التوصية

ITU-T X.1381 (03/2023)

السلسلة X شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة (2) – أمن أنظمة النقل الذكية (ITS)

مبادئ توجيهية أمنية بشأن الشبكات داخل المركبات القائمة على الإثرنت

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب	X.1140–X.1149
بروتوكولات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1360–X.1369
أمن أنظمة النقل الذكية (ITS)	**X.1370–X.1389**
أمن سجل الحسابات الموزع	X.1400–X.1429
بروتوكولات الأمن (2)	X.1450–X.1459
أمن الويب (2)	X.1470–X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
الدفاع السيبراني	X.1590–X.1599
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
مولِد الأعداد العشوائية الكمومية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية	X.1710–X.1711
تصميم أمن شبكات توزيع المفاتيح الكمومية	X.1712–X.1719
تقنيات أمن شبكات توزيع المفاتيح الكمومية	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
أمن شبكات الجيل الخامس	X.1770–X.1789
أمن الاتصالات المتنقلة الدولية-2020	X.1800–X.1819

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1381

مبادئ توجيهية أمنية من أجل الشبكات القائمة على الإثرنت داخل المركبات

ملخص

تقدم التوصية ITU-T X.1381 مبادئ توجيهية أمنية بشأن الشبكات داخل المركبات (IVN) القائمة على الإثرنت. ويتمثل الاتجاه الحالي في المعمارية الكهربائية والإلكترونية (E/E) في دمج الإثرنت مع الشبكات داخل المركبات التقليدية مثل شبكة منطقة وحدة التحكم (CAN) وشبكة التوصيل البيني المحلية (LIN) ونقل الأنظمة الموجه نحو الوسائط (MOST) وبروتوكول FlexRay. وفي الماضي، كان يُنظر إلى الإثرنت على أنها مجرد توصيل بين المركبات وبيئات خارجية. وقد استُعملت بروتوكولات معيارية لتمكين التوصيلات القائمة على بروتوكول الإنترنت عبر الإثرنت (مثل اتصالات التشخيص عبر بروتوكول الإنترنت أو بروتوكول القياس والمعايرة الشاملين) لتمكين الاتصالات بين البيئة الخارجية والمركبات. ولا تحتاج حالات الاستعمال هذه بوجه عام إلى فرض قيود صارمة في الوقت الفعلي. ولكن التطبيقات داخل المركبة التي تستعمل اتصالات الإثرنت تتطلب خصائص تشمل درجة عالية من الحساسية الزمنية والموثوقية.

وتتطلب التطورات الحالية في تكنولوجيات الاتصالات داخل المركبات زيادة عرض النطاق في الشبكة. ومقارنةً بالإثرنت، لا تكفي الشبكات التقليدية داخل المركبات لتلبية المتطلبات من عرض النطاق في التطبيقات الحالية داخل المركبة. ولذلك، تشكل الشبكات داخل المركبات القائمة على الإثرنت الآن وفي المستقبل جزءاً رئيسياً من المعمارية الكهربائية والإلكترونية (E/E).

بيد أن التدابير المضادة المعروفة من شبكات الحاسوب الشائعة لا يمكن أن تكون مناسبة لتطبيقات السيارات لأنها لم تصمم لتلبية متطلبات وقدرات السيارات.

ولتلبية هذا الطلب، تقدم هذه التوصية مبادئ توجيهية أمنية بشأن تكنولوجيا إثرنت السيارات. وتتضمن هذه التوصية نموذجاً مرجعياً لإثرنت السيارات وتحليلاً للتهديدات ومواطن الضعف في الشبكات داخل المركبات (IVN) القائمة على الإثرنت. وبالإضافة إلى ذلك، تقدم هذه التوصية متطلبات الأمن وحالات استعمال الشبكات داخل المركبات القائمة على الإثرنت.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1381	2023-03-03	17	11.1002/1000/15107

مصطلحات أساسية

أمن إثرنت السيارات، أمن نظام النقل الذكي (ITS)

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة الأمم المتحدة المتخصصة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

الصفحة

التوصية ITU-T X.1381

مبادئ توجيهية أمنية بشأن الشبكات داخل المركبات القائمة على الإثرنت

1 مجال التطبيق

تقدم هذه التوصية مبادئ توجيهية أمنية بشأن الشبكات داخل المركبات (IVN) القائمة على الإثرنت. وتغطي التوصية:

1) تحليل التهديدات الأمنية؛

2) متطلبات الأمن؛

3) حالات الاستعمال،

من منظور الأمن السيبراني. ويشير الأمن السيبراني إلى أن معمارية الاتصالات التقنية المعنية تشكل، أو يمكن أن تشكل، جزءاً أساسياً من الأنظمة السيبرانية المادية (مثل كدسات بروتوكول اتصالات الإثرنت المركَّبة في الأنظمة المدمجة).

1.1 بيانات قابلية التطبيق

تُستعمل الشبكات بوجه عام، والشبكات على الإثرنت بوجه خاص، لخدمات الاتصالات. ومن ثم، يركز السياق الأمني في هذه التوصية على أمن الاتصالات، ولكن ليس بالضرورة على أمن المعلومات تحديداُ لعقد الحوسبة ذات توصيلية الإثرنت.

وبالتالي، تشمل المبادئ التوجيهية الأمنية في هذه التوصية هندسة الشبكات للشبكات القائمة على الإثرنت المستعملة في تطبيقات السيارات، من منظور هندسة الأمن. ومن ثم، فإن معماريات الاتصالات ذات الطبقات المصاحبة لها بكدساتها البروتوكولية ذات الطبقات تشكل جزءاً أساسياً من اعتبارات الأمن هذه.

2.1 التحقق من صحة المبادئ التوجيهية الأمنية خلال الجدول الزمني

يتطور أمن معماريات الاتصالات على النحو المطلوب لشبكات الإثرنت داخل المركبات بشكل أساسي، ويرجع ذلك في المقام الأول إلى ما يلي:

1) التغييرات الممكنة في طوبولوجيات الشبكة (المدفوعة بمعماريات الحوسبة الموزعة المتطورة باستعمال شبكات الاتصالات، في اتجاه أتمتة المركبات على سبيل المثال)؛

2) معماريات البروتوكول ذات الطبقات: يمكن أن تتغير كدسات بروتوكولات الإثرنت وغير الإثرنت الحالية المستعملة، وأن تحصل على توسعات، وما إلى ذلك؛

3) تطور البروتوكول: ما زالت بروتوكولات تكنولوجيا المعلومات والاتصالات قيد الاستعمال (كالتي تملكها منظمات وضع المعايير مثل معهد مهندسي الكهرباء والإلكترونيات (IEEE)، وفريق مهام هندسة الإنترنت (IETF)، وقطاع تقييس الاتصالات (ITU-T)، والمعهد الأوروبي لمعايير الاتصالات (ETSI)، ومشروع شراكة الجيل الثالث (3GPP)) تخضع لأنشطة وتوسيعات الصيانة الجارية التي تتجلى من خلال ملفات تعريف البروتوكول (مثل التوصيل الشبكي الحساس زمنياً (TSN) لمعهد مهندسي الكهرباء والإلكترونيات لتطبيقات السيارات [b-IEEE] أو إصدارات البروتوكول؛

ملاحظة – علاوةً على ذلك، قد تخضع اعتبارات الأمن المرتبطة بمواصفة البروتوكول للتحديث أيضاً.

4) تطور الوسائل والحلول الأمنية في سياق أمن الاتصالات.

ومن ثم، تُتوقع مراجعات مستقبلية لهذه التوصية.

وتركز هذه التوصية بصفة خاصة على المبادئ التوجيهية الأمنية الأولية التي تعطيها مجموعة أولى من حالات الاستعمال. ومجال التطبيق الأساسي هو الجيل الأول (الأجيال الأولى) للشبكات داخل المركبات (IVN) القائمة على الإثرنت، المؤدية إلى أفضل الممارسات الأمنية الحالية والمبادئ التوجيهية الأمنية وقت نشر هذه التوصية.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1371] التوصية ITU-T X.1371 (2020)، *التهديدات الأمنية التي تواجهها المركبات الموصولة*.

3 التعاريف

1.3 مصطلحات معرَّفة في مصادر أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

1.1.3 المساءلة (accountability) [b-ITU-T X.800]: خاصية تضمن أن أعمال كيان ما يمكن إسنادها إلى ذلك الكيان حصراً.

2.1.3 الاستيقان (authentication) [b-ITU-T X.1252]: عملية تحقق رسمية تؤدي، في حال نجاحها، إلى هوية مستيقَّنة لكيان.

ملاحظة – يؤخذ استعمال مصطلح استيقان في سياق إدارة الهوية (IdM) على أنه يعني استيقان كيان.

3.1.3 الاستيقانية (authenticity) [b-ITU-T X.641]: حماية من أجل الاستيقان المتبادل واستيقان أصل البيانات.

4.1.3 الترخيص (authorization) [b-ITU-T X.800]: منح الحقوق، الذي يتضمن إتاحة النفاذ استناداً إلى حقوق النفاذ.

5.1.3 التيسر (availability) [b-ITU-T X.800]: خاصية إمكانية النفاذ وإمكانية الاستعمال بناءً على طلب من كيان مرخص له.

6.1.3 السرية (confidentiality) [b-ITU-T X.800]: خاصية عدم إتاحة المعلومات أو الكشف عنها لأشخاص غير مرخص لهم أو لكيانات أو عمليات غير مرخص لها.

7.1.3 سلامة البيانات (data integrity) [b-ITU-T X.800]: خاصية بقاء البيانات على حالها دون أن يطرأ عليها تغيير أو تلف بطريقة غير مرخص بها.

8.1.3 جدار الحماية (firewall) [b-ITU-T X.1039]: نوع من الحواجز الأمنية يوضع بين البيئات الشبكية. وهو يتألف من جهاز مكرس أو مجموعة من عدة مكونات وتقنيات – تمر من خلاله كل الحركة العابرة من بيئة شبكية لأخرى، وبالعكس، ولا يسمح بمرور إلا الحركة المخوَّلة التي تحددها السياسات الأمنية المحلية.

9.1.3 بوابة الأمن (security gateway) [b-ITU-T X.1039]: نقطة توصيل بين الشبكات، أو بين المجموعات الفرعية ضمن الشبكات، أو بين تطبيقات البرمجيات ضمن ميادين أمنية مختلفة بغرض حماية الشبكة وفقاً لسياسة أمنية.

10.1.3 بوابة المركبة (VG) (vehicle gateway) [b-ITU-T F.749.1]: بوابة المركبة هي جهاز في مركبة تمكِّن الاتصالات بين جهاز في المركبة وجهاز آخر قد يقع مادياً داخل المركبة أو خارجها (كما في محطة على جانب الطريق، أو مخدِّم قائم على منصة سحابية، وما إلى ذلك). وتقدم بوابة المركبة سطوحاً بينية وبروتوكولات معيارية، واتصالات عبر شبكات غير متجانسة، واختيار

الشبكة المثلى استناداً إلى احتياجات التطبيق وجودة خدمة الشبكة، والتحكيم وتكامل اتصالات الشبكة، وتوصيلات الأمن والتبديل للحفاظ على استمرارية الخدمة.

الملاحظة 1 – إن مصطلح البوابة المركزية (كما جاء في هذه التوصية) مرادف عادة لمصطلح بوابة المركبة في الشبكات المجرَّدة داخل المركبات أو بوابات حدود المركبة في معماريات الشبكات داخل المركبات (IVN) الأكثر تفصيلاً.

الملاحظة 2 – إن مصطلح بوابة نظام النقل الذكي (ITS) للمركبة مرادف أساساً لبوابة المركبة.

2.3 مصطلحات معرَّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

1.2.3 المعمارية الكهربائية والإلكترونية (معمارية E/E): معمارية مركبة مقترنة ذات مستويين تتكون من: 1) مستوي شبكة توزيع القدرة أو الطاقة الكهربائية؛ و2) مستوي معماري لشبكة معالجة المعلومات والاتصالات.

ملاحظة – يضاف وسم ثالث أحياناً إلى الرمز E/E للدلالة على التكنولوجيا الدافعة للمركبة، فيصبح حرف E مكعباً (E^3)، ويشير حرف E الثالث إلى مركبة كهربائية.

2.2.3 بوابة حدود المركبة: بوابة مركبة تتموضع عند حدود ميدان (ميادين) الشبكة الداخلية للمركبة وميدان (ميادين) الشبكة الخارجية للمركبة. وبالتالي، تسيَّر كل حركة الاتصالات من مركبة إلى كل شيء (V2X) عبر هذا النمط من بوابات المركبة.

الملاحظة 1 – يغطي مصطلح بوابة المركبة هذا المعنى أيضاً، وبالتالي فهو قد يكفي لمعماريات الشبكة داخل المركبة (IVN) المزودة ببوابة مركبة واحد فقط. ولكن يمكن لمعماريات الشبكات داخل المركبة أيضاً حصر استعمال بوابات المركبة لأغراض التوصيل البيني الداخلي والتشغيل البيني. ويمكن لسياقات الشبكة هذه أن تحيج إلى التفريق بين أنماط البوابات بطريقة أكثر تفصيلاً.

الملاحظة 2 – كثيراً ما يعبَّر عن وظائف العمل البيني المحددة المدعومة من نمط بوابة معينة باسم ممتد، يشير على سبيل المثال إلى الموقع في تراتبية شبكة (مثل مستوى شبكة النفاذ أو الشبكة الأساسية)، أو نمط الحد أو التوصيل الشبكي البيني (مثل ميادين الأمن)، أو سطوح بينية محددة للشبكة أو تكنولوجيات الاتصالات محددة.

الملاحظة 3 – تُفهم وحدة التحكم في الاتصالات كمكون تقني ينتمي إلى فئة بوابة حدود للمركبة (الوظائف).

الملاحظة 4 – تشمل الاتصالات من مركبة إلى كل شيء (V2X) جميع أنماط الحركة، من قبيل الحركة من الخدمات التلماتية أو أنظمة النقل الذكية أو الخدمات التشخيصية.

3.2.3 المعمارية الكهربائية والإلكترونية الموجهة نحو المناطق: معمارية كهربائية وإلكترونية (E/E) تَفرز المكونات داخل المركبة (الملاحظة 1) مثل أجهزة الاستشعار والمفعلات وعقد الحوسبة، حسب مواقعها (الملاحظة 2) في الميادين الفرعية للشبكة. ولكل ميدان فرعي، يسمى بمنطقة (الملاحظة 3)، عقدة حاسوبية مميزة للمركبة ذات صلة بالمنطقة (تُعرف باسم وحدة التحكم في المنطقة في تطبيقات السيارات)، موصولة بجميع المكونات ضمن الميادين الفرعية الفرعي داخل المركبة. وتوصل وحدات التحكم لكل منطقة بينياً مرة أخرى مع عقدة حوسبة أعلى رتبة وعالية الأداء داخل المركبة. وبالتالي، تنتج تراتبية للمعالجة بين المناطق ومجمل ميدان الشبكة داخل المركبة (IVN) من منظور معمارية الحوسبة الموزعة.

الملاحظة 1 – تحديد مجال تطبيق مكونات الحوسبة والتوصيل الشبكي في سياق الشبكة داخل المركبة (IVN).

الملاحظة 2 – يُفهم "الموقع" على أنه موقع الشبكة على المستوى الطوبولوجي المادي أو الافتراضي لشبكة داخل المركبة (IVN).

الملاحظة 3 – يرتبط مفهوم المنطقة هنا أساساً بمفهوم ميادين الشبكة في سياق المعماريات الكهربائية والإلكترونية (E/E). ولا تتضمن هذه المنطقة بالضرورة مفهوم منطقة الأمن أو المنطقة الموثوقة أو المنطقة المنزوعة السلاح على النحو المستعمل في التوصيات الأخرى لقطاع تقييس الاتصالات ذات الصلة بالأمن (مثل التوصية [b-ITU-T Y.2770]).

