แนวปฏิบัติด้านมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของอุปกรณ์ที่ใช้ในโครงข่ายโทรศัพท์เคลื่อนที่เทคโนโลยี 5G (5G Cybersecurity Guideline)

กสทช.
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์
และกิจการโทรคมนาคมแห่งชาติ

จัดทำโดย
สำนักกำกับดูแลกิจการโทรคมนาคม
สำนักงาน กสทช.
โทรศัพท์ 02 670 8888
อีเมล saraban_2406@nbtc.go.th

ฉบับเลขาธิการ กสทช. เห็นชอบเมื่อวันที่ 21 ธันวาคม 2566

1. บทนำ

เทคโนโลยีด้านการสื่อสารโทรคมนาคมได้มีการพัฒนาอย่างต่อเนื่อง โดยปัจจุบันประเทศไทยได้มีการให้บริการโทรศัพท์เคลื่อนที่ด้วยเทคโนโลยี 5G ซึ่งเป็นวิวัฒนาการของเทคโนโลยี 3G และ 4G ที่จะสามารถให้บริการประเภทใหม่ ๆ ตัวอย่างเช่น การสื่อสารที่มีความหน่วงต่ำ ความน่าเชื่อถือสูง (Ultra-Reliable Low-Latency Communications : URLLC) จะทำให้รถยนต์แบบไร้คนขับเกิดขึ้นได้ และการสื่อสารที่มีการเชื่อมต่อกับอุปกรณ์จำนวนมาก (Massive Machine-Type Communications : mMTC) จะสนับสนุนการผลิตอัจฉริยะ อย่างไรก็ตาม ถึงแม้เทคโนโลยี 5G จะมุ่งเน้นและให้ความสำคัญกับการรับประกันเกี่ยวกับการคุ้มครองความเป็นส่วนตัวและความมั่นคงปลอดภัยทางไซเบอร์ที่มากขึ้น แต่ก็ยังเผชิญกับปัญหาท้าทายและโอกาสด้านความมั่นคงปลอดภัยที่มาจากบริการ สถาปัตยกรรม และเทคโนโลยีใหม่ ๆ รวมถึงข้อกำหนดด้านความเป็นส่วนตัวและการคุ้มครองผู้ใช้ในระดับที่สูงขึ้น

ผู้ที่เกี่ยวข้องกับการนำเทคโนโลยี 5G ไปใช้งาน โดยเฉพาะผู้ให้บริการซึ่งเป็นเจ้าของโครงข่ายโทรคมนาคม จำเป็นต้องให้ความสำคัญกับการจัดหาหรือนำอุปกรณ์มาใช้ในการให้บริการซึ่งต้องมีมาตรฐานและเทคโนโลยีด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อเป็นหลักประกันที่ดีว่าระบบการให้บริการโทรศัพท์เคลื่อนที่ด้วยเทคโนโลยี 5G จะไม่มีช่องโหว่ที่เสี่ยงต่อการถูกโจมตีทางไซเบอร์

ปัจจุบัน มีอุปกรณ์สื่อสารเทคโนโลยี 5G ให้ผู้ให้บริการโทรศัพท์เคลื่อนที่ได้เลือกนำมาใช้ในการให้บริการอยู่อย่างหลากหลาย โดยแต่ละประเภทอุปกรณ์จะผ่านข้อกำหนดมาตรฐานด้านความปลอดภัยทางไซเบอร์ที่แตกต่างกัน ทำให้การเลือกอุปกรณ์ของผู้ให้บริการโทรศัพท์เคลื่อนที่เทคโนโลยี 5G จำเป็นต้องดำเนินการด้วยความรอบคอบและคำนึงถึงผลกระทบและความเสี่ยงที่ระบบโครงข่ายโทรศัพท์เคลื่อนที่ของตนเองจะถูกโจมตีทางไซเบอร์ ทั้งนี้ ข้อเสนอแนะต่อกรอบมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์นี้ได้พิจารณาจากเอกสารของวิทยาลัยนวัตรกรรม มหาวิทยาลัยธรรมศาสตร์ เรื่อง “กรอบข้อกำหนดมาตรฐานความปลอดภัยสำหรับอุปกรณ์โทรคมนาคม NESAS – Network Equipment Security Assurance Scheme ในระบบ 5G” และเอกสาร “แนวปฏิบัติด้านมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของอุปกรณ์ที่ใช้ในโครงข่ายโทรศัพท์เคลื่อนที่เทคโนโลยี 5G (5G Cybersecurity Guideline)” เป็นเอกสารอ้างอิง

2. ขอบเขต

แนวทางปฏิบัติด้านมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบ 5G นี้ เป็นข้อเสนอแนะเพื่อให้ผู้ให้บริการโทรศัพท์เคลื่อนที่ใช้เป็นแนวทางในการจัดหาหรือนำอุปกรณ์โครงข่ายโทรคมนาคมมาใช้เพื่อให้บริการโทรศัพท์เคลื่อนที่ด้วยเทคโนโลยี 5G ในประเทศไทย ซึ่งเป็นข้อเสนอแนะที่กำหนดไว้เฉพาะด้านความมั่นคงปลอดภัยทางไซเบอร์เท่านั้น

3. ข้อกำหนดมาตรฐานด้านความปลอดภัยทางไซเบอร์สำหรับอุปกรณ์

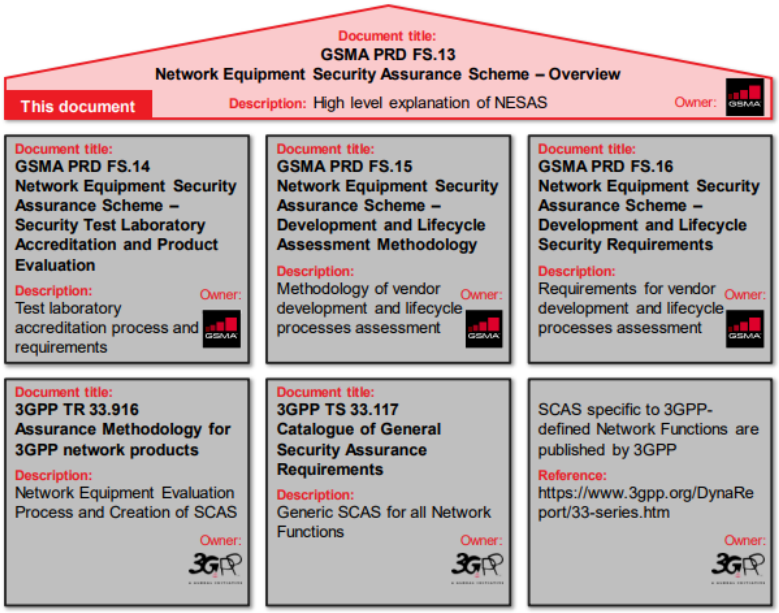
การสร้างความปลอดภัยทางไซเบอร์ในระบบโครงข่ายโทรศัพท์เคลื่อนที่เทคโนโลยี 5G ต้องคำนึงถึงถึงในทุกมิติ ตั้งแต่การพัฒนาเทคโนโลยี การออกแบบและผลิตอุปกรณ์ และการบริหารจัดการระบบ ซึ่งในเอกสารฉบับนี้ มุ่งเน้นไปที่การกำหนดกรอบมาตรฐานด้านความปลอดภัยทางไซเบอร์ในระบบโครงข่ายโทรศัพท์เคลื่อนที่เทคโนโลยี 5G โดยอ้างอิงจากการดำเนินการของสมาคม GSMA (The GSM Association) ซึ่งเป็นหน่วยงานที่รับผิดชอบในการดำเนินการประเมินและตรวจสอบผู้ผลิตอุปกรณ์

ผ่านองค์กรและหน่วยงานที่เชี่ยวชาญด้านการประเมินและตรวจสอบด้านความปลอดภัย โดยสมาคม GSMA และมีสมาคม 3GPP (The 3rd Generation Partnership Project) เป็นหน่วยงานรับผิดชอบในการกำหนดมาตรฐานความปลอดภัยและข้อกำหนดการประเมินและตรวจสอบ

สมาคม GSMA และสมาคม 3GPP ได้ร่วมมือกันเพื่อกำหนดกรอบข้อกำหนดด้านมาตรฐานความปลอดภัยสำหรับอุปกรณ์โทรคมนาคมที่ใช้ในโครงข่ายโทรศัพท์เคลื่อนที่เทคโนโลยี 5G หรือ Network Equipment Security Assurance Scheme : NESAS โดยกรอบข้อกำหนดนี้ เป็นการสร้างมาตรฐานด้านการดูแลและรักษาความปลอดภัยในการใช้เทคโนโลยี 5G และปัจจุบันกรอบข้อกำหนดดังกล่าวได้รับการยอมรับอย่างกว้างขวางในฐานะมาตรฐานกลางจากผู้ให้บริการโครงข่ายและผู้ผลิตอุปกรณ์ เช่น Huawei Technologies Co.,Ltd/ Nokia Ericson/ ZTE Corporation/ Samsung Electronics Co.,Ltd ดังนั้นในการกำหนดกรอบมาตรฐานด้านความปลอดภัยทางไซเบอร์สำหรับอุปกรณ์ที่ใช้ในโครงข่ายโทรศัพท์เคลื่อนที่เทคโนโลยี 5G ที่ได้แนะนำตามเอกสารฉบับนี้ จะใช้กรอบข้อกำหนดด้านมาตรฐานที่ NESAS ได้กำหนดไว้เป็นแนวทางให้ผู้ให้บริการโทรศัพท์เคลื่อนที่ใช้พิจารณาในการจัดหาหรือนำอุปกรณ์มาใช้ในการให้บริการ

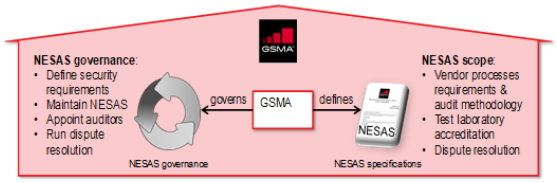
ข้อกำหนดกรอบมาตรฐานของ NESAS คลอบคลุมถึงข้อกำหนดด้านมาตรฐานความปลอดภัยและการประเมินตรวจสอบคุณภาพและคุณลักษณะของอุปกรณ์โทรคมนาคมตั้งแต่ขั้นตอนการออกแบบ การผลิต และการทดสอบอุปกรณ์ ซึ่งทุกขั้นตอนจะต้องเป็นไปตามข้อกำหนดของสมาคม GSMA และสมาคม 3GPP เช่น

- เอกสารสมาพันธ์ GSMAFS14 (GSMAdocument FS.14)
- เอกสารสมาพันธ์ GSMAFS15 (GSMAdocument FS.15)
- เอกสารสมาพันธ์GSMAFS16 (GSMA document FS.16)
- เอกสารจากสมาคม 3GPP ในส่วนขั้นตอนและกระบวนทดสอบด้านเทคนิค



นอกจากนั้น กรอบข้อกำหนดมาตรฐานของ NESAS ยังมีในเรื่องอื่น ๆ อีก ได้แก่

- กระบวนการตรวจสอบและประเมินด้านกระบวนการ ซึ่งเป็นกระบวนการที่กำหนดให้ผู้ผลิตต้อมีการกำหนดมาตรการและขั้นตอนในวงจรชีวิตของผลิตภัณฑ์ตามหรอบข้อกำหนดของ NESAS โดยหน่วยงานที่จะเป็นผู้ตรวจสอบและประเมินจะต้องเป็นหน่วยงานที่สมาคม GSMA เป็นผู้คัดเลือก
- การทดสอบและการประเมินอุปกรณ์ที่ใช้ในโครงข่าย 5G ซึ่งจะเป็นกระบวนการที่กำหนดให้ผู้ผลิตต้องส่งมอบอุปกรณ์ให้ผ่านการทดสอบแล้วให้กับหน่วยงานทดสอบที่ได้รับการรับรองจาก NESAS และต้องผ่านการรับรอง ISO17025 เพื่อทำการทดสอบด้วยข้อกำหนด 3GPP SCASes



Part 1 (NESAS)	Part 2 (SCAS)
(FS.xx series) Standards developed by GSMA SECAG	(TS 33.xx series) Standards developed by 3GPP SA3
Audit vendor's security development process & product lifecycle management process to ensure the product is securely developed	***Evaluate*** vendor's specific product (like eNB, gNB, AMF, UPF, etc.) to ensure the equipment is secure
By ***Independent Audit Team*** accredited by GSMA	By ***ISO17025 accredited lab***
21 requirements contained	100+ cases depend on products (being extended)
Output audit report	Output evaluation report

4. ข้อเสนอแนะต่อการเลือกอุปกรณ์ที่ได้รับการรับรองมาตรฐานด้านความปลอดภัยทางไซเบอร์

การจัดหาหรือนำอุปกรณ์ที่จะใช้ในโครงข่ายโทรศัพท์เคลื่อนที่เทคโนโลยี 5G ควรพิจารณาจากอุปกรณ์ที่ผ่านการรับรองมาตรฐานด้านความปลอดภัยทางไซเบอร์เป็นปัจจัยสำคัญอีกประการหนึ่ง ซึ่งในปัจจุบัน ระบบโครงข่ายโทรศัพท์เคลื่อนที่ ซึ่งมีฐานข้อมูลส่วนบุคคลของผู้ใช้บริการจำนวนมาก ทำให้ตกเป็นเป้าในการโจมตีทางไซเบอร์ได้ ดังนั้น การเลือกใช้อุปกรณ์ในการให้บริการจึงมีความสำคัญเป็นอย่างยิ่ง ดังนั้น เอกสารแนวปฏิบัติด้านมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของอุปกรณ์ที่ใช้ในโครงข่ายโทรศัพท์เคลื่อนที่เทคโนโลยี 5G (5G Security Guideline) ฉบับนี้ จึงเป็นข้อเสนอแนะสำหรับผู้ให้บริการโทรศัพท์เคลื่อนที่ทุกรายได้ตระหนักและให้ความสำคัญกับการเลือกใช้อุปกรณ์ โดยได้ยกตัวอย่างกรอบข้อกำหนดมาตรฐานของ NESAS ซึ่งมีความเข้มข้นในทุกกระบวนการเพื่อรับประกันว่าอุปกรณ์ที่ผ่านมาตรฐานจะไม่เป็นช่องโหว่ให้เกิดการโจมตี

