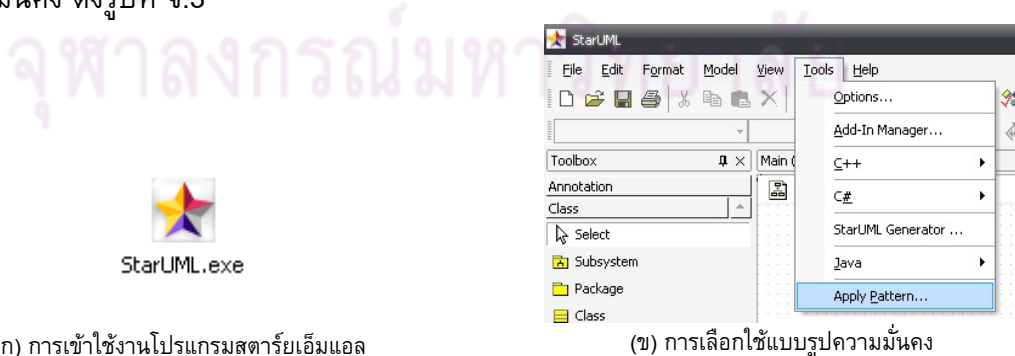
### จ.2 ตัวอย่างการใช้งานแบบรูปความมั่นคงและผลลัพธ์ที่ได้จากเครื่องมือ

การทำงานของเครื่องมือต้นแบบสำหรับแสดงแบบรูปความมั่นคงของเครื่องมือต้นแบบประกอบไปด้วย การทำงานในส่วนที่กำหนดแบบรูปความมั่นคงที่ใช้ และการทำงานในส่วนที่ช่วยเหลือผู้ใช้งาน โดยแสดงรายละเอียดดังรูปที่ จ.2



รูปที่ จ.2 แผนภาพกิจกรรมแสดงการทำงานของ เครื่องมือต้นแบบสำหรับแสดงแบบรูปความมั่นคง

เพื่อแสดงให้เห็นขั้นตอนการใช้งานของเครื่องมือ โดยจะขอยกตัวอย่างการใช้งานแบบรูปการระบุความต้องการความมั่นคงสำหรับสัทธิพ์องค์กรในการสร้างแผนภาพคลาสของแบบรูป โดยแสดงขั้นตอนการเข้าใช้งานโปรแกรมสตาร์ยูเอ็มแอล และการเลือกใช้แบบรูปความมั่นคง ดังรูปที่ จ.3

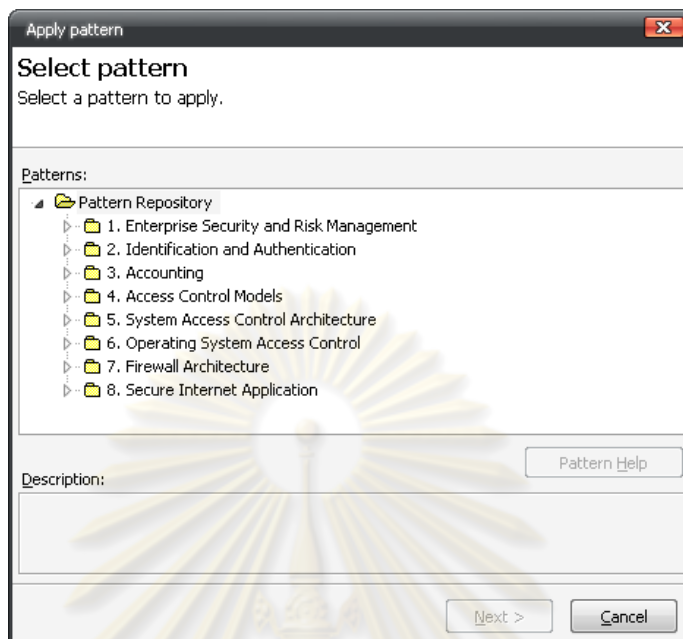


(ก) การเข้าใช้งานโปรแกรมสตาร์ยูเอ็มแอล

(ข) การเลือกใช้แบบรูปความมั่นคง

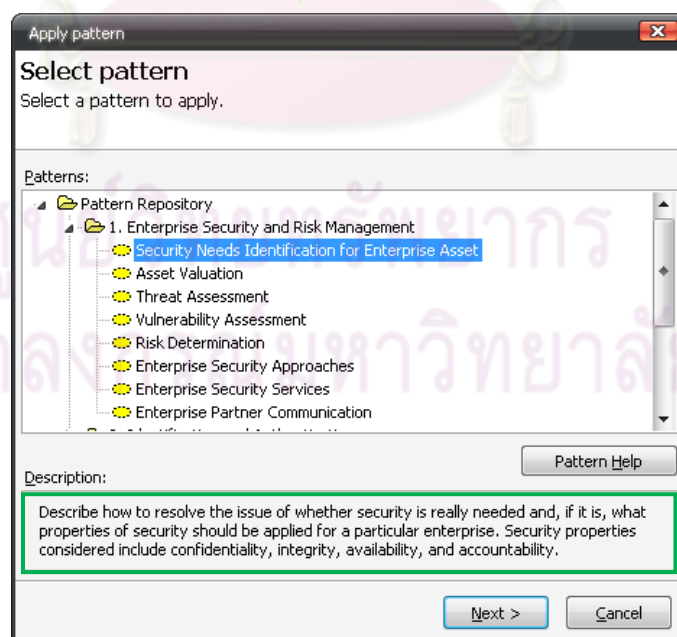
รูปที่ จ.3 ขั้นตอนการเข้าใช้แบบรูปความมั่นคงในโปรแกรมสตาร์ยูเอ็มแอล

หลังจากเข้าสู่การเลือกใช้แบบรูปความมั่นคงของโปรแกรมแล้ว จะปรากฏหน้าต่างสำหรับเลือกแบบรูปความมั่นคงที่ต้องการใช้งาน ดังรูปที่ จ.4



รูปที่ จ.4 หน้าต่างสำหรับเลือกแบบรูปความมั่นคง

ในที่นี้ขอสมมติว่า ผู้ใช้งานทำการเลือกแบบรูป “Security Needs Identification for Enterprise Asset” ที่อยู่ในกลุ่ม “Enterprise Security and Risk Management” จากนั้นเครื่องมือจะแสดงคำอธิบายแบบรูป ดังรูป จ.5 อีกทั้งผู้ใช้งานยังสามารถดูรายละเอียดของแบบรูปความมั่นคงที่เลือกได้ โดยคลิกปุ่ม “Pattern Help” โดยแสดงดังรูป จ.6



รูปที่ จ.5 หน้าจอหลักแสดงคำอธิบายแบบรูปความมั่นคงที่เลือก

### Security Needs Identification for Enterprise Asset

- [Purpose](#)
- [Structure](#)
- [Known Uses](#)
- [Consequences](#)

**Purpose**

- Describe how to resolve the issue of whether security is really needed and, if it is, what properties of security should be applied for a particular enterprise. Security properties considered include confidentiality, integrity, availability, and accountability.

**Structure**

รูปที่ จ.6 หน้าต่างแสดงรายละเอียดของแบบรูปความมั่นคงที่เลือก

โดยรายละเอียดของแบบรูปความมั่นคงที่แสดงนั้น มีดังนี้

- 1) จุดประสงค์ของแบบรูป (Purpose) เป็นจุดประสงค์ของการใช้แบบรูปที่เลือก
  - 2) โครงสร้างของแบบรูป (Structure) เป็นโครงสร้างของการออกแบบที่ใช้ในการแก้ไขปัญหาของแบบรูป รวมทั้งรายละเอียดของแต่ละองค์ประกอบในโครงสร้าง
  - 3) ตัวอย่างการประยุกต์ใช้งาน (Known Uses) คือตัวอย่างในการประยุกต์ใช้แบบรูป
  - 4) ประโยชน์ที่จะได้รับ (Consequence) เป็นประโยชน์ที่ได้รับเมื่อประยุกต์ใช้แบบรูป
- หลังจากผู้ใช้งานเลือกแบบรูปความมั่นคงที่ต้องการได้แล้ว จะปรากฏหน้าต่างสำหรับการสร้างหรือเลือกคลาสที่เป็นองค์ประกอบของแบบรูปความมั่นคง ดังรูปที่ จ.7

Apply pattern ✕

**Pattern parameter**  
Select pattern parameter.

Parameters:

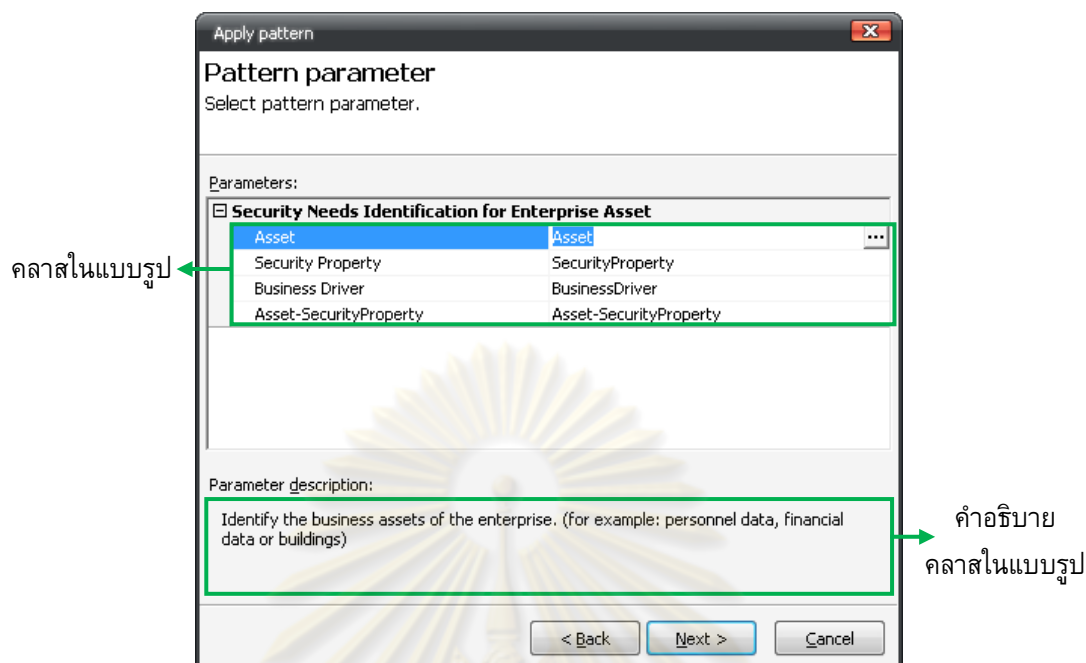
Security Needs Identification for Enterprise Asset	
Asset	Asset
Security Property	SecurityProperty
Business Driver	BusinessDriver
Asset-SecurityProperty	Asset-SecurityProperty

Parameter description:

< Back
Next >
Cancel

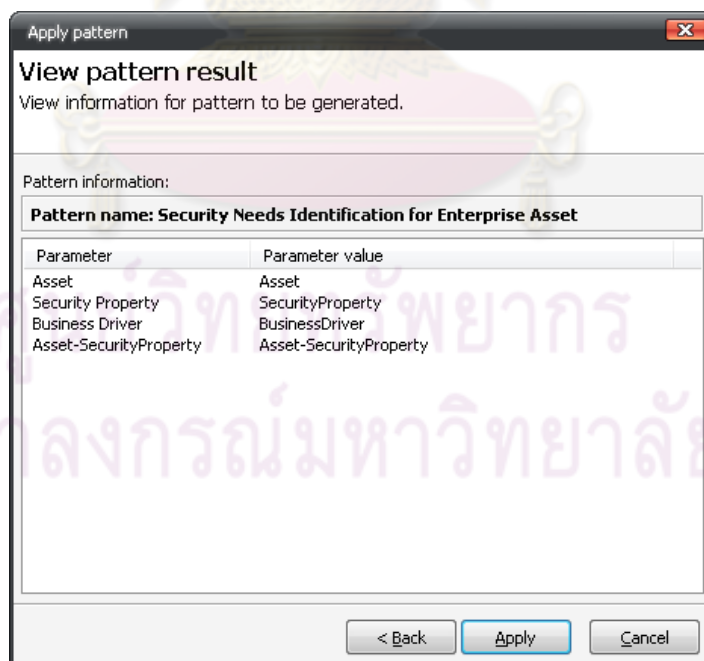
รูปที่ จ.7 หน้าต่างสำหรับการสร้างหรือเลือกคลาสที่เป็นองค์ประกอบของแบบรูปความมั่นคง