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية الاختصارات والأسماء المختصرة التالية:

ADAS النظام المتقدم لمساعدة السائق *(Advanced Driver Assistance System)*

ARP بروتوكول استخراج عنوان *(Address Resolution Protocol)*

AUTOSAR معمارية النظام المفتوح للسيارات *(Automotive Open System Architecture)*

AVB تجسير سمعي فيديوي *(Audio Video Bridging)*

CAN شبكة منطقة وحدة التحكم *(Controller Area Network)*

CGW البوابة المركزية *(Central Gateway)*

CPU وحدة المعالجة المركزية *(Central Processing Unit)*

CRC التحقق بالإطناب الدوري *(Cyclic Redundancy Check)*

DHCP بروتوكول تشكيلة المضيف الدينامية *(Dynamic Host Configuration Protocol)*

DoIP الاتصال التشخيصي عبر بروتوكول الإنترنت *(Diagnostic communication over Internet Protocol)*

DoS الحرمان من الخدمة *(Denial of Service)*

DTLS أمن طبقة نقل وحدة البيانات *(Datagram Transport Layer Security)*

ECU وحدة التحكم الإلكتروني *(Electronic Control Unit)*

E/E الكهربائية والإلكترونية *(Electrical and Electronic)*

FDB قاعدة بيانات إعادة التسيير *(Forwarding Database)*

FIB قاعدة معلومات إعادة التسيير *(Forwarding Information Base)*

HSM الوحدة النمطية لأمن العتاد *(Hardware Security Module)*

ICMP بروتوكول رسالة التحكم في الإنترنت *(Internet Control Message Protocol)*

ICT تكنولوجيا المعلومات والاتصالات *(Information and Communication Technology)*

ID معرف هوية *(Identifier)*

IDS نظام كشف التسلل *(Intrusion Detection System)*

IP بروتوكول الإنترنت *(Internet Protocol)*

IPsec أمن بروتوكول الإنترنت *(Internet Protocol Security)*

IPv4 الإصدار الرابع لبروتوكول الإنترنت *(Internet Protocol version 4)*

IPv6 الإصدار السادس لبروتوكول الإنترنت *(Internet Protocol version 6)*

ITS نظام النقل الذكي *(Intelligent Transport System)*

IVN شبكة داخل المركبة *(In-Vehicle Network)*

LIN شبكة توصيل بيني محلية *(Local Interconnect Network)*

MAC التحكم في النفاذ إلى الوسائط *(Media Access Control)*

MACsec أمن التحكم في النفاذ إلى الوسائط *(Media Access Control security)*

MCU وحدة التحكم الصغرية *(Microcontroller Unit)*

MOST نقل الأنظمة الموجهة نحو الوسائط *(Media Oriented Systems Transport)*

MPU وحدة التحكم المتعددة النقاط *(Multipoint Control Unit)*

OBD التشخيص على متن المركبة *(On-Board Diagnostic)*

OEM مصنّع المعدات الأصلية *(Original Equipment Manufacturer)*

PDU وحدة بيانات البروتوكول *(Protocol Data Unit)*

PVID معرف هوية الشبكة المحلية الافتراضية لمنفذ *(Port VLAN ID)*

QoS جودة الخدمة *(Quality of Service)*

SecOC الاتصالات الآمنة على متن المركبة *(Secure Onboard Communication)*

SR توصية أمنية *(Security Recommendation)*

TARA تحليل التهديدات وتقييم المخاطر *(Threat Analysis and Risk Assessment)*

TCP بروتوكول التحكم في الإرسال *(Transmission Control Protocol)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TP بروتوكول النقل *(Transport Protocol)*

TSN التوصيل الشبكي الحساس زمنياً *(Time-Sensitive Networking)*

UDP بروتوكول وحدة بيانات المستعمل *(User Datagram Protocol)*

UDS خدمة التشخيص الموحدة *(Unified Diagnostic Service)*

V2X من مركبة إلى كل شيء *(Vehicle to Everything)*

VG بوابة المركبة *(Vehicle Gateway)*

VID معرف هوية الشبكة المحلية الافتراضية *(VLAN Identifier)*

VLAN الشبكة المحلية الافتراضية *(Virtual Local Area Network)*

5 الاصطلاحات

تقدم هذه التوصية قائمة بالمتطلبات الأمنية المسماة اختصاراً [SR-*x*] حيث *x* هو رقم. وتستعمل المتطلبات الأمنية (SR) هذه العبارات التالية التي تؤدي المعاني المبينة فيما يلي.

"**يوصى**" أو "**ينبغي**" تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين تقديم هذا المتطلب لزعم الامتثال.

"**من الجائز**" تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تنفيذ البائع بتقديم هذا الخيار الذي يمكن أن يقدمه مشغل الشبكة أو مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه التوصية في نفس الوقت.

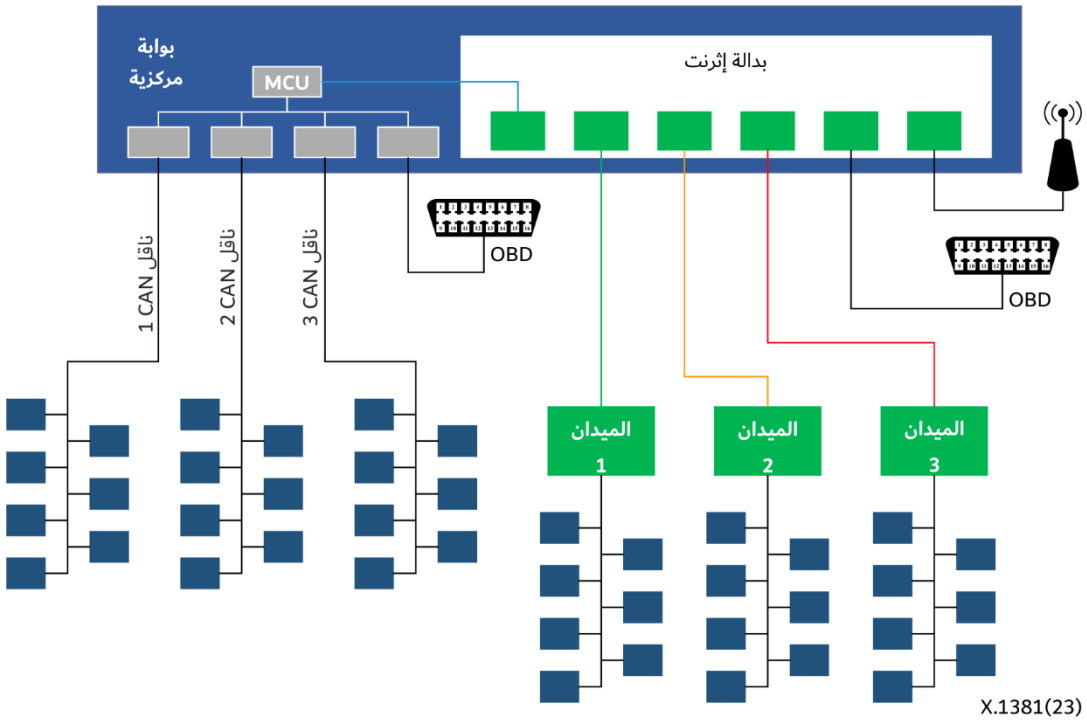
6 لمحة عامة عن معماريات السيارات القائمة على الإثرنت والمتطورة

إثرنت السيارات هي شبكة مادية تُستعمل لتوصيل المكونات ضمن مركبة باستعمال شبكة سلكية. وتُستعمل إثرنت السيارات أيضاً كاسم لشبكة الإثرنت داخل المركبة بأكملها، المؤلَّفة من جميع طبقات البروتوكول والبروتوكولات المستعمَلة في ميدان الشبكة. وهي مصممة لتلبية احتياجات سوق السيارات، بما في ذلك تلبية المتطلبات الكهربائية (بث التداخل الكهرمغنطيسي/التداخل الترددي وإمكانية التعرض) ومتطلبات عرض النطاق ومتطلبات الكمون والتزامن ومتطلبات إدارة الشبكة. ونظراً لأن تكنولوجيات

المركبة المستقلة والنظام المتقدم لمساعدة السائق (ADAS) تسترعي اهتماماً كبيراً، عادة ما تجهَّز المركبات الحديثة بكاميرات متعددة وأدوات تشخيص على متن المركبة (OBD) وأنظمة معلومات وترفيه تتطلب عرض نطاق عالياً. وعلاوة على ذلك، مع زيادة عدد الوظائف، يزداد عدد عقد الحوسبة الموصولة بينياً (مثل وحدات التحكم الإلكتروني (ECU)) في مركبة. وهو ما يؤدي إلى زيادة في ضفيرة الأسلاك وكتلة المركبة، مما يتسبب بتردي أدائها وكفاءة استهلاكها للوقود. والمعمارية الكهربائية والإلكترونية (E/E) الموجهة نحو المناطق هي مثال بارز على معمارية معيَّنة للحوسبة والشبكة داخل المركبة، حيث تُستعمل الإثرنت أيضاً في مستوى التراتبية الأعلى للشبكة، وتستعمل لتوصيل جميع المناطق (ما يسمى الشبكة الفقرية) بينياً في المعمارية بأكملها. وعندما تُدمج الإثرنت مع الشبكة التقليدية داخل المركبة، بما فيها شبكة منطقة وحدة التحكم (CAN) أو شبكة التوصيل البيني المحلية (LIN) أو نقل الأنظمة الموجه نحو الوسائط (MOST) أو بروتوكول FlexRay، يمكن استعمال كبلات الإثرنت المقيَّسة من أجل تقليص الكتلة وتقليل التكاليف كثيراً. بالإضافة إلى ذلك يمكن بفضل ارتفاع عرض النطاق، تقليل عدد أنظمة التحكم فضلاً عن التعقيد.

ولكن لن يتحول كل ميدان من ميادين الشبكة داخل المركبة (IVN)، مثل مجموعة الدفع الميكانيكي، والهيكل الخارجي، والهيكل الميكانيكي، إلى إثرنت السيارات. وهذا يعني مثلاً أن الهيكل الخارجي الذي يحتاج إلى كمية منخفضة من البيانات وعرض النطاق لا يحتاج إلى تغيير بروتوكولات التوصيل الشبكي بموارد وجهود إضافية.

ويبين الشكل 1 شبكة مختلطة داخل المركبة ذات بروتوكولات شبكة تقليدية داخل المركبة، مثل شبكة منطقة وحدة التحكم (CAN) وإثرنت السيارات. ومع ذلك، يمكن للاتصالات التي تتطلب عرض نطاق منخفضاً أن تستعمل بروتوكولات شبكة تقليدية داخل المركبة، فيما يمكن تحويل الاتصالات التي تتطلب عرض نطاق عالياً، من قبيل الوظائف المستقلة أو وظائف النظام المتقدم لمساعدة السائق (ADAS)، إلى شبكة داخل المركبة قائمة على الإثرنت.



الشكل 1 – عدم التجانس الحالي في شبكة نمطية داخل المركبة، استناداً إلى البروتوكولات التقليدية وإثرنت السيارات

من المسلم به أن هناك تطوراً متوقعاً للشبكات داخل المركبة (IVN) القائمة على الإثرنت على مر الزمن. وعادة ما يقترن تطور الشبكة بتغيرات معمارية الاتصالات (الواردة بطوبولوجيات الاتصالات وكدسات البروتوكول ذي الطبقات، وما إلى ذلك)، ستؤثر على الأرجح مرة أخرى على معماريات أمن الاتصالات المرتبطة بها.

وسبق أن نوقشت في الماضي مفاهيم الأمن للمعماريات الكهربائية والإلكترونية (E/E) الكلاسيكية، أي استناداً إلى CAN/FlexRay/LIN وأحياناً MOST، وقد شقت بعض الآليات المقترحة طريقها إلى التقييس. ولن تكون الإثرنت

وبروتوكولات الطبقة العليا المرتبطة بها بسيطة فحسب، بل أيضاً بديلاً أسرع لأنظمة ناقلات السيارات التقليدية، والأرجح كذلك لتغيير مفاهيم أساسية في معماريات E/E الحالية.

ويتيح إدخال الإثرنت فرصة هائلة لتحسين الأمن داخل المركبة لأن العديد من قضايا الأمن الملحة في تطبيقات السيارات سبق أن عولجت من أجل الإثرنت، فيما يسمى مثلاً بأعمال تكنولوجيا المعلومات والاتصالات على مستوى الشركات (من قبيل شبكات المنطقة الحضرية القائمة على الإثرنت وشبكات النفاذ الراديوي للأرض القائمة على الإثرنت)، ولكن أيضاً في أعمال تكنولوجيا المعلومات الكلاسيكية (أي الإثرنت كتوصيلية أساسية في الشبكات المحلية للشركات الخاصة). بيد أنه يثير أيضاً تحديات هائلة، بما فيها تلك الناجمة عن القيود على أنظمة السيارات أو الأنظمة المدمجة، لضمان الأمن نفسه على الأقل المتوقع حالياً للمعماريات الكهربائية والإلكترونية (E/E) القائمة المعزَّة أمنياً.

1.6 الحوسبة الكهربائية والإلكترونية ومعمارية الشبكة في مركبة

تنظر المعماريات الكهربائية والإلكترونية (E/E) السابقة في مسيِّر مركزية (CGW؛ يُعرف أيضاً باسم مسيِّر المركبات أو مسيِّر نظام النقل الذكي في ذلك النمط من الشبكات داخل المركبة (IVN)) من أجل الاتصالات داخل المركبة والتوصيل البيني بين ميادين فرعية مختلفة. ولذا توجد توصيلات من طرف إلى طرف تسيَّر عبر بوابات المركبات هذه.

الملاحظة 1 – "التسيير" في هذا السياق هو الوظيفة العامة لتسيير الحركة، وليس التسيير الآخر مثل تسيير بروتوكول الإنترنت. ولا تستعمل الشبكات داخل المركبة (IVN) القائمة على الإثرنت حالياً كيانات مسيِّر بروتوكول الإنترنت بل تقتصر على البوابات من نمط بروتوكول الإنترنت. ويؤدي استعمال بروتوكول الإنترنت والإثرنت هذا إلى شيء مثل شبكة بروتوكول الإنترنت المبدَّلة (خدمات الاتصالات القائمة على بروتوكول الإنترنت).

وهذا الجانب حاسم من منظور أمن الاتصالات لأنه يقلل من أهداف الأمن المتعلقة ببروتوكول الإنترنت (مثلاً، لن تكون هناك تهديدات أمنية نتيجة لبروتوكولات تسيير بروتوكول الإنترنت).

ويُتوقع أن تلبي الاتصالات المستهدَفة القائمة على الإثرنت متطلبات الأداء العالي في الوقت الفعلي والاتصالات الموثوقة، وأن تستفيد من تكنولوجيا وتقنية الاتصالات الناضجة والمستعملة على نطاق واسع والمثبَتة.

الملاحظة 2 – يتيح المرجع [b-IEEE 802.1]، لا سيما المرجع الفرعي [b-IEEE 802.1CB]، اتصالات موثوقة، تشمل معمارية حلقية تتضمن ميزة إطناب الطبقة 2 الرديف (R-Tag).

وعلى وجه الخصوص، فإن المكونات CAN وFlexRay وLIN وMOST تُستعمل أصلاً في الاتصالات داخل المركبة؛ وشبكة منطقة وحدة التحكم (CAN) هي أكثر الشبكات رواجاً. وتعتبر البوابة المركزية (CGW) وبوابات المركبة (VG) بشكل عام وبوابة حدود المركبة بوجه خاص عناصر بالغة الأهمية للشبكة والأمن في الشبكات ضمن المركبات ومعماريات الاتصالات. ويقدم التذييلان II وIII بعض المعلومات التكميلية التي قد تكون مفيدة من منظور أمن الاتصالات.

وفي الماضي، لم يكن من الممكن النفاذ إلى مركبة عن بُعد (من قبيل استعمال توصيلية ورشة العمل لأغراض التشخيص أو تنوع جميع أنواع خيارات الاتصالات من مركبة إلى كل شيء (V2X)). وجرى توصيل وحدات التحكم الإلكتروني داخل المركبة ببعضها البعض عبر واحد أو أكثر من الناقلات الميدانية الأصلية المستمثَلة للمركبات.

ولم يتسنَّ النفاذ القانوني بعد الإنتاج إلا بتوصيلية مادية مباشرة وقائمة على الكبلات. وبالتالي، يُستعمل التوصيل من نقطة إلى نقطة على مسافة قصيرة حصراً للخدمات التشخيصية التي تتطلب توصيلاً إلى منفذ OBD عبر بروتوكول CAN. وكان مصنعو المعدات الأصلية (OEM) على علم بالمخاطر الأمنية المعزَّة للخواص الوظيفية التشخيصية وبروتوكول CAN الأصلي الذي لا يقدم أي خواص وظيفية أمنية. وقد ركز المرجع [b-Autosar 654] على استيقان وسلامة رسائل CAN ومفاهيم الأمن المناسبة التي تستعمل أساساً شفرات استيقان الرسائل.

وتمكِّن التطورات الحالية من إجراء اتصالات قائمة على الإثرنت من الأجهزة الخارجية إلى المركبة. وتعمل عادة وحدة التحكم الإلكتروني (ECU) المخصصة ضمن المركبة كنقطة نفاذ لنمط ما من الاتصالات الخارجية. وتقوم وحدة التحكم الإلكتروني بتسيير المعلومات ذات الصلة بوحدات التحكم الإلكتروني الأخرى إذا لزم الأمر من خلال شبكات السيارات المشتركة أو تعيد تسيير الحركة من خلال توصيل قائم على الإثرنت بالبوابة المركزية (CGW) للتسيير إلى وحدات التحكم الإلكتروني الأخرى المرفَقة عادة.

2.6 مقارنة بين أمن المعمارية الكهربائية والإلكترونية المستقبلية والحالية

نظراً لعدد من حالات سوء الاستعمال المختلفة التي تنطوي على مكونات داخل المركبة، هناك آليات أمنية راسخة للمعماريات الكهربائية والإلكترونية (E/E) الحالية. وفيما يتعلق بأنظمة الاتصالات، نُشرت آليات الاستيقان لشبكة منطقة وحدة التحكم (CAN) المهيمنة، وجرى تقييسها وستطبَّق جزئياً ضمن الأجيال المقبلة من المركبات. وتوصِّف معمارية النظام المفتوح للسيارات (AUTOSAR) وحدة نمطية آمنة للاتصالات على متن المركبة تركز على استيقان وسلامة الاتصالات داخل المركبة. ويُرجى العلم بأن آلية الاستيقان لا تشير إلى مجرد استيقان الرسائل المرسَلة، بل تضمن أيضاً استيقانية شركاء الاتصالات.