ทางไซเบอร์ได้โดยง่าย อย่างไรก็ตาม ผู้ให้บริการโทรศัพท์เคลื่อนที่สามารถเลือกใช้กรอบข้อกำหนดมาตรฐานอื่นได้ หากมีการควบคุมและดูแลการผลิตอุปกรณ์ตั้งแต่กระบวนการออกแบบ การพัฒนา การทดสอบและประเมิน ที่สอดคล้องไปในแนวทางเดียวกันกับข้อกำหนดมาตรฐานของ NESAS และหน่วยงานที่ทดสอบและประเมิน การผลิตอุปกรณ์จะต้องผ่านการรับรองจากสมาคม GSMA และ 3GPP

เอกสารเผยแพร่ เรื่อง มาตรฐานความมั่นคงปลอดภัยของระบบ 5G ในประเทศไทย (5G Cybersecurity)

จัดทำโดย
สำนักกำกับดูแลกิจการโทรคมนาคม
สำนักงาน กสทช.
โทรศัพท์ 02 670 8888
อีเมล saraban_2406@nbtc.go.th

ฉบับเลขาธิการ กสทช. เห็นชอบเมื่อวันที่ 21 ธันวาคม 2566

สารบัญ

1. บทนำ 3
2. ขอบเขต 3
3. เอกสารอ้างอิง 3
4. ตัวย่อ 3
5. ระบบเกี่ยวกับ 5G 5
5.1 บริการ สถาปัตยกรรม และเทคโนโลยีใหม่ระบบ 5G 8
5.2 การทำงานร่วมกันหลายฝ่ายและความรับผิดชอบร่วมกันสำหรับความมั่นคงปลอดภัยของระบบ 5G 9
6. ความคืบหน้าในการกำหนดมาตรฐานระบบ 5G 10
7. บทนำ NESAS 11
8. ฐานความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบ 5G ของ GSMA 14
9. ข้อกำหนดทางด้านเทคนิค 17
9.1 The GSMA publishes the following documents 18
9.2 3GPP publishes the following Security Assurance Specification (SCAS) documents 19
ภาคผนวก A การพัฒนาและการใช้ NESAS ทั่วโลก 20
ภาคผนวก B เอกสารอ้างอิง 25

1. บทนำ

แนวทางปฏิบัติด้านมาตรฐานด้านความมั่นคงปลอดภัยของระบบ 5G นี้พัฒนาขึ้นเพื่อวัตถุประสงค์ในการรับรองอุปกรณ์สื่อสารภายใต้แผนการทดสอบความมั่นคงปลอดภัยของอุปกรณ์โครงข่าย (Network Equipment Security Assurance Scheme : NESAS)

แนวทางปฏิบัติด้านมาตรฐานด้านความมั่นคงปลอดภัยของระบบ 5G นี้จะยังคงมีผลใช้ได้และมีผลบังคับใช้ต่อไปจนกว่าจะมีการทบทวนหรือยกเลิก

2. ขอบเขต

แนวทางปฏิบัติด้านมาตรฐานด้านความมั่นคงปลอดภัยของระบบ 5G นี้ระบุข้อกำหนดขั้นต่ำสำหรับสถานีฐานและโครงข่ายหลักที่มีไว้สำหรับใช้ในระบบโทรคมนาคมเคลื่อนที่ IMT-2020 ในประเทศไทย

3. เอกสารอ้างอิง

เอกสารอ้างอิงต่อไปนี้เป็นสิ่งที่จำเป็นอย่างยิ่งสำหรับการใช้แนวทางปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัยของระบบ 5G นี้ สำหรับการอ้างอิงที่ลงวันที่ จะใช้เฉพาะฉบับที่อ้างถึงเท่านั้น สำหรับการอ้างอิงที่ไม่ได้ลงวันที่ จะใช้เอกสารอ้างอิงฉบับล่าสุด (รวมถึงการแก้ไขใด ๆ) ดูภาคผนวก B

4. ตัวย่อ

GSMA	Global System Mobile Association / สมาคม GSM หมายเหตุ: GSMA เป็นตัวแทนผลประโยชน์ของผู้ให้บริการโทรศัพท์เคลื่อนที่ทั่วโลก โดยรวมผู้ให้บริการมากกว่า 800 รายกับบริษัทเกือบ 400 แห่งใน 200 ประเทศ เป็นองค์กรอุตสาหกรรมที่เป็นตัวแทนผลประโยชน์ของผู้ให้บริการโครงข่ายโทรศัพท์เคลื่อนที่ทั่วโลก
3GPP	โครงการสัมพันธภาพระหว่างคู่ค้าในยุคที่ 3 (3rd Generation Partnership Project – 3GPP) หมายเหตุ: โครงการสัมพันธภาพระหว่างคู่ค้าในยุคที่ 3 (3GPP) เป็นคำที่ให้ความหมายครอบคลุมในวงกว้างสำหรับองค์กรมาตรฐานหลายแห่งที่พัฒนาเกณฑ์วิธีสำหรับการสื่อสารโทรคมนาคมเคลื่อนที่
ITU	สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union)
IMT-2020	มาตรฐานสำหรับการสื่อสารวิทยุและโทรคมนาคมระหว่างประเทศ ปี ค.ศ. 2020 (International Mobile Telecommunications-2020) หมายเหตุ: มาตรฐานสำหรับการสื่อสารวิทยุและโทรคมนาคมระหว่างประเทศ ปี ค.ศ. 2020 (มาตรฐาน IMT-2020) เป็นข้อกำหนดต่าง ๆ ที่ ITU ภาคการสื่อสารวิทยุ

	(Radiocommunication Sector : ITU-R) ของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU) ออกในปี ค.ศ. 2015 สำหรับโครงข่าย อุปกรณ์ และบริการระบบ 5G
NESAS	แผนการทดสอบความมั่นคงปลอดภัยของอุปกรณ์โครงข่าย (Network Equipment Security Assurance Scheme : NESAS)
SCAS	ข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัย (Security Assurance Specifications)
AMF	ฟังก์ชันการบริหารจัดการการเข้าถึงและการเคลื่อนที่ (Access and Mobility Management Function)
AUSF	ฟังก์ชันเซิร์ฟเวอร์การยืนยันตัวตน (Authentication Server Function)
CAB	หน่วยงานประเมินความสอดคล้อง (Conformity Assessment Body)
CB	หน่วยรับรอง (Certification Body)
CSA	พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Act)
CVE	ช่องโหว่และการรับความเสี่ยงทั่วไป (Common Vulnerability and Exposures)
ECCG	กลุ่มประสานงานความมั่นคงปลอดภัยทางไซเบอร์แห่งยุโรป (European Cybersecurity Coordination Group)
EfA	องค์ประกอบสำหรับการประเมิน (Elements for Assessment)
ENISA	องค์การสหภาพยุโรปเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (European Union Agency for Cybersecurity)
MNO	ผู้ให้บริการโครงข่ายมือถือ (Mobile Network Operator)
NAB	หน่วยรับรองระบบแห่งชาติ (National Accreditation Body)
NCCA	ผู้มีอำนาจในการรับรองความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ (National Cybersecurity Certification Authority)
NESAS CCS	แผนการรับรองความมั่นคงปลอดภัยทางไซเบอร์ของ NESAS (NESAS Cybersecurity Certification Scheme)
NEF	ฟังก์ชันการรับความเสี่ยงของโครงข่าย (Network Exposure Function)
NRF	ฟังก์ชันที่เก็บข้อมูลโครงข่าย (Network Repository Function)
NP	ผลิตภัณฑ์โครงข่าย (Network Product)
PRD	เอกสารอ้างอิงถาวร (Permanent Reference Document)
PuE	สินค้าอยู่ระหว่างการประเมิน (Product under Evaluation)

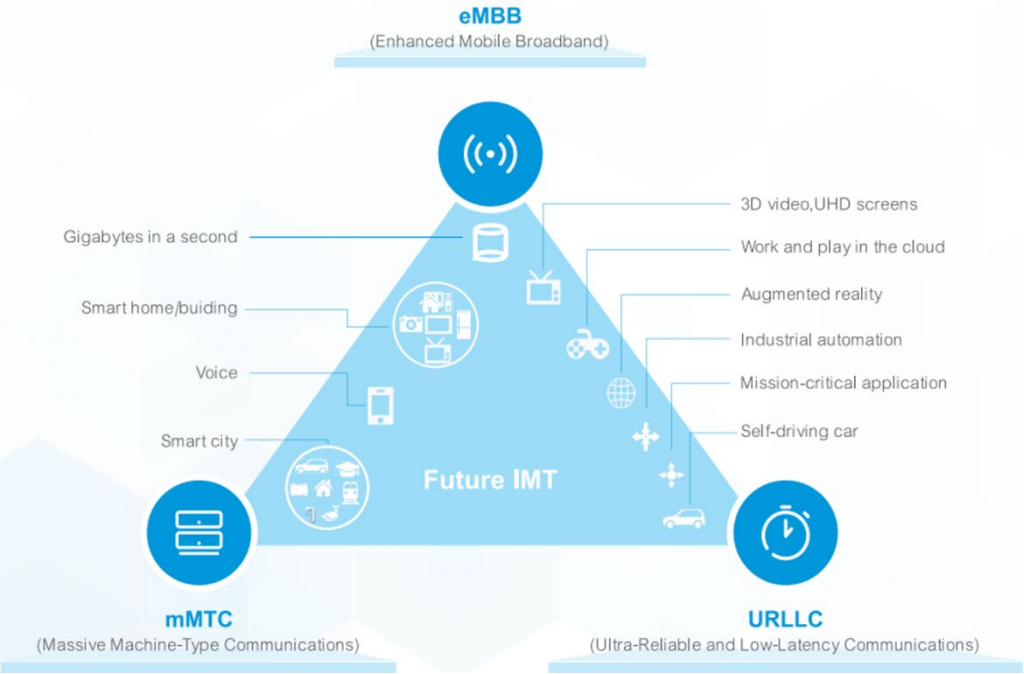
SD	เอกสารประกอบ (Supporting Document)
SECAG	กลุ่มรับประกันความมั่นคงปลอดภัย (Security Assurance Group)
SEPP	พร็อกซีการป้องกันเอดจ์ความมั่นคงปลอดภัย (Security Edge Protection Proxy)
SMF	ฟังก์ชันการบริหารจัดการเซสชัน (Session Management Function)
TL	ห้องปฏิบัติการทดสอบ (Testing Laboratory)
ToR	ขอบเขตของงาน (Terms of Reference)
UDM	การบริหารจัดการข้อมูลเบ็ดเสร็จในที่เดียว (Unified Data Management)
UPF	ฟังก์ชันส่วนข้อมูลผู้ใช้ (User Plane Function)

5. ระบบเกี่ยวกับ 5G

เมื่อบริการบรอดแบนด์เคลื่อนที่ (Mobile Broadband) เริ่มเข้าถึงทั่วทุกมุมโลก ความปรารถนาของผู้คนที่จะเปิดเผยแบบพิมพ์เขียวของโลกที่เชื่อมต่ออย่างเต็มรูปแบบที่กำลังจะมาถึงจะเพิ่มมากขึ้น ในยุคที่ทุกสิ่งจะเชื่อมต่อผ่านบริการบรอดแบนด์เคลื่อนที่ โครงข่ายระบบ 5G ต้องตอบสนองข้อกำหนดของการเชื่อมต่อที่ไม่เคยมีมาก่อนในสถานการณ์สามแบบดังนี้

- Enhanced Mobile Broadband (eMBB) คือ การใช้งานในลักษณะที่ต้องการการส่งข้อมูลความเร็วสูงในระดับกิกะบิตต่อวินาที (Gbps) ซึ่งการใช้งานลักษณะนี้ตอบสนองความต้องการการส่ง และรับข้อมูลที่มากขึ้นเรื่อย ๆ เน้นที่บริการต่าง ๆ ที่ต้องใช้แบนด์วิดท์สูงเป็นพิเศษ เช่น วิดีโอความละเอียดสูง (4K/8K) ความจริงเสมือน (Virtual Reality : VR) และความเป็นจริงเสริม (Augmented Reality : AR) ซึ่งตอบสนองความต้องการชีวิตดิจิทัลของผู้ใช้
- Massive Machine-Type Communications (mMTC) คือ การใช้งานที่มีการเชื่อมต่อของอุปกรณ์จำนวนมากในพื้นที่เดียวกัน โดยมีปริมาณมากถึงระดับล้านอุปกรณ์ต่อตารางกิโลเมตร โดยการส่งข้อมูลของอุปกรณ์ในการใช้งานลักษณะนี้ จะเป็นการส่งข้อมูลปริมาณน้อย ๆ ที่ไม่ต้องการความเร็วสูง หรือความหน่วงเวลาต่ำ อุปกรณ์โดยทั่วไปมีราคาถูกและมีอายุการใช้งานของแบตเตอรี่ที่มากกว่าอุปกรณ์ทั่วไป ซึ่งความสามารถนี้ทำให้ระบบ 5G เหมาะสมกับการทำงานของอุปกรณ์จำพวก IoT
- Ultra-Reliable and Low-Latency Communications (URLLC) คือ การใช้งานที่ต้องการ ความสามารถในการส่งข้อมูลที่มีความเสถียรมาก รวมทั้งมีความหน่วงเวลา (Latency) หรือความหน่วงในการส่งข้อมูลต่ำในระดับ 1 มิลลิวินาที (ระบบ 4G ในปัจจุบันรองรับความหน่วงเวลาในระดับ 10 มิลลิวินาที) ซึ่งความสามารถนี้ทำให้ระบบ 5G เหมาะกับการใช้งานระบบที่ต้องการความแม่นยำสูง (Critical Application) เช่น

การผ่าตัดทางไกล การควบคุมเครื่องจักรในโรงงาน หรือการควบคุมรถยนต์ไร้คนขับ เป็นต้น



ICT มีบทบาทช่วยประเทศต่าง ๆ ในการปฏิรูปเป็นเศรษฐกิจดิจิทัล มีประเทศสมาชิก UN จำนวน 156 ประเทศ จากทั้งหมด 194 ประเทศ ได้เผยแพร่แผนแม่บทการพัฒนา ICT หรือแผนบรอดแบนด์แห่งชาติ (ที่มา: ITU 2017) ซึ่งการลงทุนด้าน ICT ที่เพิ่มขึ้น 20% จะผลักดันให้ GDP เติบโตขึ้น 1% (ที่มา: Boston Consulting Group)

