الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

# ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

# X.1373

(2017/03)

السلسلة X: شبكات البيانات والاتصالات، بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنة – أمن أنظمة النقل الذكية

---

# قدرات التحديث الآمن لبرمجيات أجهزة الاتصالات في أنظمة النقل الذكية

التوصية ITU-T X.1373

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

## شبكات البيانات والاتصالات، بين الأنظمة المفتوحة ومسائل الأمن

| | |
|---|---|
| الشبكات العمومية للبيانات | X.199–X.1 |
| التوصيل البيني للأنظمة المفتوحة | X.299–X.200 |
| التشغيل البيني للشبكات | X.399–X.300 |
| أنظمة معالجة الرسائل | X.499–X.400 |
| الدليل | X.599–X.500 |
| التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام | X.699–X.600 |
| إدارة التوصيل البيني للأنظمة المفتوحة (OSI) | X.799–X.700 |
| الأمن | X.849–X.800 |
| تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI) | X.899–X.850 |
| المعالجة الموزعة المفتوحة | X.999–X.900 |
| أمن المعلومات والشبكات | |
| الجوانب العامة للأمن | X.1029–X.1000 |
| أمن الشبكة | X.1049–X.1030 |
| إدارة الأمن | X.1069–X.1050 |
| الخصائص البيومترية | X.1099–X.1080 |
| تطبيقات وخدمات آمنة | |
| أمن البث المتعدد | X.1109–X.1100 |
| أمن الشبكة المحلية | X.1119–X.1110 |
| أمن الخدمات المتنقلة | X.1139–X.1120 |
| أمن الويب | X.1149–X.1140 |
| بروتوكولات الأمن | X.1159–X.1150 |
| الأمن بين جهتين نظيرتين | X.1169–X.1160 |
| أمن معرفات الهوية عبر الشبكات | X.1179–X.1170 |
| أمن التلفزيون القائم على بروتوكول الإنترنت | X.1199–X.1180 |
| أمن الفضاء السيبراني | |
| الأمن السيبراني | X.1229–X.1200 |
| مكافحة الرسائل الاقتحامية | X.1249–X.1230 |
| إدارة الهوية | X.1279–X.1250 |
| تطبيقات وخدمات آمنة | |
| اتصالات الطوارئ | X.1309–X.1300 |
| أمن شبكات المحاسيس واسعة الانتشار | X.1339–X.1310 |
| التوصيات ذات الصلة بالبنية التحتية للمفاتيح العمومية | X.1349–X.1340 |
| أمن إنترنت الأشياء | X.1369–X.1360 |
| **أمن أنظمة النقل الذكية** | **X.1379–X.1370** |
| تبادل معلومات الأمن السيبراني | |
| نظرة عامة على الأمن السيبراني | X.1519–X.1500 |
| تبادل مواطن الضعف/الحالة | X.1539–X.1520 |
| تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية | X.1549–X.1540 |
| تبادل السياسات | X.1559–X.1550 |
| طلب المعلومات الحدسية والمعلومات الأخرى | X.1569–X.1560 |
| تعرف الهوية والاكتشاف | X.1579–X.1570 |
| التبادل المضمون | X.1589–X.1580 |
| أمن الحوسبة السحابية | |
| نظرة عامة على أمن الحوسبة السحابية | X.1601–X.1600 |
| تصميم أمن الحوسبة السحابية | X.1639–X.1602 |
| أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية | X.1659–X.1640 |
| تنفيذ أمن الحوسبة السحابية | X.1679–X.1660 |
| أمن أشكال أخرى للحوسبة السحابية | X.1699–X.1680 |

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

# قدرات التحديث الآمن لبرمجيات أجهزة الاتصالات في أنظمة النقل الذكية


## ملخص

مع تحسن تكنولوجيات النقل الذكية (ITS)، أصبح من الشائع أن تتواصل المركبات مع كيانات أخرى كالاتصال بمركبات أخرى، والاتصال من مركبة إلى مركبة (V2V) ومن مركبة إلى بنية تحتية (V2I). والأجهزة الكهربائية داخل السيارة من قبيل وحدات التحكم الإلكتروني (ECU) والنظام الكهربائي لتحصيل الرسوم (ETC) وأنظمة الملاحة في السيارات، أصبحت أكثر تطوراً. ونتيجة لذلك، يلزم تحديث وحدات البرمجيات داخل هذه الأجهزة الكهربائية على نحو ملائم لإصلاح الأعطال وتحسين الأداء والأمن تفادياً لوقوع حوادث خطيرة.