وعلاوةً على ذلك، فإن شبكة منطقة وحدة التحكم (CAN) بوصفها تكنولوجيا لناقل الطبقة المادية لا ترسل الرسائل إلا كبثّ.

الملاحظة 1 – إن الطبيعة الأساسية لاتصالات الوسائط المادية المشتركة مثل طوبولوجيا الناقل تناقض النهج المتبع في تصميم شبكة إثرنت مبدَّلة.

لذلك يمكن لكل مشارك أن يقرأ كل الحركة المرسَلة عبر ناقل شبكة منطقة وحدة التحكم (CAN). وتَفصل مختلف ميادين الشبكة القائمة على الناقلات، وكذلك الميادين الفرعية الأخرى، الحركة المرتبطة بالسلامة من أنماط أخرى، مثل حركة المعلومات المسلية أو الترفيه. ولا يمكن الاتصال بين ميادين الشبكة إلا عبر البوابة المركزية (CGW) التي تنفِّذ عادةً آليات إنفاذ قواعد السياسة المرعية (مثل القواعد المتعلقة بالمرشاح) لمنع هجمات فيض الرزم وضمان تيسر الشبكة.

ملاحظة 2 – تقدم بوابات المركبات (مثل البوابة المركزية (CGW)) مجموعة من وظائف الشبكة، حيث ترتبط مجموعة فرعية معيَّنة بأمن الاتصالات. وبالتالي، لا يقتصر الأمر على إنفاذ قواعد الأمن فحسب، بل يشمل أيضاً إنفاذ قواعد غير ذات صلة بالأمن بل بسياسة محددة (مثل العمل البيني لشبكة المنطقة المحلية الافتراضية (VLAN) أو إعادة تسيير بروتوكول الإنترنت أو وضع إجراءات لجودة خدمة قائمة على التوصيل الشبكي الحساس زمنياً (TSN)).

والإثرنت معيار راسخ للاتصال الشبكي مع طائفة واسعة من التطبيقات. وهو يُستعمل لشبكات الاتصالات الشائعة من آلة (مثل الحاسوب) لأخرى ويغطي مقاييس متعددة لشبكة منطقة (كشبكة صغيرة أو محلية أو حضرية) فضلاً عن شبكات النفاذ الراديوي للأرض فيبي الاتصالات المتنقلة. ونظراً لذلك التاريخ وخلفية الشبكة، قد تكون هناك أنماط لأمن الشبكة يُنظر في إعادة استعمالها.

ونظراً لاستعمال الإثرنت الشائع، تتعدد الهجمات على الاتصالات القائمة على الإثرنت (بما في ذلك بروتوكولات الطبقة العليا) ولكن توجد تدابير مضادة لحالات الاستعمال المختلفة. فعلى سبيل المثال، يوصى بشدة ضمن الإنترنت، بالنسبة لخدمات النقل القائمة على بروتوكول التحكم في الإرسال (TCP) (فقط)، باستعمال أمن طبقة النقل (TLS) لضمان استيقانية الاتصالات وسلامتها وسريتها. ويوصى أيضاً باستعمال أمن طبقة نقل وحدة البيانات (DTLS) المتمِم لبروتوكول النقل في خدمات النقل على أساس بروتوكول وحدات بيانات المستعمل (UDP). ويمكن لاستعمال الإثرنت كمعيار راسخ وسائد للاتصالات داخل المركبة أن يعيد استعمال آليات الأمن المرتبطة بكدسة بروتوكول الإنترنت (IP). غير أن التدابير المضادة المعروفة من شبكات الحاسوب الشائعة لا يمكن أن تناسب تطبيق سيارات لأنها لم تصمَم خصيصاً لمتطلباتها وقدراتها. فعلى سبيل المثال، قد لا توفر ضمانات في الوقت الفعلي وقد تتطلب أداءً معززاً لا يمكن أن تقدمه الأجهزة المدمجة التي تفرض قيوداً على الموارد. وبالتالي، لا يوجد، حتى وقت النشر، أي اعتبار لإدماج آليات الأمن في بروتوكولات الاتصالات القائمة على الإثرنت الحساسة زمنياً.

ويتسم فصل الاتصالات داخل المركبة بأهمية بالغة لأسباب تتعلق بالسلامة. وفي الوقت الراهن، ينظر مصنعو المعدات الأصلية (OEM) في العزل المنطقي لحركة الإثرنت باستعمال التمثيل الافتراضي للشبكة الذي يتصل بشبكة محلية افتراضية (VLAN) بوصفها شبكة خاصة افتراضية للطبقة 2 في حالة الإثرنت؛ علماً بأن تحقيق فصل الحركة داخل المركبة ممكن أيضاً بوسائل أخرى، مثل الشبكات الافتراضية الخاصة في الطبقة 1 (عن طريق شبكات إثرنت المنفصلة مادياً) أو في الطبقة 3 (باستعمال حل معروف لشبكة خاصة افتراضية (VPN) من أجل خدمات اتصالات بروتوكول الإنترنت عبر الإثرنت).

وتُعتبر الشبكة المحلية الافتراضية (VLAN) ممارسة راسخة لتقديم العزل المنطقي على طبقة وصلة البيانات في شبكات الحاسوب الشائعة. وتستعمل الشبكات المحلية الافتراضية عادة لتقسيم الشبكات المادية إلى شبكات منطقية مختلفة. ويقوم تطبيق الشبكة المحلية الافتراضية (VLAN) داخل المركبة بشكل أساسي على أن هذه الشبكة تمكن من تحديد أولويات الحركة (من خلال خارطة الارتباطات المباشرة لنقاط شفرة الأولوية في الشبكة المحلية الافتراضية مع أصناف حركة التوصيل الشبكي الحساس زمنياً (TSN)).

الملاحظة 3 – لا يشمل مجال تطبيق هذه الطبعة من هذه التوصية الاعتبارات الأمنية للشبكات المحلية الافتراضية (VLAN) ذات التراتبيات، التي قد تندرج في مجال تطبيق الشبكات المستقبلية داخل المركبة لنماذج توصيل بيني محددة من مركبة إلى كل شيء (V2X). وبالتالي، هناك فرضية هنا بشأن الشبكات المحلية الافتراضية (VLAN) ذات الوسم الواحد أو القائمة على المنفذ فقط.

وتطبيق معيار الإثرنت الواسع النطاق على الاتصالات داخل المركبات يتيح بعض الإمكانيات من ناحية، ولكن ينبغي توخي حذر خاص من ناحية أخرى. فبالإضافة إلى الافتقار إلى تطبيق لآلية الأمن، لا يُوصى أي معدات خاصة لتوصيل جهاز خارجي عبر الإثرنت بالمركبة.

ولعل المستعملين يهتمون بمحاولة توصيل حواسيبهم المحمولة بمقبس أو استعمال هواتفهم الذكية لتعزيز النفاذ إلى الشبكة داخل المركبة (IVN). ويمكن لاستعمال بدالة الإثرنت كمكون إضافي أن يسمح لشخص غير مخوَّل مدرب خصيصاً بشن هجوم مثير للاهتمام. ويمكن للمهاجمين أن ينفِّذوا هجمات معروفة انطلاقاً من الإنترنت أو من أساليب الاستغلال المنشورة لبدالات الإثرنت الشائعة. وعلى غرار أمن الاتصالات، توجد تدابير مضادة من أجل بدالات الإثرنت الشائعة. ولكن لا بد من مواصلة استكشاف وتحري بيئات السيارات.

ويبين الجدول 1 الاختلافات بين بروتوكولات الشبكة داخل المركبة (IVN) التقليدية الموجَهة نحو الناقل الميداني وتلك القائمة على الإثرنت في مستوى مجرَّد للغاية. والعمود الأول لكل هدف من أهداف المقارنة هو مستوى اكتمال المعايير المعنية الذي يمثل برمزه من قبيل "سيء" (–)، وحيادي (0)، وجيد (+)، والأفضل (++). علماً بأن الجدول 1 هو تبسيط مقصود، وأن التقييم الأكثر جدية للبروتوكول يتطلب مقارنة الإثرنت مع كل ناقل ميداني أو تكنولوجيا اتصالات نواقل مركبات.

الجدول 1 – مقارنة بين معماريات الاتصالات التقليدية وتلك القائمة على الإثرنت في المركبة

المعايير	**بروتوكولات الشبكة داخل المركبة (IVN) الموجَهة نحو الناقل الميداني (الملاحظة 1)**		**الشبكة داخل المركبة (IVN) القائمة على الإثرنت**	
البساطة	معقدة، غير متجانسة، بوابة متعددة البروتوكولات	–	متجانسة جداً ببدالات الطبقة 2 (في الغالب)	++
المرونة	صعوبة توسعة/مواءمة شبكة فرعية جديدة (سهولة ضمن الشبكات الفرعية)	–	سهولة توسيع/تكييف شبكة فرعية جديدة أو ضمن الشبكات الفرعية	++
الأداء	يعتمد على نوع الناقل	+	يصل إلى عدة غيغابتات في الثانية	++
في الوقت الفعلي	مثبتة جيداً على مدى عقود	++	قادرة ولكنها لم تخترع من أجل ذلك	–
كتلة المواد المادية المتعلقة بالشبكة	توصيل سلكي فردي لكل ناقل	–	زوج أسلاك واحد ملتو لجميع النواقل	+
التكاليف (الاستثمار وليس التشغيل)	إنتاج خاص بسيارات على دفعات صغيرة	–	إنتاج ضخم عالمي لغير السيارات أيضاً	+
درجة التقييس	معيار كثير التنوع	–	معيار قليل التنوع	+
نماذج التوصيلية في الطبقة المادية وطبقة وصلة البيانات (الملاحظة 2)	نماذج الاتصالات من نقطة إلى عدة نقاط حصراً جراء الاستعمال المشترك للوسائط المادية ("الناقل")	–	الإثرنت تدعم نموذجي الاتصالات من نقطة إلى نقطة ومن نقطة إلى عدة نقاط (الملاحظة 3).	+
سلامة الرسالة (الملاحظة 4)	التحقق بالإطناب الدوري (CRC) + تدابير خاصة بالناقل	+	التحقق بالإطناب الدوري (CRC)، شفرات الكتلة	+
التدابير الأمنية (الملاحظة 5)	غير موجودة تقريباً	–	تدابير مضافة (الإصدار الرابع لبروتوكول الإنترنت (IPv4))، أمن بروتوكول الإنترنت (IPsec)، الإصدار السادس لبروتوكول الإنترنت (IPv6))	0

الملاحظة 1 – تبين التقييمات إزاء المعايير المدرجة التصميم النمطي للبروتوكول، ولكنها لا تصلح لكل حالة من حالات تكنولوجيات الاتصالات الموجهة نحو الناقل الميداني، فعلى سبيل المثال، لا تقدم شبكة منطقة وحدة التحكم (CAN) وسائل بروتوكولية متأصلة لدعم الاتصالات في الوقت الفعلي.

الملاحظة 2 – الافتراض هنا: هو أن التطبيقات داخل المركبة تتطلب عادة خدمات اتصالات بطبولوجيات اتصال من نمطي نقطة إلى نقطة أو من نقطة إلى عدة نقاط. وتجب خدمة هذه الطبولوجيات بطبولوجيات توصيل منطقية، مما يعني ضمناً هنا النظر في طبولوجيات توصيل طبقة الوصلة كقاسم "طبقة البروتوكول" المشترك لتكنولوجيات الاتصالات موضوع المناقشة.

الملاحظة 3 – لن تُنشر شبكات الإثرنت داخل المركبات وتشغَّل إلا "بالأسلوب المبدل" (المدفوع أساساً بأهداف جودة الخدمة (QoS))، وهو ما ينطوي على دعم نماذج التوصيل من نقطة إلى نقطة حصراً عند طبقة الوسائط المادية للإثرنت. ولا يُشترك في الوسائط المادية، بل يكون لكل نقطة طرفية في طبقة الإثرنت 1 نفاذ حصري إلى موارد الطبقة المادية. ولكن تُدعم طوبولوجيات الاتصال من نقطة إلى عدة نقاط: إما بشكل مباشر بقدرة الإثرنت الأصلية المدمجة على الإرسال إلى عناوين شبكية متعددة وإلى جميع العناوين الشبكية عبر وظائف إعادة تسيير طبقة وصلة البيانات أو بشكل غير مباشر ببروتوكولات الطبقة العليا (مثل بروتوكول الإنترنت والإرسال إلى عناوين شبكية متعددة أو إلى أي من، أو إلى جميع، العناوين شبكية).

الملاحظة 4 – تشمل السلامة ذات الصلة بالأمن هنا: أ) سلامة البتات؛ ب) سلامة البيانات، أي إما نطاق السلامة الشامل لفرادى البتات في وحدة بيانات البروتوكول (PDU) أو لوحدة بيانات البروتوكول (PDU) بأكملها على نحو ما يجري (في طبقات بروتوكول محددة).

ملاحظة 5 – تُقيَّم تدابير الأمن سواء كانت توصيف البروتوكول المعني ينطوي أو لا ينطوي على خصائص أمنية متأصلة.

وتشمل معايير المقارنة الواردة هندسة الشبكات الأساسية وهندسة خدمات الاتصالات فضلاً عن الجوانب المتعلقة بالأمن.

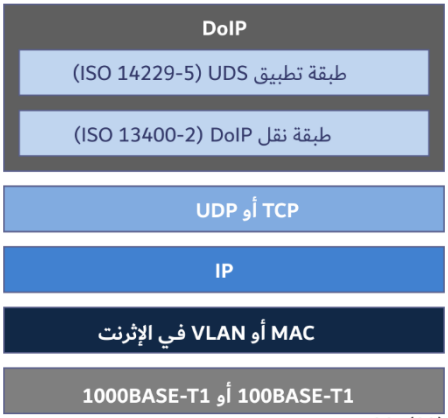
3.6 خدمات الاتصالات باستعمال الإثرنت في تطبيقات السيارات

هذه الأيام، تُستعمل إثرنت السيارات أساساً في تشخيص وإرسال تدفق الوسائط المتعددة من قبيل البيانات الفيديوية من أجهزة الاستشعار في كاميرات النظام المتقدم لمساعدة السائق (ADAS). وعلاوةً على ذلك، بدأت إثرنت السيارات في أواسط الفترة بين عامي 2010 و2020 بالسماح بعُقد الحوسبة (مثل وحدات التحكم الإلكتروني) في المركبات للتواصل عبر الإثرنت.

1.3.6 أدوات التشخيص

يتمثل أسلوب التشخيص التقليدي على متن المركبة في توصيل أداة تشخيصية بالمنفذ الثاني للتشخيص على متن المركبة (OBD-II) والتواصل مع وحدة التحكم الإلكتروني المستهدَفة من خلال بروتوكول خدمة التشخيص الموحدة (UDS). وخدمة التشخيص الموحدة هي بروتوكول على مستوى التطبيق وضعته دوائر صناعة السيارات ويسمح لأنظمة التشخيص بالتواصل مع وحدات التحكم الإلكتروني لتشخيص الأعطال وإعادة برمجة وحدات التحكم الإلكتروني وفقاً لذلك (انظر المرجع [b-ISO 14229-5]).

ويقوم الاتصال التشخيصي عبر بروتوكول الإنترنت (DoIP) على بروتوكول الإنترنت (انظر المرجع [b-ISO 13400-2]). ويتيح الاتصال التشخيصي عبر بروتوكول الإنترنت إرسال رسائل خدمة التشخيص الموحدة (UDS) بين مركبة ومعدات اختبار خارجية عبر الإثرنت، ويصبح من الممكن استخراج بيانات تشخيصية من مركبة عن بُعد، دون لزوم توصيلية مادية إلى المركبة. ويقدم الاتصال التشخيصي عبر بروتوكول الإنترنت تغليفاً لرسائل UDS ضمن رزم TCP أو وحدات بيانات UDP على النحو المبين في الشكل 2.



الشكل 2 – كدسة بروتوكول للاتصالات التشخيصية عبر تطبيق بروتوكول الإنترنت

ولا ينظر الاتصال التشخيصي عبر بروتوكول الإنترنت (DoIP) في حد ذاته في أي آليات لأمن الاتصالات. ولا تُستيقَن الرسائل عادة أو تُحفَّر بأي شكل كان. والاتصال التشخيصي عبر بروتوكول الإنترنت يأخذ الاستيقان بعين الاعتبار في الطبقة (الطبقات) العليا ولكن ذلك ليس إلزامياً.