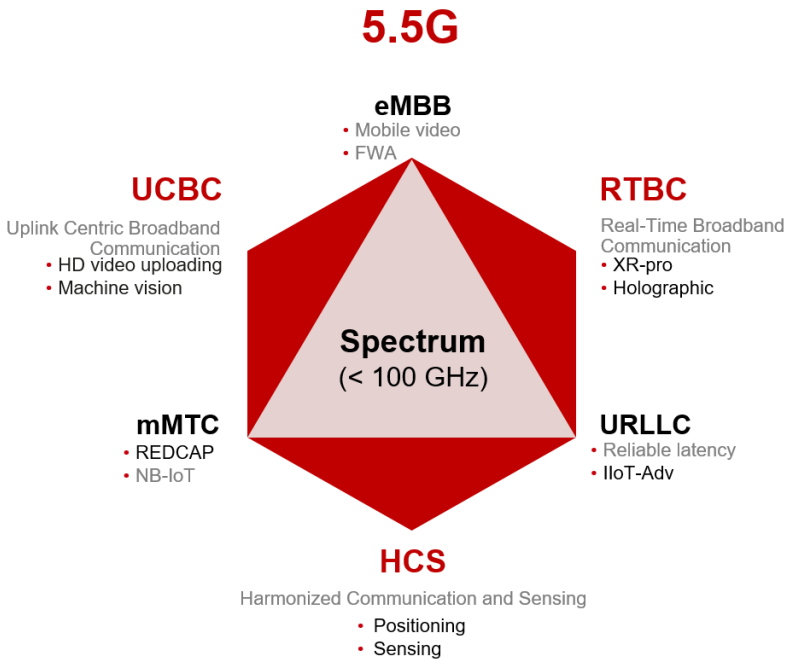
มูลค่าทางสังคมและเศรษฐกิจของ 5G แยกตามสถานการณ์ ดังนี้

- คาดว่า eMBB: AR/VR จะสร้างตลาดขนาดใหญ่ที่มีมูลค่า US$110,000 ล้านเหรียญ เมื่อเทียบกับตลาดทีวีขนาดเล็กซึ่งอยู่ที่ US$ 99,000 ล้านเหรียญ (ที่มา: รายงาน AR&VR โดย Goldman Sachs) เพื่อตอบสนองความต้องการวิดีโอ (วิดีโอความละเอียดสูง 4K/8K) และวิถีชีวิตดิจิทัล โดยมีครัวเรือนทั่วโลกจำนวน 1 พันล้านครัวเรือนที่ยังคงไม่สามารถเข้าถึงอินเทอร์เน็ต (ที่มา: ITU 2015 ICT Facts) การเข้าถึงแบบไร้สายระบบ 5G จะมีบทบาทที่สำคัญอย่างยิ่งใน "ระยะสุดท้าย" ของกลยุทธ์บรอดแบนด์ภายในบ้านและกลยุทธ์บรอดแบนด์แห่งชาติ
- mMTC: การผลิตอัจฉริยะที่รองรับ 5G จะมีมูลค่า US$ 3.4 ล้านล้านเหรียญในปี ค.ศ. 2035 (ที่มา: IHS The 5G Economy Report, 2017)
- uRLLC: ตลาดรถยนต์ไร้คนขับ/ช่วยขับขี่ทั่วโลกจะสร้างมูลค่าทางเศรษฐกิจถึง US$ 1 ล้านล้านเหรียญต่อปี (Rocky Mountain Institute 2016) โดยประหยัดน้ำมันได้ 3.1 พันล้านแกลลอน (ที่มา: Texas Transportation Institute Urban Mobility Report, 2015) และพนักงาน 12 ล้านคน (ที่มา: Global Status Report on Road Safety, World Health Organization, 2015)

เพื่อตอบสนองข้อกำหนดที่เพิ่มขึ้นสำหรับประสบการณ์และแอพพลิเคชันใหม่ ๆ จึงต้องปรับปรุงและขยายสถานการณ์จำลองระบบ 5G ผู้จำหน่าย ICT นำเสนอวิสัยทัศน์ของอุตสาหกรรม 5.5G และกำหนดสถานการณ์จำลองใหม่ 3 สถานการณ์ที่ปรับปรุงสถานการณ์จำลองระบบ 5G มาตรฐาน 3 สถานการณ์ ซึ่งทำให้เปลี่ยนจากการสนับสนุนอินเทอร์เน็ตของสรรพสิ่ง (Internet of Everything : IoE) ไปสู่การเชื่อมต่ออัจฉริยะของทุกสิ่ง และสร้างคุณค่าใหม่ ๆ สำหรับการพัฒนาสังคม และการยกระดับอุตสาหกรรม สถานการณ์จำลองใหม่ 3 สถานการณ์มีดังนี้

- Uplink Centric Broadband Communication (UCBC) จะเพิ่มแบนด์วิดท์อัปลิงก์ 10 เท่า ซึ่งเหมาะอย่างยิ่งสำหรับการอัปโหลดปริมาณมากในสถานการณ์จำลองการประกอบและสถานการณ์จำลองการผลิตสำหรับแมชชีนวิชั่นและ IoT บรอดแบนด์ขนาดใหญ่ โดยช่วยเร่งการพัฒนาไปสู่ความเป็นอัจฉริยะ
- Real-Time Broadband Communication (RTBC) รองรับแบนด์วิดท์สูงและเวลาแฝงต่ำ ซึ่งจะทำให้แบนด์วิดท์เพิ่มขึ้น 10 เท่า ณ เวลาแฝงและความน่าเชื่อถือที่กำหนดไว้ โดยมอบประสบการณ์ล้ำลึกในด้านการโต้ตอบระหว่างโลกจริงกับโลกดิจิทัล

การสื่อสารและการตรวจจับที่สอดคล้องกัน (Harmonized Communication and Sensing : HCS) ขยายขอบเขตขีดความสามารถของโครงข่ายเคลื่อนที่ และเปิดใช้งานการระบุตำแหน่งและการตรวจจับระดับเซนติเมตร ซึ่งนำไปใช้กับการบริหารจัดการดิจิทัลภายในอาคาร การขนส่งอัจฉริยะ และสถานการณ์จำลองโดรนในระดับความสูงที่ต่ำ



วิวัฒนาการระบบ 5G ได้ผ่านการนำเสนอวิสัยทัศน์ การกำหนดทิศทางทางเทคนิค และการกำหนดความเร็วมาตรฐาน ขณะนี้อยู่ระหว่างดำเนินการตามแผนปฏิบัติการ

5.1 บริการ สถาปัตยกรรม และเทคโนโลยีใหม่ระบบ 5G จะนำมาซึ่งปัญหาท้าทายด้านความมั่นคงปลอดภัย

โดยทั่วไป ภัยคุกคามและปัญหาท้าทายส่วนใหญ่ที่ความมั่นคงปลอดภัยของระบบ 5G ต้องเผชิญจะเหมือนกับภัยคุกคามและปัญหาท้าทายที่ความมั่นคงปลอดภัยของระบบ 4G ต้องเผชิญ อย่างไรก็ตาม จะต้องพิจารณาถึงปัญหาท้าทายด้านความมั่นคงปลอดภัยที่เกิดจากบริการ สถาปัตยกรรม และเทคโนโลยีใหม่ ๆ ในโครงข่ายระบบ 5G

- ในแง่ของเทคโนโลยีใหม่ มีการใช้เทคโนโลยีคลาวด์และการจำลองเสมือน (Virtualization) อย่างแพร่หลายในโครงข่ายหลักระบบ 5G ซึ่งนำความเสี่ยงด้านความมั่นคงปลอดภัยมาสู่การแบ่งปันทรัพยากรโครงสร้างพื้นฐานและการจำลองเสมือน ในอนาคตจะมีการพิจารณาผลกระทบจากการคำนวณควอนตัมที่มีต่ออัลกอริทึมการเข้ารหัสแบบดั้งเดิมด้วยเพื่อทำให้มั่นใจในความมั่นคงปลอดภัยของโครงข่าย
- ในแง่ของสถาปัตยกรรมใหม่ สถาปัตยกรรมซอฟต์แวร์ระบบ 5G ใหม่และสถาปัตยกรรมการปรับใช้โครงข่ายจะใช้ส่วนต่อประสานและอาณาเขตใหม่ สถาปัตยกรรมที่อิงตามบริการ (Service Based Architecture : SBA) ใหม่และสถาปัตยกรรมการแบ่งส่วนจะปรับให้เข้ากับข้อกำหนดใหม่ด้านความมั่นคงปลอดภัย เช่น การยืนยันตัวตนที่ใช้ SBA การป้องกันความมั่นคงปลอดภัยของการแบ่งส่วน และการบริหารจัดการความเสี่ยงแบบแบ่งหลายส่วนเพื่อป้องกันการโจมตีต่าง ๆ ในการปรับใช้โครงข่ายระบบ 5G จะมีการย้าย UPF บนโครงข่ายหลักออกจากห้องอุปกรณ์ส่วนกลางไปยัง Mobile Edge Computing (MEC) ซึ่งเป็นการใช้อาณาเขตใหม่ การบรรจบกันของการเชื่อมต่อและการคำนวณยังนำมาซึ่งปัญหาท้าทายด้านความมั่นคงปลอดภัยใหม่ ๆ
- ในแง่ของบริการใหม่ โครงข่ายระบบ 5G ช่วยทำให้อุตสาหกรรมแนวดิ่งมีประสิทธิภาพและจะให้ความสามารถในด้านความมั่นคงปลอดภัยที่ดีขึ้นสำหรับแอพพลิเคชันในอุตสาหกรรมเพื่อตอบสนองข้อกำหนดด้านความมั่นคงปลอดภัยของอุตสาหกรรมต่าง ๆ ดังกล่าว

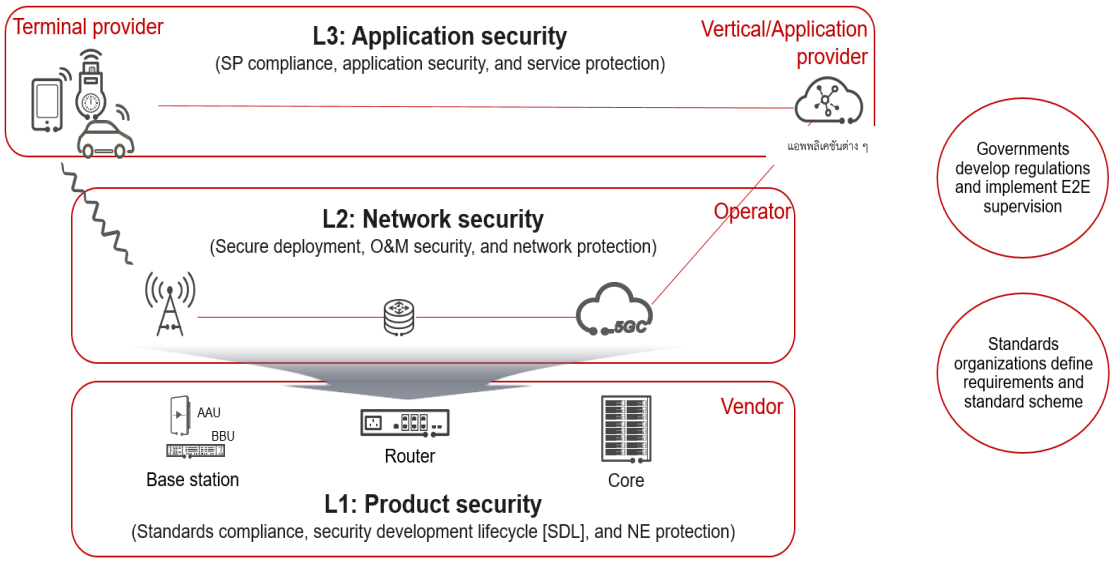
ประวัติศาสตร์พิสูจน์ให้เห็นว่า การมีเทคโนโลยีใหม่ใด ๆ เกิดขึ้น จะมาพร้อมกับปัญหาท้าทายต่าง ๆ และยังพิสูจน์ให้เห็นว่าจะเอาชนะปัญหาท้าทายเหล่านี้ได้ด้วยความพยายามของผู้มีส่วนได้ส่วนเสียทั้งหมด อุตสาหกรรมโดยรวมจะทำงานร่วมกันเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยใหม่ ๆ ที่บริการ สถาปัตยกรรม และเทคโนโลยีระบบ 5G ต้องเผชิญ และจัดการกับปัญหาท้าทายด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้นด้วยมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ระบบ 5G ที่เป็นหนึ่งเดียวทั่วโลก แนวคิดด้านความมั่นคงปลอดภัยทั่วไปของระบบ 5G และหลักปฏิบัติที่ดีที่สุด และ Framework ด้านความมั่นคงปลอดภัยระบบ 5G ที่ตกลงกันไว้ GSMA และ 3GPP ร่วมกันกำหนดแผนการทดสอบความมั่นคงปลอดภัยของอุปกรณ์โครงข่าย (Network Equipment Security Assurance Scheme : NESAS) และข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัย (Security Assurance Specification : SCAS) เพื่อประเมินความมั่นคงปลอดภัยของอุปกรณ์โครงข่ายเคลื่อนที่ ฐานความรู้ด้านความมั่นคงปลอดภัยระบบ 5G ของ GSMA นำเสนอแนวคิดด้านความมั่นคงปลอดภัยที่เป็นความรับผิดชอบร่วมกัน และนำเสนอการควบคุมความมั่นคงปลอดภัยที่ช่วยให้ผู้ให้บริการ (Operator) เข้าใจและพัฒนาสถานะความมั่นคงปลอดภัยของตนเป็นระดับพื้นฐาน

เพื่อทำให้แน่ใจว่า ความมั่นคงปลอดภัยของโครงข่ายระบบ 5G สามารถบริหารจัดการและตรวจสอบได้ หลักการการออกแบบจากบนลงล่างของสถาปัตยกรรมความมั่นคงปลอดภัยระบบ 5G ช่วยทำให้มั่นใจถึง Framework ด้านความมั่นคงปลอดภัยที่เป็นระบบไดนามิก (Dynamic System) และปรับเปลี่ยนได้ เพื่อเพิ่มความยืดหยุ่นทางไซเบอร์อย่างต่อเนื่อง

5.2 การทำงานร่วมกันหลายฝ่ายและความรับผิดชอบร่วมกันสำหรับความมั่นคงปลอดภัยของระบบ 5G