เมื่อผู้ใช้งานเลือกคลาสในแบบรูปแล้ว จะปรากฏคำอธิบายของคลาสที่เลือก ดังรูปที่ จ.8

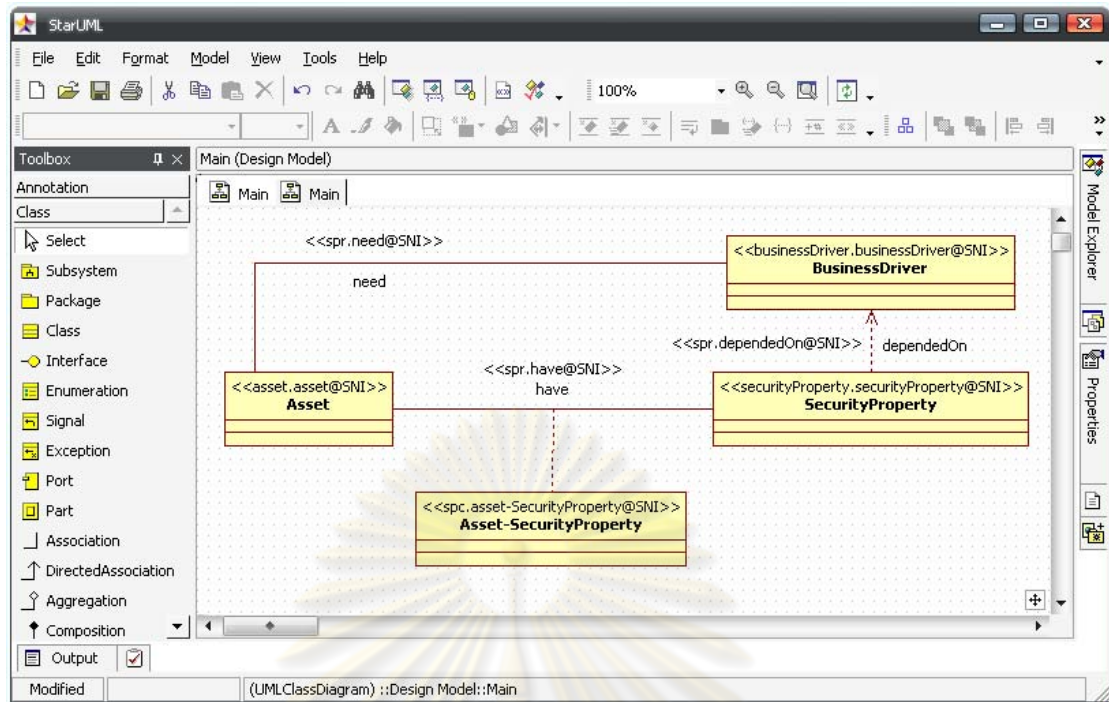


รูปที่ จ.8 หน้าต่างแสดงคำอธิบายของคลาสที่เลือก

หลังจากผู้ใช้งานจัดการคลาสที่อยู่ในแบบรูปแล้ว ผู้ใช้จะต้องทำการยืนยันการใช้แบบรูป ความมั่นคง ดังรูปที่ จ.9 โดยผลลัพธ์จากการใช้แบบรูปการระบุความต้องการความมั่นคง สำหรับสินทรัพย์องค์กรโดยใช้เครื่องมือต้นแบบแสดงดังรูปที่ จ.10



รูปที่ จ.9 หน้าต่างแสดงการยืนยันการใช้แบบรูปความมั่นคง



รูปที่ จ.10 ผลลัพธ์จากการใช้แบบรูปการระบุความต้องการความมั่นคง  
สำหรับสินทรัพย์องค์กรโดยใช้เครื่องมือต้นแบบ

ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

## ภาคผนวก จ

### การเปรียบเทียบการแสดงผลแบบรูปความมั่นคงของยูเอ็มแอล ยูเอ็มแอลเซค ยูเอ็มแอลเซคเอสพีและยูเอ็มแอลเซคเอสพี-2

ในภาคผนวกนี้จะทำการเปรียบเทียบการแสดงผลข้อมูลทางโครงสร้าง และการแสดงผลข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคงการแสดงผลแบบรูปความมั่นคงโดยใช้ยูเอ็มแอล ยูเอ็มแอลเซค ยูเอ็มแอลเซคเอสพี และยูเอ็มแอลเซคเอสพี-2 ที่ได้จากงานวิทยานิพนธ์นี้ โดยการเปรียบเทียบการแสดงผลข้อมูลทางโครงสร้าง และการแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคงมีรายละเอียด ดังตารางที่ จ.1 และ ตารางที่ จ.2 ตามลำดับ ดังนี้

ตารางที่ จ.1 การเปรียบเทียบการแสดงผลข้อมูลทางโครงสร้างของแบบรูปความมั่นคง

ยูเอ็มแอล	ไม่สามารถแสดงผลข้อมูลทางโครงสร้างของแบบรูปความมั่นคง ดังนี้ 1. องค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป 2. แบบรูปที่ใช้งาน 3. ลำดับของแบบรูปในแผนภาพ 4. บทบาทของแต่ละองค์ประกอบแบบจำลองในแบบรูป
ยูเอ็มแอลเซค	ไม่สามารถแสดงผลข้อมูลทางโครงสร้างของแบบรูปความมั่นคงได้เช่นเดียวกับการแสดงผลข้อมูลทางโครงสร้างของยูเอ็มแอล
ยูเอ็มแอลเซคเอสพี	สามารถแสดงผลข้อมูลทางโครงสร้างของแบบรูปความมั่นคง ดังนี้ 1. ใช้แม่พิมพ์ต้นแบบ spc spt และ spr ในการแสดงองค์ประกอบแบบจำลองที่เป็นส่วนประกอบของแบบรูป 2. ใช้ป้ายระบุ "role@name[instance]" แสดงบทบาทขององค์ประกอบในแบบรูป แบบรูปที่ใช้งาน และลำดับของแบบรูป
ยูเอ็มแอลเซคเอสพี-2	แสดงผลข้อมูลทางโครงสร้างของแบบรูปความมั่นคงเช่นเดียวกับการแสดงผลข้อมูลทางโครงสร้างของยูเอ็มแอลเซคเอสพี

ตารางที่ จ.2 การเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี	ยูเอ็มแอลเซคเอสพี-2
การระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร (Security Needs Identification for Enterprise Asset)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพ คือ 4. สินทรัพย์ทางด้านธุรกิจขององค์กร 5. คุณสมบัติทางด้านความมั่นคง 6. ตัวขับเคลื่อนทางด้านธุรกิจขององค์กร	ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 4. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสินทรัพย์ทางด้านธุรกิจขององค์กร 5. ใช้แม่พิมพ์ต้นแบบ "securityProperty" แสดงคุณสมบัติทางด้านความมั่นคง 6. ใช้แม่พิมพ์ต้นแบบ "businessDriver" แสดงตัวขับเคลื่อนทางด้านธุรกิจขององค์กร
การกำหนดมูลค่าสินทรัพย์ (Asset Valuation)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพ คือ 1. สินทรัพย์ทางด้านธุรกิจขององค์กร 2. ค่าของสินทรัพย์ 3. ค่าความมั่นคงของสินทรัพย์องค์กร 4. ค่าทางการเงินขององค์กร 5. ค่าผลกระทบทางธุรกิจขององค์กร	ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสินทรัพย์ทางด้านธุรกิจขององค์กร 2. ใช้แม่พิมพ์ต้นแบบ "assetValue" แสดงค่าของสินทรัพย์ 3. ใช้แม่พิมพ์ต้นแบบ "securityValue" แสดงค่าความมั่นคงของสินทรัพย์องค์กร 4. ใช้แม่พิมพ์ต้นแบบ "financialValue" แสดงค่าทางการเงินขององค์กร 5. ใช้แม่พิมพ์ต้นแบบ "businessValue" แสดงค่าผลกระทบทางธุรกิจขององค์กร
การประเมินภัยคุกคาม (Threat Assessment)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพ คือ 1. สินทรัพย์ทางด้านธุรกิจขององค์กร 2. ภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร 3. ต้นเหตุที่ทำให้เกิดภัยคุกคาม 4. ความน่าจะเป็นที่จะเกิดเหตุการณ์เสี่ยงอันตราย 5. ผลของภัยคุกคาม	ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสินทรัพย์ทางด้านธุรกิจขององค์กร 2. ใช้แม่พิมพ์ต้นแบบ "threat" แสดงภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร 3. ใช้แม่พิมพ์ต้นแบบ "threatSource" แสดงต้นเหตุที่ทำให้เกิดภัยคุกคาม 4. ใช้แม่พิมพ์ต้นแบบ "threatLikelihood" แสดงความน่าจะเป็นที่จะเกิดเหตุการณ์ที่เสี่ยงอันตราย 5. ใช้แม่พิมพ์ต้นแบบ "threatConsequence" แสดงผลของภัยคุกคาม
การประเมินจุดอ่อน (Vulnerability Assessment)	ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพ คือ 1. สินทรัพย์ทางด้านธุรกิจขององค์กร 2. ภัยคุกคามที่เกิดขึ้นกับสินทรัพย์ขององค์กร 3. จุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง 4. ระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตี	ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสินทรัพย์ทางด้านธุรกิจขององค์กร 2. ใช้แม่พิมพ์ต้นแบบ "threat" แสดงภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร 3. ใช้แม่พิมพ์ต้นแบบ "vulnerability" แสดงจุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง 4. ใช้แม่พิมพ์ต้นแบบ "severityScale" แสดงระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตี

ตารางที่ จ.2 การเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี	ยูเอ็มแอลเซคเอสพี-2
การกำหนดค่าความเสี่ยง (Risk Determination)	<p>ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพ คือ</p> <ol style="list-style-type: none"> <li>1. สินทรัพย์ทางด้านธุรกิจขององค์กร</li> <li>2. ภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร</li> <li>3. จุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง</li> <li>4. ระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตี</li> <li>5. ต้นเหตุที่ทำให้เกิดภัยคุกคาม</li> <li>6. ความน่าจะเป็นที่จะเกิดเหตุการณ์ที่เสี่ยงอันตราย</li> <li>7. ผลของภัยคุกคาม</li> <li>8. ความเสี่ยงของสินทรัพย์</li> <li>9. ระดับของความเสี่ยง</li> <li>10. ค่าของสินทรัพย์</li> <li>11. ค่าความมั่นคงของสินทรัพย์องค์กร</li> <li>12. ค่าทางการเงินขององค์กร</li> <li>13. ค่าผลกระทบทางธุรกิจขององค์กร</li> </ol>	<p>ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ</p> <ol style="list-style-type: none"> <li>1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสินทรัพย์ทางด้านธุรกิจขององค์กร</li> <li>2. ใช้แม่พิมพ์ต้นแบบ "threat" แสดงภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ขององค์กร</li> <li>3. ใช้แม่พิมพ์ต้นแบบ "vulnerability" แสดงจุดอ่อนขององค์กรที่ทำให้เกิดภาวะเสี่ยง</li> <li>4. ใช้แม่พิมพ์ต้นแบบ "severityScale" แสดงระดับความรุนแรงที่อาจเกิดขึ้นเมื่อถูกภัยคุกคามโจมตี</li> <li>5. ใช้แม่พิมพ์ต้นแบบ "threatSource" แสดงต้นเหตุที่ทำให้เกิดภัยคุกคาม</li> <li>6. ใช้แม่พิมพ์ต้นแบบ "threatLikelihood" แสดงความน่าจะเป็นที่จะเกิดเหตุการณ์ที่เสี่ยงอันตราย</li> <li>7. ใช้แม่พิมพ์ต้นแบบ "threatConsequence" แสดงผลของภัยคุกคาม</li> <li>8. ใช้แม่พิมพ์ต้นแบบ "risk" แสดงความเสี่ยงของสินทรัพย์</li> <li>9. ใช้แม่พิมพ์ต้นแบบ "riskScale" แสดงระดับของความเสี่ยง</li> <li>10. ใช้แม่พิมพ์ต้นแบบ "assetValue" แสดงค่าของสินทรัพย์</li> <li>11. ใช้แม่พิมพ์ต้นแบบ "securityValue" แสดงค่าความมั่นคงของสินทรัพย์องค์กร</li> <li>12. ใช้แม่พิมพ์ต้นแบบ "financialValue" แสดงค่าทางการเงินขององค์กร</li> <li>13. ใช้แม่พิมพ์ต้นแบบ "businessValue" แสดงค่าผลกระทบทางธุรกิจขององค์กร</li> </ol>
แนวคิดความมั่นคงองค์กร (Enterprise Security Approaches)	<p>ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพ คือ</p> <ol style="list-style-type: none"> <li>1. สินทรัพย์ทางด้านธุรกิจขององค์กร</li> <li>2. ความเสี่ยงของสินทรัพย์</li> <li>3. คุณสมบัติความมั่นคง</li> <li>4. แนวคิดความมั่นคง</li> <li>5. แนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย</li> <li>6. แนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย</li> <li>7. แนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย</li> </ol>	<p>ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ</p> <ol style="list-style-type: none"> <li>1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสินทรัพย์ทางด้านธุรกิจขององค์กร</li> <li>2. ใช้แม่พิมพ์ต้นแบบ "risk" แสดงความเสี่ยงของสินทรัพย์</li> <li>3. ใช้แม่พิมพ์ต้นแบบ "securityProperty" แสดงคุณสมบัติความมั่นคง</li> <li>4. ใช้แม่พิมพ์ต้นแบบ "securityApproach" แสดงแนวคิดความมั่นคง</li> <li>5. ใช้แม่พิมพ์ต้นแบบ "prevention" แสดงแนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย</li> <li>6. ใช้แม่พิมพ์ต้นแบบ "detection" แสดงแนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย</li> <li>7. ใช้แม่พิมพ์ต้นแบบ "response" แสดงแนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย</li> </ol>