وبغية الوفاء بالمتطلبات المذكورة أعلاه، تقدم التوصية ITU-T X.1373 إجراءات من أجل التحديث الآمن للبرمجيات بين مخدم تحديث البرمجيات والمركبات مع ضوابط أمنية ملائمة. ويمكن لشركات تصنيع السيارات والصناعات المتصلة بأنظمة النقل الذكية أن تستخدم هذه التوصية عملياً كمجموعة من القدرات المعيارية لأفضل الممارسات.



## التسلسل التاريخي

| الطبعة | التوصية | تاريخ الموافقة | لجنة الدراسات | معرف الهوية الفريد* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1373 | 2017-03-30 | 17 | 11.1002/1000/13197 |


## مصطلحات أساسية

أجهزة اتصالات، هجمة رفض الخدمة (DoS)، نظام مدمج، وحدة أمن التجهيزات (HSM)، أنظمة النقل الذكية (ITS)، برمجيات ضارة، الخصوصية، تحليل المخاطر، من مركبة إلى مركبة (V2V)، من مركبة إلى بنية تحتية (V2I)، من مركبة إلى X (مركبة/بنية تحتية) (V2X)، اتصالات لاسلكية.

* 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 متخصصة للأمم المتحدة 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 "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" 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، كان 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**

# قدرات التحديث الآمن لبرمجيات أجهزة الاتصالات في أنظمة النقل الذكية

## 1 مجال التطبيق

في سياق عمليات تحديث وحدات البرمجيات في الأجهزة الكهربائية للمركبات في بيئة الاتصالات لأنظمة النقل الذكية (ITS)، ترمي هذه التوصية إلى تقديم إجراء التحديث الآمن لبرمجيات أجهزة الاتصالات لأنظمة النقل الذكية لطبقة التطبيق من أجل منع تهديدات من قبيل التلاعب بأجهزة الاتصالات المثبتة على متن السيارات والتسلل الخبيث إليها. ويشمل هذا الإجراء نموذجاً أساسياً لتحديث البرمجيات وضوابط أمنية لتحديث البرمجيات ومواصفة نسق البيانات المجردة لوحدة برمجية التحديث.

والإجراء المتعلق بالاتصالات داخل السيارة يخرج عن مجال تطبيق هذه التوصية. وللإشارة، فإن الإجراء المستعمل داخل السيارة في هذه التوصية إعلامي.

ويُقصد بهذا الإجراء أن يُطبق على أجهزة الاتصالات الموجودة على متن مركبات أنظمة النقل الذكية في إطار الاتصال من مركبة إلى بنية تحتية (V2I) بواسطة الإنترنت و/أو الشبكات المكرسة لأنظمة النقل الذكية. ويوفر هذا الإجراء مجموعة من المبادئ التوجيهية التقنية بدون متطلبات امتثال يمكن لشركات تصنيع السيارات والصناعات المتصلة بأنظمة النقل الذكية أن تستخدمها عملياً كمجموعة من الإجراءات الآمنة والضوابط الأمنية.

