

ບົດຄວາມເຜີຍແຜ່ ມາດຕະຖານເຕັກນິກສໍາລັບອຸປະກອນໂທລະຄົມມະນາຄົມ

ໃນລະບົບ 5G

NESAS ແລະ GSMA 5G CKB

ສາລະບານ

ເນື້ອໃນ	1
ອະທິບາຍຄຳສັບ	1
1 ແນວທາງການພັດທະນາມາດຕະຖານເຕັກນິກຂອງອຸປະກອນໃນລະບົບ 5G	2
2 ມາດຕະຖານຄວາມປອດໄພຂອງອຸປະກອນ 5G	5
3 ມາດຕະຖານ NESAS	6
4 ສູນເກັບກຳຮວບຮວມຂໍ້ມູນກ່ຽວກັບຄວາມປອດໄພຂອງເຄືອຂ່າຍ 5G (GSMA 5G CKB)	9
5 ການພັດທະນາ ແລະ ສິ່ງເສີມດ້ານຄວາມປອດໄພ	13

ເນື້ອໃນ

ບົດຄວາມເຜີຍແຜ່ກ່ຽວກັບມາດຕະຖານເຕັກນິກຂອງອຸປະກອນໂທລະຄົມມະນາຄົມ NESAS ແລະ GSMA 5G CKB ໂດຍກະຊວງເຕັກໂນໂລຊີ ແລະ ການສື່ສານ. ບົດຄວາມດັ່ງກ່າວນີ້ໄດ້ອ້າງອີງຈາກມາດຕະຖານສາກົນທີ່ກ່ຽວຂ້ອງໃນຂົງເຂດວຽກງານການກຳນົດມາດຕະຖານດ້ານການສື່ສານໂທລະຄົມມະນາຄົມ. ດັ່ງລາຍລະອຽດທີ່ລະບຸໄວ້ໃນ “ເອກະສານຊ້ອນທ້າຍ A”

ອະທິບາຍຄຳສັບ

GSMA	Global System for Mobile Association / GSM Association ຫມາຍເຫດ: GSMA ແມ່ນອົງກອນຕົວແທນຜົນປະໂຫຍດຂອງຜູ້ໃຫ້ບໍລິການໂທລະສັບເຄື່ອນທີ່ໃນທົ່ວໂລກ, ກັບດູແລມາດຕະຖານການສື່ສານ ແລະ ມີບົດບາດໃນການພັດທະນາທາງດ້ານໂທລະຄົມມະນາຄົມສາກົນ ທີ່ມີສະມາຊິກຜູ້ໃຫ້ບໍລິການທາງດ້ານລະບົບໂທລະສັບເຄື່ອນທີ່ຫລາຍກວ່າ 800 ແຫ່ງໃນທົ່ວໂລກ.
3GPP	3 rd Generation Partnership Project ຫລື 3GPP: ແມ່ນສະມາຄົມທີ່ມີບົດບາດສູງໃນການກຳນົດມາດຕະຖານທາງດ້ານອຸດສາຫະກຳໂທລະຄົມມະນາຄົມສາກົນ.
ITU	International Telecommunication Union: ສະຫະພາບໂທລະຄົມມະນາຄົມລະຫວ່າງປະເທດ:
IMT-2020	International Mobile Telecommunications ແມ່ນ: ມາດຕະຖານສຳລັບການສື່ສານວິທະຍຸ ແລະ ໂທລະຄົມມະນາຄົມລະຫວ່າງປະເທດ. IMT-2020 ຖືກພັດທະນາຂຶ້ນເພື່ອເປັນມາດຕະຖານສຳລັບການໃຊ້ງານລະບົບໂທລະສັບເຄື່ອນທີ່ຍຸກ 5G. ໂດຍມີການກຳນົດຄຸນສົມບັດຄວາມຕ້ອງການດ້ານການໃຊ້ງານໃນຍຸກ 5G.
NESAS	Network Equipment Security Assurance Scheme ແມ່ນ: ມາດຕະຖານຄວາມປອດໄພຂອງອຸປະກອນໂທລະຄົມມະນາຄົມ
SCAS	Security Assurance Specifications
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
CAB	Conformity Assessment Body
CSA	Cyber Security Act
ENISA	European Union Agency for Cybersecurity
MNO	Mobile Network Operator
SD	Supporting Document
UPF	User Plane Function

1 ແນວທາງການພັດທະນາມາດຕະຖານເຕັກນິກຂອງອຸປະກອນເຄືອຂ່າຍ 5G

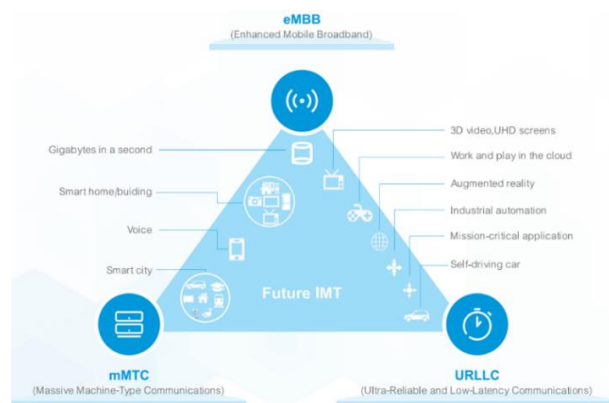
1.1 ພາບລວມຂອງ 5G

5G ເທັກໂນໂລຊີ ເປັນຍຸກວິວັດທະນາການຂອງລະບົບໂທລະສັບເຄື່ອນທີ່ຕິດມາຈາກຍຸກ 3G ແລະ 4G, ເຊິ່ງຍຸກ 5G ນີ້ໄດ້ມາພ້ອມກັບບໍລິການແບບໃໝ່ທີ່ເພີ່ມຂຶ້ນເຊັ່ນ:

- eMBB ຫລື enhance Mobile Broadband ເຮັດໃຫ້ອັດຕາຄວາມໄວຂອງການຮັບ-ສົ່ງຂໍ້ມູນໄດ້ສູງເຖິງ 20 Gbps ເຮັດໃຫ້ເອົາສາມາດຮັບຊົມພາບເຄື່ອນໄຫວທີ່ມີຄວາມລະອຽດລະດັບ 4K ຫລື 8K ໄດ້ຢ່າງເລື່ອນໄຫວ, ອີກທັງຍັງເປັນການເພີ່ມປະສິບການຂອງຜູ້ໃຊ້ງານກັບບໍລິການ AR, VR ຕ່າງໆແບບສົມຈິງຫລາຍຂຶ້ນ.

- URLLC ຫລື Ultra-reliable and Low Latency Communication ເຊິ່ງເປັນການໃຊ້ງານໃນລັກສະນະທີ່ຕ້ອງການການຮັບ-ສົ່ງຂໍ້ມູນທີ່ມີຄວາມສະຖຽນສູງລວມທັງມີຄວາມໜ່ວງເວລາ (latency) ໃນການຮັບ-ສົ່ງຂໍ້ມູນຕໍ່າໃນລະດັບມິນລິວິນາທີ (ms), ເຊິ່ງຄວາມສາມາດນີ້ເຮັດໃຫ້ລະບົບ 5G ເໝາະກັບການໃຊ້ງານລະບົບທີ່ຕ້ອງການຄວາມແມ້ນຢຳສູງ (critical application) ເຊັ່ນ: ການຜ່າຕັດທາງໄກ, ການຄວບຄຸມເຄື່ອງກົນຈັກໃນໂຮງງານ ຫລື ການຄວບຄຸມລົດແບບບໍ່ມີຄົນຂັບເປັນຕົ້ນ.

- mMTC ຫລື massive Machine Type Communications ແມ່ນການໃຊ້ງານທີ່ຕ້ອງການການເຊື່ອມຕໍ່ຂອງອຸປະກອນຈຳນວນຫລາຍໃນພື້ນທີ່ດຽວກັນທີ່ສາມາດຮອງຮັບເຖິງລ້ານອຸປະກອນຕໍ່ຫນຶ່ງຕາລາງກິໂລແມັດ. ໂດຍການຮັບ-ສົ່ງຂໍ້ມູນຂອງອຸປະກອນລັກສະນະນີ້ຈະເປັນການຮັບ-ສົ່ງຂໍ້ມູນປະລິມານໜ້ອຍທີ່ບໍ່ຕ້ອງການຄວາມໄວສູງ ຫລື ຄວາມໜ່ວງເວລາຕໍ່າ, ໂດຍອຸປະກອນດັ່ງກ່າວມີລາຄາຖືກ ແລະ ມີອາຍຸການໃຊ້ງານຂອງແບັດເຕີຣີທີ່ທົນກວ່າອຸປະກອນທົ່ວໄປ, ເຊິ່ງຄວາມສາມາດນີ້ເຮັດໃຫ້ 5G ເໝາະສຳລັບການໃຊ້ງານຂອງອຸປະກອນການເຊື່ອມຕໍ່ຂອງສັບພະສິ່ງ ຫລື IoT ແລະ ອື່ນໆ.



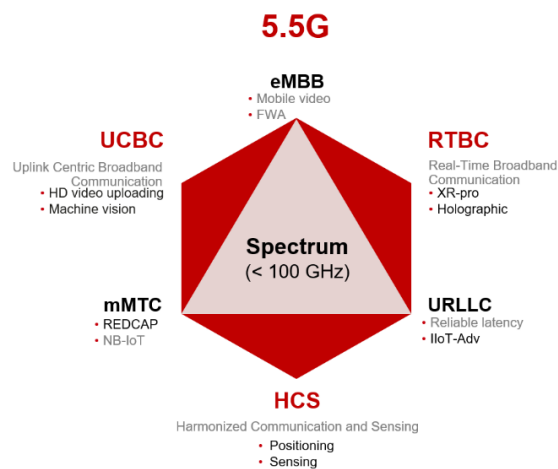
ຮູບທີ 1 ການນຳໃຊ້ 5G

ເພື່ອເຮັດໃຫ້ບັນລຸຄວາມຕ້ອງການຕໍ່ກັບການບໍລິການຮູບແບບໃໝ່ທີ່ເຂົ້າມາໂດຍເຮັດໃຫ້ການບໍລິການທາງດ້ານດິຈິຕອນມີຄວາມຫລາກຫລາຍຂຶ້ນ. ເທັກໂນໂລຊີ 5G ຕ້ອງໄດ້ມີການສົ່ງເສີມທາງດ້ານເທັກໂນໂລຊີໃໝ່ໆເພື່ອຕອບສະໜອງຕໍ່ກັບບໍລິການດັ່ງກ່າວ. ດັ່ງນັ້ນ, ຜູ້ສະໜອງອຸປະກອນທາງດ້ານ ICT ຈຶ່ງນຳສະເໜີວິໄສທັດຂອງເທັກໂນໂລຊີ 5.5G ໃນການເພີ່ມລັກສະນະການໃຊ້ງານຂອງ 5G ເພີ່ມຕື່ມອີກສາມລັກສະນະການໃຊ້ງານໃຫມ່ມີດັ່ງນີ້:

- Broadband Uplink Centric (UCBC) ຈະຍົກລະດັບອຸດສາຫະກຳສູ່ລະບົບອັດສະລິຍະ, UCBC ທີ່ຈະຊ່ວຍເພີ່ມການອັບໂຫລດຂໍ້ມູນວິດີໂອໃນລະບົບ Machine Vision ແລະ ອຸປະກອນ IoT ທີ່ນຳໃຊ້ເຄືອຂ່າຍບອດແບນຂະໜາດໃຫຍ່. ເຊິ່ງລັກສະນະການໃຊ້ງານນີ້ຈະຍົກລະດັບຜາກອຸດສາຫະກຳສູ່ລະບົບອັດສະລິຍະໄດ້ໄວຂຶ້ນ.

- Real-Time Broadband Communication (RTBC) ຮອງຮັບແບນວິດຂະໜາດໃຫຍ່ ແລະ ຄ່າຄວາມຫນ່ວງຕ່ຳ. ເປົ້າໝາຍຄືຕ້ອງເພີ່ມຄວາມກວ້າງຂອງຄື້ນຄວາມຖີ່ຂຶ້ນອີກ 10 ເທົ່າ ເພື່ອເຮັດໃຫ້ການສື່ສານມີຄວາມຍືດຫຍຸ່ນ ແລະ ເພີ່ມຄວາມໜ້າເຊື່ອຖືໃນການສົ່ງມອບປະສົບການຂອງບໍລິການໂລກສະເໝືອນໄດ້ຢ່າງສົມຈິງ.