ตารางที่ จ.2 การเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี	ยูเอ็มแอลเซคเอสพี-2
<p>บริการความมั่นคงองค์กร (Enterprise Security Services)</p>	<p>ไม่ได้แสดงผลข้อมูลทางความมั่นคงในแผนภาพ คือ</p> <ol style="list-style-type: none"> <li>1. สิทธิทางด้านธุรกิจขององค์กร</li> <li>2. คุณสมบัติความมั่นคง</li> <li>3. แนวคิดความมั่นคง</li> <li>4. บริการความมั่นคงสำหรับสิทธิในองค์กร</li> <li>5. แนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย</li> <li>6. แนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย</li> <li>7. แนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย</li> </ol>	<p>ไม่สามารถแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>ไม่สามารถแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ</p> <ol style="list-style-type: none"> <li>1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสิทธิทางด้านธุรกิจขององค์กร</li> <li>2. ใช้แม่พิมพ์ต้นแบบ "securityProperty" แสดงคุณสมบัติความมั่นคง</li> <li>3. ใช้แม่พิมพ์ต้นแบบ "securityApproach" แสดงแนวคิดความมั่นคง</li> <li>4. ใช้แม่พิมพ์ต้นแบบ "securityService" แสดงบริการความมั่นคงสำหรับสิทธิในองค์กร</li> <li>5. ใช้แม่พิมพ์ต้นแบบ "prevention" แสดงแนวคิดความมั่นคงสำหรับการป้องกันเหตุการณ์ที่เสี่ยงอันตราย</li> <li>6. ใช้แม่พิมพ์ต้นแบบ "detection" แสดงแนวคิดความมั่นคงสำหรับการค้นหาเหตุการณ์ที่เสี่ยงอันตราย</li> <li>7. ใช้แม่พิมพ์ต้นแบบ "response" แสดงแนวคิดความมั่นคงสำหรับการตอบสนองเหตุการณ์ที่เสี่ยงอันตราย</li> </ol>
<p>การสื่อสารของผู้กับหุ้นส่วน องค์กร (Enterprise Partner Communication)</p>	<p>ไม่ได้แสดงผลข้อมูลทางความมั่นคงในแผนภาพ คือ</p> <ol style="list-style-type: none"> <li>1. สิทธิทางด้านธุรกิจขององค์กร</li> <li>2. คุณสมบัติความมั่นคง</li> <li>3. บทบาทของผู้มีส่วนเกี่ยวข้อง</li> <li>4. บริการการระบุและพิสูจน์ตัวตนในการเข้าถึงสิทธิขององค์กร</li> <li>5. องค์กรภายนอก</li> <li>6. กิจกรรมการสิ้นสุด</li> <li>7. ช่องทางการติดต่อกับองค์กรภายนอก</li> <li>8. วิธีดำเนินการที่ใช้ในช่องทางการติดต่อ</li> <li>9. การเชื่อมโยงที่มีการตรวจสอบการเข้าถึงระบบระหว่างสิทธิทางด้านธุรกิจขององค์กรกับบทบาทของผู้มีส่วนเกี่ยวข้อง</li> </ol>	<p>ไม่สามารถแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ</p> <ol style="list-style-type: none"> <li>1. ใช้แม่พิมพ์ต้นแบบ "role" แสดงบทบาทของผู้มีส่วนเกี่ยวข้อง</li> <li>2. ใช้แม่พิมพ์ต้นแบบ "client" แสดงองค์กรภายนอก</li> <li>3. ใช้แม่พิมพ์ต้นแบบ "monitored" แสดงการเชื่อมโยงที่มีการตรวจสอบการเข้าถึงระบบระหว่างสิทธิทางด้านธุรกิจขององค์กรกับบทบาทของผู้มีส่วนเกี่ยวข้อง</li> </ol>	<p>แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ</p> <ol style="list-style-type: none"> <li>1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสิทธิทางด้านธุรกิจขององค์กร</li> <li>2. ใช้แม่พิมพ์ต้นแบบ "securityProperty" แสดงคุณสมบัติความมั่นคง</li> <li>3. ใช้แม่พิมพ์ต้นแบบ "I&amp;AService" แสดงบริการการระบุและพิสูจน์ตัวตนในการเข้าถึงสิทธิขององค์กร</li> <li>4. ใช้แม่พิมพ์ต้นแบบ "serviceTermination" แสดงกิจกรรมการสิ้นสุด</li> <li>5. ใช้แม่พิมพ์ต้นแบบ "channel" แสดงช่องทางการติดต่อกับองค์กรภายนอก</li> <li>6. ใช้แม่พิมพ์ต้นแบบ "exchangeMethod" แสดงวิธีดำเนินการที่ใช้ในช่องทางการติดต่อ</li> </ol>

ตารางที่ จ.2 การเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี	ยูเอ็มแอลเซคเอสพี-2
ความต้องการการระบุและการพิสูจน์ตัวตน (I&A Requirement)	<p>ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพ คือ</p> <ol style="list-style-type: none"> <li>1. สิทธิทางด้านธุรกิจขององค์กร</li> <li>2. บริการการระบุและพิสูจน์ตัวตนในการเข้าถึงสิทธิขององค์กร</li> <li>3. ความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน</li> <li>4. ปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการ</li> <li>5. ขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน</li> </ol>	<p>ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้</p> <p>เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้</p> <p>เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ</p> <ol style="list-style-type: none"> <li>1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสิทธิทางด้านธุรกิจขององค์กร</li> <li>2. ใช้แม่พิมพ์ต้นแบบ "I&amp;AService" แสดงบริการการระบุและพิสูจน์ตัวตนในการเข้าถึงสิทธิขององค์กร</li> <li>3. ใช้แม่พิมพ์ต้นแบบ "I&amp;ARequirement" แสดงความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน</li> <li>4. ใช้แม่พิมพ์ต้นแบบ "domainFactor" แสดงปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการ</li> <li>5. ใช้แม่พิมพ์ต้นแบบ "I&amp;ADomain" แสดงขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน</li> </ol>
ทางเลือกการออกแบบสำหรับการระบุและการพิสูจน์ตัวตนอัตโนมัติ (Automated I&A Design Alternatives)	<p>ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพ คือ</p> <ol style="list-style-type: none"> <li>1. สิทธิทางด้านธุรกิจขององค์กร</li> <li>2. บริการการระบุและพิสูจน์ตัวตนในการเข้าถึงสิทธิขององค์กร</li> <li>3. เทคนิคในการระบุและพิสูจน์ตัวตน</li> <li>4. ความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน</li> <li>5. ปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการ</li> <li>6. ขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน</li> </ol>	<p>ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้</p> <p>เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้</p> <p>เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ</p> <ol style="list-style-type: none"> <li>1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสิทธิทางด้านธุรกิจขององค์กร</li> <li>2. ใช้แม่พิมพ์ต้นแบบ "I&amp;AService" แสดงบริการการระบุและพิสูจน์ตัวตนในการเข้าถึงสิทธิขององค์กร</li> <li>3. ใช้แม่พิมพ์ต้นแบบ "I&amp;ATechnique" แสดงเทคนิคในการระบุและพิสูจน์ตัวตน</li> <li>4. ใช้แม่พิมพ์ต้นแบบ "I&amp;ARequirement" แสดงความต้องการในการใช้บริการการระบุและพิสูจน์ตัวตน</li> <li>5. ใช้แม่พิมพ์ต้นแบบ "domainFactor" แสดงปัจจัยที่มีผลกระทบต่อข้อกำหนดความต้องการ</li> <li>6. ใช้แม่พิมพ์ต้นแบบ "I&amp;ADomain" แสดงขอบเขตสำหรับการใช้บริการการระบุและพิสูจน์ตัวตน</li> </ol>
การออกแบบและใช้รหัสผ่าน (Password Design and Use)	<p>ไม่ได้แสดงข้อมูลทางความมั่นคงในแผนภาพ คือ</p> <ol style="list-style-type: none"> <li>1. เทคนิคในการระบุและพิสูจน์ตัวตน</li> <li>2. ที่เก็บข้อมูลของรหัสผ่านต่างๆ</li> <li>3. นโยบายทางด้านรหัสผ่าน</li> </ol>	<p>ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้</p> <p>เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>ไม่สามารถแสดงข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้</p> <p>เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล</p>	<p>แสดงข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ</p> <ol style="list-style-type: none"> <li>1. ใช้แม่พิมพ์ต้นแบบ "I&amp;ATechnique" แสดงเทคนิคในการระบุและพิสูจน์ตัวตน</li> <li>2. ใช้แม่พิมพ์ต้นแบบ "password" แสดงที่เก็บข้อมูลของรหัสผ่านต่างๆ</li> <li>3. ใช้แม่พิมพ์ต้นแบบ "passwordPolicy" แสดงนโยบายทางด้านรหัสผ่าน</li> </ol>

ตารางที่ จ.2 การเปรียบเทียบการแสดงผลข้อมูลทางความมั่นคงในแต่ละแบบรูปความมั่นคง (ต่อ)

แบบรูปความมั่นคง	ยูเอ็มแอล	ยูเอ็มแอลเซค	ยูเอ็มแอลเซคเอสพี	ยูเอ็มแอลเซคเอสพี-2
ทางเลือกการออกแบบชีวมิติ (Biometrics Design Alternatives)	ไม่ได้แสดงผลข้อมูลทางความมั่นคงในแผนภาพ คือ 1. เทคนิคในการระบุและพิสูจน์ตัวตน 2. ปัจจัยในการออกแบบทางชีวมิติ 3. วิธีการทางด้านชีวมิติ 4. คุณลักษณะของชีวมิติ	ไม่สามารถแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	ไม่สามารถแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "I&ATechnique" แสดงเทคนิคในการระบุและพิสูจน์ตัวตน 2. ใช้แม่พิมพ์ต้นแบบ "biometricFactor" แสดงปัจจัยในการออกแบบทางชีวมิติ 3. ใช้แม่พิมพ์ต้นแบบ "biometricMechanism" แสดงวิธีการทางด้านชีวมิติ 4. ใช้แม่พิมพ์ต้นแบบ "biometricCharacteristic" แสดงคุณลักษณะของชีวมิติ
ความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง (Security Accounting Requirements)	ไม่ได้แสดงผลข้อมูลทางความมั่นคงในแผนภาพ คือ 1. สิทธิ์ทางด้านธุรกิจขององค์กร 2. บทบาทของผู้มีส่วนเกี่ยวข้อง 3. ความต้องการสำหรับการบันทึกเหตุการณ์ทางด้านความมั่นคง 4. ขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง 5. ปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง 6. บริการการบันทึกเหตุการณ์ทางด้านความมั่นคง 7. การเชื่อมโยงที่มีการตรวจสอบการเข้าถึงระบบระหว่างสิทธิ์ทางด้านธุรกิจขององค์กรกับบทบาทของผู้มีส่วนเกี่ยวข้อง	ไม่สามารถแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคงได้ เช่นเดียวกับการแสดงผลข้อมูลทางความมั่นคงของยูเอ็มแอล	แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "role" แสดงบทบาทของผู้มีส่วนเกี่ยวข้อง 2. ใช้แม่พิมพ์ต้นแบบ "monitored" แสดงการเชื่อมโยงที่มีการตรวจสอบการเข้าถึงระบบระหว่างสิทธิ์ทางด้านธุรกิจขององค์กรกับบทบาทของผู้มีส่วนเกี่ยวข้อง	แสดงผลข้อมูลทางความมั่นคงที่อยู่ในแผนภาพคือ 1. ใช้แม่พิมพ์ต้นแบบ "asset" แสดงสิทธิ์ทางด้านธุรกิจขององค์กร 2. ใช้แม่พิมพ์ต้นแบบ "accountingRequirement" แสดงความต้องการสำหรับการบันทึกเหตุการณ์ทางด้านความมั่นคง 3. ใช้แม่พิมพ์ต้นแบบ "accountingDomain" แสดงขอบเขตสำหรับบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง 4. ใช้แม่พิมพ์ต้นแบบ "accountingFactor" แสดงปัจจัยที่มีผลต่อความต้องการการบันทึกเหตุการณ์ทางด้านความมั่นคง 5. ใช้แม่พิมพ์ต้นแบบ "accountingService" แสดงบริการการบันทึกเหตุการณ์ทางด้านความมั่นคง