สามารถแบ่งความมั่นคงปลอดภัยทางไซเบอร์ระบบ 5G ออกเป็นสามชั้นจากบนลงล่าง โดยอิงตามรูปแบบความมั่นคงปลอดภัยในอุตสาหกรรมการสื่อสาร ความมั่นคงปลอดภัยของแอพพลิเคชัน ความมั่นคงปลอดภัยของโครงข่าย และความมั่นคงปลอดภัยของ Network Element ความมั่นคงปลอดภัยของแอพพลิเคชัน จะเกี่ยวข้องกับทั้งผู้ใช้มือถือแบบดั้งเดิมและอุตสาหกรรมแนวดิ่งต่าง ๆ ที่ให้หรือใช้แอพพลิเคชันต่าง ๆ ความมั่นคงปลอดภัยของแอพพลิเคชันต้องการการทำงานร่วมกันระหว่างผู้ให้บริการ ผู้ผลิตอุปกรณ์ และผู้ให้บริการแอพพลิเคชัน เพื่อทำให้มั่นใจในความมั่นคงปลอดภัยของโครงข่ายระบบ 5G รวมถึงผู้ใช้และบริการต่าง ๆ ที่พวกเขารองรับ ความมั่นคงปลอดภัยของแอพพลิเคชันไม่ได้ขึ้นอยู่กับความมั่นคงปลอดภัยของท่อโครงข่ายมากนัก อุตสาหกรรมแนวดิ่งต่าง ๆ ต้องรับผิดชอบต่อความมั่นคงปลอดภัยของโซลูชันของตนเอง ปกป้องทรัพย์สินที่สำคัญในชั้นแอพพลิเคชันให้พ้นจากการโจมตีโครงข่าย ตรวจจับภัยคุกคามต่อความมั่นคงปลอดภัยทันที และกู้คืนบริการพื้นฐานอย่างรวดเร็ว ตามปกติ ผู้ให้บริการจะบริหารจัดการและดำเนินงานด้านความมั่นคงปลอดภัยของโครงข่าย โดยจะพิจารณาการปฏิบัติตามข้อกำหนดของโครงข่ายและความมั่นคงปลอดภัยของการออกแบบโครงข่าย การปรับใช้ Operation and Maintenance (O&M) การดำเนินงาน และทำการประเมินความเสี่ยงที่ครอบคลุมและต่อเนื่องโดยอิงตามส่วนประกอบของโครงข่าย ตลอดจนอุปกรณ์และสถาปัตยกรรมโครงข่ายที่ผู้จำหน่ายจัดหาให้เพื่อทำให้แน่ใจว่ามีการบริหารจัดการภัยคุกคามด้านความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ

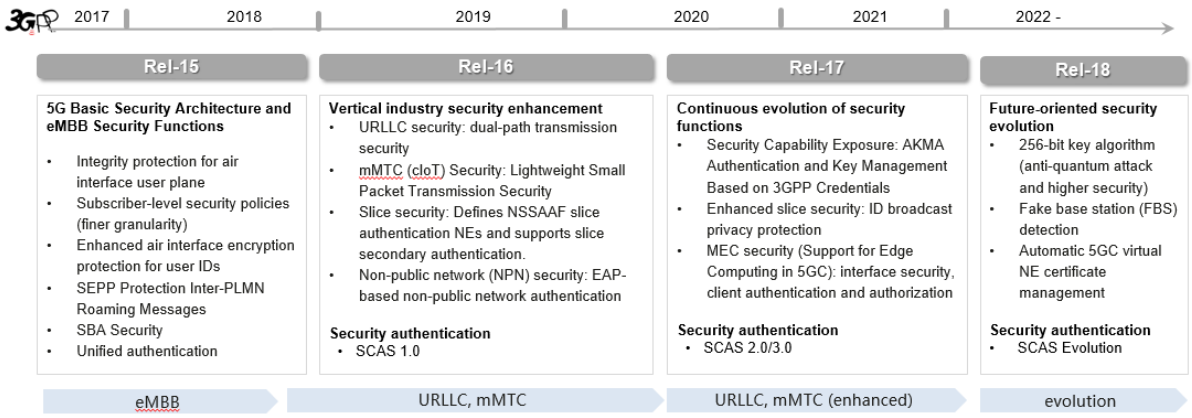
ผู้จำหน่ายอุปกรณ์ต้องจัดให้มีความมั่นคงปลอดภัยของ Network Element โดยเน้นที่การปฏิบัติตามข้อกำหนด กระบวนการพัฒนาที่ปลอดภัย และความสามารถด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ต่าง ๆ การประเมินความมั่นคงปลอดภัยมีความสำคัญต่อความมั่นคงปลอดภัยของ Network Element ซึ่งเป็นพื้นฐานสำหรับการประเมินว่า มีการออกแบบและใช้อุปกรณ์และส่วนประกอบโครงข่ายอย่างสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยหรือไม่ ความมั่นคงปลอดภัยของระบบ 5G เป็นความรับผิดชอบร่วมกันที่เกี่ยวข้องกับ ผู้มีส่วนได้ส่วนเสียที่สำคัญ ได้แก่ ผู้ให้บริการ ผู้ให้บริการการเชื่อมต่อโครงข่าย ผู้จำหน่ายอุปกรณ์ ผู้ให้บริการแอพพลิเคชัน องค์กรมาตรฐาน รัฐบาล และหน่วยงานกำกับดูแล โดยแต่ละฝ่ายมีหน้าที่ความรับผิดชอบที่กำหนดไว้อย่างชัดเจน เมื่อปฏิบัติตามความรับผิดชอบเหล่านี้อย่างสมบูรณ์แล้ว จะทำให้สามารถปรับใช้และดำเนินงานระบบ 5G ในลักษณะที่ปลอดภัย



6. ความคืบหน้าในการกำหนดมาตรฐานระบบ 5G

ระบบ 5G เผชิญกับปัญหาท้าทายและโอกาสด้านความมั่นคงปลอดภัยที่มาจากบริการ สถาปัตยกรรม และเทคโนโลยีใหม่ ๆ รวมถึงข้อกำหนดด้านความเป็นส่วนตัวและการคุ้มครองผู้ใช้ในระดับที่สูงขึ้น อุตสาหกรรมต้องเข้าใจข้อกำหนดต่าง ๆ ของสถานการณ์จำลองที่หลากหลาย และกำหนดมาตรฐานและเทคโนโลยีด้านความมั่นคงปลอดภัยของระบบ 5G ให้ดียิ่งขึ้น เพื่อจัดการกับความเสี่ยงที่เกี่ยวข้องต่าง ๆ

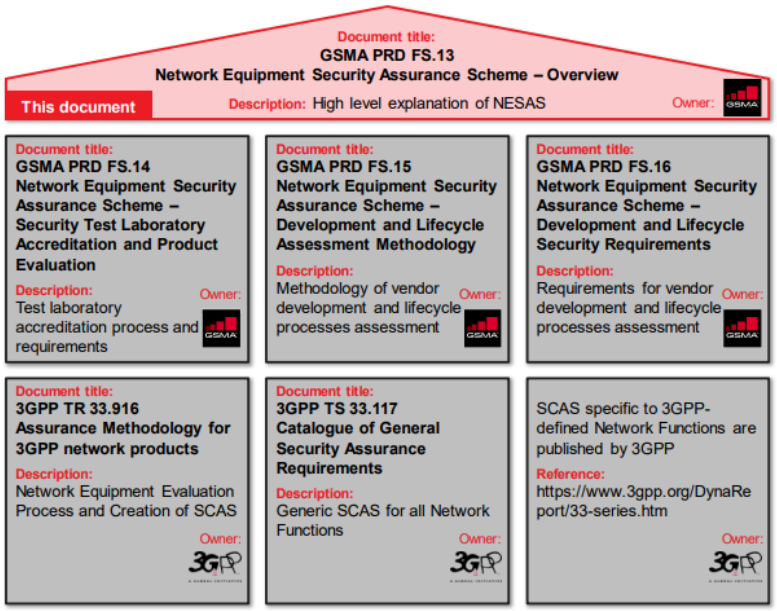
อุตสาหกรรมโดยรวมจะทำงานร่วมกันเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยใหม่ ๆ ที่สถาปัตยกรรม เทคโนโลยี และบริการของระบบ 5G ต้องเผชิญ และจัดการกับปัญหาท้าทายด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้นผ่านมาตรฐานด้านความมั่นคงปลอดภัยระบบ 5G แบบเบ็ดเสร็จ แนวคิดด้านความมั่นคงปลอดภัยของระบบ 5G แบบทั่วไป และ Framework ด้านความมั่นคงปลอดภัยของระบบ 5G ที่ตกลงกันไว้ ในช่วงปี ค.ศ. 2020 มีบริษัท 111 แห่ง (รวมถึงบริษัทในเครือ) จากทั่วโลกได้ส่งผู้เชี่ยวชาญทางเทคนิคเข้าร่วมการประชุม SA3 ทั้งหมดหกครั้ง เพื่อพัฒนามาตรฐานด้านความมั่นคงปลอดภัยของระบบ 5G คณะทำงาน 3GPP SA3 ได้จัดตั้งโครงการทั้งหมด 42 โครงการ เพื่อวิเคราะห์ภัยคุกคามและความเสี่ยงด้านความมั่นคงปลอดภัยในสถานการณ์จำลองระบบ 5G แบบต่าง ๆ ซึ่งค่อย ๆ ร่างข้อสรุปโครงการและนำไปใช้ในมาตรฐานด้านความมั่นคงปลอดภัยต่อไป



7. บทนำ NESAS

ระบบ 5G เป็นวิวัฒนาการของเทคโนโลยี 3G และ 4G ที่จะสามารถให้บริการประเภทใหม่ ๆ ตัวอย่างเช่น การสื่อสารที่มีความหน่วงต่ำ ความน่าเชื่อถือสูง (Ultra-Reliable Low-Latency Communications : URLLC) จะทำให้รถยนต์แบบไร้คนขับเกิดขึ้นได้ และการสื่อสารที่มีการเชื่อมต่อกับอุปกรณ์จำนวนมาก (Massive Machine-Type Communications : mMTC) จะสนับสนุนการผลิตอัจฉริยะ ทั้งนี้ ระหว่างสถาปัตยกรรมโครงข่ายระบบ 5G และ 4G จะไม่มีความแตกต่างขั้นพื้นฐาน โครงข่ายหลักและโครงข่ายการเข้าถึงผ่านการรับส่งทางคลื่นวิทยุ (Radio Access Networks : RAN) ยังคงแยกจากกัน ยิ่งไปกว่านั้น ระบบ 5G ยังให้การรับประกันเกี่ยวกับการคุ้มครองความเป็นส่วนตัวและความมั่นคงปลอดภัยที่เข้มงวดกว่าระบบ 3G หรือ 4G

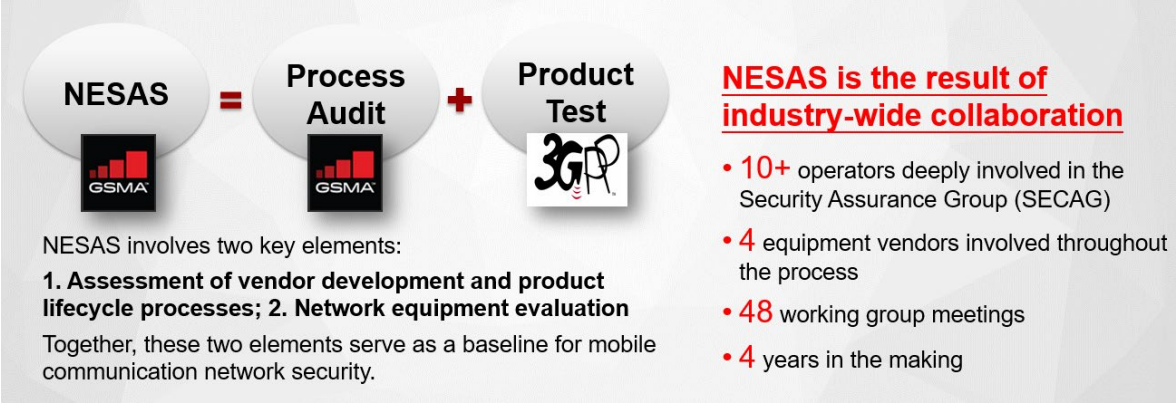
มาตรฐาน 5G ได้สืบทอดมาตรฐานด้านความมั่นคงปลอดภัยของระบบ 4G ที่มีอยู่และปรับปรุงตามมาตรฐานเหล่านี้ ในแง่ของระบบ 5G มีการออกแบบกลไกและมาตรการด้านความมั่นคงปลอดภัยใหม่สำหรับคลาวด์ โมบายล์เอดจ์คอมพิวติ้ง (Mobile Edge Computing : MEC) และการแบ่งส่วนโครงข่าย



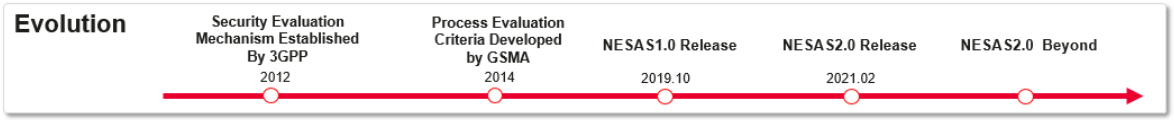
ดูรายละเอียดเพิ่มเติมของ FS.13 ภาพรวม NESAS v.2.0 ได้ที่
https://www.gsma.com/security/network-equipment-security-assurance-scheme/

กลไกการประเมินความมั่นคงปลอดภัยจะปฏิบัติตามมาตรฐานแบบเดียวกันที่เป็นที่ยอมรับกันทั่วโลกเพื่อทำให้แน่ใจว่า การดำเนินการของกลไกเหล่านี้มีความคุ้มค่าและยั่งยืนสำหรับระบบนิเวศ จะมีการใช้ NESAS ที่ GSMA และ 3GPP กำหนดร่วมกันเพื่อประเมินความมั่นคงปลอดภัยของอุปกรณ์โครงข่ายมือถือ โดยให้ Framework ของการรับประกันความมั่นคงปลอดภัยทั่วทั้งอุตสาหกรรมเพื่อปรับปรุงระดับความมั่นคงปลอดภัยในอุตสาหกรรมโทรคมนาคม NESAS กำหนดข้อกำหนดต่าง ๆ ด้านความมั่นคงปลอดภัย และ Framework การประเมินสำหรับการพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัย และกระบวนการแบบวงจรชีวิต และใช้กรณีทดสอบด้านความมั่นคงปลอดภัยในข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัย

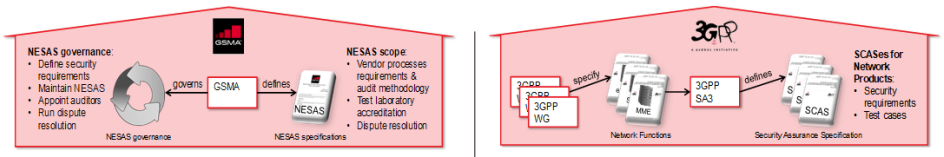
(Security Assurance Specifications : SCAS) ที่ 3GPP กำหนดเพื่อประเมินความมั่นคงปลอดภัยของอุปกรณ์โครงข่าย ปัจจุบัน 3GPP ได้เริ่มการประเมินความมั่นคงปลอดภัยของอุปกรณ์โครงข่ายระบบ 5G หลายรายการ ผู้จำหน่ายอุปกรณ์รายใหญ่ และผู้ให้บริการ ต่างเข้าร่วมในการกำหนดมาตรฐาน NESAS อย่างจริงจัง



GSMA เปิดตัว NESAS 1.0 ในเดือนตุลาคม ค.ศ. 2019 และได้มีการพัฒนา NESAS อย่างต่อเนื่องโดยอิงตามข้อกำหนดต่าง ๆ ของอุตสาหกรรม และต่อมาได้เปิดตัว NESAS 2.0 ในเดือนกุมภาพันธ์ ค.ศ. 2021 ปัจจุบัน มีการสร้างระบบนิเวศของ NESAS เกิดขึ้นแล้ว มีผู้จำหน่ายอุปกรณ์รายใหญ่ได้เข้าร่วมการประเมิน NESAS อย่างจริงจัง โดยที่โครงข่าย Radio Access Network (RAN) และโครงข่ายหลักของ Huawei เป็นรายแรกที่ผ่านการตรวจประเมินและการทดสอบฟังก์ชันความมั่นคงปลอดภัย ซึ่งหน่วยตรวจประเมินในระดับชั้นนำของโลก และห้องปฏิบัติการทดสอบที่มีชื่อเสียงและมีคุณสมบัติเหมาะสมสำหรับการประเมินผู้ให้บริการเทียร์ 1 หลายราย ได้กำหนดให้รวม NESAS อยู่ในเอกสารการประมูลระบบ 5G



NESAS ส่งเสริมความร่วมมือด้านความมั่นคงปลอดภัยและความไว้วางใจซึ่งกันและกันในอุตสาหกรรมการสื่อสารเคลื่อนที่ทั่วโลก และช่วยให้ผู้ให้บริการ ผู้จำหน่ายอุปกรณ์ และผู้มีส่วนได้ส่วนเสียอื่น ๆ ร่วมกันส่งเสริมการสร้างความมั่นคงปลอดภัยของระบบ 5G โดยนำเสนอมาตรฐานการประเมินความมั่นคงปลอดภัยทางไซเบอร์ที่ปรับแต่ง เชื่อถือได้ มีประสิทธิภาพ เป็นหนึ่งเดียว เปิดกว้าง และพัฒนาอย่างต่อเนื่องสำหรับอุตสาหกรรมการสื่อสาร และเป็นข้อมูลอ้างอิงเชิงบวกสำหรับผู้มีส่วนได้ส่วนเสียต่าง ๆ เช่น ผู้ให้บริการ ผู้จำหน่ายอุปกรณ์ และหน่วยงานกำกับดูแลของรัฐบาล



Part 1 (NESAS)	Part 2 (SCAS)
(FS.xx series) Standards developed by GSMA SECAG	(TS 33.xx series) Standards developed by 3GPP SA3
Audit vendor's security development process & product lifecycle management process to ensure the product is securely developed	***Evaluate*** vendor's specific product (like eNB, gNB, AMF, UPF, etc.) to ensure the equipment is secure
By ***Independent Audit Team*** accredited by GSMA	By ***ISO17025 accredited lab***
21 requirements contained	100+ cases depend on products (being extended)
Output audit report	Output evaluation report

NESAS ให้ประโยชน์ต่าง ๆ แก่ผู้จำหน่ายอุปกรณ์ดังนี้

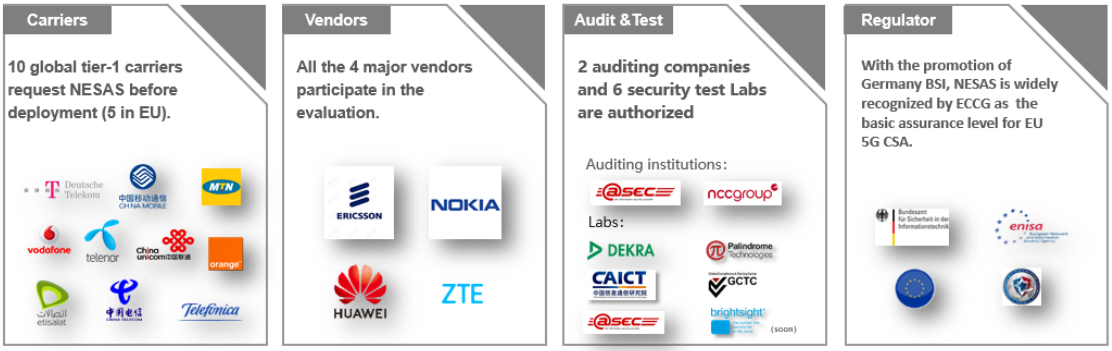
- ให้การรับรองระบบจากหน่วยงานตัวแทนอุตสาหกรรมมือถือระดับชั้นนำของโลก
- นำเสนอการตรวจสอบความมั่นคงปลอดภัยระดับโลกสำหรับกระบวนการที่เกี่ยวข้องกับความมั่นคงปลอดภัย
- เสนอวิธีการแบบเดียวกันในการตรวจสอบความมั่นคงปลอดภัย
- หลีกเลี่ยงการแยกส่วนและข้อกำหนดการรับประกันความมั่นคงปลอดภัยที่อาจขัดแย้งกันในตลาดต่าง ๆ

NESAS ให้ประโยชน์ต่าง ๆ แก่ผู้ให้บริการโทรศัพท์เคลื่อนที่ดังนี้

- กำหนดมาตรฐานด้านความมั่นคงปลอดภัยที่เข้มงวดซึ่งผู้จำหน่ายต้องมีความมุ่งมั่นในระดับสูง
- ให้ความสบายใจว่า ผู้จำหน่ายได้ใช้มาตรการและหลักปฏิบัติด้านความมั่นคงปลอดภัยที่เหมาะสม
- ไม่ต้องใช้เงินและเวลาดำเนินการตรวจประเมินผู้จำหน่ายแต่ละราย

NESAS ให้ประโยชน์ต่าง ๆ แก่หน่วยงานกำกับดูแลดังนี้

- พัฒนาโดยอุตสาหกรรมการสื่อสารเคลื่อนที่โดยรวมเพื่อป้องกันการแยกส่วนของมาตรฐาน
- เปิดเผย ดูแลรักษาโดยอุตสาหกรรม ค่อย ๆ พัฒนาและปรับปรุงอย่างต่อเนื่อง
- คุ้มค่า มีนวัตกรรม มีอุปสรรคในการเข้าสู่ตลาดที่ต่ำ ผลักดันให้เกิดประโยชน์ด้านความมั่นคงปลอดภัย



สำหรับโครงข่ายระบบ 5G นั้น NESAS ได้จัดเตรียมมาตรฐานที่เหมาะสมซึ่งสามารถกำหนดเองเชื่อถือได้ ใช้ได้ทั่วโลก มีประสิทธิภาพ เป็นหนึ่งเดียว เปิดกว้าง และค่อย ๆ พัฒนาอย่างต่อเนื่อง

จนถึงปัจจุบัน ได้มีการสร้างระบบนิเวศแบบสี่ในหนึ่งเดียว (ผู้จำหน่าย สถาบันตรวจประเมิน ห้องปฏิบัติการ และหน่วยงานกำกับดูแล) แล้ว

อุตสาหกรรมจะทำงานร่วมกันเพื่อมีส่วนร่วมเชิงบวกต่อการพัฒนาที่ยั่งยืนในการประเมินความมั่นคงปลอดภัยแบบครบวงจรระดับโลกสำหรับ 5G

8. ฐานความรู้ด้านความมั่นคงปลอดภัยระบบ 5G ของ GSMA

ฐานความรู้ด้านความมั่นคงปลอดภัยของระบบ 5G ที่ครอบคลุมจะช่วยผู้มีส่วนได้ส่วนเสียในการค้นหา ทำแผนที่ และบรรเทาความเสี่ยงต่าง ๆ ในขณะที่ผู้ให้บริการโครงข่ายมือถือ (MNO) ทั่วโลกใช้และเปิดตัวระบบ 5G โครงข่ายการสื่อสารจะเผชิญกับภัยคุกคามและปัญหาท้าทายใหม่ ๆ ในด้านความมั่นคงปลอดภัย การทำความเข้าใจ การทำแผน และการบรรเทาภัยคุกคามต่อความมั่นคงปลอดภัยที่มีอยู่และที่จะเกิดขึ้นในลักษณะที่ตรงเป้าหมาย รวดเร็ว และมีประสิทธิภาพได้กลายเป็นเรื่องที่จำเป็น เพื่อช่วยผู้ให้บริการและฝ่ายอื่น ๆ ในระบบนิเวศของระบบ 5G GSMA ได้ทำการวิเคราะห์ภัยคุกคามที่ครอบคลุมโดยเกี่ยวข้องกับผู้เชี่ยวชาญในอุตสาหกรรมจากทั่วทั้งระบบนิเวศ รวมถึง MNO ผู้จำหน่าย ผู้ให้บริการและหน่วยงานกำกับดูแล ตลอดจนเก็บรวบรวมข้อมูลประกอบจากแหล่งข้อมูลสาธารณะ เช่น 3GPP ENISA และ NIST และทำแผนที่ภัยคุกคามเหล่านี้กับการควบคุมความมั่นคงปลอดภัยที่เหมาะสมและมีประสิทธิภาพ GSMA ได้รวมการวิเคราะห์นี้เข้าในฐานความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบ 5G เพื่อให้แนวทางปฏิบัติที่เป็นประโยชน์เกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยของระบบ 5G และมาตรการบรรเทาต่าง ๆ ฐานความรู้มีจุดมุ่งหมายเพื่อให้สมาชิก GSMA ได้รับความรู้เกี่ยวกับระบบนิเวศของระบบ 5G ที่รวมไว้เพื่อเพิ่มความไว้วางใจในโครงข่ายระบบ 5G และทำให้โลกที่เชื่อมต่อถึงกันมีความมั่นคงปลอดภัยมากที่สุดเท่าที่จะเป็นไปได้ เมื่อเวลาผ่านไป ฐานความรู้จะได้รับการปรับปรุงและขยายเพื่อตอบสนองต่อภูมิทัศน์ด้านภัยคุกคามต่อความมั่นคงปลอดภัยทางไซเบอร์ที่ค่อย ๆ เปลี่ยนแปลงไป

ทำหน้าที่เป็นแนวทางปฏิบัติสำหรับ MNO ในการบริหารจัดการความมั่นคงปลอดภัยของโครงข่ายระบบ 5G

- ความมั่นคงปลอดภัยแบบครบวงจร: NESAS ให้ความมั่นคงปลอดภัยสำหรับอุปกรณ์ Network Element ระบบ 5G และฐานความรู้ด้านความมั่นคงปลอดภัยของระบบ 5G จะให้ความมั่นคงปลอดภัยสำหรับการวางแผน การสร้าง การบำรุงรักษา การเพิ่มประสิทธิภาพ และการดำเนินงานโครงข่ายของผู้ให้บริการ
- แนวทางปฏิบัติ: ผู้ให้บริการสามารถใช้ฐานความรู้ด้านความมั่นคงปลอดภัยของระบบ 5G เป็นข้อมูลอ้างอิงที่สำคัญและเป็นพื้นฐานในการปรับปรุงการรับประกันความมั่นคงปลอดภัยของระบบ 5G
- การทำงานร่วมกันกับทุกฝ่าย: ผู้ให้บริการสามารถร่วมมือกับผู้จำหน่ายอุปกรณ์ ผู้ให้บริการแอพพลิเคชัน และหน่วยงานกำกับดูแลในการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยที่ฐานความรู้กำหนดไว้
- การประเมินความมั่นคงปลอดภัย: ผู้ให้บริการสามารถใช้มาตรการควบคุมความมั่นคงปลอดภัยในฐานความรู้และทำการประเมินโดยอิงตามแบบจำลองวุฒิภาวะด้านความมั่นคงปลอดภัยของ GSMA

ฐานความรู้วิเคราะห์ความเสี่ยงต่าง ๆ วิธีการโจมตี และผลกระทบของโครงข่ายมือถืออย่างครอบคลุม

Comprehensive and structured threat analysis for mobile networks

Fields	Threats
Application	Malicious Applications
	UE Compromising
	Theft of Personal Data
UE	UICC based web browser compromise
	UICC credential theft
RAN	IMSI Catching
	DoS Against Terminal Device
	5G/4G/3G to 2G Downgrade
	DoS Attack Against the Network
	SMS Spam
	Passive Eavesdropping
	Impersonating Calls and Texts
	Active Eavesdropping
	Radio Jamming
	Breaking LTE on Layer 2
	FBS enabled LTE billing compromise
	Privacy Attacks using Side Channel Information
	5G authentication
	LTE Inspector
	IMP4GT: IMPersonation Attacks in 4G NeTworks
	REVOLTE
	Stealthy Location Identification Attack
	GPRS Cryptanalysis Security
	Hijacking TCP Connection under LTE/5G Network

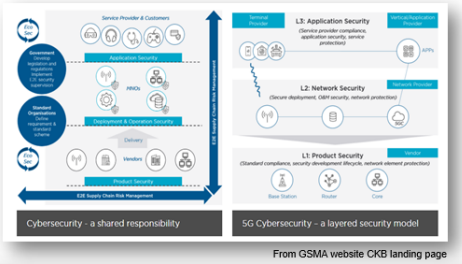
Fields	Threats
Core Network	DoS attack against core network
	Voice call eavesdropping
	Mobile communication monitoring
	NF API Exploitation
	SMS Eavesdropping
	CDR Harvesting
Cloud	Virtual Machine Abuse
	DDoS attacks against MEC
	Abuse of MEC APIs
	Unauthorized Access to the Slice Management Plane
	Network Slice Resource Pre-emption
	Network Slice Data Theft and Tampering
Inter connect	Spoofing Attack for Roaming Interconnections
	Location Data Breach
	Eavesdropping/Tampering the Data on Roaming Interconnections
	HLR Outage
	A2P SMS Re-routing
	SS7 RCE and Tunneling
Network O&M	Identity Theft or Fraud
	Exploitation of network configuration data weakness
	Log Tampering

Detailed attack methods and impact description

CORE-T1: DoS Attack against Core Network	
Threat Description	An attacker initiates (D)DoS attack against the core network through UEs, roaming interfaces, 3rd applications, the internet, base stations, and transport devices that consume network resources and make services unavailable.
Attack Methodology	In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim network originates from many different sources. DDoS messages can be crafted on a laptop connected to the core network of the victim operator and sent over the N1/N32/N9/N6/N2/N3 interfaces. The attacker can send a large amount of signaling and user data messages towards network nodes in a short period of time. These messages can trigger traffic that exceeds the processing capability of network devices. As a result, too many network resources are occupied and unavailable for normal service.
Potential Impact	Normal core network services unavailability is a critical incident that prevents customers accessing or using services at home or while roaming. Impacted customers may contact customer service who could get overwhelmed. In addition, such attacks cause severe reputational loss for networks operator.