## 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.509] التوصية ITU-T X.509 (2012) | ISO/IEC 9594-8:2014، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: أطر شهادات المفاتيح العمومية والنعوت.*

[ITU-T X.1521] التوصية ITU-T X.1521 (2011): 2011، *نظام تحديد درجات لمواطن الضعف الشائعة.*

[ISO/IEC 15408-1] ISO/IEC 15408:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.*

[ISO/IEC 27000] ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

## 3 التعاريف

### 1.3 المصطلحات المعرَّفة في وثائق أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في وثائق أخرى:

**1.1.3 تهديد (threat)** [ISO/IEC 27000]: سبب محتمل لحادث غير مرغوب يمكن أن يؤدي إلى ضرر لنظام أو لمنظمة.

### 2.3 مصطلحات معرفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

**1.2.3 درجة تقييم المخاطر (risk score)**: درجة تحسبها طريقة تحليل المخاطر لكل تهديد.

**2.2.3 بوابة الاتصالات المتنقلة للمركبة (vehicle mobile gateway) (VMG)**: وحدة نمطية تتيح الاتصال بين وحدات التحكم الإلكتروني (ECU) في شبكة منطقة وحدة التحكم (CAN) (موصلات داخل السيارة) والكيانات الخارجية لأنظمة النقل الذكية (ITS) في الشبكة الخارجية.

## 4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات والأسماء المختصرة التالية:

CA سلطة إصدار الشهادات *(Certification Authority)*

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

CD قرص مدمج *(Compact Disc)*

CRSS نظام تحديد درجة المخاطر قائم على النظام CVSS *(CVSS based Risk Scoring System)*

CVSS نظام تحديد درجات لمواطن الضعف الشائعة *(Common Vulnerability Scoring System)*

DoS رفض الخدمة *(Denial of Service)*

DVD قرص رقمي متعدد الاستخدامات *(Digital Versatile Disc)*

ECU وحدة تحكم إلكتروني *(Electronic Control Unit)*

ETC تحصيل الرسوم الإلكتروني *(Electronic Toll Collection)*

FT شجرة العطل *(Fault Tree)*

GPS النظام العالمي لتحديد المواقع *(Global Positioning System)*

GUID معرّف هوية المستعمل العالمي *(Global User ID)*

HSM وحدة أمن التجهيزات *(Hardware Security Module)*

HTTP بروتوكول نقل نصوص ترابطية *(Hypertext Transfer Protocol)*

HTTPS أمن بروتوكول نقل النصوص الترابطية *(Hypertext Transfer Protocol Secure)*

ID معرّف الهوية *(Identifier)*

IT تكنولوجيا المعلومات *(Information Technology)*

ITS أنظمة النقل *الذكية (Intelligent Transportation System)*

LIN شبكة محلية للتوصيل البيني *(Local Interconnect Network)*

MAC شفرة استيقان الرسالة *(Message Authentication Code)*

MOST نقل الأنظمة المتمحورة حول الوسائط *(Media Oriented Systems Transport)*

OBD نظام التشخيص على المتن *(On-board diagnostics)*

OEM مصنّع التجهيزات الأصلي *(Original Equipment Manufacturer)*

PC حاسوب شخصي *(Personal Computer)*

RPM عدد اللفات في الدقيقة *(Revolutions per Minute)*

RSS نظام تحديد درجة المخاطر *(Risk Scoring System)*

SD رقمي آمن *(Secure Digital)*

SHA خوارزمية البعثرة الآمنة *(Secure Hash Algorithm)*

SSL طبقة توصيل آمنة *(Secure Socket Layer)*

TLS أمن طبقة النقل *(Transport Layer Security)*

TOE هدف التقييم *(Target of Evaluation)*

TPM وحدة منصة موثوقة *(Trusted Platform Module)*

TV تلفزيون *(Television)*

UI السطح البيني للمستعمل *(User Interface)*

URL موقع الموارد الموحد *(Uniform Resource Locator)*

USB توصيل تسلسلي عالمي *(Universal Serial Bus)*

Usvr مخدم تحديث *(Update server)*

V2I من مركبة إلى بنية تحتية *(Vehicle-to-Infrastructure)*

V2V من مركبة إلى مركبة *(Vehicle-to-Vehicle)*

V2X من مركبة إلى X (مركبة/بنية تحتية) *((Vehicle-to-X (vehicle/infrastructure)*

VMG بوابة الاتصالات المتنقلة للمركبة *(Vehicle Mobile Gateway)*

Wi-Fi أمانة لاسلكية *(Wireless-Fidelity)*

XML لغة وسم موسعة *(Extended Mark-up Language)*

# 5 الاصطلاحات

لا يوجد.