2.3.6 تدفقات الوسائط في سياق الخدمات متعددة الوسائط

في النظام المتقدم لمساعدة السائق (ADAS)، يتعين على المركبات عالية الأتمتة والمستقلة تماماً أن تنشر الكثير من أجهزة الاستشعار مثل الكاميرات عالية الوضوح ووظائف التوصيلية للحصول على المعلومات الكافية لإدراك بيئة المركبة. وبالإضافة إلى ذلك، يجهَّز العديد من المركبات بأجهزة تستعمل أو ترسل تدفقات الوسائط على مستوى التطبيق (لا يتعين خلطها مع طبقات الوسائط (الفرعية) المادية في حالة الإثرنت) المستعملة في أنظمة الإعلام الترفيهي، حول أنظمة المراقبة، وأنظمة مساعدة رَكن المركبات، وأنظمة مساعدة البقاء في مَسْرَب واحد، والرؤية الليلية، وما إلى ذلك. وفي حالة الكاميرات، تتولد تدفقات وسائط كبيرة نسبياً (من حيث حجم الحركة) بأهداف جودة الخدمة المدفوعة بالتطبيق والمتمثلة بالكمون المنخفض والإرسال عالي الجودة. وإذا كان البروتوكول هو

شبكة منطقة وحدة التحكم (CAN)، يستحيل تحقيق المتطلبات السابقة بسبب التقييدات المتأصلة في تصميم البروتوكول، مثل مدى حجم الحمولة النافعة.

ويمكن لإثرنت السيارات أن تفي بهذه المتطلبات باستعمال إطار التجسير السمعي الفيديوي (AVB) لمعهد مهندسي الكهرباء والإلكترونيات.

ملاحظة – يشير مصطلح التجسير السمعي الفيديوي (AVB) إلى مجموعة من المعايير [b-IEEE 802.1]، بما فيها المعايير [b-IEEE 802.1Qav] و[b-IEEE 802.1AS] و[b-IEEE 802.1Qat]. ولذلك، غير فريق مهام التجسير السمعي الفيديوي التابع لمعهد مهندسي الكهرباء والإلكترونيات اسم فريق مهام التوصيل الشبكي الحساس زمنياً (TSN) الذي يتضمن الآن معايير التجسير السمعي الفيديوي.

ويمكن أن يستوفي التجسير السمعي الفيديوي (AVB) شروط التوصيل الشبكي الحساس زمنياً (TSN) الأعم مما يفتح الباب أمام إمكانية قيام شبكة واحدة تتعامل مع المعلومات الترفيهية والتحكم في الهيكل ومساعدة السائق وحتى الوظائف الحرجة من حيث السلامة.

وفي حالة نظام مراقبة بالرؤية المحيطة، يقدم صفيف من الكاميرات رؤية محيطية متزامنة بزاوية 360° لبيئة المركبة. ويمكن إرسال هذا التدفق للوسائط الفيديوية إلى نظام وعي السائق مثل نظام العرض بمستوى الرأس أو نظام الملاحة الفيديوية. وتمكن أيضاً مزامنة بيانات أجهزة الاستشعار الإضافية ووحدات التحكم الإلكتروني ذات الصلة من خلال شبكة التجسير السمعي الفيديوي (AVB).

3.3.6 الشبكة الفقرية للشبكة داخل المركبة

يمكن أن يكون للمركبات الحديثة أكثر من 100 وحدة تحكم إلكتروني. وتتعلق وحدة التحكم الإلكتروني أو عقدة حوسبة المركبة بعقدة شبكة في طوبولوجيا الشبكة داخل المركبة (IVN) القائمة على الإثرنت، أو بعقدة طرفية واحدة أو أكثر (بحسب عدد السطوح البينية لتوصيل الإثرنت المادية أو المنطقية أو الافتراضية لكل عقدة حوسبة). وعلاوةً على ذلك، يمكن أن يزداد عدد وحدات التحكم الإلكتروني (ECU) بشكل أكبر مما يؤدي إلى أن تبدأ الأنظمة المتقدمة لمساعدة السائق (ADAS) والمركبات المستقلة في طلب سعة نقل كبيرة (يطلق عليها اسم عرض النطاق بالعامية) للشبكة داخل المركبة (IVN).

وبالإضافة إلى ذلك، تستعمل بروتوكولات الشبكة داخل المركبة (IVN) التقليدية نظام مجموعة التوصيل السلكي الثقيلة والمكْلفة. وإذا استُعملت الإثرنت كشبكة فقرية للشبكة داخل المركبة (IVN)، يمكن خفض تكاليف التوصيل داخل المركبة بنسبة تصل إلى 80% وكتلة التوصيل السلكي بنسبة تصل إلى 30% داخل المركبة.

وعلى النحو المبين في الشكل 1، توجد عدة ميادين في الشبكة داخل المركبة (IVN) القائمة على الإثرنت. وتُستعمل بروتوكولات الشبكة داخل المركبة التقليدية ضمن كل ميدان وتُستعمل الإثرنت للتواصل بين الميادين، أي على مستوى الشبكة الأساسية (عند مقارنتها مع شبكات تكنولوجيا المعلومات والاتصالات (ICT))، ويطلق عليها أيضاً اسم الشبكة الفقرية بالعامية.

وتختلف إثرنت السيارات عن طوبولوجيا نظام الناقلات. إذ لا يوجد موصل ناقل موصول بالعديد من وحدات التحكم الإلكتروني وأجهزة الاستشعار والمفعلات؛ بل إنها موصولة بواسطة بدالة إثرنت بطريقة النقطة إلى نقطة. وإذا كان على رسائل الاتصالات أن ترسل من ميدان إلى آخر، تمكن معالجتها بسهولة من خلال وظائف العمل البيني في الشبكة، مثل تلك التي تقدمها بدالات الإثرنت وبوابات الشبكة المحلية الافتراضية (VLAN)، وربما أيضاً مسيّرات بروتوكول الإنترنت وبوابة بروتوكول الإنترنت في الشبكة داخل المركبة (IVN) القائمة على الإثرنت. وعلى النقيض من ذلك، تتطلب البروتوكولات التقليدية داخل المركبة دعم الشبكة وربما أيضاً العمل البيني للخدمة الذي يقع في البوابات عادة، عند التواصل مع النقاط الطرفية الواقعة في شبكة الإثرنت.

7 تحليل التهديدات

1.7 منهجية النهج اللازم لتحليل التهديدات

تحلل هذه الفقرة سيناريوهات التهديد الأمني في سياق شبكات الإثرنت داخل المركبات. وتصف التوصية [ITU-T X.1371] التهديدات الإجمالية المحددة في المركبات الموصولة.

وينبغي وضع أهداف أمنية لاستخلاص مفهوم الأمن. ويُضطلع بتحليل التهديدات وتقييم المخاطر (TARA) لتحديد أسلوب معالجة المخاطر في مرحلة الهدف الأمني. وللقيام بتحليل التهديدات وتقييم المخاطر، ينبغي تحديد الأصول الأمنية والأهداف الأمنية فضلاً عن التهديدات ذات الصلة. ويمكن تحديد مفهوم الأمن إذا تقرر أسلوب المعالجة للمخاطر المعنية من خلال تصنيف التأثير وتصنيف جدوى الهجوم استناداً إلى أصول أمنية وأهداف وتهديدات أمنية محددة، انظر المرجع [b-ISO/SAE 21434] للاطلاع على مزيد من المعلومات. وتحدَد، وفقاً لنهج تحليل التهديدات الوارد في المرجع [b-ISO/SAE 211434]، الأصول الأمنية وما يتصل بها من أهداف أمنية، ثم تحدَد التهديدات الأمنية أيضاً في هذه الفقرة.

ولا يشمل مجال تطبيق هذه التوصية عملية تصنيف التأثير وتصنيف جدوى الهجوم وقرار المخاطر، وهي عملية تحتاج إلى مزيد من الدراسة.

2.7 الأصول الأمنية

الأصل الأمني يعني أي كائن أو وظيفة أو مورد بيانات تنبغي حمايته. وتُدرج الأصول الأمنية المستخلَصة في الجدول 2 انطلاقاً من اعتبارات الشبكات داخل المركبة (IVN) القائمة على الإثرنت.

الجدول 2 – الأصول الأمنية

الأصول	الوصف
إدارة بيانات	تشمل بيانات إدارة بيانات الإدارة فئتين من الفئات التالية (الملاحظة 1): بيانات التشكيلة التي تميز السلوك الوظيفي لعناصر الشبكة أو وظائف الشبكة ذات توصيلية الإثرنت، مثل البوابة وبدالة الإثرنت ونظام كشف التسلل (IDS) وجدار الحماية؛ بيانات الحالة التشغيلية التي لا تصف السلوك الفعلي لكيانات الشبكة تلك فحسب، بل أيضاً جميع خدمات الإدارة باستعمال التبليغات [b-ITU-T M.3702] مثل الإبلاغ عن الإنذار [b-ITU-T M.3703] كجزء من إدارة الأعطال. وتخضع تدفقات بيانات الإدارة للفئتين معاً بين الكيان المدير والكيان المدار للحماية الأمنية في الأساس. ولكن ينبغي عادةً أن يكون التأثير الأمني، بمعالجة بيانات التشكيلة، أعلى بكثير منه في بيانات الحالة التشغيلية. ومن ناحية أخرى، قد يؤدي الكبت المزمع للإنذار الصادر عن عنصر شبكة إثرنت إلى تفاقم حالة العطل الراهنة مثلاً.
وحدات بيانات بروتوكول الطبقة 2 ذات الصلة باتصالات الإثرنت	تتألف حركة الإثرنت من حركة طبقة وصلة البيانات، أي نقل أطر التحكم في النفاذ إلى وسائط (MAC) الإثرنت (كوحدات بيانات بروتوكول (PDU) الطبقة 2) إلى الشبكة داخل المركبة (IVN) القائمة على الإثرنت.
بيانات الإدارة المتولدة بواسطة التسجيل (الملاحظة 2)	يمكن تدقيق الكشف الناجح للأحداث الأمنية وما يرتبط بها من معلومات.
المواد التجفيرية	مفاتيح وشهادات للمخططات المتناظرة وغير المتناظرة، بما في ذلك بيانات الاعتماد الأخرى مثل كلمة المرور
صورة البرامج الثابتة أو البرمجيات	الشفرة المجمَّعة المقرر تشغيلها في عقد الحوسبة في المركبات مثل وحدات التحكم الإلكتروني
الملاحظة 1 – انظر إطار إدارة الشبكة المطبَّق على الإثرنت على النحو الموصوف في التوصيات [b-ITU-T M.3010، b-ITU-T X.703، b-ITU-T G.8013، b-ITU-T Y.1730]. وتستند بيانات إدارة كيانات شبكة الإثرنت إلى لغة YANG [b-IETF RFC 6020] كلغة توصيف ونمذجة لبيانات الإدارة. ويقدم المعيار IEEE 802 (باعتباره مالك تكنولوجيا الإثرنت) نماذج بيانات الإدارة القائمة على لغة YANG لجميع كيانات الإثرنت المختلفة، أي المرجع الرئيسي لبيانات الإدارة في هذه التوصية. **الملاحظة** 2 – لا يغطي هذا الجدول إدارة وظائف التسجيل [b-ITU-T M.3705]. والتسجيل هنا يخص أحداث النظام الناشئة عن تدفقات معلومات الإدارة التي تسجَّلها وظائف التسجيل (انظر التوصية [b-ITU-T G.7710]) بشأن تدفقات بيانات الإدارة الداخلية لمعدات الشبكة). **الملاحظة** 3 – تنتمي وظيفة الكشف هذه إلى فئة الاختبار الإحصائي للفرضيات، ويعود ذلك أساساً إلى عدم اليقين في وصف الأحداث أو وصف حالة قواعد السياسة المرعية من أجل تحديد لا لبس فيه لهذه الأحداث. وبالتالي، لا يقدم الكشف الناجح إلا نتائج احتمالية بطبيعتها، تشمل التأكيدات الخاطئة بالإضافة إلى التأكيدات الصحيحة. وبالتالي ينبغي أن تكون درجة جودة الكشف مشروطة ومقدَّرة كمياً، بتقدير النسبة المتوقعة للتأكيدات غير الصحيحة.	

3.7 الأهداف الأمنية

تحلَل الأصول الأمنية (انظر الفقرة 1.7) فيما يتعلق بقائمة الأهداف الأمنية المبينة في الجدول 3.

الجدول 3 – الأهداف الأمنية

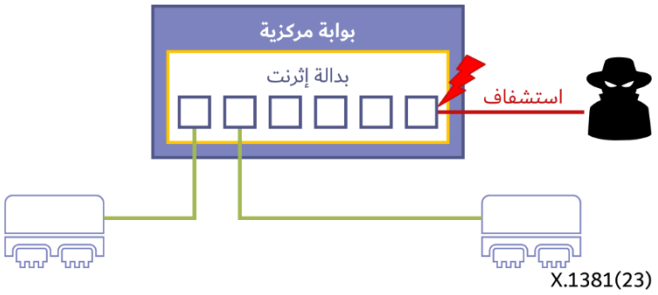
الأصول الأمنية	الأهداف الأمنية	الشرح
إدارة بيانات	السلامة، السرية	لا تنبغي معالجة البيانات التي تحدد السلوك الوظيفي لعناصر شبكة الإثرنت مثل بوابة المركبة وبدالة الإثرنت ونظام كشف التسلل وجدار الحماية.
وحدات بيانات بروتوكول الطبقة 2 ذات الصلة باتصالات الإثرنت	السرية	يحظر الكشف عن وحدات بيانات البروتوكول الخاصة بطبقة خاصة بطبقة ((Lx)-PDU) المنقولة إلى الشبكة داخل المركبة (IVN) القائمة على الإثرنت.
	التيسر	ينبغي أن تتيسر خدمات الاتصالات عبر الشبكة داخل المركبة (IVN) القائمة على الإثرنت كلما دعت الحاجة إليها في ضوء القيود المحددة بوضوح والمتعلقة بخدمة الاتصالات.
	الاستيقانية	على الاتصالات عبر الشبكة داخل المركبة (IVN) القائمة على الإثرنت أن تكشف المكونات الأخرى المنتحَلة وترفضها.
	السلامة	يُحظر التلاعب ببيانات الاتصالات المتبادلة على شبكة السيارات داخل المركبة القائمة على الإثرنت.
بيانات الإدارة المتولدة بواسطة التسجيل	السلامة	يُحظر التلاعب بالإثباتات والمعلومات المتعلقة بالأحداث الأمنية المسجَّلة التي يمكن تدقيقها دون كشفه. وتغطي السلامة سلامة البتات والبيانات المشمولة بنطاق المعلومات المسجَّلة.
المواد التجفيرية	السرية	يُحظر كشف الأسرار والمفاتيح الخاصة، وكذلك بيانات اعتماد المستعمل مثل كلمات المرور.
	السلامة	يُحظر التلاعب بمفاتيح وشهادات السلامة دون كشف.
صورة البرامج الثابتة أو البرمجيات	السرية	يُحظر كشف محتويات البرامج الثابتة والبرمجيات، من قبيل البيانات المجمعة عن الشفرة والمعايرة المتعلقة بالملكية الفكرية، لكيانات غير مخوَّلة.
	السلامة	يُحظر التلاعب بصور البرامج الثابتة والبرمجيات، من قبيل موضوع إجراءات تغيير القدرات (عن طريق البرامج الثابتة عبر الأثير مثلاً، أو إدارة البرمجيات بشكل عام).

4.7 التهديدات المحدَدة

1.4.7 التهديدات للسرية

– كشف غير مجاز لحركة اتصالات الإثرنت (كما تكونها الطبقة المادية للإثرنت (L1) أو وحدات بيانات البروتوكول (PDU) في طبقة وصلة البيانات (L2).

يمكن لمهاجم استشفاف حركة اتصالات الإثرنت بتوصيل المكون المسؤول عن الاتصال الخارجي ببدالة الإثرنت. ثم يحلل المهاجم معلومات حركة الاتصالات باستشفاف وحدات بيانات البروتوكول (PDU) ذات الصلة بالإثرنت.



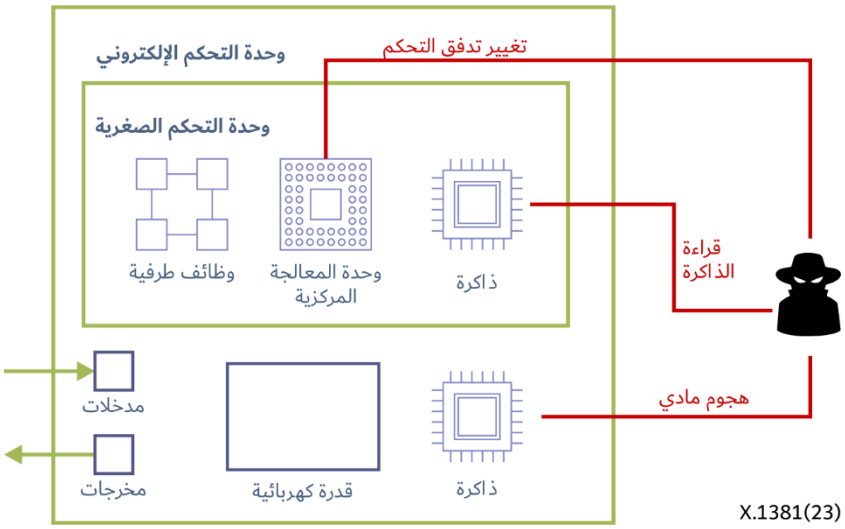
الشكل 3 – التهديدات للسرية بالاستشفاف

– كشف غير مجاز للمواد التجفيرية

ويمكن للمهاجم استشفاف المواد التجفيرية عن طريق:

- الحصول على المواد التجفيرية بفتح مصادر التخزين مادياً؛

- قراءة المواد التجفيرية من ذاكرة كل مكون تُستعمل فيه المواد التجفيرية؛
- تعديل البرامج الثابتة وتغيير تدفق التحكم لكشف المواد التجفيرية.