- Harmonized Communication and Sensing (HCS) ຂະຫຍາຍຂອບເຂດຄວາມສາມາດຂອງເຄືອຂ່າຍໂທລະສັບເຄື່ອນທີ່ເພື່ອເຮັດໃຫ້ຍານພາຫະນະທຸກຄັນລວມທັງແບບຍານພາຫະນະແບບບໍ່ມີຄົນຂັບມີການເຊື່ອມຕໍ່ສື່ສານກັນໄດ້ເພື່ອເຮັດໃຫ້ການຂັບເຄື່ອນແບບອັດຕະໂນມັດເກີດຂຶ້ນໄດ້ຢ່າງສົມບູນແບບ.



ຮູບທີ 2 ການເພີ່ມບໍລິການນຳໃຊ້ 5.5G

1.2 ການບໍລິການຮູບແບບໃໝ່ໃນລະບົບເຄືອຂ່າຍ 5G ແລະ ພື້ນຖານໂຄງລ່າງດ້ານເຄືອຂ່າຍນຳໄປສູ່ສິ່ງທ້າທາຍດ້ານຄວາມປອດໄພ

ຄວາມທ້າທາຍດ້ານຄວາມປອດໄພຂອງອຸປະກອນເຄືອຂ່າຍ 5G ແມ່ນສິ່ງທີ່ເຮົາຈະຕ້ອງພິຈາລະນາເຊັ່ນດຽວກັບເຄືອຂ່າຍໃນຍຸກ 4G. ຢ່າງໃດກໍຕາມ ບັນດາສິ່ງທ້າທາຍທາຍເຫລົ່ານີ້ຈຳເປັນຕ້ອງໄດ້ຮັບການພິຈາລະນາເປັນພິເສດເນື່ອງຈາກມີຫລາກຫລາຍບໍລິການທີ່ເພີ່ມຕື່ມເຂົ້າມາ.

ໃນສ່ວນຂອງເຕັກໂນໂລຊີທີ່ເກີດຂຶ້ນໃໝ່: ເຕັກໂນໂລຊີ codification ແລະ virtualization ຖືກນຳໃຊ້ຢ່າງກວ້າງຂວາງໃນເຄືອຂ່າຍຫລັກຂອງ 5G (5G Core network), ຊຶ່ງນຳຄວາມສ່ຽງດ້ານຄວາມປອດໄພຂອງອຸປະກອນເຄືອຂ່າຍໃນລະບົບ ທີ່ມີການໃຊ້ງານຂໍ້ມູນຮ່ວມກັນ. ໃນອະນາຄົດ, ຄວນຕັ້ງຄວາມພິເສດທີ່ມີວິທີການເຂົ້າລະຫັດແບບສັບຊ້ອນຈະໄດ້ຖືກນຳໃຊ້ເພື່ອເສີມສ້າງຄວາມປອດໄພໃນລະບົບເຄືອຂ່າຍ 5G.

ສະຖາປັດຕະຍະກຳເຄືອຂ່າຍແບບໃໝ່: ສະຖາປັດຕະຍະກຳເຄືອຂ່າຍ 5G ທັງຮາດແວ ແລະ ຊ່ອຍແວເຮັດໃຫ້ເກີດມີການເຊື່ອມຕໍ່ໃນຮູບແບບໃໝ່ກວ່າທີ່ແຕກຕ່າງຈາກສະຖາປັດຕະຍະກຳເຄືອຂ່າຍໃນອະດີດ.

ການບໍລິການໃຫມ່: ການໃຫ້ບໍລິການເຄືອຂ່າຍ 5G ໃນພາກອຸດສາຫະກຳຄວນຈະຄຳນຶງເຖິງຄວາມອາດສາມາດ ຕໍ່ມາດຕະການຮັກສາຄວາມປອດໄພຂອງອຸປະກອນເຄືອຂ່າຍເພື່ອຄອບສະໜອງຕໍ່ຄວາມຕ້ອງການຂອງບໍລິການ ດັ່ງກ່າວ.

ດັ່ງນັ້ນ, ຕໍ່ກັບຄວາມຈຳເປັນຂອງວຽກງານດັ່ງກ່າວ ຈຶ່ງໄດ້ມີການພັດທະນາມາດຕະຖານ NESAS ເຊິ່ງພັດທະ ໂດຍການຮ່ວມມືຂອງອົງກອນກຳກັບດູແລມາດຕະຖານໂທລະຄົມມະນາຄົມ ຫລື GSMA (Global System for Mobile Association) ເປັນຜູ້ຮັບຜິດຊອບໃນການດຳເນີນການປະເມີນ, ທົດສອບຜູ້ຜະລິດອຸປະກອນເຄືອຂ່າຍ, ໜ່ວຍງານທີ່ຊ່ຽວຊານດ້ານການປະເມີນ, ການກວດສອບດ້ານເຕັກນິກຂອງອຸປະກອນເຄືອຂ່າຍ ແລະ ກຸ່ມມາດຕະຖານ ອຸດສາຫະກຳດ້ານໂທລະຄົມມະນາຄົມ ຫລື 3GPP (3rd Generation Partnership Project) ຮັບຜິດຊອບດ້ານການ ກຳນົດມາດຕະຖານຄວາມປອດໄພທາງເຕັກນິກຂອງອຸປະກອນເຄືອຂ່າຍ ແລະ ຂໍ້ກຳນົດດ້ານການປະເມີນການທົດ ສອບ. NESAS ວາງຂໍ້ກຳນົດ ແລະ ການປະເມີນສຳລັບຂະບວນການພັດທະນາຜະລິດຕະພັນ ແລະ ວົງຈອນຄວາມ ປອດໄພທາງເຕັກນິກຂອງອຸປະກອນ ເພື່ອສອດຄ່ອງຕາມຂໍ້ກຳນົດ Security Assurance Specification (SCAS) ທີ່ກຳນົດໂດຍ 3GPP ເພື່ອສົ່ງເສີມຄວາມຮ່ວມມືດ້ານມາດຕະຖານເຕັກນິກຂອງອຸປະກອນໃຫ້ມີຄວາມໂປ່ງໃສ, ຄວາມ ໄວ້ວາງໃຈເຊິ່ງກັນ ແລະ ກັນ, ຊ່ວຍຜູ້ປະກອບການ, ຜູ້ຜະລິດອຸປະກອນ ແລະ ພາກສ່ວນອື່ນໆທີ່ກ່ຽວຂ້ອງຮ່ວມກັນ ສົ່ງເສີມໃນການສ້າງປະສິດທິພາບຂອງການບໍລິການເຄືອຂ່າຍ 5G. ໂດຍໃຫ້ມາດຕະຖານດັ່ງກ່າວນີ້ ເປັນມາດຕະຖານ ກາງຂອງການປະເມີນດ້ານມາດຕະຖານເຕັກນິກຄວາມປອດໄພຂອງອຸປະກອນເຄືອຂ່າຍໃຫ້ສາມາດຈັດການໄດ້, ມີ ປະສິດທິພາບ, ເປັນເອກະພາບ, ມີການພັດທະນາຢ່າງຕໍ່ເນື່ອງສຳລັບອຸດສາຫະກຳໂທລະຄົມມະນາຄົມ ແລະ ເປັນຂໍ້ມູນ ອ້າງອີງທາງບວກສຳລັບພາກສ່ວນທີ່ກ່ຽວຂ້ອງເຊັ່ນ: ຜູ້ປະກອບການ, ຜູ້ຜະລິດອຸປະກອນ ແລະ ໜ່ວຍງານຂອງ ລັດຖະບານ.

1.3 ການຮ່ວມມືໃນການຮັບປະກັນດ້ານຄວາມປອດໄພຂອງອຸປະກອນເຄືອຂ່າຍໃນລະບົບນິເວດຂອງເທັກໂນ ໂລຊີ 5G

ຄວາມປອດໄພຂອງລະບົບເຄືອຂ່າຍ 5G ສາມາດແບ່ງໄດ້ເປັນ 3 ພາກສ່ວນໂດຍອີງຕາມຮູບແບບການສື່ສານ ໂທລະຄົມມະນາຄົມເຊັ່ນ: ຄວາມປອດໄພຂອງການໃຊ້ງານ, ຄວາມປອດໄພຂອງເຄືອຂ່າຍ ແລະ ຄວາມປອດໄພດ້ານ ມາດຕະຖານເຕັກນິກຂອງອຸປະກອນ.

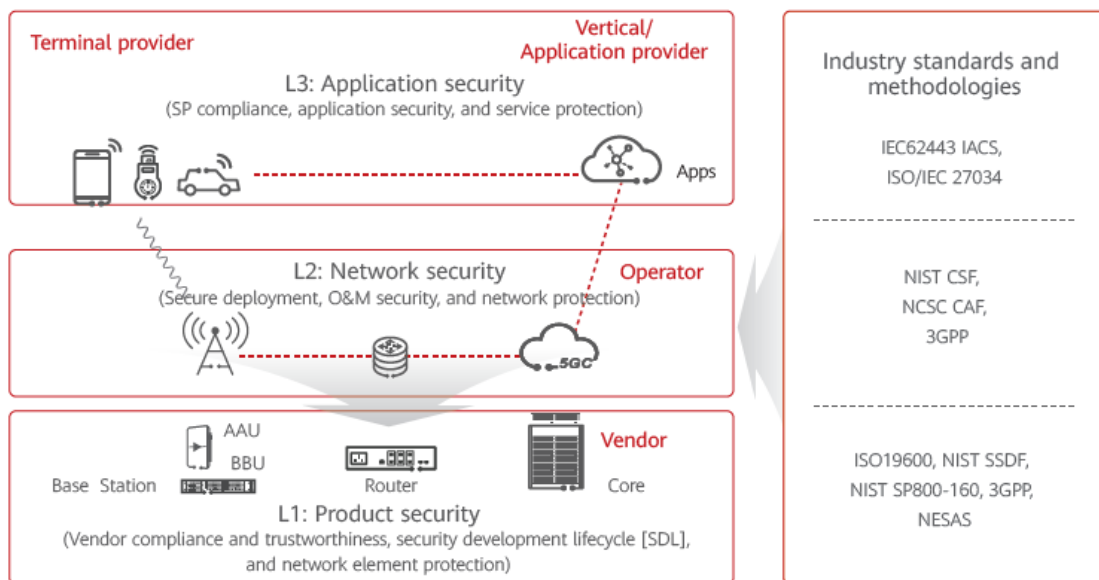
- ຄວາມປອດໄພຂອງການໃຊ້ງານ (Application security) ແມ່ນມີຄວາມສຳຄັນໃນລະບົບເຄືອຂ່າຍ ໂທລະສັບເຄືອນທີ່, ຂອງການບໍລິການພາກອຸດສາຫະກຳທີ່ມາພ້ອມກັບການໃຊ້ງານຮູບແບບໃໝ່. ພາກສ່ວນນີ້ ຕ້ອງມີ ການຮັບປະກັນໃຫ້ກັບຜູ້ໃຊ້ງານໃນລະບົບເຄືອຂ່າຍ 5G. ສິ່ງເຫລົ່ານີ້ທຸກພາກສ່ວນບໍ່ວ່າຈະເປັນຜູ້ໃຫ້ບໍລິການເຄືອຂ່າຍ, ຜູ້ຜະລິດອຸປະກອນ ແລະ ຜູ້ໃຫ້ບໍລິການແຜຣດຟອມຕ່າງໆ ຕ້ອງຜ່ານມາດຕະຖານຄວາມປອດໄພທີ່ໄດ້ຮັບການຢັ້ງຢືນ ຈາກສາກົນ.

- ຄວາມປອດໄພຂອງເຄືອຂ່າຍ (Network security) ແມ່ນຈະໄດ້ຮັບການບໍລິຫານຈັດການໂດຍຜູ້ໃຫ້ ບໍລິການເຄືອຂ່າຍ, ເຊິ່ງຈະພິຈາລະນາຕາມຂໍ້ກຳນົດ ແລະ ຄວາມປອດໄພຂອງການອອກແບບເຄືອຂ່າຍ, ມີການບໍລິຫານ ຈັດການປັບປຸງລະບົບຢ່າງສະໝໍ່າສະເໝີ ເພື່ອເຮັດໃຫ້ສາມາດປະເມີນຄວາມສ່ຽງ ແລະ ສາມາດຈັດການໄພຄຸກຄາມ ໃຫ້ທ່ວງທັນ ແລະ ມີປະສິດທິພາບ.

- ຄວາມປອດໄພຂອງອຸປະກອນ (Product security) ຕ້ອງໄດ້ຮັບການຮັບປະກັນຄວາມປອດໄພທາງດ້ານ

ເຕັກນິກຂອງອຸປະກອນເຄືອຂ່າຍໂດຍເຈົ້າຂອງຜູ້ຜະລິດ. ເຊິ່ງຕ້ອງເນັ້ນການປະຕິບັດຕາມລະບຽບການ, ຂະບວນການ ພັດທະນາ ແລະ ຜະລິດຕະພັນຕ້ອງເປັນໄປຕາມມາດຕະຖານສາກົນຂອງ 3GPP, NESAS ແລະ ອື່ນໆ.