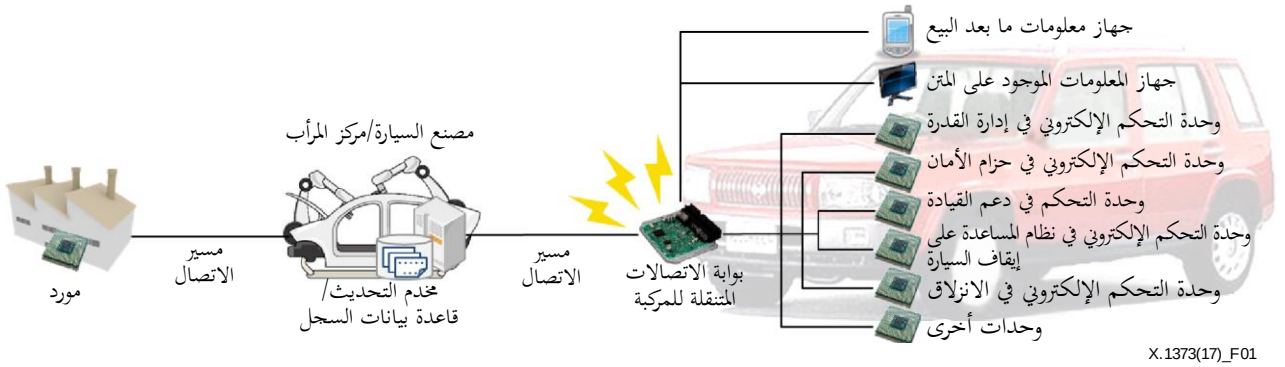
# 6 نموذج أساسي لتحديث البرمجيات عن بُعد

تقدم هذه الفقرة نموذجاً أساسياً لمعمارية تقليدية لتحديث البرمجيات حيث يُقدم تعريف للوحدات الأساسية وعمليات تحديث البرمجيات النموذجية، وذلك لاعتبارات تتعلق بمعمارية أمنية عملية.

## 1.6 وحدات بيئة أنظمة النقل الذكية من أجل تحديث البرمجيات

يعرض الشكل 1 منظراً للوحدات الأساسية الموجودة حول مركبة ما لتحديث البرمجيات عن بعد في بيئة اتصالات أنظمة النقل الذكية. وتشمل الوحدات الأساسية أجهزة المعلومات ووحدات التحكم الإلكتروني (ECU) وبوابة الاتصالات المتنقلة للمركبة (VMG) على متن السيارة ومخدم التحديث (Usvr) وقاعدة بيانات سجلات مصنّع السيارة وموزّدها. وهذا الإجراء المتعلق

بالاتصالات داخل المركبة (بين وحدات التحكم الإلكتروني وبوابة الاتصالات المتنقلة للمركبة مثلاً) يخرج عن مجال تطبيق هذه التوصية. وفيما يلي وصف بطريقة إعلامية للوحدات المستخدمة من أجل الاتصالات داخل المركبة (مثل "السطح البيني للمستعمل" و"وحدات التحكم الإلكتروني").




**الشكل 1 – الوحدات الأساسية في السيارة**

### 1.1.6 السطح البيني للمستعمل (إعلامي)

السطح البيني للمستعمل (UI) هو عموماً جهاز متاح على المتن أو جهاز معلومات ما بعد البيع يشمل شاشة عرض وأجهزة إدخال على متن أي مركبة. ويُوصل جهاز المعلومات بالأجهزة الأخرى على المتن مباشرة (مثل بوابة الاتصالات المتنقلة للمركبة (VMG) أو وحدة التحكم الإلكتروني (انظر الفقرة 2.1.6)) بحيث يتمكن من الحصول على معلومات بشأن مختلف أوضاع المركبة وعرضها مثل السرعة وعدد لفات الموتور في الدقيقة (RPM) ومستوى الوقود وغير ذلك. وبوجه خاص، يُستعمل السطح البيني للمستعمل في هذه التوصية لإخطار قائدي السيارات بضرورة إجراء تحديثات.