الشكل 4 – التهديدات لسرية المواد التجفيرية

2.4.7 التهديدات للسلامة

يقتصر سياق السلامة على كائنات البيانات بوجه عام، على النحو الذي تورده هنا حالات استعمال أمنية محددة.

– التلاعب ببيانات التشكيلة

يمكن للمهاجم التلاعب ببيانات تشكيلة بدالة الإثرنت.

– التلاعب ببيانات السجل

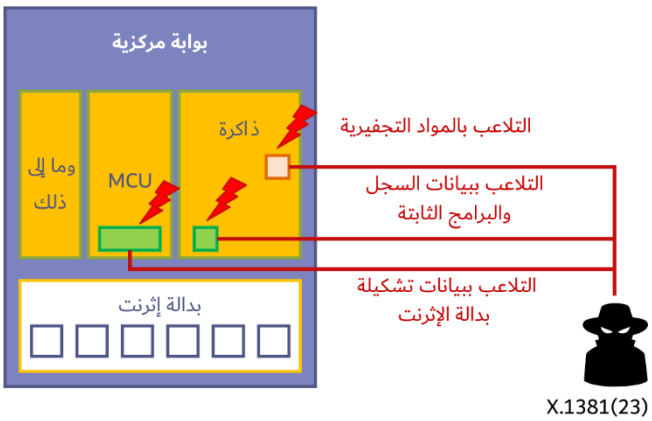
يمكن للمهاجم حذف وتعديل بيانات السجلات، خاصة سجلات تدقيق الأحداث الأمنية من نظام كشف التسلل (IDS) وجدار الحماية والنظام عبر الأثير.

– التلاعب بالمواد التجفيرية

يمكن للمهاجم تغيير المواد التجفيرية الصالحة بمفرده.

– التلاعب في البرامج الثابتة

يمكن للمهاجم أن يغير البرامج الثابتة إلى برامج ثابتة خبيثة.



الشكل 5 – التهديدات لسلامة وحدات البيانات خلال الاتصالات

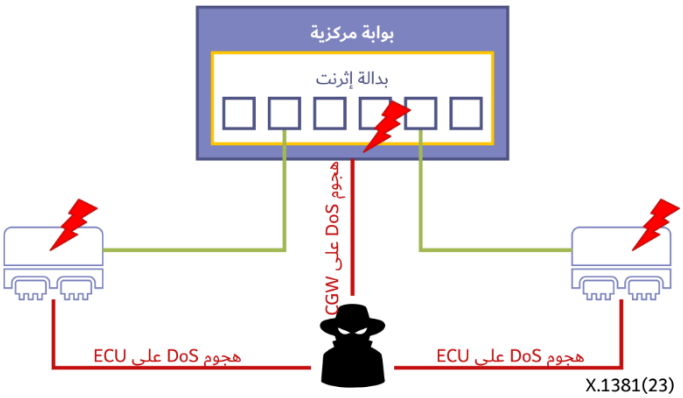
3.4.7 التهديدات للتيسر

يتصل تيسر نعت جودة النظام هنا بتيسر خدمة الاتصالات للاتصالات القائمة على الإثرنت التي تحدث تحوّلات في متطلبات تيسر التوصيل في الشبكات أو الطبقات بوجه عام، مما قد يؤدي مرة أخرى، مثلاً، إلى تيسر مسير الإثرنت في حالة الشبكة داخل المركبة (IVN) القائمة على الإثرنت ذات المسير الرديف.

– التهديدات الخاصة بالتيسر: هجوم الحرمان من الخدمة (DoS) على الشبكة داخل المركبة (IVN) القائمة على الإثرنت

يمكن للمهاجم أن يشن هجوم الحرمان من الخدمة من أجل إعاقة وظائف معيَّنة لوحدة التحكم الإلكتروني (ECU) بما فيها البوابة المركزية (CGW) أو بوابة حدود المركبة أو وحدة التحكم في التوصيلية.

وعلى النحو المبين في الشكل 6، يمكن لمهاجم أن يجعل وحدة تحكم إلكتروني (ECU) معينة وبوابة مركزية (CGW) غير متاحة لوحدات التحكم الإلكتروني المضادة المرغوبة التي تستعمل تقنيات هجوم الحرمان من الخدمة (DoS) المعروفة مثل الهجمات الخاصة ببروتوكول نقل بروتوكول الإنترنت (IP)، مثل هجمات فيض أو بعثرة رزم TCP SYN. وبالإضافة إلى ذلك، يستطيع المهاجم استنفاد موارد الشبكة داخل المركبة (IVN) باستعمال هجمات مثل عواصف الإرسال إلى جميع العناوين الشبكية في الطبقة 2 بحيث يتعذر بعدئذ تبادل أطر التحكم في النفاذ إلى وسائط (MAC) الإثرنت العادية (كوحدات بيانات البروتوكول (PDU) في الطبقة 2).

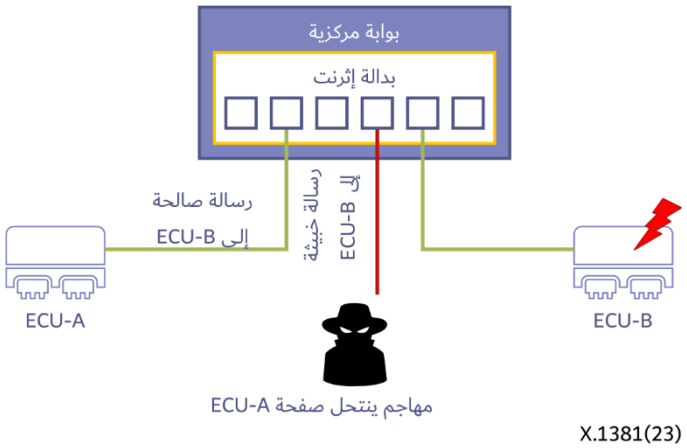


الشكل 6 – التهديدات للتيسر

4.4.7 التهديدات للاستيقانية

– انتحال صفة عُقد حوسبة المركبة (مثل وحدات التحكم الإلكتروني)

يمكن لمهاجم انتحال صفة مكون صالح مثل وحدة تحكم إلكتروني وإرسال رسائل خبيثة إلى مكونات أخرى. ويمكن للمهاجم أن يتظاهر بأنه نقطة طرفية صالحة للاتصالات (تستضيفها وحدة التحكم الإلكتروني (ECU) مثلاً) وأن يرسل رسائل ضارة أو يطّلع على حركة الاتصالات المرسَلة. وفي المثال المبين في الشكل 7، تتمثل الحالة العادية في توصيلي الطبقة العليا بين وحدتي التحكم الإلكتروني A وB (ECU-A وECU-B) (كتوصيلي نقل بروتوكول الإنترنت (IP) من نقطة إلى نقطة)، وبالتالي ترسل الوحدة ECU-A حركة إثرنت إلى الوحدة ECU-B (وربما العكس). فيدعي المهاجم أنه الوحدة ECU-A باستعمال أساليب مثل انتحال صفة بروتوكول استخراج عنوان (ARP) أو انتحال صفة بروتوكول الإنترنت (انظر مثلاً المراجع [b-IETF RFC 2827] و[IETF RFC 4953] و[b-IETF RFC 6575] و[b-IETF RFC 6959])، ثم يرسل رسالة خبيثة إلى الوحدة ECU-B.



الشكل 7 – التهديدات للاستيقانية

8 المتطلبات الأمنية

تصف هذه الفقرة المتطلبات الأمنية لمواجهة التهديدات المحددة في بيئات الشبكة داخل المركبة (IVN) القائمة على الإثرنت.

1.8 السرية

- [SR-01] يوصى بالنسبة لوحدة التحكم الإلكتروني التي تخزن وتستعمل المواد التجفيرية استعمال تخزين آمن مثل الوحدة النمطية لأمن العتاد (HSM) من أجل تخزين المواد التجفيرية بشكل آمن.
- [SR-02] يوصى بنشر خوارزميات وبروتوكولات معروفة تماماً توصِّفها، على سبيل المثال، منظمات معايير دولية.
- [SR-03] يوصى بآليات الأمن لمنع التنصت كي تُستعمل في الرسالة في اتصالات الإثرنت.

ويمكن اختيارياً تطبيق مجموعة متنوعة من بروتوكولات الأمن الخاصة بالطبقة على طبقة البروتوكول المقابلة لتجفيرها وعلى وحدة بيانات البروتوكول (PDU) الخاصة بالبروتوكول (كلياً أو جزئياً) كجزء من حركة الاتصالات القائمة على الإثرنت في مركبة ما. ومن أمثلة بروتوكولات أمن الاتصالات هذه أمن التحكم في النفاذ إلى الوسائط (MACsec) وIPsec وTLS وDTLS.

- [SR-04] يحظر على كيان غير مخوَّل الكشف عن مواد تجفيرية حساسة.

ولا تبقى آلية الأمن في المركبة آمنة عندما تنكشف مواد تجفيرية لكيانات غير مخوَّلة.

- [SR-05] يوصى بحصر التعامل مع المواد التجفيرية خلال مرحلة الإنتاج بالموظفين المخوَّلين والمعدات المخوَّلة وفقاً لسياسة التحكم في النفاذ في مركبة.
- [SR-06] يُوصى بتشكيل جدول عناوين التحكم في النفاذ إلى وسائط (MAC) بدالة الإثرنت تشكيلاً سكونياً.

ويمكن لوحدات التحكم الإلكتروني المحددة مسبقاً النفاذ إلى إثرنت في السيارة من خلال تشكيل جدول عناوين التحكم في النفاذ إلى الوسائط في بدالة الإثرنت بشكل سكوني.

ويمكن للعناوين الدينامية للتحكم في النفاذ إلى الوسائط أن تتسبب في مشاكل أمنية مثل انتحال الصفة وفيضانات التحكم في النفاذ إلى الوسائط (MAC). ويمكن للبدالة أن ترسل إطار البيانات إلى جميع منافذ الشبكة عند تخزين عدد كبير من عناوين التحكم في النفاذ إلى الوسائط في الجدول. وفي حالة المركبة، يمكن تشكيل جدول عناوين التحكم في النفاذ إلى الوسائط سكونياً لمنع هذه الإشكالات الأمنية، حيث إن وحدة التحكم الإلكتروني (ECU) التي تتواصل مع البدالة موصَّفة بالفعل.

- [SR-07] يوصى بتعطيل وظيفة التحصيل الدينامي لجدول عناوين التحكم في النفاذ إلى الوسائط في بدالة الإثرنت.

ويمكن منع تعطيل وظيفة التحصيل الدينامي لجدول عناوين التحكم في النفاذ إلى الوسائط (MAC)، وفيضانات التحكم في النفاذ إلى الوسائط التي يمكن أن تتسبب في إرسال رسائل الإثرنت إلى مقاصد غير مقصودة.

ومع ذلك، إذا كان تشغيل المركبة أو صيانتها ضرورياً، ينبغي ألا تخزن البدالة عنوان التحكم في النفاذ إلى الوسائط (MAC) المحصَّل لفترة محدودة فقط.

- [SR-08] يوصى للسطوح البينية لشبكة بروتوكول الإنترنت (IP) الخاصة بوظائف مضيف بروتوكول الإنترنت (مثل تلك التي تستضيفها وحدات التحكم الإلكتروني) التي تستعمل الإثرنت بأن تحصل على عناوين بروتوكول الإنترنت السكونية التي تخصصها وظيفة إدارة الشبكة المسؤولة.

ملاحظة – الوظائف الخاصة بإدارة الشبكة هنا هي إدارة الهوية، بما في ذلك إدارة عناوين الشبكة. ويمكن أداء وظائف الإدارة هذه خلال مختلف مراحل دورة الحياة والتشغيل في الشبكة داخل المركبة (IVN) القائمة على الإثرنت، من قبيل إدارة التشكيلة السكونية تماماً بداهةً والخليط السكوني والدينامي لإدارة التشكيلة، ويعتمد ذلك أيضاً على استعمال أو عدم استعمال بروتوكولات تشغيل الشبكة في طبقات الإثرنت والإنترنت.

ولا ينطبق هذا المتطلب الأمني (SR) على وحدات التحكم الإلكتروني (ECU) الفردية ككل فحسب وإنما أيضاً على كل قسم أو عقدة داخل شبكة إثرنت (مثل كل آلة افتراضية).

2.8 السلامة

- [SR-09] يُوصى بحماية بيانات التسجيل والتشكيلة لبدالة إثرنت من التعديل والحذف غير المرخص بهما.
- [SR-10] يوصى بأن تقوم الكيانات المخولة حصراً بتحديث بيانات التشكيلة.
- [SR-11] يُوصى بأن تستعمل وحدة التحكم الإلكتروني ميزات الإقلاع الآمن إلى جانب التحقق من سلامة البرامج الثابتة.

وينبغي التحقق من سلامة البرامج الثابتة لوحدة التحكم الإلكتروني (ECU) وبيانات بدالة الإثرنت المخزنة في ذاكرة وحدة التحكم الإلكتروني قبل التنفيذ أو أثناءه. ويمكن استعمال التحقق من سلامة التشكيلة ومعلمات مدخلات البرامج الثابتة من أجل الإقلاع الآمن.

3.8 التيسر

يتعلق معنى التيسر في هذا السياق بتيسر ميادين الإثرنت في الشبكة أي تيسر خدمة الاتصالات. ويمكن للهجمات الأمنية أن تؤثر على أهداف التيسر هذه، ولكنها قد تؤثر كذلك على أنواع أخرى من الأحداث غير الخاصة بالأمن (مثل انقطاع مكون أو تعطل الاتصالات).

وبالتالي، فإن متطلبات التيسر (في هذه الفقرة) هي في الواقع متطلبات أمنية ذات تأثير محتمل على أهداف التيسر.

- [SR-12] يُوصى بالنظر في هجمات الحرمان من الخدمة ضد الشبكة داخل المركبة (IVN) القائمة على الإثرنت في مرحلة تصميم المركبة.
- [SR-13] يُوصى بأن تكشف البدالة، وتحمي من، هجوم الحرمان من الخدمة من خلال رسائل اتصالات الإثرنت.

ومن الأهمية بمكان مراقبة تدفقات الحركة بين وحدات التحكم الإلكتروني والتحكم فيها من أجل تقليل مخاطر هجمات الحرمان من الخدمة إلى أدنى حد في الشبكة داخل المركبة.

- [SR-14] يوصى بوظائف حرجة للسلامة من أجل العزل عن الشبكات الأخرى في المركبة.

4.8 الاستيقانية

الاستيقانية تعني القدرة على ضمان بأن المعلومات المقدمة لم تتعرض لأي تعديل أو تزوير وأنها ناتجة حقاً عن الكيان الذي يدعي أنه قدم المعلومات.

- [SR-15] يُوصى بتقديم تدابير مضادة لحماية رسائل اتصالات الإثرنت من هجمات انتحال الهوية.
- [SR-16] يوصى للسطوح البينية لعناصر الشبكة داخل المركبة (IVN) القائمة على الإثرنت المادية، غير المقصود استعمالها في مركبة إنتاج، بأن تقدم القدرة على إجراء تغييرات في الحالة الإدارية الزمانية (تفعيل، تعطيل)، باستعمال قيمة التشكيلة المبدئية الخاصة "بالتعطيل".

ملاحظة – من الواضح أن هذا المتطلب المتعلق بإدارة الشبكة ينطوي على دعم نموذج بيانات الإدارة دقيق التفاصيل المقابل من أجل الإثرنت.

ويحد هذا المتطلب من مساحة الهجوم بتخفيض عدد نقاط الدخول المتاحة.

- [SR-17] يوصى بأن يقتصر النفاذ إلى السطح البيني للاتصالات، سواء المنجز في ميدان العتاد أو ميدان البرمجيات، وفقاً لمبدأ أقل امتياز يفي بالغرض.
- [SR-18] يوصى بتشكيل سطح بيني لإزالة الأخطاء البرمجية في وحدة التحكم الإلكتروني للحماية من الكيانات غير المخوَّلة. ويغطي هذا المتطلب السطوح البينية لإزالة الأخطاء البرمجية في عقدة الحوسبة المحلية فضلاً عن السطوح البينية لإزالة الأخطاء البرمجية عن بعد ذات النفاذ القائم على الشبكة داخل المركبة (IVN) إلى مثل هذه العقدة الشبكية.

ويبين الجدول 4 التقابل بين التهديدات المحددة في الفقرة 7 والمتطلبات الأمنية الواردة في الفقرة 8.