ເທັກໂນໂລຊີ 5G ເປັນຄວາມຮັບຜິດຊອບຮ່ວມກັນຂອງຜູ້ມີສ່ວນໄດ້ສ່ວນເສຍໃນອຸດສາຫະກຳໂທລະ ຄົມມະນາຄົມໄດ້ແກ່: ຜູ້ໃຫ້ບໍລິການເຄືອຂ່າຍ, ຜູ້ຜະລິດອຸປະກອນ, ຜູ້ໃຫ້ບໍລິການແອັບພິເຄຊັນ, ອົງກອນກຳນົດ ມາດຕະຖານ, ລັດຖະບານ ແລະ ຜູ້ໃຊ້ງານ ທີ່ຕ້ອງມີຄວາມຮັບຜິດຊອບທີ່ຊັດເຈນ. ເຊິ່ງຄວາມຮັບຜິດຊອບເຫຼົ່ານີ້ ເມື່ອນຳມາປະຕິບັດເປັນມາດຕະການບວກກັບເງື່ອນໄຂຕ່າງໆ ກໍຈະສາມາດເຮັດໃຫ້ລະບົບຄວາມປອດໄພຂອງເຄືອຂ່າຍ 5G ມີປະສິດທະພາບຍິ່ງຂຶ້ນ.



ຮູບທີ 3 ການມີສ່ວນຮ່ວມຂອງທຸກພາກສ່ວນໃນການສົ່ງເສີມຄວາມປອດໄພຂອງ 5G [3]

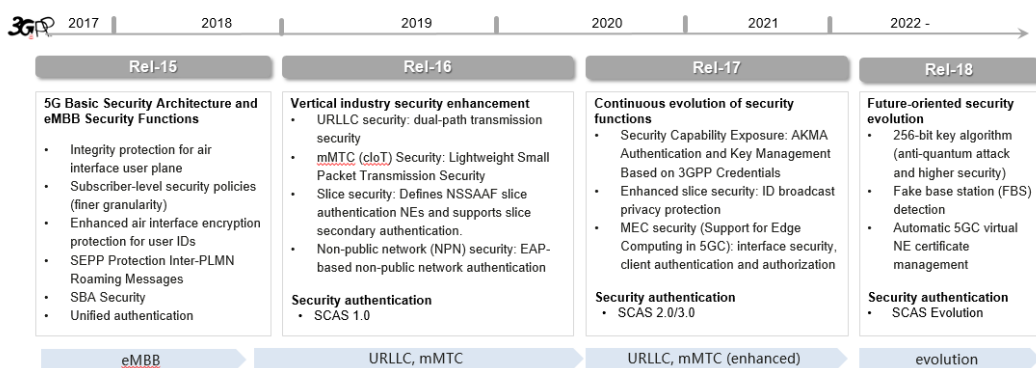
2 ຄວາມເປັນມາກ່ຽວກັບມາດຕະຖານຂອງເຄືອຂ່າຍ 5G

5G ໄດ້ປະເຊີນກັບສິ່ງທ້າທາຍໃໝ່ໆດ້ານມາດຕະຖານເຕັກນິກຂອງອຸປະກອນເຄືອຂ່າຍ. ດັ່ງນັ້ນຜູ້ທີ່ມີສ່ວນໄດ້ສ່ວນເສຍທີ່ຢູ່ໃນອຸດສາຫະກຳທາງດ້ານໂທລະຄົມມະນາຄົມຈຳເປັນຈະຕ້ອງມີຄວາມເຂົ້າໃຈຂໍ້ກຳນົດມາດຕະຖານດ້ານເຕັກນິກ ແລະ ເທັກໂນໂລຊີ 5G ໃຫ້ຫລາຍຂຶ້ນ. ເພື່ອເພີ່ມສັກກາຍະພາບຕໍ່ການປ້ອງກັນບັນຫາຄວາມສ່ຽງຕ່າງໆທີ່ອາດຈະເກີດຂຶ້ນໄດ້. ສະນັ້ນ, ອົງກອນທີ່ບົດບາດຫລັກໃນ ອຸດສາຫະກຳດ້ານໂທລະຄົມມະນາຄົມໄດ້ມີການເຮັດວຽກຮ່ວມກັນເພື່ອຈັດການກັບຄວາມສ່ຽງໃໝ່ໆທີ່ອາດຈະເກີດຂຶ້ນຈາກການບໍລິການຂອງເທັກໂນໂລຊີໃໝ່ນີ້ ໂດຍຜ່ານແນວຄວາມຄິດດ້ານການປະເມີນ ແລະ ວາງຂອບເຂດການມາດຕະຖານທາງເຕັກນິກຂອງອຸປະກອນຂອງ 5G ໃຫ້ເປັນມາດຕະຖານກາງ ທັງສາມາດເປັນທີ່ຍອມຮັບໃນລະດັບສາກົນໄດ້. ໂດຍພາຍໃຕ້ການຮ່ວມມືຂອງສອງອົງກອນທີ່ສຳຄັນຄື: GSMA ແລະ 3GPP ທີ່ໄດ້ຮ່ວມກັນວາງຂໍ້ກຳນົດດ້ານຫລັກການປະເມີນ ແລະ ມາດຕະຖານດ້ານຄວາມປອດໄພສຳລັບອຸປະກອນໂທລະຄົມມະນາຄົມ ຫລື Network Equipment Security Assurance Scheme-NESAS. ສະນັ້ນ, ຖ້າຫາກອຸປະກອນເຄືອຂ່າຍ 5G ຂອງຜູ້ຜະລິດອຸປະກອນ ໄດ້ຜ່ານມາດຕະຖານນີ້ກໍຈະສາມາດເຮັດໃຫ້ທຸກພາກສ່ວນມີຄວາມເຊື່ອໝັ້ນ, ສາມາດຕິດຕາມ, ດຳເນີນການ ແລະ ກວດສອບໄດ້ດ້ວຍຄວາມໂປ່ງໃສ.

5G R15 ໄດ້ກຳນົດສະຖາປັດຕະຍະກຳຄວາມປອດໄພດ້ານເຕັກນິກຂອງອຸປະກອນໃນພາກສ່ວນການໃຊ້ງານ eMBB ໃນເຄືອຂ່າຍ ທີ່ເປັນ 5G Standalone (SA) ແລະ Non-Standalone (NSA), ເຊິ່ງຕໍ່ມາມາດຕະຖານ 5G

R16 ແລະ 5G R17 ແມ່ນໄດ້ເພີ່ມປະສິດທິພາບສໍາລັບການໃຊ້ງານໃນຮູບແບບ mMTC ແລະ URLLC ເພື່ອເຮັດໃຫ້ໂຄງສ້າງດ້ານເຕັກນິກຂອງອຸປະກອນມີຄວາມປອດໄພໃນທຸກການບໍລິການຂອງເຄືອຂ່າຍ 5G.

ພາກສ່ວນທີ່ກ່ຽວຂ້ອງກັບການພັດທະນາເທັກໂນໂລຊີ 5G ໄດ້ເລັ່ງເຫັນເຖິງຄວາມສໍາຄັນຮ່ວມກັນຕໍ່ກັບຄວາມປອດໄພທາງລະບົບເຄືອຂ່າຍທີ່ອາດຈະເກີດຂຶ້ນ ໂດຍມີການນໍາສະເໜີແນວຄວາມຄິດໃນສ້າງມາດຕະຖານຄວາມປອດໄພຂອງອຸປະກອນ ທີ່ຈະຕ້ອງເປັນທີ່ຍອມຮັບຮ່ວມກັນ ແລະ ເປັນມາດຕະຖານສາກົນ. ໃນໄລຍະປີ 2020, ຜູ້ທີ່ມີສ່ວນໄດ້ສ່ວນເສຍໃນອຸດສາຫະກຳໂທລະຄົມມະນາຄົມທັງ 111 ບໍລິສັດໄດ້ເຂົ້າຮ່ວມກອງປະຊຸມ 3GPP SA3 ເພື່ອຈຸດປະສົງໃນການພັດທະນາມາດຕະຖານຄວາມປອດໄພຂອງອຸປະກອນເຄືອຂ່າຍ 5G ຮ່ວມກັນ. 3GPP SA3 ໄດ້ດໍາເນີນ 42 ໂຄງການ ເພື່ອວິເຄາະໄພຂົ່ມຂູ່ດ້ານຄວາມປອດໄພ ແລະ ຄວາມສ່ຽງໃນຮູບແບບຕ່າງໆຂອງການໃຊ້ງານ 5G ຢູ່ໃນສະຖານະການຂອງການໃຊ້ງານຮູບແບບຕ່າງໆ ແລະ ສຸດທ້າຍຈຶ່ງໄດ້ຜົນສະຫຼຸບອອກມາເປັນມາດຕະຖານດ້ານຄວາມປອດໄພທາງດ້ານເຕັກນິກອັນເປັນທີ່ຍອມຮັບຮ່ວມກັນ.

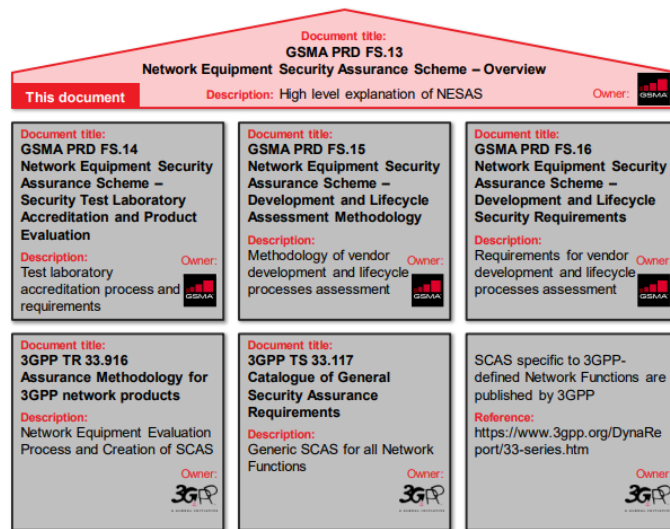


ຮູບທີ 4 ການພັດທະນາດ້ານຄວາມປອດໄພມາດຕະຖານດ້ານເຕັກນິກຂອງອຸປະກອນເຄືອຂ່າຍ 5G

ມາດຕະຖານຄວາມປອດໄພທາງດ້ານເຕັກນິກຂອງ 3GPP 5G ໄດ້ເພີ່ມຂີດຄວາມສາມາດຂໍ້ຈໍາກັດຈາກມາດຕະຖານ 4G. ເຊິ່ງວ່າມາດຕະຖານເຕັກນິກຄວາມປອດໄພຂອງເຄືອຂ່າຍ 5G ໄດ້ຖືກອອກແບບມາເພື່ອໃຫ້ມີຄວາມສອດຄ່ອງກັບການໃຊ້ງານສໍາລັບການປະມວນຜົນຜ່ານລະບົບຄຣາວໄລຍະໃກ້ (Mobile edge computing: MEC) ແລະ ເຄືອຂ່າຍສະເໝືອນທີ່ມີຫລາຍໆເຄືອຂ່າຍຢູ່ໃນເຄືອຂ່າຍດຽວ (Network Slicing).