ฐานความรู้กำหนดความรับผิดชอบในการบรรเทาความเสี่ยงของผู้มีส่วนได้ส่วนเสีย

GSMA CKB responsibility sharing model



From GSMA website CKB landing page

GSMA CKB points out that 5G cybersecurity is a shared responsibility that involves key stakeholders

- ✓ **Application Security** main responsibility of application developers and service providers
- ✓ **Network Security** commonly managed, controlled and operated by the MNO, but some elements might also be outsourced to specialized service providers.
- ✓ **Product Security** main responsibility of vendors

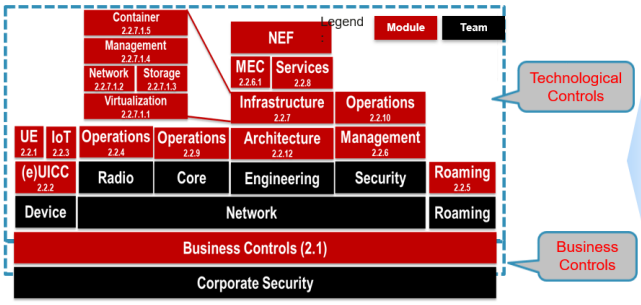
Mitigation measures recommended to stakeholders

CORE-T1: DoS Attack against Core Network		
Mitigation Measures	**Service Provider**	Ensure the security of apps and monitor application server behaviours to prevent hackers from controlling the apps to start DDoS attacks.
	Operator (FS.31 BC-014, RI-001, NO-007, NO-012, NO-013, NO-015, NO-016)	Request NESAS compliance to ensure equipment has a baseline level of security prior to equipment delivery. Deploy anti-DDoS devices between gNodeBs and the core network, and between the core network and the Internet. Deploy security edge protection proxies (SEPPs) and signalling firewalls on the control plane of the core network to filter out attack signalling packets from roaming networks. Enable flow control and DDoS attack pattern packet filtering mechanisms within core network devices.
	Vendor	Provide flow control and DDoS attack pattern packet filtering mechanisms within core network devices and/or anti-DDoS devices. Provide the SEPP function based on 3GPP specifications to filter out abnormal signalling over roaming interfaces.
References	Reuters Staff "Vodafone hit by three-hour mobile network outage in Germany" Reuters. 23 Nov 2020. 3GPP 33.821.	

สำหรับตัวอย่างของ Core-T1 เราจะเห็นมาตรการบรรเทาความเสี่ยงต่าง ๆ ที่แนะนำให้ผู้มีส่วนได้ส่วนเสียทั้งสามประเภทเหล่านี้ สำหรับผู้ให้บริการ ความมั่นคงปลอดภัยของแอพพลิเคชันในอุตสาหกรรมแนวดิ่งจะต้องการการทำงานร่วมกันของหลายฝ่ายเพื่อทำให้แน่ใจว่าแอพพลิเคชัน 5G มีความมั่นคงปลอดภัยแบบครบวงจร โดยไม่ใช่แค่พึ่งพิงความมั่นคงปลอดภัยของโครงข่ายของผู้ให้บริการเท่านั้น สำหรับผู้ให้บริการ ความมั่นคงปลอดภัยของโครงข่ายและความมั่นคงปลอดภัยของ Operation and Maintenance (O&M) เป็นหน้าที่ความรับผิดชอบของผู้ให้บริการ ผู้ให้บริการต่าง ๆ จะวางแผน ออกแบบและปรับใช้อุปกรณ์และความสามารถด้านความมั่นคงปลอดภัยที่ผู้จำหน่ายในโครงข่ายทั้งหมดมอบให้ สำหรับผู้จำหน่ายความมั่นคงปลอดภัยของ Network Element เป็นหน้าที่ความรับผิดชอบของผู้ให้บริการอุปกรณ์เป็นหลัก โดยเน้นที่การปฏิบัติตามข้อกำหนดของผู้จำหน่าย วงจรชีวิตในการพัฒนาที่มั่นคงปลอดภัย

(Secure Development Lifecycle : SDL) และความสามารถในการป้องกันการโจมตีต่อด้านความมั่นคงปลอดภัยของผลิตภัณฑ์

GSMA ให้การควบคุมความมั่นคงปลอดภัยเส้นฐานที่ผู้ให้บริการสัญญาณเคลื่อนที่สามารถพิจารณาปรับใช้ได้

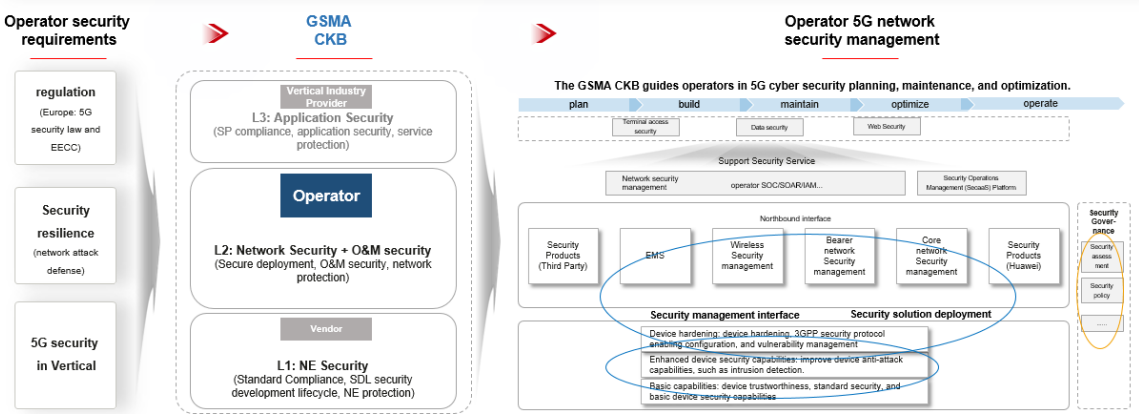


Technological Controls
User Equipment and Mobile Equipment Controls
(e)UICC Management Controls
Internet of Things Controls
Radio Network Controls
Roaming and Interconnect Controls
Core Network Management Controls
Network Operations Controls
Security Operations Controls

No.	Business Controls
BC-001	Board Level Engagement
BC-002	Role formally recognising security
BC-003	Organisational policies
BC-004	GRC (Governance, risk and compliance)
BC-005	Secure by design
BC-006	Data protection/privacy assessment
BC-007	Secure Software Development Life Cycle (SDLC) implemented
BC-008	Business Continuity Management (BCM)
BC-009	Physical security controls (ISMS such as cameras)
BC-010	Procurement controls
BC-011	Outsourcing controls
BC-012	Decommissioning of equipment

ฐานความรู้กำหนดเส้นฐานการควบคุมความมั่นคงปลอดภัยสำหรับการใช้การอ้างอิงโครงข่ายมือถือ ซึ่งจำแนกเป็นการควบคุมธุรกิจและการควบคุมเทคโนโลยี ผู้ให้บริการที่ใช้การควบคุมเหล่านี้สามารถเปรียบเทียบการควบคุมในรายการกับการควบคุมความมั่นคงปลอดภัยภายในที่ปรับใช้ ค้นหาและประเมินช่องว่างที่อาจเกิดขึ้น จากนั้น ตอบสนองต่อช่องว่างที่โดดเด่นภายในองค์กรของตนเอง

ฐานความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบ 5G เป็นสะพานเชื่อมระหว่าง "ข้อกำหนดของผู้ให้บริการเพื่อทำให้มั่นใจว่ามีการปฏิบัติตามระเบียบข้อบังคับ ยกระดับความมั่นคงปลอดภัย/ความยืดหยุ่น และทำให้อุตสาหกรรมแนวดิ่งสามารถสร้างรายได้" และ "การพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยในการวางแผน การก่อสร้าง การบำรุงรักษาการเพิ่มประสิทธิภาพ และการดำเนินงานโครงข่ายระบบ 5G"



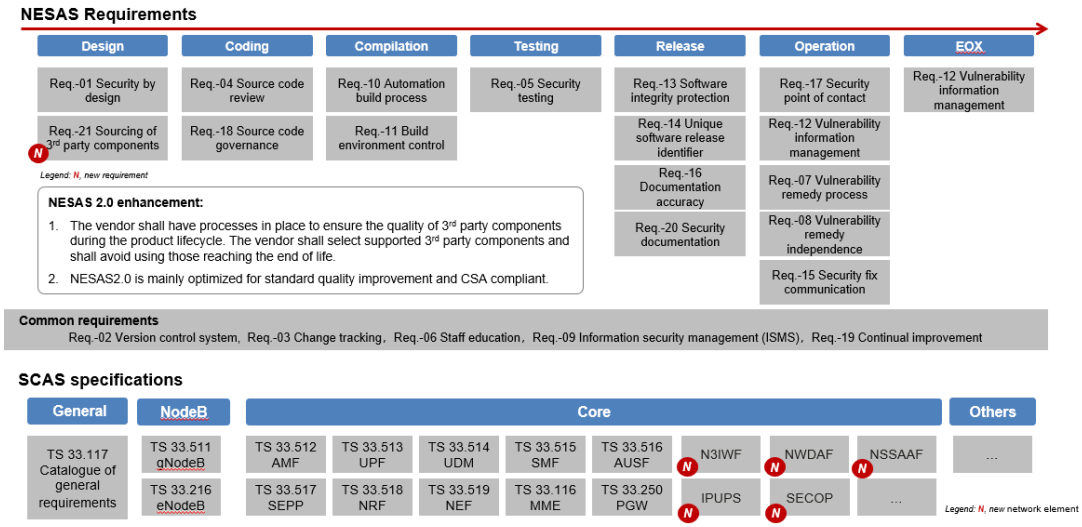
ตามความเป็นจริงแล้ว GSMA CKB ทำหน้าที่เป็นสะพานเชื่อมระหว่างข้อกำหนดของการปฏิบัติตามการควบคุมดูแลของผู้ให้บริการ การปรับปรุงความยืดหยุ่นด้านความมั่นคงปลอดภัย และการเปิดใช้งานความมั่นคงปลอดภัยของแอพพลิเคชันระบบ 5G กับการก่อสร้างโครงข่ายระบบ 5G การวางแผน

การบำรุงรักษา และขีดความสามารถด้านความมั่นคงปลอดภัยในการดำเนินงาน ในขณะที่ผู้ให้บริการโครงข่ายมือถือ (Mobile Network Operators : MNOs) ทั่วโลกใช้และเปิดตัวระบบ 5G โครงข่ายการสื่อสารจะเผชิญกับภัยคุกคามและความท้าทายด้านความมั่นคงปลอดภัยใหม่ ๆ การทำความเข้าใจ การทำแผนที่และการบรรเทาภัยคุกคามต่อความมั่นคงปลอดภัยที่มีอยู่และที่จะเกิดขึ้นเหล่านี้ในลักษณะที่เป้าหมายทันท่วงที และมีประสิทธิภาพกลายเป็นสิ่งที่จำเป็น GSMA ได้ทำการวิเคราะห์ภัยคุกคามอย่างครอบคลุมที่เกี่ยวข้องกับผู้เชี่ยวชาญในอุตสาหกรรมจากทั่วทั้งระบบนิเวศ และทำแผนที่ภัยคุกคามเหล่านี้กับการควบคุมความมั่นคงปลอดภัยที่เหมาะสมและมีประสิทธิภาพ ซึ่งหมายความว่า GSMA CKB อาจเป็นทางเลือกในการแนะนำผู้ให้บริการในการวางแผน การบำรุงรักษา และการเพิ่มประสิทธิภาพความมั่นคงปลอดภัยทางไซเบอร์ของระบบ 5G ร่วมด้วยความช่วยเหลือที่จำเป็นจากผู้จำหน่าย

ดูรายละเอียดเพิ่มเติมเรื่อง GSMA 5G CKB ได้ที่ :
https://www.gsma.com/security/5g-cybersecurity-knowledge-base/

9. แนวทางปฏิบัติด้านมาตรฐานด้านความมั่นคงปลอดภัยของระบบ 5G เพื่อรับรองอุปกรณ์สื่อสารภายใต้แผนการทดสอบความมั่นคงปลอดภัยของอุปกรณ์โครงข่าย (Network Equipment Security Assurance Scheme : NESAS)

ในช่วง 30 ปีที่ผ่านมา ได้มีการสร้างวิธีการรับรองความมั่นคงปลอดภัยที่หลากหลายเพื่อประเมินสถานะความมั่นคงปลอดภัยของผู้ผลิตและผู้ให้บริการต่าง ๆ ทั้งนี้ NESAS จะทำให้ความมั่นคงปลอดภัยเกิดความก้าวหน้าโดยมุ่งเป้าไปที่การสื่อสารของระบบ 5G สำหรับกรอบการทำงานของ NESAS นั้นครอบคลุมข้อกำหนดของมาตรฐานด้านความมั่นคงปลอดภัยและการประเมินคุณภาพและลักษณะของอุปกรณ์โทรคมนาคมตั้งแต่ขั้นตอนการวางแผน การออกแบบ และพัฒนา การผลิตและการทดสอบที่ให้ประโยชน์กับผู้ผลิตอุปกรณ์โทรคมนาคมและผู้ให้บริการโทรคมนาคม กรอบการทำงานของ NESAS ประกอบด้วยข้อกำหนดของมาตรฐานด้านความมั่นคงปลอดภัยและการประเมินคุณภาพและคุณลักษณะของอุปกรณ์โทรคมนาคมตั้งแต่ขั้นตอนการวางแผน การออกแบบ พัฒนาการผลิต และการทดสอบที่ให้ประโยชน์กับผู้ผลิตอุปกรณ์โทรคมนาคม และผู้ประกอบกิจการโทรคมนาคม ผู้ประกอบกิจการโทรคมนาคมสามารถใช้กรอบการทำงานของ NESAS พัฒนานโยบายและมาตรการต่าง ๆ เพื่อให้บริการโทรคมนาคมที่มีความมั่นคงปลอดภัยมากที่สุด สร้างมาตรฐานด้านความมั่นคงปลอดภัยที่เป็นกลางและโปร่งใส ตลอดจนวิธีการปฏิบัติตามข้อกำหนดซึ่งรวมถึงการทวนสอบและการทดสอบที่ได้มาตรฐาน ซึ่งแสดงภาพได้ดังนี้