الجدول 4 – التقابل بين المتطلبات الأمنية والتهديدات الأمنية

التهديدات	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
كشف غير مجاز لرسالة اتصالات عبر الإثرنت	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
كشف غير مجاز للمواد التجفيرية	Y	Y	–	Y	Y	–	–	–	–	–	–	–	–	–	–	–	–	Y
التلاعب ببيانات التشكيلة	Y	Y	–	–	–	Y	Y	–	Y	Y	Y	–	–	–	–	–	–	Y
التلاعب ببيانات السجل	Y	Y	–	–	–	–	–	–	Y	–	Y	–	–	–	–	–	–	Y
التلاعب بالمواد التجفيرية	Y	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	Y
هجوم الحرمان من الخدمة (DoS) على الشبكة داخل المركبة (IVN) القائمة على الإثرنت	–	–	–	–	–	–	–	–	–	–	–	Y	Y	Y	–	–	–	–
انتحال صفة وحدة التحكم الإلكتروني (ECU)	–	Y	–	–	–	Y	Y	Y	–	–	–	–	–	Y	Y	Y	Y	Y

ويمكن التصدي لكل تهديد محدد من خلال الإيفاء بمتطلبات الأمن المقابلة الموسومة بحرف Y. فعلى سبيل المثال، تكون متطلبات الأمن فيما يتعلق بالتهديد الأول بشأن كشف غير مجاز لرسالة اتصالات عبر الإثرنت هي [SR-2] و[SR-3] و[SR-18].

9 تنفيذ الشبكات داخل المركبات القائمة على الإثرنت المزوَدة بالأمن

1.9 الاعتبارات المتعلقة بالتنفيذ مقدماً

تعرض هذه التوصية الاعتبارات المتعلقة بالتنفيذ من أجل:

- تحديد الجوانب الأمنية التي تمليها القيود التقنية؛
- توضيح قضايا الأمن الخاصة بالتنفيذ في المعمارية التقنية النمطية للشبكة داخل المركبة.

وتقترن قيمة هذه المعلومات الأمنية بطبيعتها اقتراناً وثيقاً بالرؤية التقنية المحددة حصراً، وبالتالي قد تتقادم في المستقبل، إذا تغيرت المعماريات التقنية للشبكة داخل المركبة (IVN) مثلاً.

ولكن ليس هناك بعد نماذج مرجعية غير تقنية ومعماريات مرجعية للشبكات داخل المركبات يمكن استعمالها كأساس لمناقشة جوانب الأمن الخاصة بتنفيذ معين. ولذا فإن هذه التوصية تعرض على الأقل بعض الاعتبارات الأمنية من خلال النظر على سبيل المثال في الأنظمة التقنية للشبكة داخل المركبة (IVN) (على النحو الوارد في الفقرة 6).

2.9 وظائف بوابة الأمن المرتبطة بإثرنت السيارات

من المهم مراقبة وضبط تدفق الاتصالات بين مختلف ميادين الشبكة المنطقية (مثل شبكة المنطقة المحلية الافتراضية (VLAN) والشبكة الفرعية للإصدار الرابع لبروتوكول الإنترنت (IPv4) والشبكة الفرعية المعرفة بسابقة الإصدار السادس لبروتوكول الإنترنت (IPv6)؛ ويمثل كل ميدان شبكة منطقية ميدان أمن محدد بنعوته الأمنية) للتقليل إلى أدنى حد من مخاطر هجمات النفاذ غير المخوَّل وهجمات الحرمان من الخدمة في الشبكات داخل المركبة (IVN) القائمة على الإثرنت. وتُستعمل جدران الحماية بوجه خاص أو بوابات الأمن بوجه عام لإتاحة أو منع بيانات الاتصالات وفقاً لقواعد محددة مسبقاً في الشبكة داخل المركبة أو في الرابطة بين الشبكات داخل المركبة وخارجها من أجل زيادة مستوى أمن المركبة.

ويوصى بالمكونات التقنية التالية التي يمكنها مراقبة رسائل الاتصال الواردة من خارج المركبة أو من الشبكة داخل المركبة (IVN) لتنفيذ وظائف بوابة الأمن هذه (مثل جدران الحماية)، كما هي معروفة في المعمارية الكهربائية والإلكترونية (E/E) التقنية الحالية والنمطية داخل المركبة.

– بدالة الإثرنت.

الملاحظة 1 – يمثل مكون بدالة الإثرنت المنطقي نمط عقدة الشبكة وليس عقدة طرفية. وهناك خياران لتنفيذ الشبكة داخل المركبة (IVN)، بدالة إثرنت كمكون تقني مستقل أو مُدمجة بصورة متكاملة كعقدة أمامية أو طرفية في عقدة حوسبة المركبة.

– بوابة حدود المركبة.

الملاحظة 2 – الخيار الأصلي لأن ذلك المكون التقني يمثل نقطة رصد واحدة لحركة الاتصالات العادية من مركبة إلى كل شيء (V2X).

– وحدة التحكم الإلكتروني (ECU): عندما يكون لوحدة التحكم الإلكتروني اتصال خارجي مباشر.

الملاحظة 3 – يمكن لعقدة حوسبة المركبة أن تقدم سطوحاً بينية إضافية لاتصالات المركبة الخارجية المباشرة (أي بتجاوز بوابة حدود المركبة)، لأغراض التشخيص مثلاً.

ويستعمل جدار الحماية عدة آليات لاصطفاء الرزم، بما في ذلك اصطفاء الرزم السكوني، والتفحص دون حالة مخزَّنة أو بحالة مخزَّنة، وتفحص الرزم الضحل أو المتوسط العمق أو حتى المعمَّق.

الملاحظة 4 – يتعين رسم خارطة ارتباطات المصطلحين المجازيين "ضحل" و"عميق" وما إليهما وربطها بما يلي: أ) طبقة البروتوكول؛ وب) نمط سياق معلومات وحدة بيانات بروتوكول (PDU) (انظر، على سبيل المثال، التوصيتين [b-ITU-T Y.2770] و[b-ITU-T Y.2771]) لكيلا يكون أي لبس فيها، فعلى سبيل المثال، سيقابل "تفحص الحزمة الضحل" عادةً تفحصَ رأسية الطبقة L3،4 في حالة حركة الإنترنت.

وعلى وجه الخصوص، تستند آلية اصطفاء الرزم الساكنة إلى قواعد سياسة عامة محددة مسبقاً. لذلك، يُوصى بوضع قاعدة سياسة عامة محددة وفقاً لمعمارية المركبة الكهربائية والإلكترونية (E/E) وبروتوكول الاتصالات المطبق. وبالإضافة إلى ذلك، تسري سياسة جدار الحماية على أسلوب القائمة البيضاء مبدئياً، حيث تمنع أساساً كل الاتصالات غير المسموح بها صراحةً.

وتتمثل إحدى الميزات الرئيسية لجدار الحماية في الدفاع ضد هجمات الحرمان من الخدمة (DoS). ويمكن لجدران الحماية أن تحمي الشبكة من هجمات الحرمان من الخدمة بتحديد عتبات باستعمال القيم المخزَّنة مسبقاً مثل العدادات أو باستعمال مراشيح التواتر.

ومن الميزات التكميلية الأخرى لجدار الحماية، وظيفة التسجيل (أي أن عنصر شبكة جدار الحماية بوصفه كياناً مداراً يقدم وظيفة إدارة تسجيل متكاملة وفقاً للتوصية [b-ITU-T M.3705]). ويُتوقع أن تخضع الأحداث المتعلقة بالأمن لخدمات التسجيل بوجه عام. ولذلك، فإن جدران الحماية أو أنظمة كشف التسلل (IDS) أو بوابات الأمن في معلومات السجل العام عند وقوع حدث أمني، لا

تقتصر على مساعدة المتخصصين في مجال الأدلة الجنائية في تحليل حالة الحدث وإنما تعزز أيضاً دقة سياسة جدار الحماية من خلال دراسات مثل حجب السجلات. وبالتالي، عند تخزين السجل، من الضروري استعمال الآلية التجفيرية لضمان السلامة.

3.9 تشكيلة الشبكة المحلية الافتراضية (VLAN) المأمونة

من المهم جداً تشكيل شبكة محلية افتراضية آمنة من أجل أمن الاتصالات في الشبكة داخل المركبة (IVN) لتلبية المتطلَبين الأمنيين [SR-14] و[SR-17]. ومصنّعو المعدات الأصلية (OEM) هم السلطة المسؤولة عن توصيف الشبكة المحلية الافتراضية لأن تشكيلة الشبكة المحلية الافتراضية تعتمد على معمارية المركبة الكهربائية والإلكترونية (E/E) التي يختارها مصنّعو المعدات الأصلية.

ولكل شبكة محلية افتراضية (VLAN) قيمة فريدة تسمى معرف (ID) الشبكة المحلية الافتراضية. ووفقاً لتوصيف الشبكة المحلية الافتراضية، يمكن استعمال معرف هوية الشبكة المحلية الافتراضية (VID) من 0 إلى 094 4، ولكن ينبغي عدم استعمال معرف الشبكة المحلية الافتراضية المحدَد مسبقاً الوارد وصفه في الجدول 5. ويمكن أيضاً استعمال معرّف الشبكة المحلية الافتراضية 1 (VLAN ID 1) في الهجمات التي تستعمل الوسم المزدوج، لذلك ينبغي للبدالة تغيير معرّف الشبكة المحلية الافتراضية 1 إلى معرف آخر للشبكة المحلية الافتراضية.

الجدول 5 – معرِّف شبكة محلية افتراضية (VLAN) المحجوز

قيمة VID (سداسي عَشَرية)	المعنى/الاستعمال
0	يدل المعرف VID الصفري على أن رأسية الوسم لا تحتوي إلا على معلومات الأولوية؛ وعلى غياب أي معرف VID في الإطار. وينبغي ألا تشكَّل قيمة VID هذه كمنفذ معرف VLAN ID (PVID) أو كعضو في مجموعة معرفات VID، وألا تشكَّل في أي قيد لقاعدة بيانات إعادة التسيير (FDB) أو في أي عملية إدارة.
1	قيمة PVID المبدئية المستعملة لتصنيف الأطر عند الدخول عبر منفذ جسر. ويمكن للإدارة تغيير قيمة PVID لمنفذ.
FFF	محجوزة لاستعمال التنفيذ. وينبغي ألا تشكَّل قيمة VID هذه كمنفذ PVID أو كعضو في أحد معرفات VID أو أحد عناصر رأسية الوسم. ويمكن استعمال قيمة VID هذه للدلالة على مواءمة سمة تنوعية للمعرف VID في عمليات الإدارة أو قيود FDB.

ويمكن للمهاجم مراقبة حركة الإثرنت بالنفاذ غير المخوَّل من شبكة محلية افتراضية (VLAN) أخرى عن طريق هجوم "القفز بين شبكات VLAN". وللتخفيف من حدة هذا الهجوم، ينبغي تشكيل الأطر غير الموسومة لدى الشبكات المحلية الافتراضية (VLAN) بحيث يصار إلى إسقاطها. ولكن يمكن وجود الاستثناءات التالية. وبالنسبة لتزامن الوقت، تُرسَل الرسائل عبر بروتوكول الوقت الدقيق الذي يتطلب إرسال الأطر دون وسم الشبكة المحلية الافتراضية وفقاً للمعيار [b-IEEE 802.1AS].

ويمكن للمهاجم المشمول في شبكة محلية افتراضية (VLAN) أصلية أن يشن هجوماً بوسمين باستعمال معرف هوية أصلية مبدئية للشبكة المحلية الافتراضية (VLAN). فيضيف المهاجم وسمين إلى الإطار، يتضمن الأول المعرف الأصلي المبدئي للشبكة المحلية الافتراضية (VLAN)، والثاني معرّف هوية الشبكة المحلية الافتراضية المستهدَف من المهاجم. وعند مرور الإطار ذي الوسمين المضافين عبر البدالة الأولى، يُزال الوسم الأول ويعاد تسيير الإطار ذي الوسم الثاني إلى البدالة التالية. وتقوم تلك البدالة بعد ذلك بإعادة تسيير الإطار إلى الشبكة المحلية الافتراضية المستهدَفة باستعمال الوسم الثاني المتبقي. وبهذه الطريقة، يمكن للمهاجم إرسال الرسالة إلى الشبكة المحلية الافتراضية المستهدفة. ولذلك ينبغي تغيير الهوية الأصلية للشبكة المحلية الافتراضية (VLAN ID) لمنع هذا الهجوم.

4.9 أمن بدالات الإثرنت في سياق السيارات

إن جسر الإثرنت في معهد مهندسي الكهرباء والإلكترونيات، المعروف أيضاً باسم بدالة الإثرنت، يقدم في الأصل قاعدة معلومات إعادة التسيير (FIB) كوسيلة أصلية لعملية إعادة التسيير والتبديل. وتتضمن قاعدة معلومات إعادة التسيير هذه جدول عناوين التحكم في النفاذ إلى الوسائط (MAC).

الملاحظة 1 – تستعمل هذه التوصية نموذج تبديل إثرنت مجرداً للغاية، مع حصر التركيز على وظائف الشبكة التي يحتمل أن تخضع لاعتبارات أمنية. وترد نظرة عامة شاملة على جميع وظائف بدالة الإثرنت الأساسية في المعيار [b-IEEE Std 802.1Q].

الملاحظة 2 – على سبيل المثال، يوصِّف المعيار [b-IEEE 802.1Q] نموذج قواعد (سياسة) لمعالجة إطار التحكم في النفاذ إلى الوسائط (MAC) في الإثرنت، وهو نموذج مقسم إلى قواعد الدخول وإعادة التسيير والخروج. ويسترعي ذلك اهتماماً خاصاً في سياق الشبكة المحلية الافتراضية (VLAN) مثلاً.

وتقدم بدالات الإثرنت النمطية آليات تحصيل العناوين الدينامي للشبكات التي تتطلب المرونة. وعند توصيل وحدة التحكم الإلكتروني الجديدة بمنفذ بدالة، يضاف تلقائياً إلى جدول عناوين التحكم في النفاذ إلى وسائط (MAC) قيد لعنوان التحكم في النفاذ إلى وسائط عقدة إثرنت طرفية بحيث يمكنه التواصل مع وحدات التحكم الإلكتروني الأخرى في ميدان شبكة الإثرنت بأكمله من خلال مرحلة التبديل هذه.

الملاحظة 3 – قد توجد أكثر من بدالة إثرنت واحدة في مسير الاتصالات من طرف إلى طرف.

وتسهل ميزة تحصيل عناوين MAC الدينامي النفاذ غير المخوَّل إلى الشبكة وينبغي تعطيلها. ويمكن أن تكون هذه الميزة مطلوبة إذا كانت أجهزة التشخيص الخارجية مطلوبة لأغراض الصيانة أو التشخيص. وفي هذه الحالة، ينبغي للبدالة أن تدعم القدرة على الحد من زمن صلاحية عناوين MAC المحصَّلة دينامياً. ومن الواضح أن هاتين التوصيتين متناقضتان، ولكنهما تعتمدان في الواقع على سياق تشغيلي محدد لشبكة الإثرنت داخل المركبة: بتوصيلية خارجية أو بدونها مع ميدان الاتصال التشخيصي عبر بروتوكول الإنترنت (DoIP) في شبكة الإثرنت على سبيل المثال. ويمكن أن تؤدي هذه التبعيات للسياق التشغيلي للشبكة إلى توصيات أمنية مشروطة، من قبيل نافذة زمنية محدودة ومقيّدة ذات تحصيل عناوين دينامي مفعّل أو ما شابه ذلك.

وانتحال عنوان MAC هو هجوم معروف على شبكات الحاسوب يمكن تنفيذه في سيناريوهات هجوم على المركبات. ولحماية الشبكة داخل المركبة (IVN)، ينبغي ضمان الاستيقان والموثوقية للأجهزة الموصولة التي تستعمل التحكم في النفاذ إلى شبكة قائمة على منفذ إذا استُعمل نفاذ مغاير. فيستيقن هذا التحكم مكوناً قبل منح النفاذ إلى الشبكة. ولا تتواصل بدالة الإثرنت مع الشبكة إلا إذا نجح الاستيقان.

وللتخفيف من هجمات الحرمان من الخدمة ينبغي أن تمنع البدالة عواصف الإرسال إلى جميع العناوين الشبكية وأن تدعم حدود المعدل القائمة على المنفذ على الرزم المستقَبلة (انظر التحكم في معلمات حركة الإثرنت في التوصية [b-ITU-T Y.1222]).

ولضمان أمن البدالة، ينبغي ضمان سلامة بيانات إدارة تشكيلة البدالة، وينبغي ألا يتسنى ذلك إلا من خلال آلية برمجة آمنة أو بروتوكول إدارة آمن للتحديثات.

- وبوجه عام، تتمثل الوظائف الأمنية اللازمة لتشغيل وإدارة بدالات الإثرنت في تطبيقات السيارات التي تتضمن معالجها الخاص بما يلي: التخزين الآمن

  ويكفل التخزين الآمن سرية البيانات المخزنة وسلامتها. وتنبغي حماية بيانات مثل المفاتيح والتحكم في النفاذ إلى وسائط (MAC) باستعمال تخزين آمن مثل الوحدة النمطية لأمن العتاد (HSM).

- الإقلاع الآمن

  يتحقق الإقلاع الآمن من سلامة البرمجيات في كل دورة إقلاع. وعند الإقلاع الأولي، تولَّد شفرة استيقان رسالة صورة البرمجيات وتُخزَّن في ذاكرة آمنة. وفي الإقلاع التالي، إذا كانت شفرة استيقان الرسائل المولدة حديثاً مماثلة لتلك المخزنة، تُضمن سلامة البرمجيات.