3 ມາດຕະຖານ NESAS

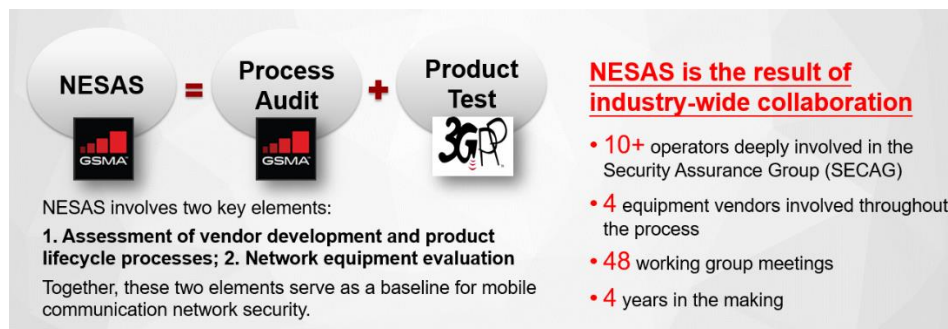
ມາດຕະຖານດ້ານເຕັກນິກສໍາລັບອຸປະກອນໂທລະຄົມມະນາຄົມສໍາລັບເຄືອຂ່າຍ 5G ຫລື Network Equipment Security Assurance Scheme – NESAS ເຊິ່ງເປັນມາດຕະຖານສາກົນທີ່ເກີດຈາກການຮ່ວມມືກັນຂອງ GSMA ແລະ 3GPP ທີ່ມີວັດຖຸປະສົງເພື່ອກໍານົດມາດຕະຖານກາງດ້ານການປະເມີນ, ການກວດສອບຄຸນນະພາບ ແລະ ຄຸນລັກສະນະຂອງອຸປະກອນໂທລະຄົມມະນາຄົມຕັ້ງແຕ່ການວາງແຜນອອກແບບ, ພັດທະນາ, ການຜະລິດ ແລະ ການທົດສອບ. NESAS ຍັງສາມາດຊ່ວຍໃຫ້ຜູ້ຜະລິດອຸປະກອນໂທລະຄົມມະນາຄົມສາມາດນໍາຂໍ້ກໍານົດນີ້ໄປໃຊ້ເປັນແບບແຜນເພື່ອການພັດທະນາ ແລະ ການຜະລິດອຸປະກອນທີ່ມີຄຸນນະພາບມີລັກສະນະດ້ານຄວາມປອດໄພສູງອີກທັງຜູ້ໃຫ້ບໍລິການດ້ານໂທລະຄົມເອງ ສາມາດນໍາໃຊ້ຂໍ້ກໍານົດນີ້ ໃນການພັດທະນານະໂຍບາຍ ແລະ ມາດຕະການບໍລິການໂທລະຄົມທີ່ມີຄວາມປອດໄພສູງເຊັ່ນດຽວກັນ. ສໍາລັບອົງກອນທີ່ຮັບຜິດຊອບດູແລດ້ານການກໍານົດມາດຕະຖານທາງເຕັກນິກຂອງອຸປະກອນຂອງເຄືອຂ່າຍ 5G ກໍສາມາດນໍາເອົາຂໍ້ກໍານົດ NESAS ເປັນມາດຕະຖານກາງເພີ່ມຕື່ມໄດ້.



ຮູບທີ 5 ເອກະສານສໍາຄັນທີ່ກ່ຽວຂ້ອງກັບຂໍ້ກຳນົດມາດຕະຖານ NESAS [4]

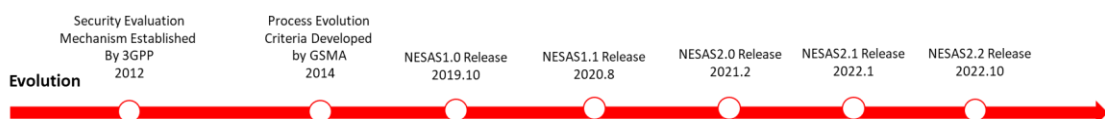
ລາຍລະອຽດເພີ່ມເຕີມເປັນ: FS.13 NESAS Overview v.2.2

<https://www.gsma.com/security/network-equipment-security-assurance-scheme/>



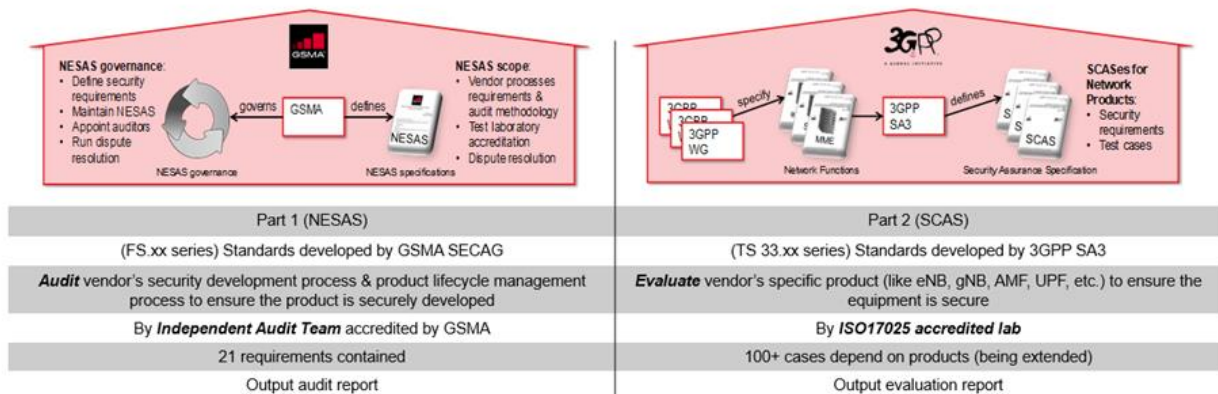
ຮູບທີ 6 ການຮ່ວມມືຂອງ NESAS

GSMA ໄດ້ປະກາດໃຊ້ NESAS 1.0 ໃນເດືອນຕຸລາ ປີ 2019 ແລະ ສືບຕໍ່ພັດທະນາ ເພື່ອໃຫ້ຖືກຕ້ອງຕາມຄວາມຕ້ອງການຂອງອຸດສາຫະກຳໂທລະຄົມມະນາຄົມ ແລະ ໄດ້ປະກາດເວີຊັນລ້າສຸດ NESAS 2.2 ໃນເດືອນຕຸລາ ປີ 2022 ເຊິ່ງຈະຊ່ວຍສ້າງມາດຕະຖານໃຫ້ກັບຜູ້ໃຫ້ບໍລິການເຄືອຂ່າຍ 5G ຂອງທັງຜູ້ໃຫ້ບໍລິການເຄືອຂ່າຍ, ຜູ້ຜະລິດ ສະຖາບັນ ແລະ ຫ້ອງແລັບທີ່ມີທັກສະກວດສອບ ແລະ ລັດຖະບານ. ເຊິ່ງພາກສ່ວນດັ່ງກ່າວຕ່າງກໍໄດ້ສົ່ງເສີມໃຫ້ເປັນມາດຕະຖານສາກົນໃນການອອກໃບຮັບຮອງດ້ານຄວາມປອດໄພທາງເທັກນິກຂອງອຸປະກອນການສື່ສານຜ່ານໂທລະສັບເຄື່ອນທີ່ໃນຍຸກ 5G.



ຮູບທີ 7 ການພັດທະນາຂອງ NESAS ໃນແຕ່ລະໄລຍະ

ເຊິ່ງອຸປະກອນເຄືອຂ່າຍໂທລະຄົມມະນາຄົມໃນພາກສ່ວນຂອງການເຂົ້າເຖິງເຄືອຂ່າຍວິທະຍຸ ຫລື RAN (Radio Access Network) ແລະ ເຄືອຂ່າຍຫລັກ ຫລື Core network ຂອງບໍລິສັດ Huawei ເປັນບໍລິສັດທຳອິດທີ່ຜ່ານການກວດສອບ ແລະ ທົດສອບຜ່ານມາດຕະຖານດ້ານຄວາມປອດໄພທາງເຕັກນິກຂອງ NESAS, ຈາກນັ້ນຕາມມາດ້ວຍ Ericson, Nokia, ZTE ກໍຜ່ານມາດຕະຖານການທົດສອບຂອງ NESAS ເຊັ່ນກັນ. ຜູ້ໃຫ້ບໍລິການໂທລະສັບເຄື່ອນທີ່ລະດັບຊັ້ນນຳຂອງໂລກເຊັ່ນ: Vodafone, China Mobile, MTC, telenor... ໄດ້ລະບຸວ່າອຸປະກອນທີ່ຈະຕ້ອງໄດ້ນຳມາໃຊ້ພາຍໃນເຄືອຂ່າຍຕ້ອງຜ່ານມາດຕະຖານ NESAS ກ່ອນ.



ຮູບທີ 8 ບົດບາດຂອງ GSMA ແລະ 3GPP [6]

NESAS ໄດ້ນຳເອົາຜົນປະໂຫຍດຕ່າງໆທີ່ຈະຊ່ວຍໃຫ້ຜູ້ມີສ່ວນໄດ້ສ່ວນເສຍໃນອຸດສາຫະກຳໂທລະຄົມມະນາຄົມສາມາດນຳປັບໃຊ້ໄດ້ທັນທີ ເພື່ອເຮັດໃຫ້ການບໍລິການລະບົບ 5G ມີປະສິດທິພາບສູງທີ່ສຸດ ແລະ ຜົນດີດັ່ງກ່າວສາມາດສົ່ງຜົນໃຫ້ແຕ່ລະພາກສ່ວນດັ່ງນີ້:

NESAS ໄດ້ນຳປະໂຫຍດມາສູ່ຜູ້ຜະລິດອຸປະກອນໂທລະຄົມມະນາຄົມຄື:

- ເປັນຂໍ້ອ້າງອີງເຖິງການປະຕິບັດຕາມຂໍ້ກຳນົດດ້ານມາດຕະຖານທາງເຕັກນິກຂອງອຸປະກອນຄວາມປອດໄພຕໍ່ຜູ້ມີສ່ວນໄດ້ສ່ວນເສຍໃນອຸດສາຫະກຳໂທລະຄົມມະນາຄົມ.
- ສາມາດສະແດງໃຫ້ເຫັນເຖິງຈຸດເດັ່ນຂອງຜູ້ຜະລິດອຸປະກອນໃນການພັດທະນາ, ບຳລຸງຮັກສາ ແລະ ມາດຕະການດ້ານຄວາມເຊື່ອໝັ້ນຂອງລະບົບ.
- ຫລີກລ່ຽງຂໍ້ຂັດແຍ້ງ ແລະ ຂໍ້ກຳນົດການຮັບປະກັນມາດຕະຖານທີ່ແຕກຕ່າງກັນ.
- ຊ່ວຍເຮັດໃຫ້ການພັດທະນາຜະລິດຕະພັນອຸປະກອນເຄືອຂ່າຍສາມາດເຂົ້າເຖິງຕະຫຼາດໄດ້ທົ່ວໂລກເນື່ອງຈາກມີມາດຕະຖານກາງທີ່ຮອງຮັບ.

NESAS ໄດ້ນຳປະໂຫຍດມາສູ່ຜູ້ໃຫ້ບໍລິການໂທລະຄົມມະນາຄົມຄື:

- ສາມາດຕິດຕາມກວດກາມາດຕະຖານດ້ານເຕັກນິກຄວາມປອດໄພຂອງຜູ້ຜະລິດອຸປະກອນເຄືອຂ່າຍ ແລະ ເຮັດໃຫ້ອຸປະກອນເຄືອຂ່າຍຂອງຕົນເອງໄດ້ຮັບຄວາມເຊື່ອໝັ້ນຂອງລະບົບກ່ອນການນຳໃຊ້.

- ເຮັດໃຫ້ອົງກອນໄດ້ຮັບຄວາມໄວ້ເນື້ອເຊື່ອໃຈຈາກຜູ້ໃຊ້ບໍລິການເນື່ອງຈາກໄດ້ນຳໃຊ້ອຸປະກອນຈາກບໍລິສັດຜູ້ຜະລິດທີ່ປະຕິບັດຕາມດ້ານແນວທາງມາດຕະຖານຂອງສາກົນ NESAS.

- ຊ່ວຍປະຫຍັດເວລາ ແລະ ງົບປະມານທີ່ຈະໄປນຳໃຊ້ໃນການກວດສອບຜູ້ຜະລິດສິນຄ້າແຕ່ລະບໍລິສັດ.

NESAS ໄດ້ນຳປະໂຫຍດຕໍ່ໄປນີ້ມາສູ່ໜ່ວຍງານພາກລັດທີ່ຮັບຜິດຊອບດ້ານໂທລະຄົມມະນາຄົມຄື:

- ສ້າງຄວາມເອື້ອອຳນວຍຕໍ່ແຜນການພັດທະນາການສື່ສານທາງດ້ານໂທລະຄົມມະນາຄົມເປັນໄປຕາມມາດຕະຖານດ້ານເຕັກນິກຂອງອຸປະກອນຄວາມປອດໄພດຽວກັນ.

- ສາມາດຕິດຕາມກວດສອບຕໍ່ກັບການພັດທະນາມາດຕະຖານໄດ້ຢ່າງຕໍ່ເນື່ອງ.

- ປະຫຍັດງົບປະມານຕໍ່ການກວດສອບເຄືອຂ່າຍ, ສິ່ງເສີມໃຫ້ມີເທັກໂນໂລຊີໃໝ່ໆເກີດຂຶ້ນ ແລະ ໃຫ້ຜົນປະໂຫຍດໃຫ້ກັບຜູ້ມີສ່ວນໄດ້ສ່ວນເສຍ.