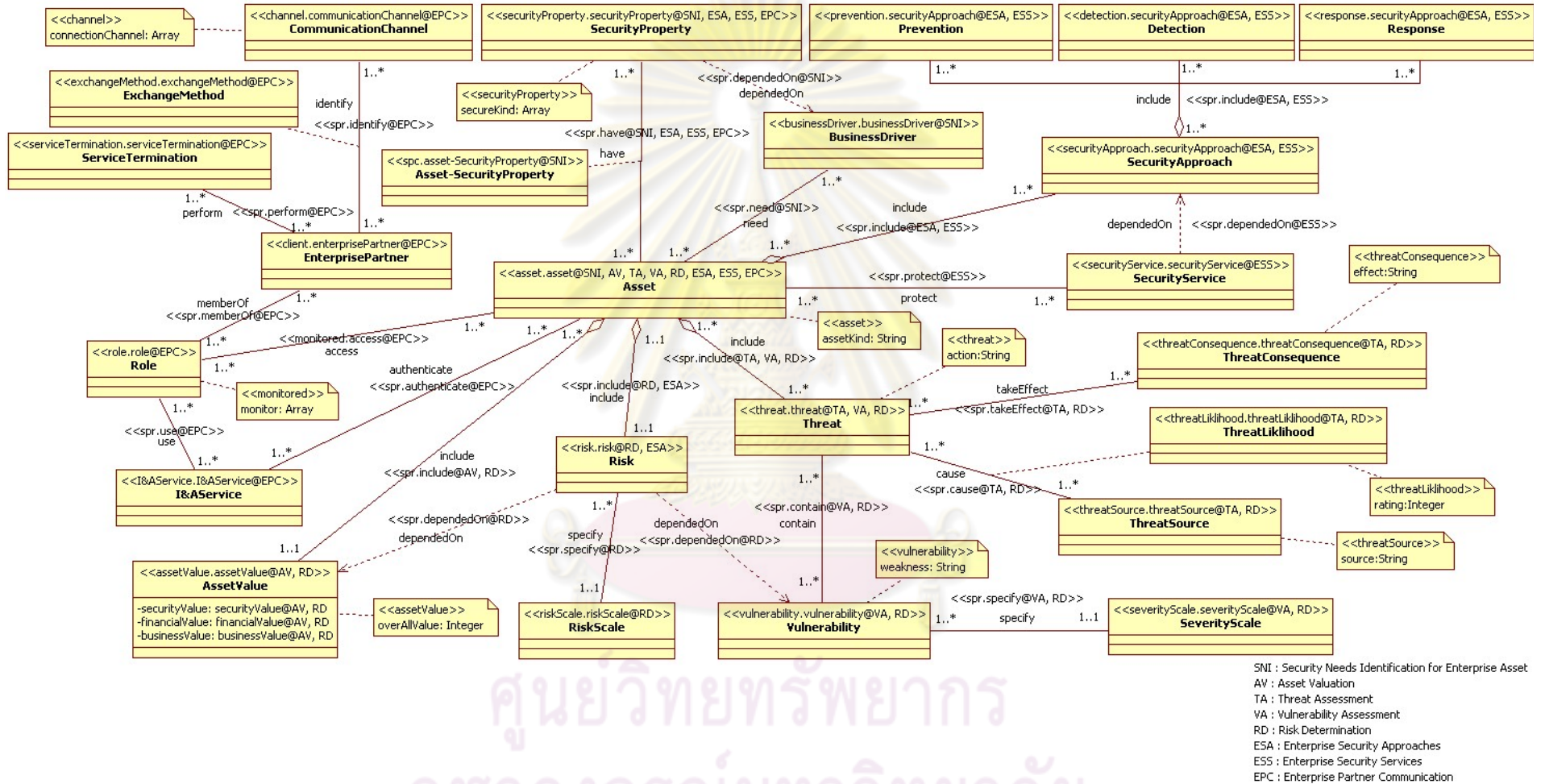
## ภาคผนวก ข

### แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพี-2

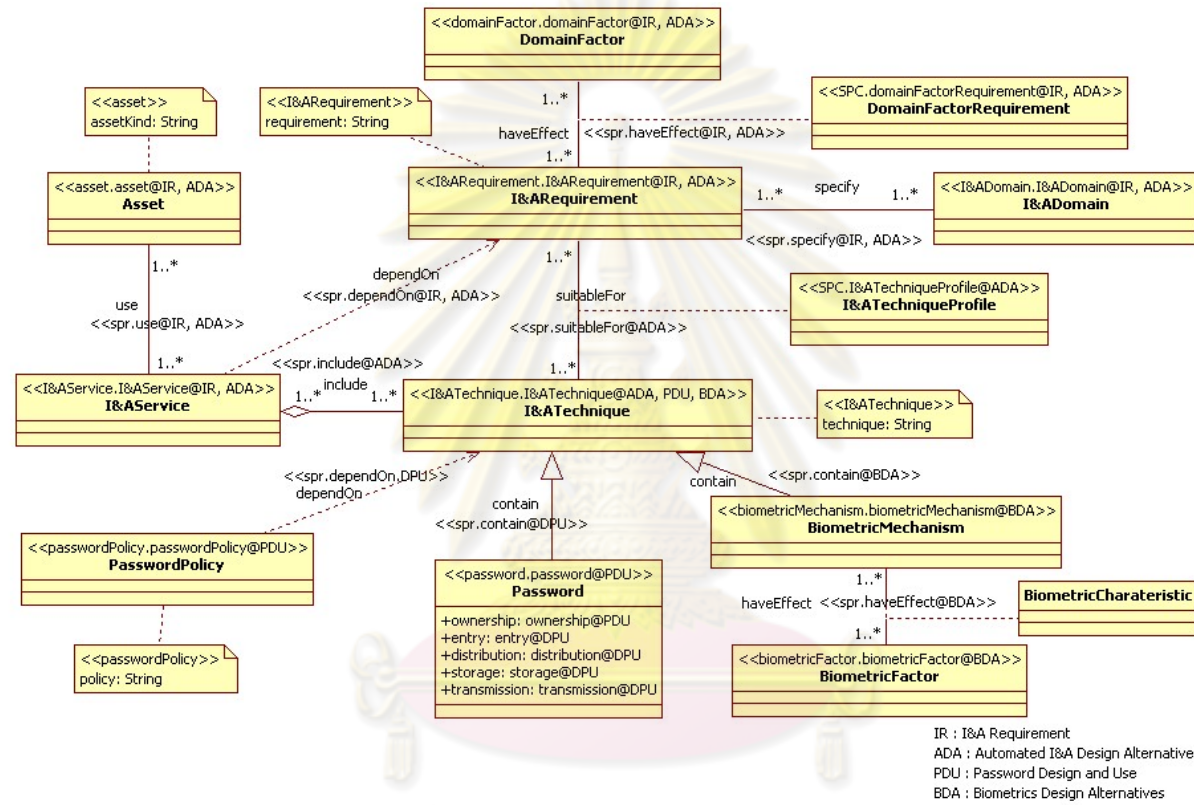
แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพี-2 เป็นแผนภาพคลาสที่เกิดจากการบูรณาการแบบรูปความมั่นคงในแต่ละกลุ่มแบบรูปความมั่นคงในขอบเขตของงานวิทยานิพนธ์นี้ โดยแสดงข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงโดยใช้ยูเอ็มแอลเซคเอสพี-2 ดังนี้



ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย



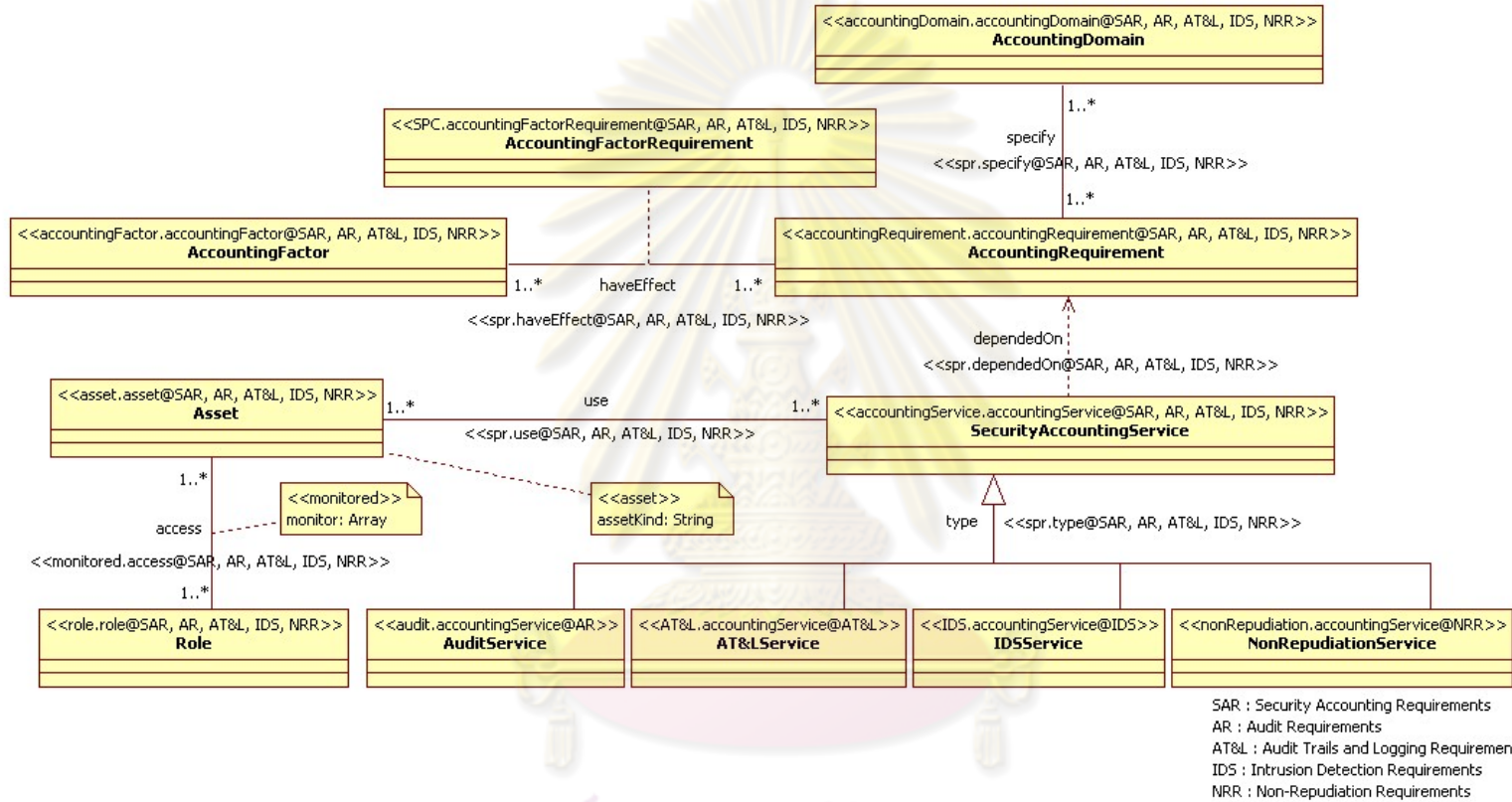
รูปที่ ข.1 แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพี-2 ของกลุ่มแบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง



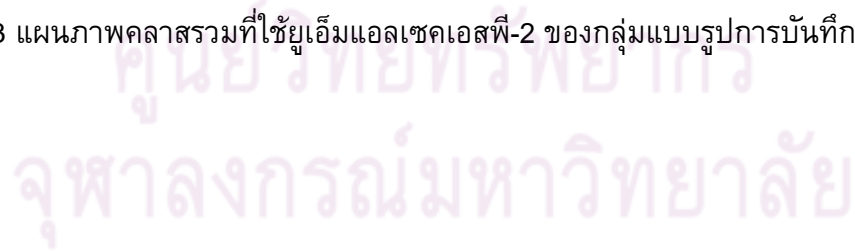
รูปที่ ข.2 แผนภาพคลาสรวมที่ใช้เอ็มแอลเซคเอสพี-2 ของกลุ่มแบบรูปการระบุตัวตนและการพิสูจน์ตัวตน

ศูนย์วิจัยทรัพยากร  
 จุฬาลงกรณ์มหาวิทยาลัย





รูปที่ ช.3 แผนภาพคลาสรวมที่ใช้ยูเอ็มแอลเซคเอสพี-2 ของกลุ่มแบบรูปการบันทึกเหตุการณ์



## ภาคผนวก ซ

### ผลงานตีพิมพ์

ผู้วิจัยได้เขียนบทความเพื่อตีพิมพ์ผลงานในวารสารวิชาการและการประชุมวิชาการในประเทศ คือ บทความวิชาการเรื่อง “การสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงโดยการขยายยูเอ็มแอล (Security Patterns Structural Model Construction by Extending UML)” ซึ่งได้รับการคัดเลือกเพื่อนำเสนอและตีพิมพ์ในงาน “การประชุมวิชาการทางวิทยาการคอมพิวเตอร์และวิศวกรรมคอมพิวเตอร์แห่งชาติ ครั้งที่ 13 (The 13<sup>th</sup> National Computer Science and Engineering Conference: NCSEC 2009)” ระหว่างวันที่ 4 – 6 พฤศจิกายน 2552 ณ โรงแรมมณเฑียรริเวอร์ไซด์ กรุงเทพฯ โดยมีรายละเอียดดังนี้



ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย

# การสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงโดยการขยายยูเอ็มแอล

## Security Patterns Structural Model Construction by Extending UML

ณพล วงศ์ไชยกุล และ นครทิพย์ พร้อมพูล

ห้องปฏิบัติการวิศวกรรมซอฟต์แวร์ ศูนย์เชี่ยวชาญเฉพาะทางด้านวิศวกรรมซอฟต์แวร์

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

อีเมล : Napol.W@student.chula.ac.th และ Nakornthip.S@chula.ac.th

### บทคัดย่อ

ความมั่นคงของระบบซอฟต์แวร์เป็นสิ่งสำคัญที่ทุกองค์กรควรตระหนักถึง ทั้งนี้เนื่องจากมีการปรากฏภัยคุกคามที่มากขึ้นและหลากหลายในปัจจุบัน ดังนั้นหลักการทางด้านความมั่นคงจึงมีความจำเป็นอย่างมากในการป้องกันระบบที่พัฒนาจากการถูกโจมตี ซึ่งจะช่วยให้ระบบดังกล่าวมีประสิทธิภาพในการทำงาน โดยแบบรูปความมั่นคง (Security Pattern) [1,2] ได้ถูกเสนอเพื่อช่วยแก้ไขปัญหาการออกแบบความต้องการความมั่นคงของระบบ ซึ่งจะอธิบายแนวทางของปัญหาทางด้านความมั่นคงต่างๆ และมีการนำไปใช้งานอย่างแพร่หลาย ดังนั้นงานวิจัยนี้จึงนำเสนอแนวคิดในการพัฒนาเครื่องมือสำหรับการสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงโดยการขยายแผนภาพคลาสของยูเอ็มแอลสำหรับแสดงแบบรูปความมั่นคงให้มีความสมบูรณ์และชัดเจน อีกทั้งได้พัฒนาเครื่องมือสำหรับจัดการแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง ซึ่งจะช่วยให้ผู้พัฒนาระบบเข้าใจและสามารถประยุกต์ใช้โครงสร้างของแบบรูปความมั่นคงได้อย่างง่าย อีกทั้งทำให้รู้ว่าการดำเนินการ (Operation) หรือลักษณะประจำ (Attribute) ใดที่ต้องจัดเก็บเพื่อที่จะตอบสนองการใช้งานในการออกแบบระบบทางด้านความมั่นคงให้มีความสอดคล้องกับความต้องการทางด้านความมั่นคง

คำสำคัญ: แบบรูปความมั่นคง, ยูเอ็มแอลเซค, ยูเอ็มแอลโพรไฟล์

### Abstract

Security of software system is an important issue which many enterprises have to consider because various kinds of threats occur increasingly in present. Principles of security are essential to prevent system from attacking, that can help system operate efficiently. Security patterns are offered to solve the design problem of security requirements. It described solutions to various kinds of security problems and can be applied in many cases. In this paper, we present

a concept for constructing a security structural model based on security patterns by extending UML class diagram and also present a prototyping tool supports our concept. These can be beneficial for developer to understand and apply the defined model. Operations and attributes are specified for each class in order for the security system design that complies with security requirements.

Keywords: Security Patterns, UMLsec, UML Profile

### 1. คำนำ

ในปัจจุบันความต้องการความมั่นคง (Security Requirements) [3] มีความสำคัญต่อการพัฒนาระบบซอฟต์แวร์เป็นอย่างมาก ทั้งนี้เพราะเป็นความต้องการที่เกี่ยวข้องกับจุดอ่อนของระบบและวิธีป้องกันจุดอ่อนดังกล่าว จากการถูกโจมตี ซึ่งจะช่วยให้ระบบที่พัฒนาขึ้นนั้นมีประสิทธิภาพในการทำงานมาก ซึ่งเป็นที่มาของแบบรูปความมั่นคง ที่ถูกเสนอเพื่อช่วยแก้ไขปัญหาการออกแบบความต้องการความมั่นคงของระบบ แบบรูปความมั่นคงจะอธิบายเกี่ยวกับแนวทางหรือผลเฉลยของปัญหาทางด้านความมั่นคงต่างๆ ที่ถูกแก้ปัญหามาแล้ว นอกจากนี้ยังสนับสนุนการนำกลับมาใช้ใหม่อีกด้วย โดย D.M. Kienzle และคณะ [4] ได้เสนอแบบรูปความมั่นคงสำหรับการแก้ไขปัญหาการออกแบบความมั่นคงของเว็บไซต์ อีกทั้ง Schumacher และคณะ [5] ได้เสนอแบบรูปความมั่นคงสำหรับแก้ไขปัญหาการออกแบบความมั่นคงของระบบทั่วไป พร้อมทั้งนำเสนอส่วนประกอบและความสัมพันธ์ที่สำคัญของแบบรูปความมั่นคงสำหรับการออกแบบซอฟต์แวร์

แต่อย่างไรก็ตามการศึกษาและวิเคราะห์แบบรูปความมั่นคงเพื่อนำมาประยุกต์ใช้ในการออกแบบซอฟต์แวร์นั้นทำได้ยาก เนื่องจากผู้พัฒนาต้องศึกษาและทำความเข้าใจโครงสร้าง คุณสมบัติ เงื่อนไขบังคับ และผลเฉลยของแบบรูปความมั่นคง ซึ่งหากไม่ศึกษาและวิเคราะห์ให้เข้าใจอย่างถ่องแท้ อาจทำให้เกิดผลเสียต่อระบบตามภายหลังได้ เช่น

ระบบที่พัฒนาที่มีความปลอดภัยไม่เพียงพอ ทำให้ผู้โจมตีมองเห็นจุดอ่อนของระบบได้โดยง่าย ก่อให้เกิดการสูญเสียตามมาอย่างมากมาย เช่น ข้อมูลถูกขโมยหรือทำลาย หรือข้อมูลถูกเปลี่ยนแปลง เป็นต้น

ยูเอ็มแอลเซค (UMLsec) [3,4] เป็นส่วนขยายของยูเอ็มแอลที่สนับสนุนการแสดงโครงสร้างในรูปแบบภาพคลาสเพื่อการพัฒนากระบวนการความมั่นคง แต่ยูเอ็มแอลเซคสามารถออกแบบได้สภาพแวดล้อมหนึ่งเท่านั้น ซึ่งไม่สอดคล้องตามแบบรูปความมั่นคง อีกทั้งยังมีการแสดงโครงสร้างของแบบรูปความมั่นคงได้ไม่ชัดเจนเท่าที่ควร เช่น ขาดองค์ประกอบที่ระบุโครงสร้างของแบบรูปความมั่นคง ขาดอิสระในการตั้งชื่อคลาสหรือองค์ประกอบอื่น เนื่องจากต้องตั้งชื่อให้สอดคล้องกับหน้าที่ในแบบรูปความมั่นคง เป็นต้น

ดังนั้นงานวิจัยนี้ จึงมีแนวคิดที่จะปรับปรุงยูเอ็มแอล เพื่อช่วยให้ผู้พัฒนาเข้าใจถึงโครงสร้างของแบบรูปความมั่นคงในยูเอ็มแอลได้อย่างชัดเจน อีกทั้งทำให้รู้ว่ามีมีการดำเนินการ (Operation) หรือคุณลักษณะ (Attribute) ใดที่ต้องจัดเก็บเพื่อที่จะตอบสนองการใช้งานในการออกแบบระบบทางด้านความมั่นคง ให้มีความสอดคล้องกับความต้องการทางด้านความมั่นคงมากที่สุด

โดยผู้วิจัยมุ่งเน้นในการศึกษา วิเคราะห์และปรับปรุงยูเอ็มแอลเพื่อแสดงแบบรูปความมั่นคง ซึ่งจะใช้แบบรูปความมั่นคงที่นำเสนอในหนังสือ แบบรูปความมั่นคง การบูรณาการความมั่นคงและวิศวกรรมระบบ (Security Patterns: Integrating Security and Systems Engineering) ที่นำเสนอโดย Schumacher และคณะ [2] ที่แตกต่างไปจากแบบรูปความมั่นคงที่ เกียรติศักดิ์ ไชยสมบูรณ์ และคณะ [8] ได้ทำไว้ จากนั้นทำการปรับปรุงเพื่อให้เหมาะสมสำหรับการนำมาใช้งานในการออกแบบพัฒนาซอฟต์แวร์และปรับปรุงส่วนที่มีความซ้ำซ้อนกัน พร้อมทั้งแนวคิดในการพัฒนาเครื่องมือที่ช่วยสนับสนุนการใช้แบบรูปความมั่นคง ซึ่งการออกแบบความมั่นคงโดยใช้แบบรูปความมั่นคงนั้นจะช่วยให้การออกแบบความมั่นคงของระบบมีประสิทธิภาพมากยิ่งขึ้น

## 2. งานวิจัยที่เกี่ยวข้อง

Fernandez [9] นำเสนอส่วนประกอบต่างๆ และความสัมพันธ์ที่เป็นของแบบรูปการใช้อำนาจในการออกแบบซอฟต์แวร์ ในมุมมองของสถาปัตยกรรมชั้นเมตาตาตาของการ โปรแกรมเชิงวัตถุ โดยมีกรวดตัวอย่างให้เห็นถึงการประยุกต์ใช้มุมมองของสถาปัตยกรรมชั้นเมตาตาตาของแบบรูปการใช้อำนาจนี้ โดยมุมมองสถาปัตยกรรมชั้นเมตาตาตาจะช่วยในการควบคุมพฤติกรรมและการให้อำนาจแก่ผู้ใช้ระบบให้เป็นไปตามแบบรูปการใช้อำนาจ Schumacher และคณะ [2] นำเสนอ

แบบรูปความมั่นคง จำนวน 46 แบบรูป เพื่อใช้สำหรับแก้ไขปัญหาการออกแบบความมั่นคงของระบบทั่วไป พร้อมทั้งนำเสนอส่วนประกอบและความสัมพันธ์ที่สำคัญของแบบรูปความมั่นคง เพื่อเป็นแนวทางในการกำหนดส่วนประกอบและความสัมพันธ์ของแบบรูปความมั่นคงในการออกแบบซอฟต์แวร์