นอกจากนี้ กสทช. ยังสนับสนุนและตระหนักถึงความสำคัญของการนำมาตรฐานด้านความมั่นคงปลอดภัยมาใช้ เช่น ฐานความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ระบบ 5G ของ GSMA NESAS เนื่องจากสามารถใช้มาตรฐานและมาตรการเหล่านี้เป็นพื้นฐานทางระเบียบข้อบังคับเพื่อสร้างมาตรฐานบริการโทรคมนาคมที่มีประสิทธิภาพและให้ความมั่นคงปลอดภัยในระดับสูงสุดสำหรับผู้ใช้บริการ ประโยชน์ที่สำคัญที่สุด คือ กระบวนการที่ทุกภาคส่วนมีบทบาทในการขับเคลื่อนบริการโทรคมนาคมที่ทันสมัยและมั่นคงปลอดภัย โดยเฉพาะ การร่วมมือกันพัฒนาบริการโทรคมนาคมที่มั่นคงปลอดภัยมากยิ่งขึ้นโดยใช้กรอบการทำงานของ NESAS และฐานความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของระบบ GSMA NESAS เป็นแนวทางปฏิบัติหลัก โดยแบ่งออกเป็น 2 ส่วน คือ 1) GSMA เป็นผู้กำหนด scheme’s processes และ requirements และ 2) 3GPP specifications เป็นผู้กำหนดนิยามของ scheme

9.1 The GSMA publishes the following documents:

GSMA PRD FS.13	NESAS Overview
GSMA PRD FS.14	NESAS Security Test Laboratory Accreditation
GSMA PRD FS.15	NESAS Development and Lifecycle Assessment Methodology
GSMA PRD FS.16	NESAS Development and Lifecycle Security Requirements
GSMA PRD FS.46	NESAS Audit Guidelines
GSMA PRD FS.47	NESAS Product and Evidence Evaluation Methodology
GSMA PRD FS.50	Security Assurance Specification Development Guidelines

9.2 3GPP publishes the following Security Assurance Specification (SCAS) documents

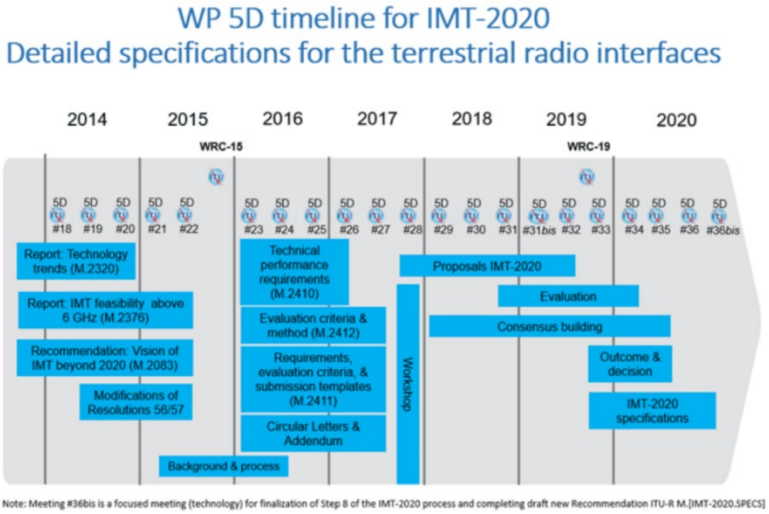
TS 33.116	MME network product class
TS 33.117	Catalogue of general security assurance requirement
TS 33.216	Evolved Node B (eNB) network product class
TS 33.250	PGW network product class
TS 33.326	Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class
TS 33.511	Next generation Node B (gNodeB) network product class
TS 33.512	Access and Mobility management Function (AMF). 5G SCAS
TS 33.513	User Plane Function (UPF) 5G SCAS
TS 33.514	Unified Data Management (UDM) network product class. 5G SCAS
TS 33.515	Session Management Function (SMF) network product class. 5G SCAS
TS 33.516	Authentication Server Function (AUSF) network product class. 5G SCAS
TS 33.517	Security Edge Protection Proxy (SEPP) network product class. 5G SCAS
TS 33.518	Network Repository Function (NRF) network product class. 5G SCAS
TS 33.519	Network Exposure Function (NEF) network product class. 5G SCAS
TS 33.521	Network Data Analytics Function (NWDAF). 5G SCAS
TS 33.522	Service Communication Proxy (SCP). 5G SCAS
TS 33.523	Split gNB product classes 5G SCAS
TS 33.526	Management Function (MnF) 5GSCAS
TS 33.527	3GPP virtualized network products 5GSCAS

ภาพผนวก A

การพัฒนาและการใช้ NESAS ทั่วโลก

อุตสาหกรรมร่วมมือกันมีส่วนร่วมเชิงบวกต่อการพัฒนาการประเมินความมั่นคงปลอดภัยแบบครบวงจรทั่วโลกสำหรับระบบ 5G ที่ยั่งยืนในระดับโลก ระบบ 3GPP 5G ได้กลายเป็นมาตรฐานทางเทคนิค ITU IMT-2020 5G อย่างเป็นทางการเมื่อวันที่ 10 กรกฎาคม ค.ศ. 2020

[วันที่ 10 กรกฎาคม ค.ศ. 2020] การประชุมทางไกล ITU-R WP 5D#35e ซึ่งมีผู้แทนและผู้เชี่ยวชาญมากกว่า 200 คนจากหน่วยงานรัฐบาล องค์กรการผลิตและการดำเนินงานโทรคมนาคม และสถาบันวิจัยทั่วโลก) เข้าร่วม ประกาศว่า เทคโนโลยีระบบ 3GPP 5G (รวมถึง NB-IoT) ตรงตามข้อกำหนดต่าง ๆ ของมาตรฐานทางเทคนิคระบบ 5G ของ IMT-2020 และได้รับการยอมรับอย่างเป็นทางการว่าเป็นมาตรฐานทางเทคนิค ITU IMT-2020 5G อนึ่ง ด้วยความร่วมมือจากประเทศและอุตสาหกรรมต่าง ๆ ทั่วโลกอย่างใกล้ชิด ITU ได้บรรลุหลักชัยของมาตรฐานเทคโนโลยีระบบ 5G ของ IMT-2020 ตามที่วางแผนไว้ และพาเข้าสู่โลกอัจฉริยะแห่งอินเทอร์เน็ตของสรรพสิ่ง มาตรฐานทางเทคนิค IMT-2020 เป็นชื่อที่กำหนดโดย ITU สำหรับมาตรฐานระบบ 5G ซึ่งคือ เทคโนโลยีการสื่อสารเคลื่อนที่ยุคถัดไปที่จะนำมาใช้หลังปี ค.ศ. 2020 ทั้งนี้ เพื่อทำให้แน่ใจในความก้าวหน้าของเทคโนโลยีระบบ 5G ทาง ITU ได้กำหนดวิธีการประเมินโดยละเอียดและข้อกำหนดตัวบ่งชี้ ตั้งแต่ปี ค.ศ. 2016 จนถึงปัจจุบัน มีการประเมินเทคโนโลยีที่ได้รับคัดเลือกโดยละเอียดในสถานการณ์จำลองแอพพลิเคชันเป้าหมายระบบ 5G สามสถานการณ์ ได้แก่ eMBB (Enhanced Mobile Broadband หรือบริการบรอดแบนด์เคลื่อนที่ที่เร็ว) URLLC (Low-Latency and High-Reliability Communication หรือ การสื่อสารที่มีเวลาแฝงต่ำและความน่าเชื่อถือสูง) และ mMTC (Large Machine-to-Machine Communication หรือการสื่อสารระหว่างเครื่องจักรกับเครื่องจักรขนาดใหญ่) เทคโนโลยี 3GPP 5G เป็นไปตามข้อกำหนดของมาตรฐานทางเทคนิค IMT-2020 ในแง่ของบริการ คลื่นความถี่ และตัวบ่งชี้สมรรถนะทางเทคนิค และมีขีดความสามารถทางเทคนิคขั้นสูง เช่น อัตราสูงสุดที่เกิน 20 Gbit/วินาที ความล่าช้าในการสื่อสารน้อยกว่า 1 มิลลิวินาที และรองรับอุปกรณ์ 1 ล้านเครื่องต่อตารางกิโลเมตร ที่ตรงตามข้อกำหนดการใช้งานระบบ 5G ที่หลากหลาย



ITU-R WP 5D เป็นคณะทำงานที่สำคัญมากที่สุดคณะหนึ่งของ ITU ซึ่งมีหน้าที่รับผิดชอบในการกำหนดมาตรฐานของเทคโนโลยีการสื่อสารแบบไร้สายภาคพื้นดินของโทรคมนาคมเคลื่อนที่สากล (International Mobile Telecommunications : IMT) ในช่วง 20 ปีที่ผ่านมา เทคโนโลยีการสื่อสารเคลื่อนที่ระบบ 3G (IMT-2000) และ 4G (IMT-Advanced) ที่พัฒนาโดย ITU-R WP 5D ประสบความสำเร็จอย่างสูงทั่วโลก ภายใต้การนำของ ITU-R WP 5D ประเทศและองค์กรระดับภูมิภาคต่าง ๆ ทั่วโลกจะยังคงร่วมมือกันอย่างต่อเนื่อง

ITU-T Study Group 17 (Security) หรือ กลุ่มศึกษา ITU-T (ความมั่นคงปลอดภัย) ปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัยของ 3GPP SA3 และวิจัยด้านความมั่นคงปลอดภัยของเทคโนโลยีที่ทันสมัย ดูรายละเอียดเพิ่มเติมได้ที่ https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx

ITU-T ทำโปรแกรม SG17 X.5Gsec-guide โดยอิงตามสถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ 3GPP 5G

ตามขั้นตอนของ ITU ที่อธิบายไว้ใน คำแนะนำของ ITU-T A.5 กลุ่มศึกษาหรือคณะทำงานต้องประเมินการอ้างอิงเชิงบรรทัดฐานใด ๆ สำหรับเอกสารที่จัดทำนอก ITU (นอกเหนือจากหนังสืออบรม ISO และ IEC) ก่อนที่จะตัดสินใจรวมการอ้างอิงไว้ในคำแนะนำของ ITU-TTD นี้ประกอบด้วยข้อมูลเหตุผล A.5 สำหรับ X.5Gsec-guide ใหม่ "แนวทางปฏิบัติด้านความมั่นคงปลอดภัยสำหรับระบบการสื่อสาร 5G" คำแนะนำฉบับร่างนี้อิงตามสถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ 3GPP 5G

[2017-2020] : [SG17] : [Q2/17]

[Declared patent(s)]

Work item:	X.5Gsec-guide
Status:	[Carried to next study period]
Approval process:	TAP
Type of work item:	Recommendation
Version:	New
Provisional name:	-
Equivalent number:	-
Timing:	-
Liaison:	3GPP, GSMA
Supporting members:	-
Subject/title:	Security guideline for 5G communication system
Summary:	Connected IoT devices and mobile applications require wireless network access that is resilient, secure and able to protect individuals' privacy. The 5G communication system should be designed to meet these high level requirements. There is a need for defining security framework for 5G communication system, which could be a concrete ground for developing further detailed technical Recommendations in 5G security subjects. This Recommendation provides security guidelines for 5G communication system. It identifies all components related to security of 5G communication system. It describes generic 5G architecture and its domain identifies threats to and provides security capabilities of each component, taking into account unique network features. This draft recommendation is based on the 3GPP 5G security architecture.
Comment:	-
Base text(s):	[SG17-TD4160/PLEN (2022-01)]
Contact(s):	Mee Yeon Kim, Editor Keundug Park, Editor Heung Youl Youm, Editor

ดูรายละเอียดเพิ่มเติมที่ https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=15006