ຮູບທີ 9 ການມີສ່ວນຮ່ວມໃນການສ້າງລະບົບນິເວດຄວາມປອດໄພຂອງອຸປະກອນໃນເຄືອຂ່າຍ 5G

ສຳລັບເຄືອຂ່າຍ 5G, NESAS ໄດ້ນຳສະເໜີມາດຕະຖານທີ່ເໝາະສົມ, ຈັດການໄດ້, ກວດສອບໄດ້, ເປັນມາດຕະຖານສາກົນທີ່ຍືດຍຸ່ນ, ມີປະສິດທິພາບ, ເປັນມາດຕະຖານດຽວກັນ, ເປີດກວ້າງ ແລະ ມີການພັດທະນາຢ່າງຕໍ່ເນື່ອງ. ເຮັດໃຫ້ປັດຈຸບັນລະບົບນິເວດແບບສີ່ໃໝ່ໜຶ່ງ (ຜູ້ຜະລິດ, ຜູ້ກວດສອບ, ສະຖານບັນທຶກລອງ ແລະ ໜ່ວຍງານກຳກັບດູແລ) ໄດ້ຖືກສ້າງຂຶ້ນ. ອີກທັງ ອຸດສາຫະກຳທາງດ້ານໂທລະຄົມມະນາຄົມໄດ້ມີການທຳງານຮ່ວມກັນເພື່ອສ້າງການມີສ່ວນຮ່ວມທາງບວກຕໍ່ການພັດທະນາທີ່ຍິ່ງຍືນຂອງການປະເມີນທາງດ້ານເຕັກນິກຂອງອຸປະກອນໃຫ້ມີຄວາມປອດໄພແບບລວມສູນສາກົນສຳລັບເຄືອຂ່າຍ 5G.

4 ແຫລ່ງຂໍ້ມູນ ແລະ ຄຳແນະນຳກ່ຽວກັບຄວາມປອດໄພຂອງເຄືອຂ່າຍ 5G (GSMA 5G CKB)

ໃນຂະນະທີ່ຜູ້ໃຫ້ບໍລິການໂທລະສັບເຄື່ອນທີ່ (Mobile Network Operators: MNOs) ໃນທົ່ວໂລກໄດ້ມີການວາງແຜນ ແລະ ເປີດໂຕການໃຫ້ບໍລິການເຄືອຂ່າຍ 5G ຢູ່ນັ້ນ. ສິ່ງດັ່ງກ່າວອາດຈະກຳລັງປະເຊີນກັບໄພຂົ່ມຂູ່ ແລະ ສິ່ງທ້າທາຍດ້ານຄວາມປອດໄພໃນຮູບແບບໃໝ່. ການຫລຸດຜ່ອນສິ່ງທ້າທາຍດ້ານຄວາມປອດໄພຂອງອຸປະກອນຮູບແບບໃໝ່ນີ້, ໄດ້ເປັນເປົ້າໝາຍທີ່ຈະໄດ້ຝຶກຈາລະນາເພື່ອຫຼຸດຜ່ອນໄພຂົ່ມຂູ່ດ້ານຄວາມປອດໄພ. ສິ່ງເຫລົ່ານີ້ເປັນຈຸດປະສົງຫລັກທີ່ທາງ GSMA ຈະຕ້ອງໄດ້ຮັບການຝຶກຈາລະນາ ແລະ ຈຳເປັນທີ່ຈະຕ້ອງໄດ້ມີການດຳເນີນການຢ່າງວ່ອງໄວ ແລະ ທັງຕ້ອງມີປະສິດທິພາບສູງ.

ເພື່ອຊ່ວຍຜູ້ໃຫ້ບໍລິການດ້ານໂທລະຄົມ ແລະ ຜູ້ໃຫ້ບໍລິການອື່ນໆທີ່ກ່ຽວຂ້ອງກັບລະບົບນິເວດຂອງເຄືອຂ່າຍ 5G, GSMA ໄດ້ຮວບຮວມຜູ້ຊ່ຽວຊານເພື່ອດຳເນີນການວິເຄາະໄພຂົ່ມຂູ່ດ້ານຄວາມປອດໄພຂອງອຸປະກອນໃຫ້ຄວບຄຸມໃນທຸກໆພາກສ່ວນເຊັ່ນ: ຜູ້ຜະລິດ, ຜູ້ໃຫ້ບໍລິການເຄືອຂ່າຍ, ຜູ້ວາງນະໂຍບາຍ ແລະ ຜູ້ນຳໃຊ້. ເຊິ່ງໄດ້ມີການເກັບກຳຮວບລວມຂໍ້ມູນຈາກອົງກອນທີ່ມີບົດບາດສູງໃນອຸດສາຫະກຳໂທລະຄົມມະນາຄົມເຊັ່ນ: 3GPP, ENISA ແລະ NIST, ເພື່ອກຳນົດແຜນການຄວບຄຸມຄວາມປອດໄພຂອງອຸປະກອນທີ່ເໝາະສົມທີ່ສຸດ ແລະ ຕ້ອງມີປະສິດທິພາບ.

GSMA ໄດ້ຮວບຮວມຖານຄວາມຮູ້ດ້ານຄວາມປອດໄພ 5G ເພື່ອເປັນບ່ອນອ້າງອີງ, ໃຫ້ຄຳແນະນຳທີ່ເປັນປະໂຫຍດກ່ຽວກັບຄວາມສ່ຽງດ້ານຄວາມປອດໄພຂອງລະບົບເຄືອຂ່າຍ 5G ເພື່ອເຮັດໃຫ້ສະມາຊິກຂອງ GSMA ໄດ້ນຳໃຊ້ຂໍ້ມູນດັ່ງກ່າວນີ້ໄປປັບໃຊ້ໃນການຈັດຕັ້ງວາງແຜນການໃຫ້ບໍລິການເຄືອຂ່າຍ 5G ຂອງຕົນ, ເພື່ອສ້າງຄວາມໄວ້ເນື້ອເຊື່ອໃຈໃຫ້ກັບຜູ້ໃຊ້ບໍລິການເຊິ່ງຜູ້ໃຊ້ງານເອງກໍ່ຈະຕ້ອງມີສ່ວນຮ່ວມຕໍ່ການປັບປຸງມາດຕະຖານດ້ານຄວາມປອດໄພດັ່ງກ່າວເພື່ອໃຫ້ສອດຄ່ອງກັບການໃຊ້ງານໃນປັດຈຸບັນ.

GSMA ເຮັດໜ້າທີ່ເປັນແນວທາງການປະຕິບັດສຳລັບ MNOs ໃນການຈັດການຄວາມປອດໄພຂອງອຸປະກອນໃນເຄືອຂ່າຍ 5G

- ຕິດຕາມຄວາມປອດໄພຕັ້ງແຕ່ເລີ່ມຕົ້ນ: ມາດຕະຖານ NESAS ໄດ້ຮັບປະກັນດ້ານຄວາມປອດໄພສຳລັບອຸປະກອນ 5G, ແລະ ຖານຄວາມຮູ້ຄວາມປອດໄພ 5G ຈະເຮັດໃຫ້ຜູ້ໃຫ້ບໍລິການໂທລະສັບເຄື່ອນທີ່ມີແນວທາງໃນການວາງແຜນລະບົບເຄືອຂ່າຍ, ການບຳລຸງຮັກສາ, ການປັບປຸງ ແລະ ການດຳເນີນງານຕ່າງໆພາຍໃນເຄືອຂ່າຍຂອງຕົນ.
- ຄຳແນະນຳທາງດ້ານເຕັກນິກ: ຜູ້ໃຫ້ບໍລິການໂທລະສັບເຄື່ອນທີ່ສາມາດໃຊ້ຖານຄວາມຮູ້ຄວາມປອດໄພ 5G ນີ້ເປັນຈຸດອ້າງອີງພື້ນຖານເພື່ອປັບປຸງຄວາມປອດໄພ 5G.
- ການຮ່ວມມືກັບທຸກໆພາກສ່ວນ: ບັນດາຜູ້ຊ່ຽວຊານດ້ານເຕັກນິກສາມາດຮ່ວມມືກັບຜູ້ຜະລິດອຸປະກອນ, ຜູ້ໃຫ້ບໍລິການເຄືອຂ່າຍ, ຜູ້ໃຊ້ງານ ແລະ ອົງກອນພາກລັດທີ່ເປັນຜູ້ກຳນົດລະບຽບການໃນການຈັດຕັ້ງປະຕິບັດສິ່ງເສີມຄວາມຮູ້ດ້ານຄວາມປອດໄພຂອງອຸປະກອນ.
- ການປະເມີນຜົນດ້ານຄວາມປອດໄພຂອງເຄືອຂ່າຍ: ຜູ້ໃຫ້ບໍລິການດ້ານໂທລະຄົມສາມາດໃຊ້ຖານຄວາມຮູ້ດ້ານຄວາມປອດໄພຂອງເຄືອຂ່າຍນີ້ໃນການກຳນົດມາດຕະການຄວບຄຸມ ແລະ ດຳເນີນການປະເມີນຜົນໂດຍອີງຕາມຮູບແບບການກຳນົດມາດຕະຖານດ້ານຄວາມປອດໄພຂອງອຸປະກອນເຄືອຂ່າຍຂອງ GSMA.

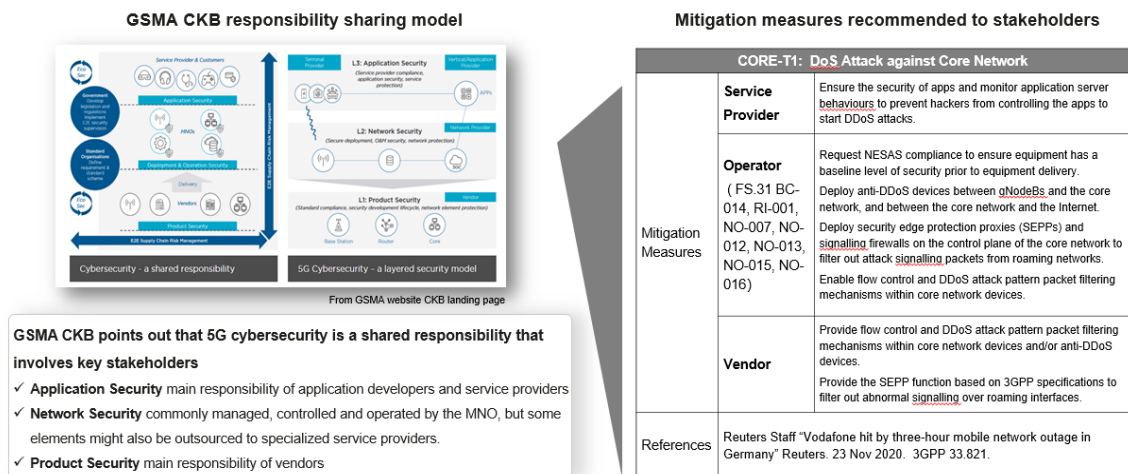
ຖານຄວາມຮູ້ໃນການວິເຄາະຄວາມສ່ຽງຄວາມປອດໄພຂອງອຸປະກອນ, ວິທີການໂຈມຕີ, ແລະ ຜົນກະທົບຂອງເຄືອຂ່າຍໂທລະສັບເຄື່ອນທີ່.