J. Jürjens [6,7] นำเสนอยูเอ็มแอลเซค (UMLsec) หรือการสร้างส่วนขยายของยูเอ็มแอล สำหรับพัฒนากระบวนการความมั่นคงและสนับสนุนการออกแบบส่วนประกอบและความสัมพันธ์ทางความมั่นคงของระบบทั่วไป อีกทั้งยังสนับสนุนการออกแบบความมั่นคงของระบบโดยใช้แบบรูปความมั่นคงอีกด้วย แต่ในการนำยูเอ็มแอลเซคมาใช้งานกับแบบรูปความมั่นคงนั้นยังมีข้อจำกัดอยู่ เนื่องจากไม่สามารถอธิบายส่วนประกอบและความสัมพันธ์ของแบบรูปความมั่นคงได้อย่างชัดเจนและสมบูรณ์เท่าที่ควร Dong และคณะ [10] นำเสนอการปรับปรุงยูเอ็มแอลโรไฟล์สำหรับแสดงส่วนประกอบและความสัมพันธ์ของแบบรูปการออกแบบ (Design Pattern) ในโปรแกรมประยุกต์โดยใช้แผนภาพคลาส ซึ่งช่วยให้ผู้พัฒนาสามารถมองเห็นส่วนประกอบและความสัมพันธ์ของแบบรูปการออกแบบทั้งหมด ที่มีความซับซ้อนได้ชัดเจนยิ่งขึ้น ซึ่งช่วยให้นำแบบรูปการออกแบบไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

เกียรติศักดิ์และคณะ [8] นำเสนอการวิเคราะห์และปรับปรุงยูเอ็มแอลเซคเพื่อสนับสนุนการแสดงแบบรูปความมั่นคง ซึ่งจะใช้แบบรูปความมั่นคงที่นำเสนอใน [2] เพื่อสามารถนำมาใช้งานจริงในการออกแบบและพัฒนาซอฟต์แวร์ พร้อมทั้งพัฒนาเครื่องมือที่ช่วยสนับสนุนการใช้แบบรูปความมั่นคง ซึ่งการออกแบบความมั่นคงโดยใช้แบบรูปความมั่นคงนั้นจะช่วยให้การออกแบบความมั่นคงของระบบมีประสิทธิภาพมากยิ่งขึ้น โดยนำแบบรูปความมั่นคงที่ได้รับการออกแบบและตรวจสอบความถูกต้องแล้ว 5 กลุ่มแบบรูปซึ่งมีทั้งหมด 27 แบบรูป

ในบทความนี้ นำเสนอแนวคิดการวิเคราะห์และปรับปรุงยูเอ็มแอลเซคเพื่อแสดงแบบรูปความมั่นคง ซึ่งจะใช้แบบรูปความมั่นคงที่นำเสนอใน [2] ที่แตกต่างไปจากแบบรูปความมั่นคงของงานวิจัย [8] โดยครอบคลุมแบบรูปความมั่นคงทั้งหมด 8 กลุ่มแบบรูปซึ่งมีทั้งหมด 44 แบบรูป เพื่อช่วยให้การออกแบบความมั่นคงของระบบมีประสิทธิภาพมากยิ่งขึ้น

## 3. แบบรูปความมั่นคง

แบบรูปความมั่นคง [1,2] เป็นแบบรูปที่นำเสนอปัญหาความมั่นคงที่เคยปรากฏในอดีต รวมทั้งผลเฉลยที่พิสูจน์แล้วว่าสามารถแก้ไข

ปัญหาได้เป็นอย่างดี อีกทั้งยังสามารถประยุกต์ใช้กับการออกแบบโครงสร้างของการแก้ปัญหาความมั่นคงได้อย่างเป็นรูปธรรม เนื่องจากแบบรูปความมั่นคงดังกล่าวได้รวบรวมองค์ความรู้ด้านความมั่นคงไว้ อย่างมีโครงสร้างจากผู้ชำนาญการด้านความมั่นคง วิศวกรรมความมั่นคง และวิศวกรรมซอฟต์แวร์ แบบรูปความมั่นคงสามารถแบ่งได้เป็น 3 ประเภท ได้แก่

1) แบบรูปการวิเคราะห์ความมั่นคง (Security Analysis Patterns) เป็นแบบรูปที่แก้ปัญหการวิเคราะห์ความมั่นคงของระบบ

2) แบบรูปการออกแบบความมั่นคง (Security Design Patterns) เป็นแบบรูปที่แก้ปัญหการออกแบบโครงสร้างความมั่นคงของระบบ

3) แบบรูปกระบวนการความมั่นคง (Security Process Patterns) เป็นแบบรูปที่แก้ปัญหการออกแบบความมั่นคงให้กับกระบวนการของระบบ

ในงานวิจัยนี้ได้ใช้แนวคิดของวิเคราะห์และปรับปรุงยูเอ็มแอลเพื่อแสดงแบบรูปความมั่นคง ซึ่งจะใช้แบบรูปความมั่นคงที่นำเสนอใน [7] ที่แตกต่างไปจากแบบรูปความมั่นคงที่งานวิจัย [8] ได้ทำไว้ โดยจะครอบคลุมแบบรูปความมั่นคงทั้งหมด เพื่อช่วยให้การออกแบบความมั่นคงของระบบมีประสิทธิภาพมากยิ่งขึ้น ซึ่งประกอบด้วยแบบรูป 17 แบบรูป หรือ 3 กลุ่มแบบรูป ดังนี้

1. แบบรูปการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยง (Enterprise Security and Risk Management)

2. แบบรูปการระบุตัวตนและการพิสูจน์ตัวตน (Identification and Authentication)

3. แบบรูปการบันทึกเหตุการณ์ (Accounting)

#### 4. ยูเอ็มแอลโพรไฟล์

ยูเอ็มแอลโพรไฟล์ [11,12] เป็นองค์ประกอบหนึ่งของแผนภาพยูเอ็มแอล ที่รองรับผู้ใช้ให้สามารถปรับเปลี่ยนหรือกำหนดคกฎให้เหมาะสมกับโดเมนที่ต้องการใช้งานได้ ยูเอ็มแอลโพรไฟล์ประกอบไปด้วยองค์ประกอบย่อยที่มีหน้าที่แตกต่างกัน ดังต่อไปนี้

1) แม่พิมพ์ต้นแบบ (Stereotype) เป็นองค์ประกอบที่ใช้ในการระบุประเภทต่างๆ ขององค์ประกอบแบบจำลอง (Model Element) ในแผนภาพยูเอ็มแอล ซึ่งช่วยในการรวมกลุ่มของข้อมูลที่เกี่ยวข้องกันเข้าด้วยกัน โดยรูปแบบทั่วไปของแม่พิมพ์ต้นแบบ คือ

<< ชื่อแม่พิมพ์ต้นแบบ >>

ตัวอย่างของแม่พิมพ์ต้นแบบ เช่น แม่พิมพ์ต้นแบบ “interface” เป็นแม่พิมพ์ต้นแบบที่ระบุองค์ประกอบที่เป็นส่วนต่อประสาน เป็นต้น นอกจากนี้แม่พิมพ์ต้นแบบอาจมีค่าป้ายระบุและเงื่อนไขบังคับที่สัมพันธ์กับแม่พิมพ์ต้นแบบดังกล่าว เพื่อใช้ในการระบุข้อมูลที่จำเพาะขององค์ประกอบดังกล่าวให้ชัดเจนยิ่งขึ้น

2) ค่าป้ายระบุ (Tagged Value) เป็นข้อมูลจำเพาะของแม่พิมพ์ต้นแบบ ค่าป้ายระบุช่วยกำหนดคุณลักษณะของแม่พิมพ์ต้นแบบ โดยรูปแบบทั่วไปของค่าป้ายระบุ คือ

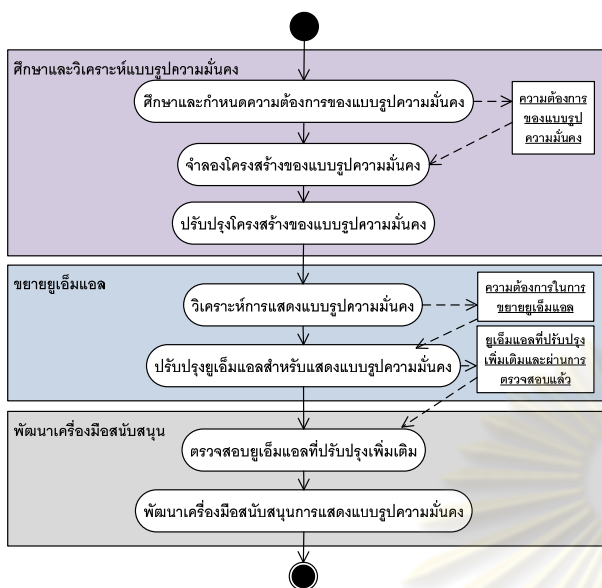
ชื่อป้ายระบุ (Tag name) = ค่าของป้ายระบุ (Value of tag)

ตัวอย่างเช่น ค่าป้ายระบุ “assetKind=InformationType” เป็นค่าป้ายระบุของแม่พิมพ์ต้นแบบ “asset” ที่ระบุว่า ชนิดของสินทรัพย์ทางด้านธุรกิจขององค์กรคือ “InformationType” เป็นต้น

3) เงื่อนไขบังคับ (Constraint) เป็นข้อบังคับของแม่พิมพ์ต้นแบบที่จำเป็นต้องพิจารณาเมื่อมีการใช้งานที่จำเป็นต้องพิจารณา เพื่อบอกถึงเงื่อนไขในการใช้งานแม่พิมพ์ต้นแบบหรือค่าป้ายระบุ อีกทั้งเงื่อนไขบังคับยังช่วยกำหนดขอบเขตของการใช้แม่พิมพ์ต้นแบบหรือค่าป้ายระบุ ซึ่งโดยทั่วไปเงื่อนไขบังคับจะถูกเขียนด้วยภาษาโอซีแอล (Object Constraint Language: OCL) [13] ทั้งนี้เพราะภาษาโอซีแอลเป็นภาษามาตรฐานในการระบุเงื่อนไขบังคับของยูเอ็มแอล เช่น เงื่อนไขบังคับ “self.base.name -> notEmpty” หมายถึง ชื่อของอ็อบเจกต์นั้นจะต้องไม่ใช่ค่าว่าง เป็นต้น

#### 5. การปรับปรุงยูเอ็มแอลสำหรับการแสดงแบบรูปความมั่นคงและการพัฒนาเครื่องมือ

จากการที่ยูเอ็มแอลเซคไม่สามารถแสดงแบบรูปความมั่นคงในยูเอ็มแอลได้สมบูรณ์และชัดเจนเท่าที่ควร และเมื่อขยายยูเอ็มแอลเซคจะทำให้เกิดความไม่สะดวกในการใช้งาน เช่น ข้อมูลของแบบรูปมีลักษณะเป็นข้อความ ซึ่งอาจทำให้ผู้ใช้งานกำหนดข้อมูลของแบบรูปได้ไม่สะดวก อีกทั้งในการออกแบบแบบจำลองของระบบนั้น ผู้ใช้งานจะต้องทำการสร้างคลาสเพื่อประกอบเป็นโครงสร้างของแบบรูป ซึ่งทำให้เสียเวลาในการสร้างโครงสร้างของแบบรูปนั้น เป็นต้น ดังนั้นงานวิจัยนี้จึงทำการขยายยูเอ็มแอล เพื่อแสดงแบบรูปความมั่นคงได้อย่างมีประสิทธิภาพ และทำการพัฒนาเครื่องมือสำหรับช่วยสนับสนุนการใช้งานแบบรูปความมั่นคงที่สามารถนำไปใช้ประโยชน์ในการพัฒนาซอฟต์แวร์ได้จริง โดยมีขั้นตอนการสร้างแบบจำลอง ดังรูปที่ 1



รูปที่ 1 แผนภาพกิจกรรมขั้นตอนการสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงโดยการขยายยูเอ็มแอลแซค