- سطح بيني مؤمَّن لإزالة الأخطاء البرمجية

  يحول السطح البيني الآمن لإزالة الأخطاء البرمجية دون النفاذ غير المجاز إلى السطح البيني لإزالة الأخطاء البرمجية. وعادة ما يوصى بإزالة السطوح البينية لإزالة الأخطاء البرمجية بحيث يتعذر توصيل أي كيانات مزيلة للأخطاء البرمجية. ومع ذلك، إذا كانت السطوح البينية ضرورية لضمان أو صيانة المنتَج، ينبغي السماح بالنفاذ للكيانات المخوَّلة حصراً.

- تحديث البرمجيات الآمن

  لا يسمح التحديث الآمن للبرمجيات بإعادة برمجة إلا إذا كانت موثوقية البرمجية مضمونة. ويولد مورِّد البرمجيات توقيعاً رقمياً باستعمال مفتاحه الخاص ويرسل التوقيع الرقمي وصورة البرمجيات معاً. وعندما يتحقق جهاز الاستقبال من أن التوقيع الرقمي يولده مورِّد باستعمال المفتاح العمومي للمورِّد، تكون استيقانية البرمجيات مضمونة.

التذييل I

وصف بعض بروتوكولات الشبكة داخل المركبة القائمة على الإثرنت مع نقاط الاتصالات الطرفية الموجودة في عُقد حوسبة معمارية النظام المفتوح للسيارات (AUTOSAR) أو غيرها من المعماريات

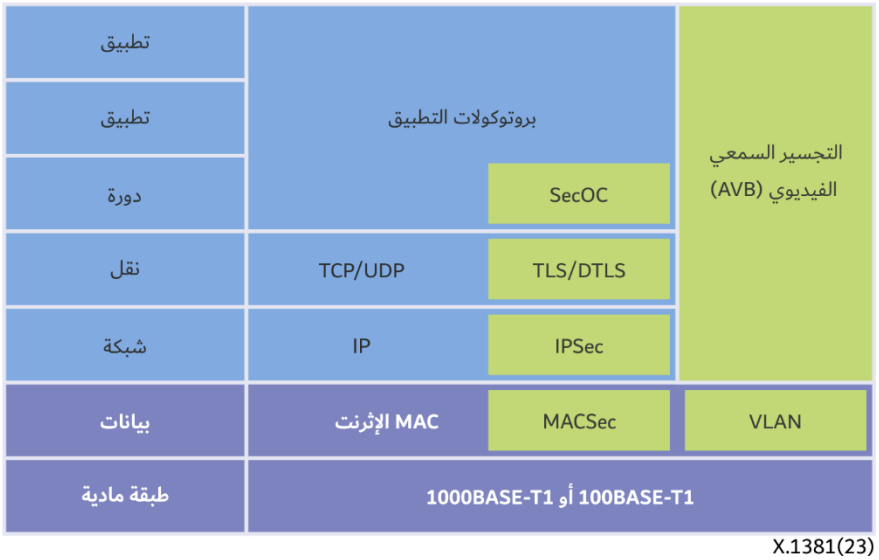
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

تتعدد بروتوكولات الاتصالات للشبكة القائمة على الإثرنت، وينفِّذ الكثير من حالات الاستعمال المستعمَلة في الاتصالات داخل المركبة القائمة على الإثرنت واحداً منها أو توليفة منها. وعلاوةً على ذلك، لا يقتصر تشغيل عُقد الحوسبة في الشبكة داخل المركبة (IVN) على نظام يعمل طبقاً لمعماريات البرمجيات القائمة على النظام المفتوح للسيارات (AUTOSAR) (مثل منصة AUTOSAR الكلاسيكية، ومنصة AUTOSAR التكيفية)، بل إنه يستعمل أيضاً معماريات الاتصالات القائمة على البرمجيات المغايرة لنظام AUTOSAR.

وبالتالي، يُفترض أساساً أن الشبكة داخل المركبة (IVN) تتألف من مزيج من عُقد الحوسبة المطابقة والمغايرة لمعمارية AUTOSAR في سياق هندسة الشبكة داخل المركبة في إطار شبكتي الإثرنت والإنترنت.

1.I نظرة عامة ومجال التطبيق

يوضح هذا التذييل بإيجاز البروتوكولات المزمع استعمالها في الاتصالات داخل المركبة القائمة على الإثرنت، على النحو المبين في الشكل 1.I.



X.1381(23)

الشكل 1.I – خدمات الاتصالات القائمة على بروتوكول الإنترنت وتلك بدون بروتوكول الإنترنت عبر الإثرنت مع ما يرتبط بها من بروتوكولات الأمن الخاصة بطبقات معيَّنة على النحو المستهدَف في الشبكات داخل المركبة

ويلاحَظ أن الشكل 1.I يركز على خدمات نقل الاتصالات، وليس على بروتوكولات الدورة وطبقة التطبيق. فعلى سبيل المثال، لا يشمل مجال تطبيق هذه التوصية البرمجيات الوسيطة الموجَّهة نحو الخدمة والقابلة للتوسيع والقائمة على معمارية AUTOSAR عبر بروتوكول الإنترنت، وبروتوكول طبقة الدورة والعرض، وخدمات الاتصالات القائمة على بروتوكول الإنترنت الموجَّهة نحو الخدمة.

2.I الاتصالات الآمنة داخل مركبة ذات معمارية AUTOSAR الشاملة لبروتوكولات أمن طبقة البروتوكول الأدنى

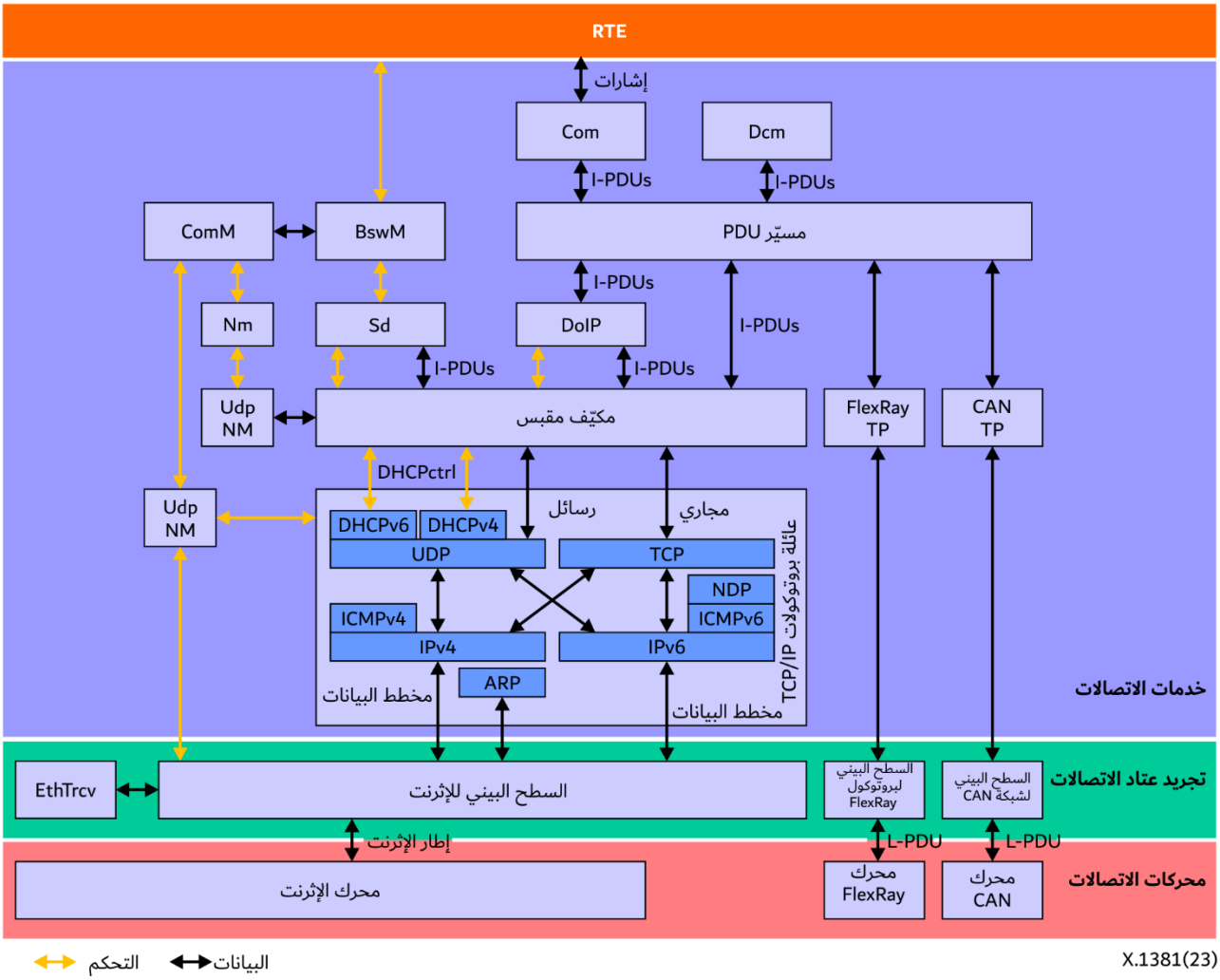
يذكَّر بأن معمارية AUTOSAR تحدد معمارية برمجية، وبالتالي تستبعد معماريات النشر. ومن ثم، تكثر الخيارات بشأن كيفية رسم خارطة ارتباطات نظام البرمجيات التالي مع عناصر المعالج (باستعمال مفهوم التطابق والتوازي، والاستعاضة عن كدسة الاتصالات التي تعرِّفها معمارية AUTOSAR بكدسة تجارية جاهزة، وما إلى ذلك).

وما برحت الإثرنت جزءاً من معيار معمارية AUTOSAR منذ الإصدار الكلاسيكي 4.0 [b-Autosar 654]. وفي معمارية AUTOSAR، تقع كدسة اتصالات الإثرنت بالتوازي (ضمن معمارية البرمجيات) مع حالات كدسة CAN وLIN وFlexRay.

ويكون مسيّر AUTOSAR PDU مسؤولاً عن التسيير الداخلي لعقدة حوسبة وحدات AUTOSAR PDU بين تطبيقات AUTOSAR والسطوح البينية للشبكة المرتبطة بنقطة الاتصالات الطرفية.

الملاحظة 1 – بالتالي، تتداخل وظيفة مسيّر AUTOSAR PDU، ولكن ينبغي عدم الخلط بينها وبين وظائف تسيير الحركة التقليدية في نقاط الاتصالات الطرفية في المعماريات المغايرة لمعمارية AUTOSAR.

وترسَل الرسالة التي يولدها التطبيق إلى مسيّر وحدة بيانات البروتوكول (PDU) الذي يرسل رسالة إلى وحدة السطح البيني أو بروتوكول النقل (TP) المقابلين. ويرسل كل سطح بيني/بروتوكول نقل الرسالة إلى السطح البيني للشبكة عبر محرك ذي صلة. وفي حالة الإثرنت، يرسل مسيّر وحدة بيانات البروتوكول رسالة إلى مكيّف مقبس (أي نقطة نفاذ الطبقة 4 إلى خدمة الاتصالات القائمة على بروتوكول TCP أو UDP) فترسَل إلى السطح البيني للإثرنت عبر وحدة بروتوكول التحكم في الإرسال/بروتوكول الإنترنت (TCP/IP). ويبين الشكل 2.I تدفق التحكم والبيانات في كدسة اتصالات AUTOSAR الموسعة.



الشكل 2.I – كدسة اتصالات AUTOSAR الموسعة (معمارية البرمجيات حصراً) (المصدر: [b-AUTOSAR 617])

الملاحظة 2 – أدخلت معمارية AUTOSAR ترميزاً لوحدة بيانات البروتوكول (PDU) يختلف عن دلالات وحدة PDU التقليدية المستعملة في تكنولوجيا المعلومات والاتصالات (على النحو الموصَّف في التوصية [b-ITU-T X.200]). وتوجد خارطة ارتباطات لوحدات I-PDU أو N-PDU أو L-PDU الداخلية في نظام برمجيات AUTOSAR أو تظهر عند السطوح البينية المستعملة للاتصالات الشبكية بوصفها وحدات PDU للطبقة *x*، والتي يشار لها عموماً بالرمز L*x*-PDU)، حسب أي من كدسات البروتوكول التسع وعشرين المحدَدة المستعمَلة.

1.2.I الاتصالات الآمنة على متن المركبة

تقدَّم الخدمات التجفيرية في معمارية AUTOSAR بواسطة خدمة التجفير وتجريد عتاد الأمن ومحرك التجفير ويطلق على هذه العناصر الثلاثة معاً كدسة التجفير. ويعتمد محرك التجفير على وحدة التحكم الدقيقة ويقدم السطح البيني الذي يمكنه النفاذ إلى العتاد. ويقدم تجريد عتاد الأمن سطحاً بينياً مشتركاً كبرمجية وسيطة بين خدمة التجفير وعتاد الأمن. ويقدم السطح البيني المشترك الاستقلالية بين محرك تجفير يعتمد على عتاد الأمن وخدمة التجفير باعتبارها خدمة طبقة عليا. ومدير خدمة التجفير (CSM) هو الوحدة النمطية الوحيدة التي يتعين إدراجها في الخدمة التجفيرية.

والاتصالات الآمنة على متن المركبة (SecOC) هي خدمة من مدير خدمة التجفير (CSM) توفر سلامة رسائل الاتصالات.

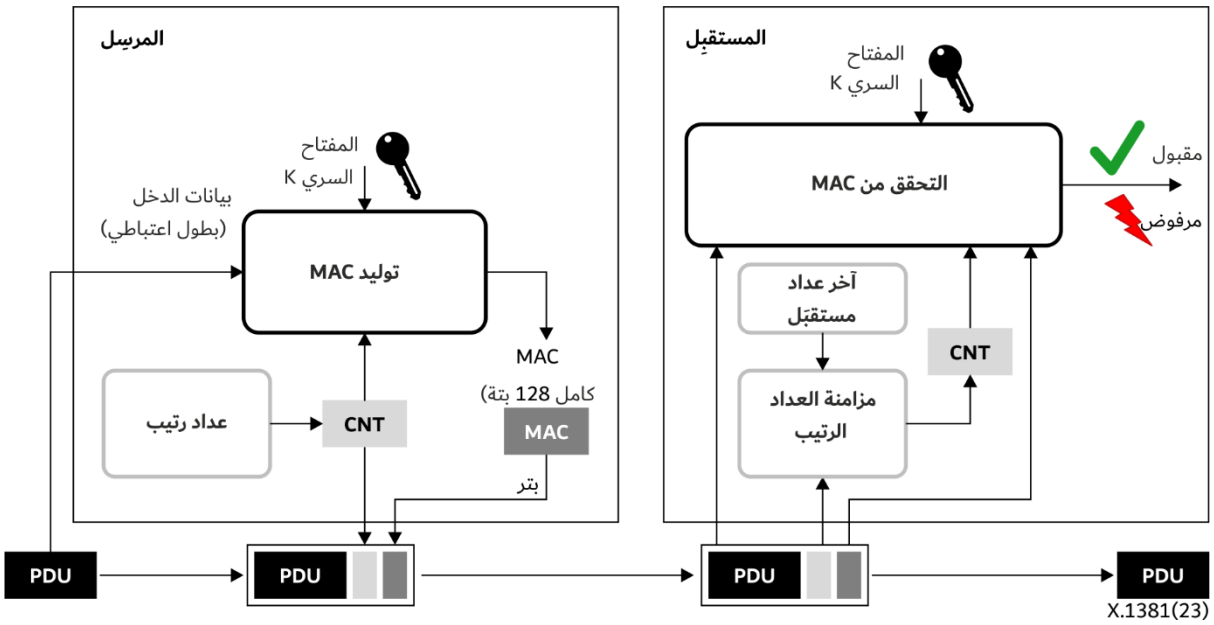
ويتمثل هدف الاتصالات الآمنة على متن المركبة (SecOC) في تقديم آليات استيقان عملية وفعالة على مستوى برمجيات (أو طبقة بروتوكول) وحدة بيانات البروتوكول (PDU). ويستعمل هذا النوع من آليات الاستيقان شفرة استيقان رسائل تستند إلى خوارزمية تجفير متناظرة لأنها ينبغي أن تقلل إلى أدنى حد من استهلاك الموارد كي تضاف إلى الأنظمة التقليدية.

وتستعمل الاتصالات الآمنة على متن المركبة (SecOC) رسالة مدير خدمة التجفير (CSM) لتوليد شفرة استيقان الرسالة والتحقق منها. ويمكن لمدير خدمة التجفير أن يسرّع من حساب شفرة استيقان الرسالة باستعمال مثل الوحدة النمطية لأمن العتاد (HSM).

ويعرض الشكل 3.I نظرة عامة وظيفية للاتصالات الآمنة على متن المركبة (SecOC).

ويولد المرسل وحدة بيانات بروتوكول (PDU) آمنة بإضافة وسم استيقان يحتوي على شفرة استيقان الرسالة وقيمة حداثة إلى وحدة PDU. ويمكن أن تكون قيمة الحداثة قيمة عداد أو خاتم زمني.