Comprehensive and structured threat analysis for mobile networks				Detailed attack methods and impact description	
Fields	Threats	Fields	Threats	CORE-T1: DoS Attack against Core Network	
Application UE RAN	Malicious Applications	Core Network	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.
	UE Compromising		Voice call eavesdropping		
	Theft of Personal Data		Mobile communication monitoring		
	UICC based web browser compromise	Cloud	NF API Exploitation	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.
	UICC credential theft		SMS Eavesdropping		
	IMSI Catching		CDR Harvesting		
	DoS Against Terminal Device	Inter connect	Virtual Machine Abuse	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.
	5G/4G/3G to 2G Downgrade		DDoS attacks against MEC		
	DoS Attack Against the Network		Abuse of MEC APIs		
	SMS Spam	Network O&M	Unauthorized Access to the Slice Management Plane		
	Passive Eavesdropping		Network Slice Resource Pre-emption		
	Impersonating Calls and Texts		Network Slice Data Theft and Tampering		
	Active Eavesdropping		Spoofing Attack for Roaming Interconnections		
	Radio Jamming		Location Data Breach		
	Breaking LTE on Layer 2		Eavesdropping/Tampering the Data on Roaming Interconnections		
	FBS enabled LTE billing compromise		HLR Outage		
	Privacy Attacks using Side Channel Information		A2P SMS Re-routing		
	5G authentication		SS7 RCE and Tunneling		
	LTE Inspector		Identity Theft or Fraud		
	IMP4GT: IMPersonation Attacks in 4G NeTworks		Exploitation of network configuration data weakness		
	REVOLTE		Log Tampering		
	Stealthy Location Identification Attack				
	GPSR Cryptanalysis Security				
	Hijacking TCP Connection under LTE/5G Network				

ຮູບທີ 10 ຄູ່ມືຄໍາແນະນຳຂອງ 5G CKB ໃນການຈັດການຄວາມປອດໄພຂອງເຄືອຂ່າຍ

(ຮູບພາບ: <https://www.gsma.com/security>)

ກຳນົດຄວາມຮັບຜິດຊອບໃນການຫຼຸດຄວາມສ່ຽງຂອງຜູ້ມີສ່ວນໄດ້ສ່ວນເສຍໃນອຸດສາຫະກຳໂທລະຄົມມະນາຄົມ



ຮູບທີ 11 ການຮ່ວມກັນທຸກພາກສ່ວນເພື່ອຄວາມປອດໄພຂອງເຄືອຂ່າຍ

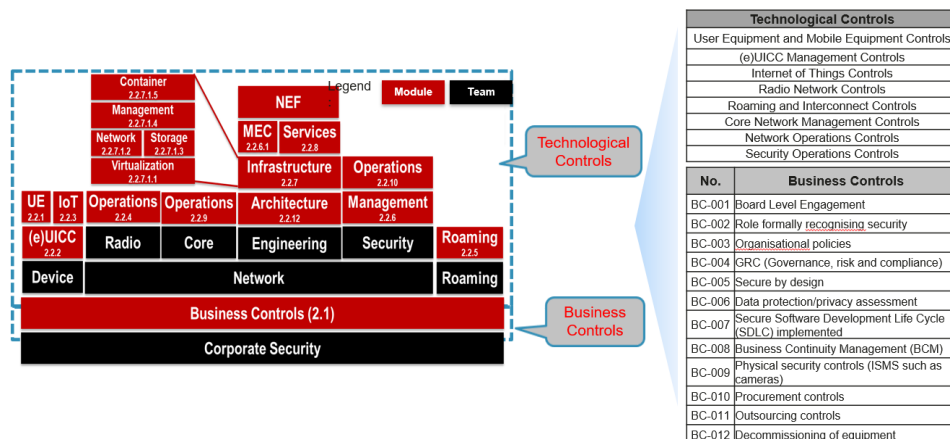
(ຮູບພາບ: <https://www.gsma.com/security>)

ສໍາລັບຕົວຢ່າງຂອງ Core-T1, ມາດຕະການທີ່ແນະນຳສໍາລັບຜູ້ມີສ່ວນໄດ້ສ່ວນເສຍໃນອຸດສາຫະກຳໂທລະຄົມມະນາຄົມທັງ 3 ພາກສ່ວນ:

ສໍາລັບຜູ້ໃຫ້ບໍລິການ: ຄວາມປອດໄພດ້ານການໃຊ້ງານໃນພາກອຸດສາຫະກຳການຜະລິດຈຳເປັນຕ້ອງມີຫລາຍພາກສ່ວນເຮັດວຽກຮ່ວມກັນເພື່ອຮັບປະກັນດ້ານຄວາມປອດໄພໃນເຄືອຂ່າຍ 5G ຕັ້ງແຕ່ຕົ້ນທາງຈົນເຖິງປາຍທາງ ເຊິ່ງສິ່ງເຫຼົ່ານີ້ແມ່ນຈະບໍ່ພຽງແຕ່ຈະຂຶ້ນກັບຄວາມປອດໄພຂອງເຄືອຂ່າຍຜູ້ໃຫ້ບໍລິການເທົ່ານັ້ນ ຈຳເປັນຈະຕ້ອງໄດ້ມີສ່ວນຮ່ວມນຳກັນ. ສໍາລັບຜູ້ໃຫ້ບໍລິການແມ່ນຮັບຜິດຊອບການຮັບປະກັນດ້ານຄວາມປອດໄພຂອງອຸປະກອນໃນເຄືອຂ່າຍເພື່ອຄວາມປອດໄພຂອງ ການວາງແຜນບຳລຸງຮັກສາ O&M, ການວາງແຜນເຄືອຂ່າຍ ແລະ ການຕິດຕັ້ງອຸປະກອນເປັນຕົ້ນ.

ສໍາລັບຜູ້ຜະລິດ: ແມ່ນຮັບຜິດຊອບໃນສ່ວນຂອງການຮັບປະກັນຄວາມປອດໄພຂອງອຸປະກອນຕັ້ງແຕ່ຂັ້ນຕອນລິເລີ່ມຕົ້ນຂະບວນຜະລິດ, ໃນການຮັບປະກັນດ້ານຄວາມປອດໄພຂອງອຸປະກອນໂດຍເນັ້ນໜັກໄປທີ່ການປະຕິບັດຕາມຂໍ້ກຳນົດຂອງວົງຈອນການພັດທະນາທີ່ປອດໄພ Lifecycle Development Secure (SDL), ແລະ ສາມາດໃນການປ້ອງກັນຄວາມສ່ຽງຕ່າງໆທີ່ອາດຈະເກີດຂຶ້ນຂັ້ນຕອນການຜະລິດ.

GSMA ໄດ້ສ້າງແຫລ່ງສູນລວມຂໍ້ມູນເພື່ອຜູ້ມີສ່ວນໄດ້ສ່ວນເສຍໃນອຸດສາຫະກຳໂທລະຄົມມະນາຄົມສາມາດເອົາໄປປັບໃຊ້ເປັນແຫລ່ງອ້າງອີງໃນການວາງແຜນເຄືອຂ່າຍພາຍໃນອົງກອນຂອງຕົນ.



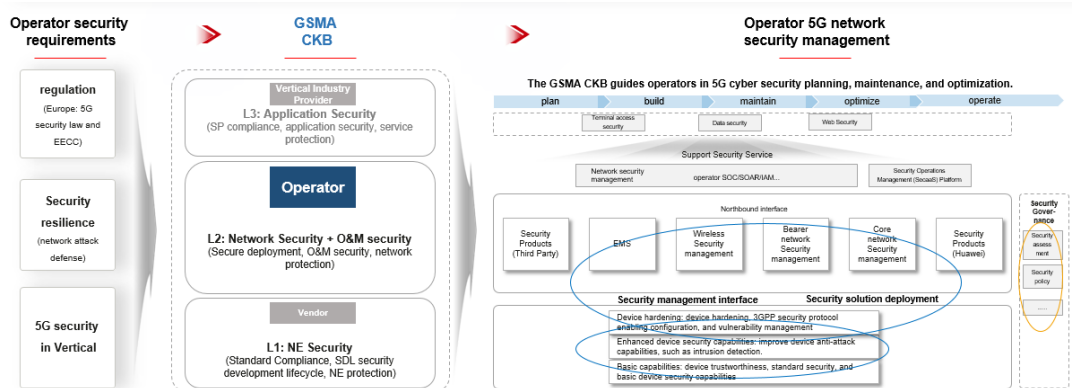
ຮູບທີ 12 ຄໍາແນະນຳພື້ນຖານສໍາລັບການພິຈາລະນາພື້ນຖານດ້ານຄວາມປອດໄພຂອງເຄືອຂ່າຍ

(ຮູບພາບ: <https://www.gsma.com/security>)

ຖານຄວາມຮູ້ດ້ານການຈັດການດ້ານຄວາມປອດໄພສໍາລັບຜູ້ໃຫ້ບໍລິການເຄືອຂ່າຍໂທລະຄົມມະນາຄົມໄດ້ແບ່ງອອກເປັນ 2 ພາກສ່ວນຄື: ພາກສ່ວນການຄວບຄຸມໃນສ່ວນຂອງການບໍລິການ ແລະ ການຄວບຄຸມທາງເຕັກໂນໂລຊີທີ່ນຳໃຊ້. ຜູ້ໃຫ້ບໍລິການສາມາດປັບໃຊ້ຖານຄວາມຮູ້ເຫຼົ່ານີ້ໃຫ້ກັບການຮັກສາຄວາມປອດໄພຂອງອຸປະກອນ, ການບໍລິການ ແລະ ເພື່ອປະເມີນຊ່ອງວ່າງທີ່ອາດຈະເກີດຂຶ້ນພາຍໃນອົງກອນຂອງຕົນ.

ຖານຄວາມຮູ້ຂອງດ້ານຄວາມປອດໄພຂອງເຄືອຂ່າຍ 5G CKB ແມ່ນຂົວຕໍ່ລະຫວ່າງ "ຄວາມຕ້ອງການຂອງຜູ້ປະກອບການເພື່ອຮັບປະກັນດ້ານສອດຄ່ອງຂອງອຸປະກອນ, ຄວາມປອດໄພ/ຄວາມຍືດຍຸ່ນ ແລະ ສ້າງຄວາມປອດໄພໃຫ້

ກັບພາກອຸດສາຫະກຳການຜະລິດ” ແລະ "ຄວາມອາດສາມາດໃນການພັດທະນາລະບົບເຄືອຂ່າຍ 5G ໃຫ້ມີຄວາມປອດໄພໃນການວາງແຜນລະບົບ, ພື້ນຖານໂຄງລ່າງເຄືອຂ່າຍ, ການບຳລຸງຮັກສາ, ແລະ ການດຳເນີນງານຕ່າງໆ"



ສຳລັບຜູ້ໃຫ້ບໍລິການເຄືອຂ່າຍການສື່ສານໂທລະຄົມມະນາຄົມ, ທີ່ຈະຕ້ອງໄດ້ຄຳນຶງເຖິງຄວາມປອດໄພຂອງອຸປະກອນທີ່ນຳມາຕິດຕັ້ງໃນລະບົບເຄືອຂ່າຍຂອງຕົນ ລວມໄປເຖິງຮູບແບບການບໍລິການຕ່າງໆ, ຈຳເປັນຕ້ອງໄດ້ພິຈາລະນາເຖິງແນວທາງການຈັດການກັບບໍລິການທີ່ຫລາກຫລາຍ ແລະ ມີຮູບແບບໃໝ່ທີ່ເກີດຂຶ້ນໃນການບໍລິການຂອງ 5G. ຢ່າງໃດກໍຕາມທາງຜູ້ໃຫ້ບໍລິການເອງກໍສາມາດຊອກຫາແນວທາງໃນການຈັດຕັ້ງປະຕິບັດເພື່ອຈັດການ ແລະ ຮັບມືກັບສິ່ງດັ່ງກ່າວໃນການວາງແຜນເຄືອຂ່າຍຂອງຕົນເພື່ອຮັບປະກັນດ້ານຄວາມປອດໄພຂອງລະບົບ ສາມາດອ້າງອີງໄດ້ຈາກ GSMA CKB ທີ່ໄດ້ເປັນບ່ອນຮວບຮວມ ແລະ ໃຫ້ຄຳແນະນຳຈາກບັນດາຜູ້ຊ່ຽວຊານໃນອຸດສາຫະກຳໂທລະຄົມມະນາຄົມ, ບັນດາຜູ້ຜະລິດອຸປະກອນຕ່າງໆໃນການເປັນລະບົບນິເວດຫນຶ່ງເພື່ອເປັນແນວທາງໃຫ້ກັບທຸກພາກສ່ວນທີ່ມີສ່ວນໄດ້ສ່ວນເສຍໃນເທັກໂນໂລຊີ 5G. ລາຍລະອຽດເພີ່ມຕື່ມ GSMA 5G CKB

<https://www.gsma.com/security/5g-cybersecurity-knowledge-base/>

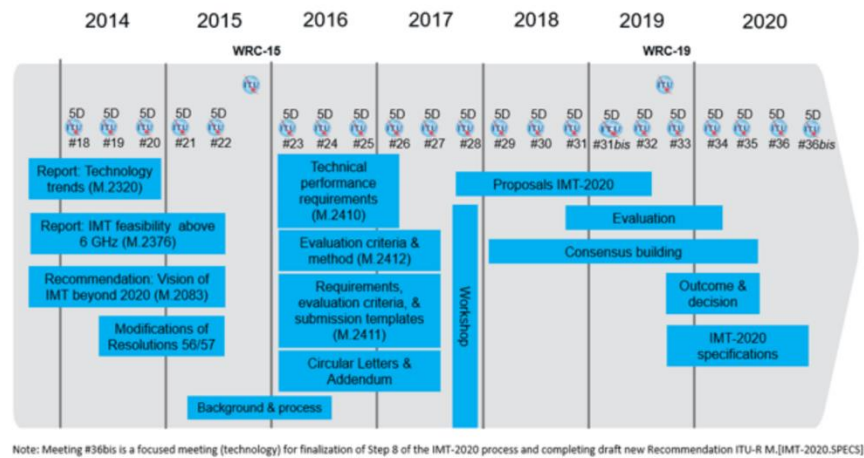
5 ການພັດທະນາ ແລະ ສົ່ງເສີມດ້ານຄວາມປອດໄພ

5.1 ການພັດທະນາ ແລະ ການຊຸກຍູ້ສົ່ງເສີມຈາກສາກົນຂອງມາດຕະຖານ NESAS

ຜູ້ມີສ່ວນໄດ້ສ່ວນເສຍໃນອຸດສາຫະກຳໂທລະຄົມມະນາຄົມໄດ້ສົ່ງເສີມການຮ່ວມມືເພື່ອການພັດທະນາມາດຕະຖານຄວາມປອດໄພທີ່ຢັ້ງຢືນໃນຮູບແບບການລວມສູນເອກະພາບກັນໃນທົ່ວໂລກສຳລັບເທັກໂນໂລຊີ 5G. 3GPP 5G ໄດ້ກາຍເປັນມາດຕະຖານທາງເທັກນິກ ITU IMT-2020 ຢ່າງເປັນທາງການໃນວັນທີ 10 ມັງກອນ 2020.