1) ศึกษาและกำหนดความต้องการของแบบรูปความมั่นคง

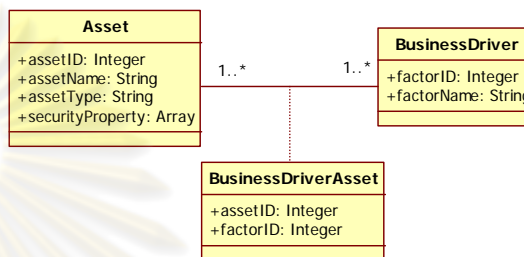
การศึกษาและกำหนดความต้องการของแบบรูปความมั่นคง ผู้วิจัยใช้แบบรูปการระบุความต้องการความมั่นคงสำหรับสินทรัพย์องค์กร ในกลุ่มการจัดการความมั่นคงองค์กรและการจัดการความเสี่ยงมาเป็นกรณีศึกษา โดยแบบรูปการระบุตัวขับเคลื่อนทางด้านธุรกิจที่มีผลต่อสินทรัพย์ขององค์กร เป็นแบบรูปที่นำเสนอการพิจารณาสินทรัพย์ขององค์กร ว่ามีขับเคลื่อนทางด้านธุรกิจใดที่มีปัจจัยให้เกิดความต้องการสินทรัพย์ขององค์กร โดยแสดงรายการของปัญหา บริบทของปัญหา และผลเฉลยของปัญหา ดังตารางที่ 1

ตารางที่ 1 รายการปัญหา บริบท และผลเฉลยของแบบรูปการระบุตัวขับเคลื่อนทางด้านธุรกิจที่มีผลต่อสินทรัพย์ขององค์กร

รายการ	รายละเอียด
ปัญหา	องค์กรต้องการกำหนดความมั่นคงให้กับสินทรัพย์ขององค์กร
บริบท	องค์กรต้องการกำหนดความมั่นคงให้กับสินทรัพย์ แต่จะต้องระบุสินทรัพย์และปัจจัยทางด้านธุรกิจ (Business factor) เสียก่อน
ผลเฉลย	1. ระบุสินทรัพย์ทางด้านธุรกิจขององค์กร (Asset) 2. ระบุตัวขับเคลื่อนทางด้านธุรกิจขององค์กรที่เป็นปัจจัยให้เกิดความต้องการของแต่ละสินทรัพย์ (BusinessDriver) 3. กำหนดความสัมพันธ์ระหว่างสินทรัพย์และปัจจัยทางธุรกิจ 4. กำหนดคุณสมบัติให้กับสินทรัพย์ (assetType) 5. ระบุคุณสมบัติทางด้านความมั่นคง (securityProperty)

2) จำลองโครงสร้างของแบบรูปความมั่นคง

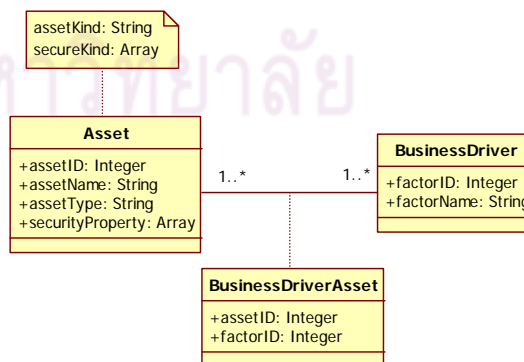
ในการจำลองโครงสร้างของแบบรูปความมั่นคงนั้น จะนำความต้องการของแบบรูปความมั่นคงมาใช้ในการพิจารณา โดยแสดงแผนภาพคลาสที่แสดงโครงสร้าง (Structure) ของแบบรูปการระบุตัวขับเคลื่อนทางด้านธุรกิจที่มีผลต่อสินทรัพย์ขององค์กร จากส่วนของ “Structure” ของแบบรูป ดังรูปที่ 2



รูปที่ 2 แผนภาพคลาสแสดงโครงสร้างแบบแบบรูปการระบุตัวขับเคลื่อนทางด้านธุรกิจที่มีผลต่อสินทรัพย์ขององค์กร

3) ปรับปรุงโครงสร้างของแบบรูปความมั่นคง

การปรับปรุงโครงสร้างของแบบรูปความมั่นคง เป็นการนำส่วนของ “Structure” ของแบบรูปมาปรับปรุง โดยพิจารณาจากส่วนประกอบอื่นของแบบรูป ได้แก่ Dynamic, Implementation, Solution, Example Resolved และ Variant ทั้งนี้เนื่องจากโครงสร้างของแบบรูปความมั่นคงที่ได้จากส่วนประกอบดังกล่าวอาจไม่ครอบคลุมองค์ประกอบทางโครงสร้างของส่วนประกอบอื่น ดังนั้นในการขยายยูเอ็มแอลจึงจำเป็นต้องพิจารณาที่ส่วนประกอบอื่นของแบบรูปความมั่นคงด้วย เพื่อให้ยูเอ็มแอลที่ปรับปรุงเพิ่มเติมสามารถแสดงองค์ประกอบของแบบรูปความมั่นคงได้สมบูรณ์ที่สุด โดยแสดงแผนภาพคลาสที่แสดงโครงสร้างของแบบรูปการระบุตัวขับเคลื่อนทางด้านธุรกิจที่มีผลต่อสินทรัพย์ขององค์กรที่ปรับปรุงแล้ว ดังรูปที่ 3



รูปที่ 3 แผนภาพคลาสแสดงโครงสร้างแบบรูปการระบุตัวขับเคลื่อนทางด้านธุรกิจที่มีผลต่อสินทรัพย์ขององค์กรที่ปรับปรุงแล้ว

#### 4) วิเคราะห์การแสดงผลแบบรูปความมั่นคง

การวิเคราะห์การแสดงผลแบบรูปความมั่นคง เป็นการนำโครงสร้างของแบบรูปความมั่นคงที่ได้รับการปรับปรุงเพิ่มเติมและข้อมูลของแบบรูปความมั่นคงมาวิเคราะห์ โดยจะวิเคราะห์การแสดงผลข้อมูลทางโครงสร้างของแบบรูปความมั่นคงและการแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคง เพื่อหาความต้องการในการปรับปรุงยูเอ็มแอลสำหรับแสดงผลแบบรูปความมั่นคง โดยมีรายละเอียดดังนี้

(1) วิเคราะห์การแสดงผลข้อมูลทางโครงสร้างของแบบรูปความมั่นคง เป็นการวิเคราะห์หาความต้องการในการแสดงผลข้อมูลอธิบายโครงสร้างของแบบรูปความมั่นคง ประกอบไปด้วย 1) ความต้องการในการแสดงผลข้อมูลทางโครงสร้างโดยรวมของแบบรูป ซึ่งเป็นความต้องการในการแสดงผลข้อมูลอธิบายลักษณะที่เป็นภาพรวมของแบบรูปความมั่นคง และ 2) ความต้องการในการแสดงผลข้อมูลทางโครงสร้างขององค์ประกอบแบบจำลองในแบบรูป เป็นความต้องการในการแสดงผลข้อมูลอธิบายลักษณะขององค์ประกอบแบบจำลองในแบบรูป

(2) วิเคราะห์การแสดงผลข้อมูลทางความมั่นคงของแบบรูปความมั่นคง เป็นการวิเคราะห์หาความต้องการในการแสดงผลข้อมูลที่เป็นองค์ประกอบทางด้านความมั่นคงของแบบรูป ประกอบไปด้วย 1) ความต้องการในการแสดงผลองค์ประกอบทางความมั่นคง ซึ่งเป็นความต้องการในการแสดงผลองค์ประกอบแบบจำลองที่มีนัยสำคัญทางด้านความมั่นคง และ 2) ความต้องการในการแสดงผลลักษณะขององค์ประกอบทางความมั่นคง เป็นความต้องการในการแสดงผลข้อมูลอธิบายลักษณะขององค์ประกอบทางความมั่นคงให้ชัดเจนมากยิ่งขึ้น

จากความต้องการในการแสดงผลข้อมูลทางโครงสร้างและข้อมูลทางความมั่นคงของแบบรูปความมั่นคงข้างต้น จะถูกนำมาใช้ในขั้นตอนของการปรับปรุงยูเอ็มแอลสำหรับแสดงผลแบบรูปความมั่นคงต่อไป

#### 5) ปรับปรุงยูเอ็มแอลสำหรับแสดงผลแบบรูปความมั่นคง

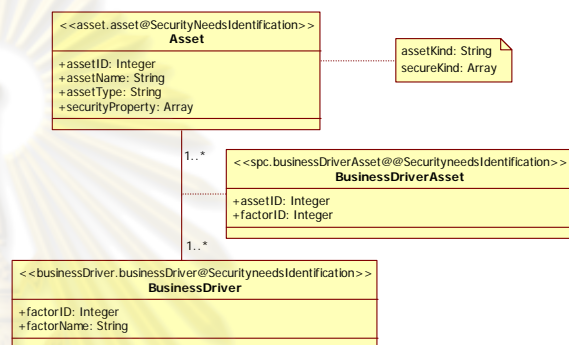
หลังจากทำการวิเคราะห์การแสดงผลแบบรูปความมั่นคงแล้ว ขั้นตอนต่อมาคือ การปรับปรุงยูเอ็มแอลเพื่อแสดงผลแบบรูปความมั่นคง ซึ่งใช้หลักการดังนี้

(1) แสดง โครงสร้าง ของ แบบ รูป ความ มั่น คง ที่ มี ลักษณะเฉพาะ ซึ่งเป็นการแสดงคลาส การดำเนินการ คุณลักษณะและองค์ประกอบอื่นที่สำคัญของแต่ละแบบรูปความมั่นคง

(2) ลดความซับซ้อนของการแสดงผลแบบรูปความมั่นคง โดยจะทำการลดความซับซ้อนจากการแสดงผลข้อมูลของแบบรูปความมั่นคง

โดยใช้ยูเอ็มแอล รวมทั้งปรับปรุงรูปแบบการแสดงผลของยูเอ็มแอลบางองค์ประกอบเพื่อที่จะแสดงผลข้อมูลของแบบรูปความมั่นคง

จากหลักการดังกล่าว ทำให้จำเป็นต้องมีการเพิ่มแม่พิมพ์ต้นแบบและป้ายระบุ เพื่อทำหน้าที่ในการระบุนองค์ประกอบของแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง ดังตารางที่ 2 และตารางที่ 3 และแสดงแผนภาพคลาสที่แสดงโครงสร้างของแบบรูปการระบุตัวขับเคลื่อนทางด้านธุรกิจที่มีผลต่อสินทรัพย์ขององค์กรที่ปรับปรุงสมบูรณ์แล้ว ดังรูปที่ 4



รูปที่ 4 แผนภาพคลาสแสดงโครงสร้างของแบบรูปการระบุตัวขับเคลื่อนทางด้านธุรกิจที่มีผลต่อสินทรัพย์ขององค์กรที่ปรับปรุงสมบูรณ์แล้ว

#### 6) ตรวจสอบยูเอ็มแอลที่ปรับปรุงเพิ่มเติม

ในการตรวจสอบยูเอ็มแอลที่ปรับปรุงเพิ่มเติมนั้นจะพิจารณาจากข้อกำหนดความต้องการของยูเอ็มแอลโพรไฟล์ (UML Profile Specification) ตามที่ [8] ได้กล่าวไว้ โดยรายละเอียดของคุณสมบัติมาตรฐานของยูเอ็มแอลโพรไฟล์มีดังต่อไปนี้

(1) เป็นซัพเซตของยูเอ็มแอลเมตาโมเดล (UML Metamodel) โดยยูเอ็มแอลที่ปรับปรุงเพิ่มเติมนั้นมาจากการขยายยูเอ็มแอลที่เป็นกลไกภายในยูเอ็มแอลเมตาโมเดล ดังนั้นยูเอ็มแอลที่ปรับปรุงเพิ่มเติมจึงเป็นซัพเซตของยูเอ็มแอลเมตาโมเดล

(2) มีกฎการควบคุมรูปแบบการใช้งาน (Well-Formedness Rules) ขององค์ประกอบที่ได้สร้างไว้กล่าวคือ ยูเอ็มแอลเซตที่ปรับปรุงเพิ่มเติมได้กำหนดเงื่อนไขบังคับในการควบคุมรูปแบบการใช้งานของแม่พิมพ์ต้นแบบซึ่งอยู่ในรูปของภาษาไอซีแอล ดังตารางที่ 2

(3) ใช้ระบุนองค์ประกอบที่นอกเหนือจากองค์ประกอบมาตรฐานของยูเอ็มแอลกล่าวคือ แม่พิมพ์ต้นแบบ คำป้ายระบุ และเงื่อนไขบังคับที่เกิดจากการขยายนั้นสามารถระบุเป็นองค์ประกอบของยูเอ็มแอล