ويتحقق المستقبِل من وسم الاستيقان في وحدة بيانات البروتوكول (PDU) الآمنة المستقبَلة، أي يولد المستقبِل شفرة استيقان الرسالة على أساس بيانات وحدة PDU الآمنة المستقبَلة ويقارنها مع شفرة استيقان الرسالة المستقبَلة.



الشكل 3.I – استيقان الرسالة والتحقق من الحداثة [b-Autosar 654]

2.2.I أمن طبقة النقل

يقدم أمن طبقة النقل (TLS) خدمات اتصالات آمنة من طرف إلى طرف عبر نقاط اختبار (TP) موثوقة مثل بروتوكول التحكم في الإرسال (TCP).

ولا تدعم معمارية AUTOSAR إصدارات أمن طبقة النقل (TLS) الأقدم من إصدار TLS 1.2.

ملاحظة – انظر أيضاً المرجع [b-IETF RFC 8996] بشأن إلغاء إصداري TLS 1.0 و1.1.

ولاستعمال أمن طبقة النقل (TLS) في معمارية AUTOSAR، يسمح مدير الخدمة التجفيرية بتنفيذ مهام التجفير وعمليات المفاتيح التي يستعملها أمن طبقة النقل والوحدة الفرعية لأمن بروتوكول الإنترنت (IPsec). ويمكن الاطلاع على المتطلبات والمواصفات المفصَّلة في المرجع [b-AUTOSAR 617].

3.2.I أمن طبقة نقل مخطط البيانات

يحتاج هذا الموضوع لمزيد من الدراسة من أجل طبعة لاحقة لهذه التوصية.

4.2.I أمن بروتوكول الإنترنت

يشكل أمن بروتوكول الإنترنت (IPsec) أساساً بروتوكول أمن طبقة الشبكة الأصلية للشبكات القائمة على بروتوكول الإنترنت، ويدعم الاستيقان والتجفير. أمن بروتوكول الإنترنت اختياري للإصدار IPv4، ولكنه إلزامي للإصدار IPv6. ويصار إلى نشر أمن بروتوكول الإنترنت (IPsec) في تكنولوجيا المعلومات والاتصالات عادةً، في حال نشره أصلاً، إذا كان مقصوراً على شبكات بروتوكول الإنترنت في منطقة صغيرة، ولكنه غير مستعمل في منطقة واسعة، بسبب المحدودية وكذلك الشمولية التامة لتوصيلية بروتوكول الإنترنت من طرف إلى طرف (من قبيل الانقطاعات الناجمة عن إخفاء طوبولوجيا بروتوكول الإنترنت للبوابات أو بوابات أمن بروتوكول الإنترنت).

ولكن شبكات بروتوكول الإنترنت داخل المركبة تنتمي إلى فئة الشبكات ذات المساحة الصغيرة (جداً) وتخضع لسلطة واحدة لإدارة الشبكة التي ينبغي ألا تحول دون استعمال أمن بروتوكول الإنترنت (IPsec) الذي يقتصر على ميدان (لميادين) شبكة (شبكات) بروتوكول الإنترنت داخل المركبة.

ووفقاً للمرجع [b-AUTOSAR 617]، فإن أسلوب نفق أمن IPsec غير متاح حالياً في معمارية AUTOSAR. ويمكن استعمال أسلوب النقل فقط. وهي لا تدعم أيضاً الإصدار IPv6 والإرسال إلى عناوين متعددة. ويمكن الاطلاع على المتطلبات والمواصفات المفصَّلة في المرجع [b-AUTOSAR 970].

ملاحظة – لا ترد في هذه الطبعة من هذه التوصية اعتبارات أمنية خاصة بإصدار معيَّن لبروتوكول الإنترنت (IP) من أجل أمن بروتوكول الإنترنت (IPsec).

3.I الاتصال التشخيصي عبر بروتوكول الإنترنت

الاتصال التشخيصي عبر بروتوكول الإنترنت (DoIP) لأغراض التشخيص، دون أي وسيلة أمنية مدمجة.

الاتصال التشخيصي عبر بروتوكول الإنترنت (DoIP) هو نقطة اختبار (TP) قائمة على بروتوكول الإنترنت موصَّفة في المرجع [b-ISO 13400-2]. ويمكن الاتصال التشخيصي عبر بروتوكول الإنترنت نقل الرسائل بين خدمات التشخيص الموحدة (UDS) في مركبة ومعدات اختبار خارجية عبر الإثرنت. ويعتمد الاتصال التشخيصي عبر بروتوكول الإنترنت على البروتوكولات التالية:

- DHCP؛
- ICMP؛
- البحث عن عناوين التحكم في النفاذ إلى الوسائط (MAC) القائم على عنوان بروتوكول الإنترنت (الإصدار الرابع من بروتوكول الإنترنت (IPv4): ARP، الإصدار السادس من بروتوكول الإنترنت (IPv6): بروتوكول اكتشاف الجوار).

وفي بروتوكول UDP، تحتوي كل وحدة بيانات على رسالة DoIP واحدة. وبالنسبة للبيانات القائمة على بروتوكول التحكم في الإرسال (TCP)، تفصل الرأسية بين فرادى رسائل DoIP ضمن مجرى البيانات.

وينبغي أن يُستعمل منفذ TCP 13400 المعروف لدى هيئة تخصيص أرقام الإنترنت (IANA) من أجل الاتصال التشخيصي عبر بروتوكول الإنترنت (DoIP) (طلبات تشخيصية واستجابات تشخيصية) من معدات التشخيص الخارجية إلى وحدة التحكم الإلكتروني في المركبة.

ولا ينظر الاتصال التشخيصي عبر بروتوكول الإنترنت (DoIP) في أي آلية لأمن الاتصالات. ولا تُستيقن الرسائل ولا تجفَّر بأي شكل كان. ولذلك ينبغي لمهندسي الأمن عند تصميم خدمات DoIP النظر في استعمال طبقات مختلفة من البروتوكولات الأمنية.

4.I أمن التحكم في النفاذ إلى الوسائط

التحكم في النفاذ إلى الوسائط (MACsec) هو بروتوكول أمني معياري [b-IEEE 802.1AE] يقدم اتصالات آمنة لمجمل الحركة في طبقة وصلة البيانات. ويدعم أمن التحكم في النفاذ إلى الوسائط (MACsec) الأمن من طرف إلى طرف أو من قفزة إلى قفزة في مستوى توصيل الطبقة 2 للإثرنت (أي "وصلات" من طرف إلى طرف أو وصلات محلية) بين العُقد الطرفية للإثرنت أو عُقد البدالة. ويشمل أمن MACsec الاستيقان والتجفير أو فك التجفير مما يسمح بتعرف هوية معظم التهديدات الأمنية ومنعها، بما في ذلك هجمات الحرمان من الخدمة، والتسلل، والتدخل الوسيط، والتنكر، والتنصت السلكي السلبي، وإعادة التشغيل.

التذييل II

بوابات المركبة المزودة بتوصيلية الإثرنت أو بروتوكول الإنترنت أو الإنترنت

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

1.II المسوغات

بشكل عام، تقدم البوابة المركزية (CGW) أو البوابة الحدودية للمركبات أو بوابات المركبات (VG) دوراً حاسماً في معمارية أمن الاتصالات داخل المركبة، ولا سيما بالنسبة لميداني الشبكة القائمين على الإثرنت وبروتوكول الإنترنت، ولخدمات الاتصالات. والموقع الطوبولوجي في الشبكة للبوابة المركزية بوصفه بوابة حدود المركبة يعني ضمناً ويحدد دور البوابة الأمنية بين ميادين الشبكة الداخلية والخارجية للمركبة.

ويرتبط عادة توصيف وتقييس أنماط عناصر الشبكة هذه بالاعتبارات الأمنية الصريحة أو حتى بالمبادئ التوجيهية والمواصفات الأمنية.

2.II الغرض من هذا التذييل

يقدم هذا التذييل قائمة غير حصرية بمعايير البوابات ذات الصلة بالأمن والتي قد تعود بالفائدة، بفضل معلومات أمن الاتصالات التكميلية، ضمن مجال تطبيق هذه التوصية. وقد يخضع هذا التذييل لتحديثات في الطبعات اللاحقة لهذه التوصية.

3.II توصيات مختارة تتضمن معلومات أمنية بشأن بوابة المركبة

تدرج هذه الفقرة توصيات تتصل بالأمن دون أي تقييم لتوصيات الأمن المحددة.

- التوصية [b-ITU-T F.749.1]: تتضمن المتطلبات الوظيفية للأمن؛
- التوصية [b-ITU-T F.749.2]: تقدم فقرات مكرسة بشأن متطلبات أمن الاتصالات ومتطلبات الأمن في الطبقة العليا؛
- التوصية [b-ITU-T H.550]: جوانب الأمن المتعلقة أساساً بإدارة أمن البوابات؛
- التوصية [b-ITU-T H.560]: جوانب الأمن المتعلقة أساساً بالسطح البيني لاتصالات البوابات المستعملة في الاتصالات الخارجية.

التذييل III

أمن نظام النقل الذكي داخل المركبات

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية.)

1.III معلومات أساسية

يتضمن مفهوم أنظمة النقل الذكية معمارية اتصالات للمركبات تغطي نظام الاتصالات الداخلية في المركبة إضافةً إلى التوصيل البيني بأنظمة وخدمات الاتصالات الخارجية في المركبة. وأهم عنصر للشبكة والاتصالات في المعمارية العامة يقع داخل المركبة، ويدعى محطة أنظمة النقل الذكية، انظر على سبيل المثال المرجعين [b-ETSI EN 302 665] و[b-ETSI TR 101 607].

وتمثل محطة نظام النقل الذكي شبكة اتصالات داخل المركبة، قد تكون قائمة على الإثرنت وتقدم خدمات اتصالات غير ذات صلة ببروتوكول الإنترنت أو تكون قائمة على بروتوكول الإنترنت. ويتوافق هذا الحل التقني لأنظمة النقل الذكية مع مجال تطبيق هذه التوصية.

2.III شبكات أنظمة النقل الذكية داخل المركبة

تتألف معمارية الشبكة داخل المركبة الموصَّفة في نظام النقل الذكي من نفس عناصر الشبكة على النحو الموضح في متن هذه التوصية، وهي: بوابة أنظمة النقل الذكية للمركبات؛ ومضيف أنظمة النقل الذكية للمركبات؛ ومسيّر أنظمة النقل الذكية للمركبات؛ ومسيّر أو بوابة حدود أنظمة النقل الذكية للمركبات، وما إلى ذلك. وبالتالي، تنطبق المبادئ التوجيهية لأمن أنظمة النقل الذكية أيضاً على هذه التوصية إلى حد كبير، خاصة عندما تتماثل تكنولوجيات الاتصالات (أي البروتوكولات وكدسات البروتوكولات) ومعمارية الاتصالات.

3.III أمن أنظمة النقل الذكية

ليس الغرض من هذه التوصية تقييم الأمن المحدد من أنظمة النقل الذكية. غير أن تحليل التهديدات ومواطن الضعف والمخاطر الذي يجرى في إطار أنظمة النقل الذكية أو المبادئ التوجيهية لأمن أنظمة النقل الذكية أو الخدمات الأمنية أو المعمارية الأمنية قد يقدم قراءة تكميلية مفيدة، خاصةً في حالة أمن الاتصالات. انظر المعيار [b-ETSI TS 102 731] للاطلاع على مزيد من المعلومات والمراجع الأمنية.

بيبليوغرافيا

[b-ITU-T F.749.1] Recommendation ITU-T F.749.1 (2015), *Functional requirements for vehicle gateways*.

[b-ITU-T F.749.2] Recommendation ITU-T F.749.2 (2017), *Service requirements for vehicle gateways*.

[b-ITU-T G.7710] Recommendation ITU-T G.7710/Y.1701 (2020), *Common equipment management function requirements*.

[b-ITU-T G.8013] Recommendation ITU-T G.8013/Y.1731 (2015), *Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks*.

[b-ITU-T H.550] Recommendation ITU-T H.550 (2017), *Architecture and functional entities of vehicle gateway platforms*.

[b-ITU-T H.560] Recommendation ITU-T H.560 (2017), *Communications interface between external applications and a vehicle gateway platform*.

[b-ITU-T M.3010] Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*.

[b-ITU-T M.3702] Recommendation ITU-T M.3702 (2010), *Common management services – Notification management – Protocol neutral requirement and analysis*.

[b-ITU-T M.3703] Recommendation ITU-T M.3703 (2010), *Common management services – Alarm management – Protocol neutral requirement and analysis*.

[b-ITU-T M.3705] Recommendation ITU-T M.3705 (2013), *Common management services – Log management – Protocol neutral requirements and analysis*.

[b-ITU-T X.200] Recommendation ITU-T X.200 (1994), *Information technology – Open systems interconnection – Basic reference model: The basic model*.

[b-ITU-T X.641] Recommendation ITU-T X.641 (1997), *Information technology – Quality of service: framework*.

[b-ITU-T X.703] Recommendation ITU-T X.703 (1997), *Information technology – Open distributed management architecture*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.1039] Recommendation ITU-T X.1039 (2016), *Technical security measures for implementation of ITU-T X.805 security dimensions*.

[b-ITU-T Y.1222] Recommendation ITU-T Y.1222 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services*.

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2021), *Baseline identity management terms and definitions*.

[b-ITU-T Y.1730] Recommendation ITU-T Y.1730 (2004), *Requirements for OAM functions in Ethernet-based networks and Ethernet services*.

[b-ITU-T Y.2770] Recommendation ITU-T Y.2770 (2012), *Requirements for deep packet inspection in next generation networks*.

[b-ITU-T Y.2771] Recommendation ITU-T Y.2771 (2014), *Framework for deep packet inspection*.

[b-Autosar 617] AUTOSAR 617 (2021), *Specification of TCP/IP stack*, AUTOSAR CP R21-11.

[b-Autosar 654] AUTOSAR 654 (2017), *Specification of secure onboard communication*, AUTOSAR CP Release 4.3.1.

[b-Autosar 970] AUTOSAR 970 (2019), *Requirements on IPsec Protocol*, AUTOSAR FO R19-11.

[b-ETSI EN 302 665] European Standard ETSI EN 302 665 V1.1.1 (2010), *Intelligent transport systems (ITS); Communications architecture*.

[b-ETSI TR 101 607] Technical Report ETSI TR 101 607 V1.2.1 (2020), *Intelligent transport systems (ITS); Cooperative ITS (C-ITS); Release 1*.

[b-ETSI TS 102 731] Technical Specification ETSI TS 102 731 V1.1.1 (2010), *Intelligent transport systems (ITS); Security; Security services and architecture*.

[b-IEEE 802.1] IEEE 802.1 (Internet). *Welcome to the IEEE 802.1 Working Group*. Available [viewed 2022-06-30]: https://1.ieee802.org/

[b-IEEE 802.1AE] IEEE 802.1AE-2018, *IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) security*.

[b-IEEE 802.1AS] IEEE 802.1AS (Internet), *Standard for Local and metropolitan area networks – Timing and synchronization for time-sensitive applications in bridged local area networks.* Available [viewed 2022-06-30]: https://www.ieee802.org/1/pages/802.1as.html

[b-IEEE 802.1CB] IEEE 802.1CB-2017, *IEEE Standard for local and metropolitan area networks – Frame replication and elimination for reliability*.

[b-IEEE 802.1Q] IEEE 802.1Q-2018, *IEEE Standard for local and metropolitan area network – Bridges and bridged networks*.

[b-IEEE 802.1Qat] IEEE 802.1Qat (Internet), *Standard for Local and metropolitan area networks – Virtual bridged local area networks - Amendment 9: Stream reservation protocol (SRP).* Available [viewed 2022-06-30]: https://www.ieee802.org/1/pages/802.1at.html

[b-IEEE 802.1Qav] IEEE 802.1Qav-2009, *IEEE Standard for Local and metropolitan area networks – Virtual bridged local area networks amendment 12: Forwarding and queuing enhancements for time-sensitive streams*.

[b-IEEE 1722-2016] IEEE 1722-2016, *Standard for a Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks*.

[b-IETF RFC 2827] IETF RFC 2827 (1997), *Network ingress filtering: Defeating IP source address spoofing denial of service attacks*.

[b-IETF RFC 4953] IETF RFC 4953 (2007), *Defending TCP against spoofing attacks*.

[b-IETF RFC 6020] IETF RFC 6020 (2010), *YANG – A data modeling language for the network configuration protocol (NETCONF)*.

[b-IETF RFC 6575] IETF RFC 6575 (2012), *Address resolution protocol (ARP) mediation for IP interworking of layer 2 VPNs*.

[b-IETF RFC 6959] IETF RFC 6959 (2013), *Source address validation improvement (SAVI) threat scope*.

[b-IETF RFC 8996] IETF RFC 8996 (2021), *Deprecating TLS 1.0 and TLS 1.1*.

[b-ISO 13400-2] International Standard ISO 13400-2:2019, *Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 2: Transport protocol and network layer services*.

[b-ISO 14229-5] International Standard ISO 14229-5:2022, *Road vehicles – Unified diagnostic services (UDS) – Part 5: Unified diagnostic services on Internet Protocol implementation (UDSonIP)*.

[b-ISO/SAE 21434] International Standard ISO/SAE 21434:2021, *Road vehicles – Cybersecurity engineering*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2023