ວັນທີ 10 ກໍລະກົດ 2020, ມີຕົວແທນ ແລະ ຜູ້ຊ່ຽວຊານຫລາຍກວ່າ 200 ທ່ານ ຈາກໜ່ວຍງານພາກລັດ, ບໍລິສັດຜູ້ຜະລິດ, ຜູ້ໃຫ້ບໍລິການດ້ານເຄືອຂ່າຍໂທລະຄົມມະນາຄົມ ແລະ ບັນດານັກວິໄຈຈາກທົ່ວໂລກ ໄດ້ມີການປະຊຸມທາງໄກ ITU-R WP 5D#35e ໄດ້ມີການປະກາດຮ່ວມກັນວ່າເທັກໂນໂລຊີ 3GPP 5G (ລວມເຖິງ NB-IoT) ມີຄຸນສົມບັດກົງຕາມຂໍ້ກຳນົດຂອງມາດຕະຖານທາງເທັກນິກ IMT-2020 5G ແລະ ໄດ້ຮັບການຍອມຮັບຢ່າງເປັນທາງການວ່າເປັນ ITU IMT-2020 ເປັນມາດຕະຖານທາງເທັກນິກຂອງ 5G ດ້ວຍການຮ່ວມມືຢ່າງໃກ້ຊິດຈາກບັນດາປະເທດຕ່າງໆ ແລະ ພາກອຸດສາຫະກຳຕ່າງໆທົ່ວໂລກ. ITU ໄດ້ບັນລຸຄວາມສຳເລັດຂອງມາດຕະຖານເທັກໂນໂລຊີ 5G ຂອງ IMT-2020 ຕາມແຜນ ແລະ ນຳພາໂລກເຂົ້າສູ່ຍຸກອັດສະລິຍະຂອງການເຊື່ອມຕໍ່ຂອງສິ່ງສັບພະສິ່ງ (Internet of Thing).

WP 5D timeline for IMT-2020 Detailed specifications for the terrestrial radio interfaces



ຮູບທີ 13 ໄລຍະເວລາຂອງ ITU-R WP-5D IMT 2020

(ຮູບພາບ: <https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx>)

ITU-R WP 5D ແມ່ນໜຶ່ງໃນກຸ່ມເຮັດວຽກທີ່ສຳຄັນທີ່ສຸດຂອງ ITU. ທີ່ຮັບຜິດຊອບໃນການກຳນົດມາດຕະຖານຂອງການສື່ສານພາກພື້ນດິນ (International Mobile Telecommunication (IMT)). ໃນໄລຍະ 20 ກວ່າປີທີ່ຜ່ານມາ, ເທັກໂນໂລຢີການສື່ສານມີຖື 3G (IMT-2000) ແລະ 4G (IMT-Advanced) ທີ່ພັດທະນາໂດຍ ITU-R WP 5D ໄດ້ປະສົບຜົນສຳເລັດເປັນຢ່າງສູງໃນທົ່ວໂລກພາຍໃຕ້ການນຳຂອງ ITU-R WP 5D ປະເທດ ແລະ ອົງກອນລະດັບພູມມິພາກຈະຍັງຄົງຮ່ວມມືກັນຕໍ່ໄປ ITU-T Study Group 17 (Security) ປະຕິບັດຕາມມາດຕະຖານຄວາມປອດໄພ 3GPP SA3 ແລະ ການວິໄຈດ້ານຄວາມປອດໄພຂອງເທັກໂນໂລຢີທີ່ທັນສະໄໝ.

ITU-T Study Group 17 (Security) ແມ່ນກຸ່ມສຶກສາດ້ານຄວາມປອດໄພໂດຍ 3GPP SA3 ໄດ້ ປະຕິບັດຕາມມາດຕະຖານຄວາມປອດໄພ ແລະ ການຄົ້ນຄວ້າກ່ຽວກັບຄວາມປອດໄພເທັກໂນໂລຢີທີ່ມີການສື່ສານ.

ຮ່າງການດຳເນີນການ ITU-T SG17 X.5Gsec ອີງຕາມໂຄງການຄວາມປອດໄພ 3GPP 5G.

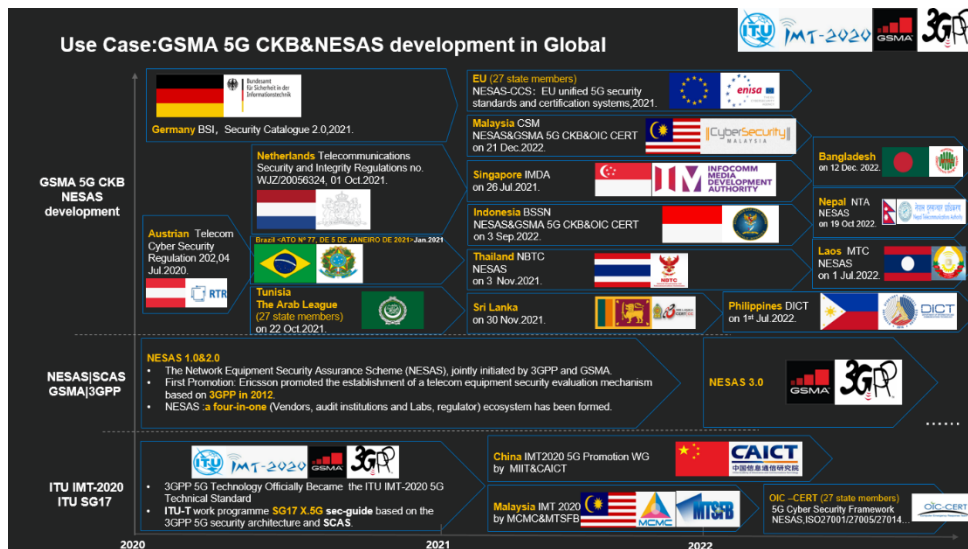
ຂະບວນການທຳງານຂອງ ITU, ດັ່ງທີ່ອະທິບາຍໃນຄຳແນະນຳຂອງ ITU-T A.5, ອ້າງອີງເຖິງເອກະສານທີ່ເຜີຍແຜ່ ITU (ນອກຈາກ ISO ແລະ IEC) ຈຳເປັນຕ້ອງໄດ້ຮັບການປະເມີນຜົນໂດຍກຸ່ມການສຶກສາ ITU-T Study Group ກ່ອນ ເຊິ່ງອ້າງອີງໃນຄຳແນະນຳຂອງ ITU-T. ໃນເອກະສານລຸ່ມນີ້ໄດ້ຮວບຮວມຂໍ້ມູນ A.5 ສຳລັບ ຂອງ X.5Gsec "ຄູ່ມືຄວາມປອດໄພສຳລັບລະບົບສື່ສານ 5G" ຮ່າງຄຳແນະນຳລຸ່ມນີ້ແມ່ນອ້າງອີງຈາກສະຖາປັດຕະຍະກຳຄວາມປອດໄພຂອງ 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) 61
Contact(s):	Mee Yeon Kim, Editor Keundug Park, Editor Heung Youl Youm, Editor

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



ຮູບທີ 14 ການພິຈາລະນາ GSMA 5G CKB ແລະ NESAS

Rang	Achievement
Global	3GPP 5G has officially become the ITU IMT-2020 5G technical standard in July 10, 2020. ITU-T work programme SG17 X.5Gsec-guide based on the 3GPP 5G security architecture. Note : International Mobile Telecommunications-2020 (IMT-2020 Standard) are the requirements issued by the ITU Radiocommunication Sector (ITU-R) of the International Telecommunication Union (ITU) in 2015 for 5G networks, devices and services.
EU	EU recognizes the NESAS-CCS as a unified certification standard under the EU Cyber Security Act from. https://www.enisa.europa.eu/news/enisa-news/calling-on-you-5g-experts-join-us-on-5g-cybersecurity-certification
Germany	Germany Security Catalogue 2.0 recognized NESAS as a 5G security certification standard and worked with all parties to promote the development of a unified 5G certification standard in the EU from 2020. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220705_Zertifizierung_5G-Komponenten.html
Austria	The Austrian telecom regulator RTR has adopted the SCAS standard for telecom security regulation in the Telecom Cyber Security Regulation 2020 (TK-NSiV 2020). Official support for inclusion of NESAS into the EU cyber security certification framework 2020.07. 04 https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/Telekom-Netzsicherheitsverordnung_2020_(TK-NSiV_2020.de.htm
Netherlands	Regulation of the Minister of Economic Affairs and Climate of 1 October 2021, no. WJZ/20056324, containing further rules regarding the security and integrity of public electronic communications networks and services (Telecommunications Security and Integrity Regulations). https://zoek.officielebekendmakingen.nl/stcrt-2021-42618.html
Brazil	Item 2 of <ATO N° 77, DE 5 DE JANEIRO DE 2021> Cyber Security Requirements for Telecommunications Equipment, released by Anatel in 2020 and effective in 2021, lists NESAS/SCAS as the reference standard for telecommunications equipment, 2021.01. https://www.in.gov.br/web/dou/-/ato-n-77-de-5-de-janeiro-de-2021-297933302
China	NESAS has been approved as the basic standard for 5G security assessment and has been implemented by China's IMT 2020 promotion team. All 5G equipment suppliers in the Chinese market comply with the NESAS standard system.

	Approximately 1.5 million 5G sites in China's 5G networks (as of December 2021) were expected to be NESAS compliant and certified. http://www.caict.ac.cn/kxyj/qwfb/bps/202002/t20200204_274118.htm
Singapore	Singapore government has acknowledged NESAS (IMDA 21 GHz Public Consultation Document) on 26 July 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
Thailand	The Office of the National Broadcasting and Telecommunications Commission (NBTC) officially released the national 5G security guideline to call for stakeholders of Thailand telecom industry to comply NESAS standards on 3rd Nov. 2021. https://www.nbtct.go.th/News/govnewspartner/51190.aspx
Philippines	Philippines Department of Information and Communications Technology (DICT) officially released the national 5G security guideline, recognized and adopted NESAS to call for stakeholders of Philippines telecom industry to comply NESAS standards on 1st July 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
Laos	Laos Ministry of Technology and Communications (MTC) officially released the national 5G security guideline, recognized and adopted NESAS on 1st July 2022. https://mtc.gov.la/index.php?r=site%2Fdetail&id=897
Tunisia/The Arab League	The Arab League officially recognized and adopted the NESAS standard by cyber security white paper on October 22, 2021. https://www.mtcn.gov.tn/index.php?id=119&L=-1%5C%27&tx_ttnews%5Btt_news%5D=4335&cHash=8004500dd3cd4237a6fa9226d916c7df
OIC-CERT 5G Security Framework Promotion Plan	Mutual Certification Mechanism Implementation: implement the certification mechanism with security standards (NESAS/SCAS, cloud security, etc) in some key/pilot OIC member states in 2022, which would be selected from different regions and states, later. The finally confirmed key/pilot countries should satisfy with following one or more conditions: ① Have friendly relationships with each other selected ones; ② Be good at propagation and impact expansion; ③ Have good wiliness to strength cyber security capacity. 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
Indonesia	On September 3, 2022, Indonesia BSSN&ITDel jointly released the a BOOK of strategic Analysis for Indonesia Cyber Security Toward To 5G Technology Era, which officially recognized and adopted NESAS SCAS, OIC CERT 5G security framework, and 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/
Nepal	Nepal Telecommunications Authority (NTA) officially released the national 5G security guideline to recognized and adopted NESAS on 19 Oct. 2022. https://nta.gov.np/en/consultation-paper/ https://nta.gov.np/wp-content/uploads/2022/10/Review-Paper-about-NESAS.pdf
Bangladesh	Bangladesh BRTC officially acknowledged NESAS(ITU、GSMA、3GPP) in national mobile service on 12 Dec. 2022. http://www.brtc.gov.bd/
Malaysia	CSM under KKMM of the Malaysia Ministry of Communications publicly recognized and adopted the NESAS&GSMA 5G CKB&OIC CERT 5G security framework and officially released a guideline on the CSM official website on 21 Dec.2022. https://www.cybersecurity.my/en/knowledge_banks/articles/main/detail/2372/index.html https://www.cybersecurity.my/data/content_files/13/2383.pdf
Sri Lanka	Sri Lanka cert and multi-stakeholder achieved the consensus on NESAS scheme to be national 5G security standard on 30th Nov 2021. https://www.ft.lk/it-telecom-tech/5G-roll-out-challenges--Governance--legislation--awareness--capacity-and-NESAS-standards/50-726824