ตารางที่ 2 แม่พิมพ์ต้นแบบและป้ายระบุที่เพิ่มเติม

แม่พิมพ์ต้นแบบ	ความหมาย	นำไปใช้งานใน	ค่าป้ายระบุ	เงื่อนไขบังคับ
spc (Security Pattern Class)	แม่พิมพ์ต้นแบบที่ใช้ในการระบุคลาสที่เป็นองค์ประกอบในแบบรูปความมั่นคง	คลาส (Class)	บทบาท@ ชื่อแบบรูป [ลำดับ]	1> self.taggedValue.dataValue.name -> notEmpty 2> self.taggedValue.name -> forall(v1, v2:name   v1.name <> v2.name) implies (v1.instance -> isEmpty and v2.instance -> isEmpty) 3> self.taggedValue.name -> exists(v1, v2:name   v1.name = v2.name) implies (v1.instance -> notEmpty and v2.instance -> notEmpty and v1.instance <> v2.instance)
spt (Security Pattern Data Type)	แม่พิมพ์ต้นแบบที่ใช้ในการระบุชนิดข้อมูลในแบบรูปความมั่นคง	คลาส (Class)		
spr (Security Pattern Relationship)	แม่พิมพ์ต้นแบบที่ใช้ในการระบุความสัมพันธ์ที่เป็นองค์ประกอบในแบบรูปความมั่นคง	ความสัมพันธ์ (Relationship)		

ตารางที่ 3 ป้ายระบุสำหรับแสดงข้อมูลทางโครงสร้างของแบบรูปต่างๆ

ป้ายระบุ	แม่พิมพ์ต้นแบบ	ค่าป้ายระบุ	ค่าของป้ายระบุ	มัลติพลิซิติ	คำอธิบาย
บทบาท@ชื่อแบบรูป [ลำดับ]	แม่พิมพ์ต้นแบบที่สร้างทั้งหมด	บูลีนแสดงลักษณะองค์ประกอบดังกล่าวในแบบรูป	true หรือ false	*	- ระบุว่า องค์ประกอบดังกล่าวมีบทบาทอะไรในแบบรูปความมั่นคงนั้น และมีลำดับของแบบรูปความมั่นคงในแผนภาพหรือไม่

(4) มีการกำหนดความหมายของแต่ละองค์ประกอบกล่าวคือ ยูเอ็มแอลที่ปรับปรุงเพิ่มเติมได้อธิบายความหมายของแต่ละองค์ประกอบในรายการของแม่พิมพ์ต้นแบบ ดังตารางที่ 2 และรายการของป้ายระบุในตารางที่ 3

(5) มีการกำหนดองค์ประกอบแบบจำลองที่ใช้ในองค์ประกอบที่ได้สร้างไว้กล่าวคือ ยูเอ็มแอลที่ปรับปรุงเพิ่มเติมได้กำหนดคลาสพื้นฐานของแต่ละแม่พิมพ์ต้นแบบที่แสดงถึงประเภทขององค์ประกอบแบบจำลอง ดังตารางที่ 2

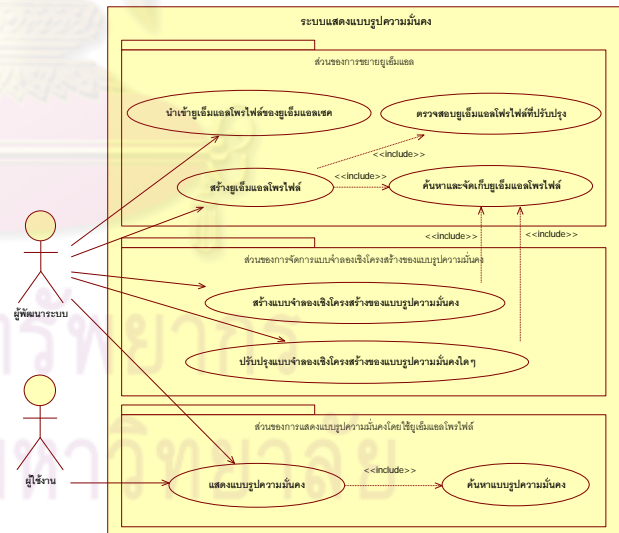
จากการตรวจสอบยูเอ็มแอลที่ปรับปรุงเพิ่มเติมจากคุณสมบัติมาตรฐานของยูเอ็มแอลโพรไฟล์ พบว่า ยูเอ็มแอลที่ปรับปรุงเพิ่มเติมมีข้อมูลและลักษณะขั้นพื้นฐานของยูเอ็มแอลโพรไฟล์ไม่แตกต่างจากยูเอ็มแอลโพรไฟล์ทั่วไป ดังนั้นสรุปได้ว่า ยูเอ็มแอลที่ปรับปรุงเพิ่มเติมนี้มีความถูกต้องตามมาตรฐานของยูเอ็มแอลโพรไฟล์

7) พัฒนาคำอธิบายสนับสนุนการแสดงผลแบบรูปความมั่นคง

ในการพัฒนาเครื่องมือสนับสนุนนั้นผู้วิจัยได้ทำการศึกษาโอเพนซอร์ซเพื่อที่จะสร้างโปรแกรมเสริมจากโอเพนซอร์ซนั้นสำหรับแสดงโครงสร้างของแบบรูปความมั่นคง เบื้องต้นได้ทำการศึกษาโอเพนซอร์ซที่ชื่อว่า “StarUML” ที่มีความยืดหยุ่นและสามารถขยายความสามารถของโปรแกรมได้โดยการสร้างส่วนขยายของโปรแกรมเพื่อเสริมความสามารถในส่วนที่ต้องการได้

ดังนั้นงานวิจัยนี้จึงแนวคิดที่จะพัฒนาโปรแกรมเสริมที่ช่วยในการแสดงผลแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลเซคที่ได้รับการปรับปรุง

จากหัวข้อ 3) ปรับปรุงโครงสร้างของแบบรูปความมั่นคง และ 5) ปรับปรุงยูเอ็มแอลสำหรับแสดงแบบรูปความมั่นคง อีกทั้งทำให้การแสดงผลแบบรูปความมั่นคงโดยใช้ยูเอ็มแอลมีประสิทธิภาพอีกด้วย โดยเครื่องมือมีหน้าที่การทำงานเบื้องต้น ดังรูปที่ 4



รูปที่ 4 หน้าที่การทำงานเบื้องต้นของเครื่องมือ

(1) การสร้างส่วนขยายยูเอ็มแอล เมื่อผู้พัฒนาต้องการที่จะเพิ่มส่วนขยายของยูเอ็มแอลสำหรับแสดงแบบรูปความมั่นคงใดๆ นั้น จะเริ่มจากการค้นหายูเอ็มแอลโพรไฟล์ที่ได้จับเก็บไว้ เพื่อลดความซ้ำซ้อนที่อาจเกิดขึ้น หลังจากนั้นจะทำการเพิ่มยูเอ็มแอลโพรไฟล์ ซึ่งยูเอ็มแอลโพรไฟล์ที่เพิ่มขึ้นนั้น ผู้พัฒนาอาจจะสร้างขึ้นเองหรือนำมาจากยูเอ็มแอล



โพรไฟล์ของยูเอ็มแอลเซค และเมื่อสร้างส่วนขยายเสร็จ ระบบจะทำการตรวจสอบยูเอ็มแอลโพรไฟล์ และทำการจัดเก็บต่อไป

(2) การจัดการแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง ในส่วนนี้ผู้พัฒนาสามารถสร้าง ปรับปรุงแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงได้ โดยสามารถเลือกยูเอ็มแอลโพรไฟล์ที่ได้สร้างไว้

(3) การแสดงแบบรูปความมั่นคงโดยยูเอ็มแอลโพรไฟล์ เมื่อผู้ใช้ต้องการใช้แบบรูปความมั่นคงใดๆ นั้น ระบบจะทำการค้นหาแบบรูปความมั่นคงที่ได้จัดเก็บไว้ จากนั้นจะแสดงแบบรูปความมั่นคงที่ผู้ใช้เลือก เพื่อนำไปใช้ในกระบวนการต่างๆ ของการพัฒนาซอฟต์แวร์ต่อไป

#### 4. สรุป

งานวิจัยนี้ได้ทำการสร้างแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงโดยการขยายยูเอ็มแอล โดยทำการวิเคราะห์ ออกแบบ และมีแนวคิดที่จะขยายยูเอ็มแอลและพัฒนาเครื่องมือสำหรับแสดงแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคงสำหรับแสดงแบบรูปความมั่นคงให้มีความสมบูรณ์และชัดเจน ซึ่งครอบคลุมทุกๆ แบบรูปความมั่นคงที่น่าเสนอใน [2] อีกทั้งได้พัฒนาเครื่องมือสำหรับจัดการแบบจำลองเชิงโครงสร้างของแบบรูปความมั่นคง ซึ่งจะช่วยให้ผู้ออกแบบสามารถออกแบบความมั่นคงให้กับระบบได้สมบูรณ์มากยิ่งขึ้น รวมทั้งเสนอส่วนการแสดงผลแบบรูปความมั่นคงโดยยูเอ็มแอลโพรไฟล์ เพื่อให้ผู้ใช้นำแบบรูปความมั่นคงไปใช้ในกระบวนการต่างๆ ของการพัฒนาซอฟต์แวร์ได้อย่างมีประสิทธิภาพ

#### เอกสารอ้างอิง

- [1] B. Blakley, C. Heath and members of The Open Group Security Forum, *Security Design Patterns*, The Open Group U.K., April 2004.
- [2] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann and P. Sommerlad, *Security Patterns: Integrating Security and Systems Engineering*, John Wiley & Sons, 2005.
- [3] M. Schumacher, *Security Engineering with Patterns*, Springer-Verlag Berlin Heidelberg, 2002.
- [4] D.M. Kienzle, M.C. Elder, D. Tyree and J. Edwards-Hewitt, *Security Patterns Repository Version 1.0*, 2002.
- [5] D.M. Kienzle, M.C. Elder, D. Tyree and J. Edwards-Hewitt, *Security Patterns Repository Version 1.0*, 2002.

- [6] J. Jürjens, *UMLsec: Extending UML for Secure Systems Development*, Springer-Verlag, 2002.
- [7] J. Jürjens, *Secure Systems Development with UML*, Springer-Verlag, 2003.
- [8] C. Kiattisak and P. Nakornthip. UMLsec-SP: An Extension of UMLsec for System Security Modeling based on Security Patterns. Proceedings of JCSSE2009, Thailand, May 13-15, 2009.
- [9] E.B. Fernandez, *Metadata and authorization patterns*, 2000.
- [10] J. Dong, S. Yang and K. Zhang, *Visualizing Design Patterns in Their Applications and Composition*, IEEE Transactions on software engineering, 2007. 33(7): p. 433-453.
- [11] G. Booch, J. Rumbaugh, I. Jacobson, *The Unified Modeling Language Reference Manual*, United State of America, Addison-Wesley, 2nd ed., 2004.
- [12] K. Hamilton and R. Miles, *Learning UML 2.0*, O'Reilly, 2006.
- [13] Object Management Group, *UML 2.0 OCL Specification* [Computer file], Available from: <http://www.omg.org> [2009, March 27].



ศ. นครทิพย์ พร้อมพล สำเร็จการศึกษาในระดับปริญญาโท สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ จาก George Washington University ปัจจุบันเป็นอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย มีความสนใจทางด้าน Software Engineering, Software Requirement Engineering, Software Process



นายณพล วงศ์ไชยกุล สำเร็จการศึกษาในระดับปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ จากคณะวิทยาศาสตร์ เทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ปัจจุบันกำลังศึกษาต่อในระดับปริญญาโท ณ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย มีความสนใจทางด้าน Software Engineering, Security Patterns

## ประวัติผู้เขียนวิทยานิพนธ์

นายอิทธิพัทธ์ วงศ์ไชยกุล เกิดวันที่ 7 เมษายน พ.ศ. 2528 สำเร็จการศึกษาระดับปริญญาวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2549 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2550 ที่อยู่ปัจจุบันที่สามารถติดต่อได้คือ 42/706 หมู่บ้านจามจรี ถนนกิ่งแก้ว ตำบลราชาเทวะ อำเภอบางพลี จังหวัดสมุทรปราการ หมายเลขโทรศัพท์ 081-744-6362 อีเมล kookkai1150@gmail.com



ศูนย์วิทยทรัพยากร  
จุฬาลงกรณ์มหาวิทยาลัย