ขอบเขต	ความสำเร็จ
ทั่วโลก	ระบบ 3GPP 5G ได้กลายเป็นมาตรฐานทางเทคนิคระบบ 5G ของ ITU IMT-2020 อย่างเป็นทางการเมื่อวันที่ 10 กรกฎาคม ค.ศ. 2020 **ITU-T ทำโปรแกรม SG17 X.5Gsec-guide โดยอิงตามสถาปัตยกรรมด้านความมั่นคงปลอดภัยของระบบ 3GPP 5G** หมายเหตุ : **มาตรฐานสำหรับการสื่อสารวิทยุและโทรคมนาคมระหว่างประเทศ ปี ค.ศ. 2020 (International Mobile Telecommunications-2020** (IMT-2020 Standard)) เป็นข้อกำหนดต่าง ๆ ที่ออกโดย ITU Radiocommunication Sector (ITU-R) ของ International Telecommunication Union (ITU) ในปี ค.ศ. 2015 สำหรับโครงข่าย อุปกรณ์ และบริการระบบ 5G https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=15006
สหภาพยุโรป	สหภาพยุโรปยอมรับ NESAS-CCS เป็นมาตรฐานการรับรองแบบครบวงจรภายใต้กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ของสหภาพยุโรป https://www.enisa.europa.eu/news/enisa-news/calling-on-you-5g-experts-join-us-on-5g-cybersecurity-certification
ประเทศเยอรมนี	Germany Security Catalog 2.0 ยอมรับ NESAS เป็นมาตรฐานการรับรองความมั่นคงปลอดภัยระบบ 5G และทำงานร่วมกับทุกฝ่ายเพื่อส่งเสริมการพัฒนามาตรฐานการรับรองระบบ 5G แบบครบวงจรในสหภาพยุโรปตั้งแต่ปี ค.ศ. 2020 https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220705_Zertifizierung_5G-Komponenten.html
ประเทศออสเตรีย	RTR ซึ่งเป็นหน่วยงานกำกับดูแลโทรคมนาคมของออสเตรีย ได้นำมาตรฐาน SCAS สำหรับระเบียบข้อบังคับด้านความมั่นคงปลอดภัยของโทรคมนาคมมาใช้ในระเบียบข้อบังคับด้านความมั่นคงปลอดภัยทางไซเบอร์ของโทรคมนาคมปี ค.ศ. 2020 (TK-NSiV 2020) การสนับสนุนอย่างเป็นทางการสำหรับการรวม NESAS ไว้ในกรอบการทำงานในการรับรองความมั่นคงปลอดภัยทางไซเบอร์ของสหภาพยุโรป 2020.07 04 https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/Telekom-Netzsicherheitsverordnung_2020_(TK-NSiV_2020.de.htm
ประเทศเนเธอร์แลนด์	ระเบียบข้อบังคับของกระทรวงเศรษฐกิจและสภาพอากาศ ลงวันที่ 1 ตุลาคม 2564 ฉบับที่ WJZ/20056324 มีกฎเกณฑ์เพิ่มเติมเกี่ยวกับความมั่นคงปลอดภัยและความสมบูรณ์ของโครงข่ายและบริการสื่อสารอิเล็กทรอนิกส์สาธารณะ (ระเบียบข้อบังคับด้านความมั่นคงปลอดภัยและความสมบูรณ์ของโทรคมนาคม) https://zoek.officielebekendmakingen.nl/stcrt-2021-42618.html
ประเทศบราซิล	ข้อที่ 2 ของ <ATO N° 77, DE 5 DE JANEIRO DE 2021> ข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับอุปกรณ์โทรคมนาคม ซึ่งเผยแพร่โดย Anatel ในปี ค.ศ. 2020 และมีผลบังคับใช้ในปี ค.ศ. 2021 ระบุให้ NESAS/SCAS เป็นมาตรฐานอ้างอิงสำหรับอุปกรณ์โทรคมนาคม 2021.01 https://www.in.gov.br/web/dou/-/ato-n-77-de-5-de-janeiro-de-2021-297933302
ประเทศจีน	NESAS ได้รับการอนุมัติให้เป็นมาตรฐานขั้นพื้นฐานสำหรับการประเมินความมั่นคงปลอดภัยของระบบ 5G และดำเนินการโดยทีมส่งเสริม IMT 2020 ของประเทศจีน ผู้ผลิตอุปกรณ์ระบบ 5G ทุกรายในตลาดจีน

ขอบเขต	ความสำเร็จ
	ปฏิบัติตามระบบมาตรฐาน NESAS คาดว่า เว็บไซต์ระบบ 5G ประมาณ 1.5 ล้านเว็บไซต์ในโครงข่ายระบบ 5G ของประเทศจีน (ข้อมูล ณ เดือนธันวาคม ค.ศ. 2021) จะปฏิบัติตามและได้รับการรับรองจาก NESAS http://www.caict.ac.cn/kxyj/qwfb/bps/202002/t20200204_274118.htm
ประเทศสิงคโปร์	รัฐบาลสิงคโปร์ยอมรับ NESAS (IMDA 21 GHz Public Consultation Document) เมื่อวันที่ 26 กรกฎาคม ค.ศ. 2021 https://www.imda.gov.sg/-/media/Imda/Files/Regulations-and-Licensing/Regulations/Consultations/2021/Next-Wave-of-5G-Growth-and-Deployment-in-Singapore/21-GHz-Public-Consultation-Document.pdf?la=en&hash=871CDE093D95FA731129030985E8DECD
ประเทศไทย	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) เผยแพร่แนวทางปฏิบัติด้านความมั่นคงปลอดภัยของระบบ 5G แห่งชาติอย่างเป็นทางการเพื่อเรียกร้องให้ผู้มีส่วนได้ส่วนเสียในอุตสาหกรรมโทรคมนาคมของประเทศไทยปฏิบัติตามมาตรฐาน NESAS เมื่อวันที่ 3 พฤศจิกายน ค.ศ. 2021 https://www.nbtc.go.th/News/govnewspartner/51190.aspx
ประเทศฟิลิปปินส์	กรมเทคโนโลยีสารสนเทศและการสื่อสาร (Department of Information and Communications Technology (DICT)) ของฟิลิปปินส์ เผยแพร่แนวทางปฏิบัติด้านความมั่นคงปลอดภัยระบบ 5G แห่งชาติอย่างเป็นทางการ ยอมรับและปรับใช้ NESAS เพื่อเรียกร้องให้ผู้มีส่วนได้ส่วนเสียในอุตสาหกรรมโทรคมนาคมของประเทศฟิลิปปินส์ปฏิบัติตามมาตรฐาน NESAS เมื่อวันที่ 1 กรกฎาคม ค.ศ. 2022 https://dict.gov.ph/ https://dict.gov.ph/wp-content/uploads/2022/07/The-Need-for-Philippines-Security-Standards-and-Framework-in-5G-Equipment-2022-07-01.pdf
ประเทศลาว	กระทรวงเทคโนโลยีและการสื่อสาร (Ministry of Technology and Communications (MTC)) ของประเทศลาว เผยแพร่แนวทางปฏิบัติด้านความมั่นคงปลอดภัยระบบ 5G แห่งชาติอย่างเป็นทางการ ยอมรับและปรับใช้ NESAS เมื่อวันที่ 1 กรกฎาคม ค.ศ. 2022 https://mtc.gov.la/index.php?r=site%2Fdetail&id=897
ประเทศตูนิเซีย/สันนิบาตอาหรับ	สันนิบาตอาหรับยอมรับมาตรฐาน NESAS อย่างเป็นทางการโดยสมุดปกขาวด้านความมั่นคงปลอดภัยทางไซเบอร์เมื่อวันที่ 22 ตุลาคม ค.ศ. 2021 https://www.mtcen.gov.tn/index.php?id=119&L=-1%5C%27&tx_ttnews%5Btt_news%5D=4335&cHash=8004500dd3cd4237a6fa9226d916c7df
แผนส่งเสริมกรอบการทำงานด้านความมั่นคงปลอดภัย	**การดำเนินกลไกการรับรองร่วมกัน:** ดำเนินกลไกการรับรองกับมาตรฐานด้านความมั่นคงปลอดภัย (NESAS/SCAS, ความมั่นคงปลอดภัยบนคลาวด์ ฯลฯ) ในบางประเทศสมาชิก OIC ที่สำคัญ/นำร่องในปี ค.ศ. 2022 ซึ่งจะถูกเลือกจากภูมิภาคและรัฐต่าง ๆ ในภายหลัง ประเทศหลัก/ประเทศนำร่องที่ได้รับการยืนยันในขั้นสุดท้ายควรเป็นไปตามเงื่อนไขต่อไปนี้อย่างน้อยหนึ่งข้อ: ① มีความสัมพันธ์ที่เป็นมิตรต่อกันกับประเทศที่คัดเลือกไว้

ขอบเขต	ความสำเร็จ
ระบบ 5G ของ OIC-CERT	②เชี่ยวชาญด้านการเผยแพร่และการขยายผลกระทบ ③มีไหวพริบที่ดีในการเสริมสร้างศักยภาพด้านความมั่นคงปลอดภัยทางไซเบอร์ https://www.oic-cert.org/en/events/5g/index.html#.YodGRKhByUk https://www.zawya.com/en/press-release/companies-news/oic-cert-5g-security-framework-working-group-kicks-off-global-series-of-cybersecurity-workshops-in-malaysia-bn7ttyiy
ประเทศอินโดนีเซีย	เมื่อวันที่ 3 กันยายน ค.ศ. 2022 BSSN&ITDel ของอินโดนีเซียได้ร่วมกันเผยแพร่ BOOK of Strategic Analysis for Indonesia Cyber Security Toward To 5G Technology Era (หนังสือการวิเคราะห์เชิงกลยุทธ์สำหรับความมั่นคงปลอดภัยทางไซเบอร์ของอินโดนีเซียสู่ยุคเทคโนโลยีระบบ 5G) ซึ่งได้รับการยอมรับอย่างเป็นทางการและใช้กรอบการทำงานด้านความมั่นคงปลอดภัยระบบ 5G ของ NESAS|SCAS, OIC CERT และ GSMA 5G CKB! https://bssn.go.id/menko-marves-luhut-binsar-panjaitan-dan-kepala-bssn-hinsa-siburian-luncurkan-buku-tinjauan-strategis-keamanan-siber-indonesia-menuju-era-5g-hasil-penelitian-bersama-poltek-ssn-dengan/
ประเทศเนปาล	หน่วยงานโทรคมนาคมแห่งเนปาล (Nepal Telecommunications Authority (NTA)) เผยแพร่แนวทางปฏิบัติด้านความมั่นคงปลอดภัยระบบ 5G แห่งชาติอย่างเป็นทางการเพื่อยอมรับและใช้ NESAS เมื่อวันที่ 19 ตุลาคม ค.ศ. 2022 https://nta.gov.np/en/consultation-paper/ https://nta.gov.np/wp-content/uploads/2022/10/Review-Paper-about-NESAS.pdf
ประเทศบังคลาเทศ	BRTC ของบังกลาเทศได้ยอมรับ NESAS (ITU、 GSMA、 3GPP) อย่างเป็นทางการในบริการโทรศัพท์เคลื่อนที่ระดับประเทศเมื่อวันที่ 12 ธันวาคม ค.ศ. 2022 http://www.brtc.gov.bd/
ประเทศมาเลเซีย	CSM ภายใต้ KKMM ของกระทรวงการสื่อสารของมาเลเซียได้ยอมรับต่อสาธารณชนและนำกรอบการทำงานด้านความมั่นคงปลอดภัยของ NESAS&GSMA 5G CKB&OIC CERT 5G มาใช้ และเผยแพร่แนวทางปฏิบัติอย่างเป็นทางการบนเว็บไซต์อย่างเป็นทางการของ CSM เมื่อวันที่ 21 ธันวาคม ค.ศ. 2022 https://www.cybersecurity.my/en/knowledge_banks/articles/main/detail/2372/index.html https://www.cybersecurity.my/data/content_files/13/2383.pdf
ประเทศศรีลังกา	Cert ของศรีลังกาและผู้มีส่วนได้ส่วนเสียหลายกลุ่มบรรลุฉันทามติในการให้แผน NESAS เป็นมาตรฐานด้านความมั่นคงปลอดภัยระบบ 5G แห่งชาติเมื่อวันที่ 30 พฤศจิกายน ค.ศ. 2021 https://www.ft.lk/it-telecom-tech/5G-roll-out-challenges--Governance--legislation--awareness--capacity-and-NESAS-standards/50-726824

ภาพผนวก B

เอกสารอ้างอิง

หมายเลขอ้างอิง	หมายเลขเอกสาร	หัวข้อ
[1]	GSMA PRD FS.13	ภาพรวม NESAS ฉบับที่ 2.0
[2]	GSMA PRD FS.14	การรับรองห้องปฏิบัติการทดสอบความมั่นคงปลอดภัยของ NESAS ฉบับที่ 2.0
[3]	GSMA PRD FS.15	วิธีการในการพัฒนาและประเมินวงจรชีวิตของ NESAS ฉบับที่ 2.0
[4]	GSMA PRD FS.16	ข้อกำหนดด้านความมั่นคงปลอดภัยในการพัฒนาและวงจรชีวิตของ NESAS ฉบับที่ 2.0
[5]	GSMA PRD FS.46	NESAS Audit Guidelines
[6]	GSMA PRD FS.47	NESAS Product and Evidence Evaluation Methodology
[7]	GSMA PRD FS.50	Security Assurance Specification Development Guidelines
	TS 33.116	Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัย สำหรับระดับชั้นผลิตภัณฑ์โครงข่าย MME
	TS 33.117	แคตตาล็อกข้อกำหนดการรับประกันความมั่นคงปลอดภัยทั่วไป
	TS 33.216	Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัย สำหรับระดับชั้นผลิตภัณฑ์โครงข่ายโหนด B ที่พัฒนาแล้ว (eNB)
	TS 33.250	Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัย สำหรับระดับชั้นผลิตภัณฑ์โครงข่าย PGW
	TS 33.326	
	TS 33.511	Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัย สำหรับระดับชั้นผลิตภัณฑ์โครงข่ายโหนด B ยุดถัดไป (gNodeB)
	TS 33.512	5G Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัยระบบ 5G; Access and Mobility management Function (AMF) หรือฟังก์ชันการบริหารจัดการการเข้าถึงและการเคลื่อนไหว
	TS 33.513	5G Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัยระบบ 5G; User Plane Function (UPF) หรือฟังก์ชันส่วนข้อมูลผู้ใช้
	TS 33.514	5G Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัยระบบ 5G สำหรับระดับชั้นผลิตภัณฑ์โครงข่าย

หมายเลขอ้างอิง	หมายเลขเอกสาร	หัวข้อ
		ของการบริหารจัดการข้อมูลเบ็ดเสร็จในที่เดียว (Unified Data Management (UDM))
	TS 33.515	5G Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัยระบบ 5G สำหรับระดับชั้นผลิตภัณฑ์โครงข่ายของการบริหารจัดการข้อมูลเซสชัน (Session Management Function (SMF))
	TS 33.516	5G Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัยระบบ 5G สำหรับระดับชั้นผลิตภัณฑ์โครงข่ายฟังก์ชันเซิร์ฟเวอร์การยืนยันตัวตน (Authentication Server Function (AUSF))
	TS 33.517	5G Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัยระบบ 5G สำหรับระดับชั้นผลิตภัณฑ์โครงข่ายของพร็อกซีการป้องกันเอดจ์ความมั่นคงปลอดภัย (Security Edge Protection Proxy (SEPP))
	TS 33.518	5G Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัยระบบ 5G สำหรับระดับชั้นผลิตภัณฑ์โครงข่ายของฟังก์ชันที่เก็บข้อมูลโครงข่าย (Network Repository Function (NRF))
	TS 33.519	5G Security Assurance Specification (SCAS) หรือข้อมูลจำเพาะการรับประกันความมั่นคงปลอดภัยระบบ 5G สำหรับระดับชั้นผลิตภัณฑ์โครงข่ายของฟังก์ชันการรับความเสี่ยงของโครงข่าย (Network Exposure Function (NEF))
	TS 33.521	Network Data Analytics Function (NWDAF). 5G SCA
	TS 33.522	Service Communication Proxy (SCP). 5G SCAS
	TS 33.523	Split gNB product classes 5G SCAS
	TS 33.526	Management Function (MnF) 5GSCAS
	TS 33.527	3GPP virtualized network products 5GSCAS
	ISO/IEC 17025	ข้อกำหนดทั่วไปสำหรับความสามารถของห้องปฏิบัติการทดสอบและสอบเทียบ