6 ບົດສະຫຼຸບ ແລະ ແນວທາງ

ວິທີການຍັງຢືນຄວາມປອດໄພຕ່າງໆໄດ້ຖືກສ້າງຕັ້ງຂຶ້ນຫລາຍກວ່າ 30 ປີເພື່ອປະເມີນຜົນຄວາມປອດໄພຂອງຜູ້ສະໜອງອຸປະກອນ ແລະ ຜູ້ໃຫ້ບໍລິການໂທລະສັບເຄື່ອນທີ່. NESAS ແມ່ນມາດຕະຖານເພື່ອຮັບປະກັນໃຫ້ກັບອຸປະກອນໂທລະສັບມະນາຄົມໃນຍຸກຂອງການສື່ສານ 5G, ຂອບເຂດ NESAS ກວມເອົາມາດຕະຖານຄວາມປອດໄພ ແລະ ການປະເມີນຜົນຄຸນນະພາບ ແລະ ຄຸນນະສົມບັດຂອງອຸປະກອນສື່ສານນັບຕັ້ງແຕ່ການວາງແຜນ, ອອກແບບ ແລະ ການຜັດທະນາ. ສິ່ງເຫລົ່ານີ້ຈະສ້າງຜົນປະໂຫຍດໃຫ້ກັບທັງຜູ້ຜະລິດອຸປະກອນ ແລະ ຜູ້ໃຫ້ບໍລິການເຄືອຂ່າຍ. NESAS ນີ້ສາມາດເປັນແນວທາງໃຫ້ກັບຜູ້ຜະລິດເພື່ອຜັດທະນາ ແລະ ຜະລິດອຸປະກອນຂອງຕົນທີ່ມີຄຸນນະພາບສູງ ແລະ ຮັບປະກັນດ້ານຄວາມປອດໄພ. ຜູ້ໃຫ້ບໍລິການໂທລະສັບເຄື່ອນທີ່ຍັງສາມາດນຳໃຊ້ໂມເດວມາດຕະຖານຂອງ NESAS ເພື່ອຜັດທະນານະໂຍບາຍ ແລະ ມາດຕະຖານເພື່ອໃຫ້ບໍລິການເຄືອຂ່າຍທີ່ປອດໄພທີ່ສຸດ. NESAS ສາມາດນຳໄປໃຊ້ເປັນມາດຕະຖານຄວາມປອດໄພທີ່ເປັນກາງ ແລະ ໂປ່ງໃສທັງໃນລະດັບປະເທດ, ແລະ ສາກົນໄດ້ສຳລັບໜ່ວຍງານພາກລັດທີ່ຮັບຜິດຊອບດ້ານນະໂຍບາຍ.

ມາດຕະຖານຄວາມປອດໄພທາງດ້ານອຸປະກອນການສື່ສານແບບຄົບວົງຈອນ, ລວມໄປເຖິງວິທີການປະຕິບັດຕາມກົດລະບຽບ ແລະ ການທົດສອບມາດຕະຖານ. ສາມາດຊ່ວຍເຫຼືອໃຫ້ຜູ້ໃຊ້ງານມີຄວາມເຊື່ອໝັ້ນຫລາຍຂຶ້ນຕໍ່ກັບລະບົບຂອງຜູ້ໃຫ້ບໍລິການເອງ. ໃນທາງກົງກັນຂ້າມກັບການມີມາດຕະຖານທີ່ຫລາກຫລາຍ ແລະ ຫ່ວງໄສອຸປະທານຕ່າງໆ, ຄວາມປອດໄພຂອງລະບົບທີ່ນຳມາເປັນມາດຕະຖານດຽວຮ່ວມກັນຈະສົ່ງເສີມເຮັດໃຫ້ມີການແຂ່ງຂັນທີ່ຫລາຍຂຶ້ນ ເຊິ່ງຜົນທີ່ໄດ້ກໍຄື ອຸປະກອນໂທລະສັບມະນາຄົມມີຄຸນນະພາບສູງໃນລາຄາທີ່ຖືກລົງ, ເກີດມີນະວັດຕະກຳໃໝ່ເກີດຂຶ້ນ, ເພື່ອຄວາມຫນ້າເຊື່ອຖືໃຫ້ກັບທຸກພາກສ່ວນ ແລະ ມີຄວາມຍືດຍຸ່ນ.

ຜື້ນຖານຄວາມຮູ້ດ້ານຄວາມປອດໄພຂອງອຸປະກອນທາງໄຊເບີປະກອບດ້ວຍການລົງປະຊາມະຕິເຫັນດີເຫັນພ້ອມຈາກພາກສ່ວນທີ່ກ່ຽວຂ້ອງໃນອຸດສາຫະກຳໂທລະສັບມະນາຄົມ, ຍຸດທະສາດການປ້ອງກັນດ້ານຄວາມສ່ຽງຕ່າງໆ ພ້ອມທັງມີແບບແຜນແນວທາງຕໍ່ການວາງແຜນ, ຄຳແນະນຳ ແລະ ທັງເປັນເຄື່ອງມືທີ່ມີປະສິດທິພາບໃນການຊ່ວຍໃຫ້ເຮົາເຂົ້າໃຈ ແລະ ຕໍ່ສະໜອງຕໍ່ຄວາມສ່ຽງຕ່າງໆໃນເຄືອຂ່າຍ 5G ໄດ້ໃນລະດັບເທັກນິກ.

ການນຳໃຊ້ມາດຕະຖານ NESAS ແລະ ຖານຄວາມຮູ້ຂອງ GSMA 5G CKB ສາມາດເປັນປະໂຫຍດໃນທຸກຂະແໜງການ ແລະ ໃນຫຼາຍຮູບແບບຂອງຄວາມປອດໄພໃນອຸດສາຫະກຳໂທລະສັບ. ຜູ້ຜະລິດອຸປະກອນໃຊ້ມາດຕະຖານ NESAS ເພື່ອຊື້ເປັນແນວທາງຊີ້ນຳການອອກແບບຂະບວນການຜັດທະນາຜະລິດຕະພັນທີ່ສົມບູນດ້ວຍການປະຕິບັດໃຫ້ສອດຄ່ອງກັບຄວາມປອດໄພ ແລະ ຜະລິດອຸປະກອນທີ່ມີຄຸນສົມບັດຄວາມປອດໄພຕາມມາດຕະຖານ ແລະ ຄຸນນະສົມບັດທີ່ນຳໃຊ້ໃນເຄືອຂ່າຍໂທລະສັບ. ຜູ້ໃຫ້ບໍລິການໂທລະສັບເຄື່ອນທີ່, ອົງກອນພາກລັດທີ່ເປັນຜູ້ອອກນະໂຍບາຍ ແລະ ອົງການຕ່າງໆທີ່ກ່ຽວຂ້ອງກໍໄດ້ຮັບຜົນປະໂຫຍດຈາກມາດຕະຖານດັ່ງກ່າວເພາະມີການຍັງຢືນຈາກຕົ້ນທາງຈົນເຖິງປາຍທາງໃນການກວດສອບ ແລະ ປະເມີນຜົນ. ຜື້ນຖານຄວາມຮູ້ຂອງ GSMA 5G CKB ໄດ້ຊ່ວຍເຫຼືອ ແລະ ຊຸກຍູ້ການຮ່ວມມືທຸກພາກສ່ວນເພື່ອເພື່ອສ້າງຄວາມເຂັ້ມແຂງໃຫ້ກັບເຄືອຂ່າຍ ແລະ ການບໍລິການ, ເພື່ອຫຼຸດຜ່ອນຄວາມສ່ຽງຕ່າງໆທີ່ອາດຈະເກີດຂຶ້ນ. ຖານຄວາມຮູ້ເຫລົ່ານີ້ຈະຊ່ວຍເພີ່ມຄວາມອາດສາມາດ ແລະ ຄວາມສາມາດດ້ານຄວາມປອດໄພຂອງອຸປະກອນ 5G ແລະ ຈະເສີມສ້າງຄວາມເຂັ້ມແຂງຂອງການປະຕິບັດງານຂອງກອນ, ທຸລະກິດ, ພາກສ່ວນຂອງລັດ. ໃນລະດັບການປະຕິບັດງານຖານຄວາມຮູ້ເຫລົ່ານີ້ມີຄຳແນະນຳທີ່ຊັດເຈນສຳລັບການດຳການໃນແຕ່ລະຂັ້ນຕອນເພື່ອສ້າງຄວາມໝັ້ນໃຈດ້ານຄວາມປອດໄພໃນການພິຈາລະນາເຖິງຄວາມສ່ຽງທີ່ອາດຈະເກີດຂຶ້ນໃນລະບົບ

5G ແບບ End to End. ກະຊວງເທັກໂນໂລຊີ ແລະ ການສື່ສານ ໄດ້ສະໜັບສະໜູນ ແລະ ໃຫ້ຄວາມສໍາຄັນໃນການນໍາເອົາມາດຕະຖານດ້ານຄວາມປອດໄພຂອງອຸປະກອນເຄືອຂ່າຍເຊັ່ນ: NESAS ແລະ GSMA 5G CKB ເນື່ອງຈາກສາມາດນໍາໃຊ້ມາດຕະຖານນີ້ເປັນບ່ອນອີງໃນການຄຸ້ມຄອງອຸປະກອນເຄືອຂ່າຍ 5G ໃຫ້ມີຄວາມປອດໄພສູງສຸດກ່ອນນໍາເຂົ້າ ແລະ ນໍາໃຊ້ໃນ ສປປ ລາວ. ມາດຕະຖານດັ່ງກ່າວແມ່ນມີບົດບາດໃນການຂັບເຄື່ອນການບໍລິການໂທລະຄົມມະນາຄົມໃຫ້ທັນສະໄໝ ແລະ ມີຄວາມປອດໄພຫຼາຍຂຶ້ນໂດຍນໍາໃຊ້ມາດຕະຖານ NESAS ແລະ ຖານຄວາມຮູ້ຂອງ GSMA 5G CKB.

ເອກະສານຊ້ອນທ້າຍ A

ລດ	ເອກະສານ	ເນື້ອໃນ
[1]	TS 33.116	Security Assurance Specification (SCAS) for the MME network product class
[2]	TS 33.117	Catalogue of general security assurance requirements
[3]	TS 33.216	Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class
[4]	TS 33.250	Security assurance specification for the PGW network product class
[5]	TS 33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
[6]	TS 33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
[7]	TS 33.513	5G Security Assurance Specification (SCAS); User Plane Function (UPF)
[8]	TS 33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
[9]	TS 33.515	5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class
[10]	TS 33.516	5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class
[11]	TS 33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
[12]	TS 33.518	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
[13]	TS 33.519	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class
[14]	FS.13	NESAS Overview v.2.0
[15]	FS.14	NESAS Security Test Laboratory Accreditation v.2.0
[16]	FS.15	NESAS Development and Lifecycle Assessment Methodology v.2.0
[17]	FS.16	NESAS Development and Lifecycle Security Requirements v.2.0
[18]	ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories
[19]	3GPP TS 37.145-1	3GPP TS 37.145-1 version 15.3.0 Release 15, <i>Active Antenna System (AAS) Base Station (BS) conformance testing; Part 1: conducted conformance testing</i>
[20]	3GPP TS 37.145-2	3GPP TS 37.145-2 version 15.3.0 Release 15, <i>Active Antenna System (AAS) Base Station (BS) conformance testing; Part 2: radiated conformance testing</i>

ລດ	ເອກະສານ	ເນື້ອໃນ
[21]	3GPP TS 38.104	3GPP TS 38.104 version 15.5.0 Release 15, <i>NR; Base Station (BS) radio transmission and reception</i>
[22]	3GPP TS 38.141-1	3GPP TS 38.141-1 version 15.2.0 Release 15, <i>NR; Base Station (BS) conformance testing Part 1: Conducted conformance testing</i>
[23]	3GPP TS 38.141-2	3GPP TS 38.141-2 version 15.3.0 Release 15, <i>NR; Base Station (BS) conformance testing Part 2: Radiated conformance testing</i>

ບົດຄວາມ: ໂດຍກົມຄົ້ນຄວາມຖີ່ວິທະຍຸສື່ສານ, ກະຊວງ ເຕັກໂນໂລຊີ ແລະ ການສື່ສານ.