### 2.1.6 وحدة التحكم الإلكتروني (ECU) (إعلامي)

وحدة التحكم الإلكتروني مصطلح عام يشير إلى الحواسيب التي تتحكم في مختلف أنواع الأجهزة في أي مركبة. وفي السنوات المبكرة لوحدات التحكم الإلكتروني تمثلت وظائفها الرئيسية في التحكم في توقيت الإشعال والحقن وضبط حالة الخمول ومحدد للمحرك لتحسين كفاءة استهلاك الوقود والحد من انبعاثات الغازات. وتبعاً لحوسبة المركبات، وسّعت وحدات التحكم الإلكتروني تطبيقاتها لتشمل أنواعاً أخرى من الوظائف كإدارة القدرة والتحكم في حزام الأمان ودعم القيادة والمساعدة على إيقاف السيارة والتحكم في الانزلاق والإرسال الأوتوماتي وما إلى ذلك. وفي السنوات الأخيرة، ازداد عدد وحدات التحكم الإلكتروني داخل السيارة من 50 إلى 100 وحدة وتزداد أهمية وحدات التحكم الإلكتروني من أجل مراقبة السلامة والاتصالات بوجه خاص. ومع ذلك، نظراً إلى أن تطوير وحدات التحكم الإلكتروني ينطوي على عمليات تنفيذ لبرمجيات معقدة، فإن الزيادة الأخيرة في وحدات التحكم الإلكتروني في المركبات تفرض عبئاً ثقيلاً على الشركات المصنعة للسيارات.

### 3.1.6 بوابة الاتصالات المتنقلة للمركبة

بوابة الاتصالات المتنقلة للمركبة هي وحدة مخصصة لمواجهة "مخدم التحديث" (في الفقرة 4.1.6) لكي تتمكن المركبة من تحديث البرمجيات. وعملية تحديث البرمجيات المتاحة في المركبة تخرج عن مجال تطبيق هذه التوصية. ويمكن لبوابة الاتصالات المتنقلة للمركبة أن تكون كياناً مفاهيمياً يُنفذ عملياً بمجموعة من المكونات المتعددة. فعلى سبيل المثال، يمكن استخدام كيان إدارة التوصيل (المعروف أيضاً باسم "البوابة المركزية" أو "وحدة الرأس" أو "وحدة الرأس الخاصة بالاتصالات" أو "بوابة المركبة (VG)") للقيام بدور بوابة الاتصالات المتنقلة للمركبة في هذا السياق، ويمكن أيضاً استخدام أي أجهزة لتحديث البرمجيات. وتستخدم شبكة خلوية (شبكة متنقلة) وشبكة ثابتة عبر نظام لاسلكي كمسير اتصال بين بوابة الاتصالات المتنقلة للمركبة والكيانات الخارجية لأنظمة النقل الذكية.

### 4.1.6 مخدم التحديث وقاعدة بيانات السجل

يوجد مخدم التحديث في شركات تصنيع السيارات أو في مراكز الصيانة بهدف جمع معلومات عن حالة وحدات البرمجيات من المركبات وتوزيع وحدات تحديث البرمجيات على المركبات. وعلى غرار ذلك، فإن إحدى الوظائف الهامة لمخدم التحديث في أحدث الحواسيب الموصولة شبكياً كالحواسيب الشخصية والهواتف الذكية، تتمثل في إدارة البرمجية والتحكم فيها بشكل كامل من داخل المركبات. وبغية إدارة وضع البرمجيات هذه أوتوماتياً في كل مركبة، ينبغي لمخدم التحديث أن يعمل مع قاعدة بيانات السجل التي تخزّن معلومات الحالة لبرمجيات السيارة كشواهد. ويُلاحظ أن أي مخدم تحديث يمكن نشره ليس فقط لدى إحدى شركات التصنيع بل وأيضاً لدى أحد المورّدين أو طرف ثالث.

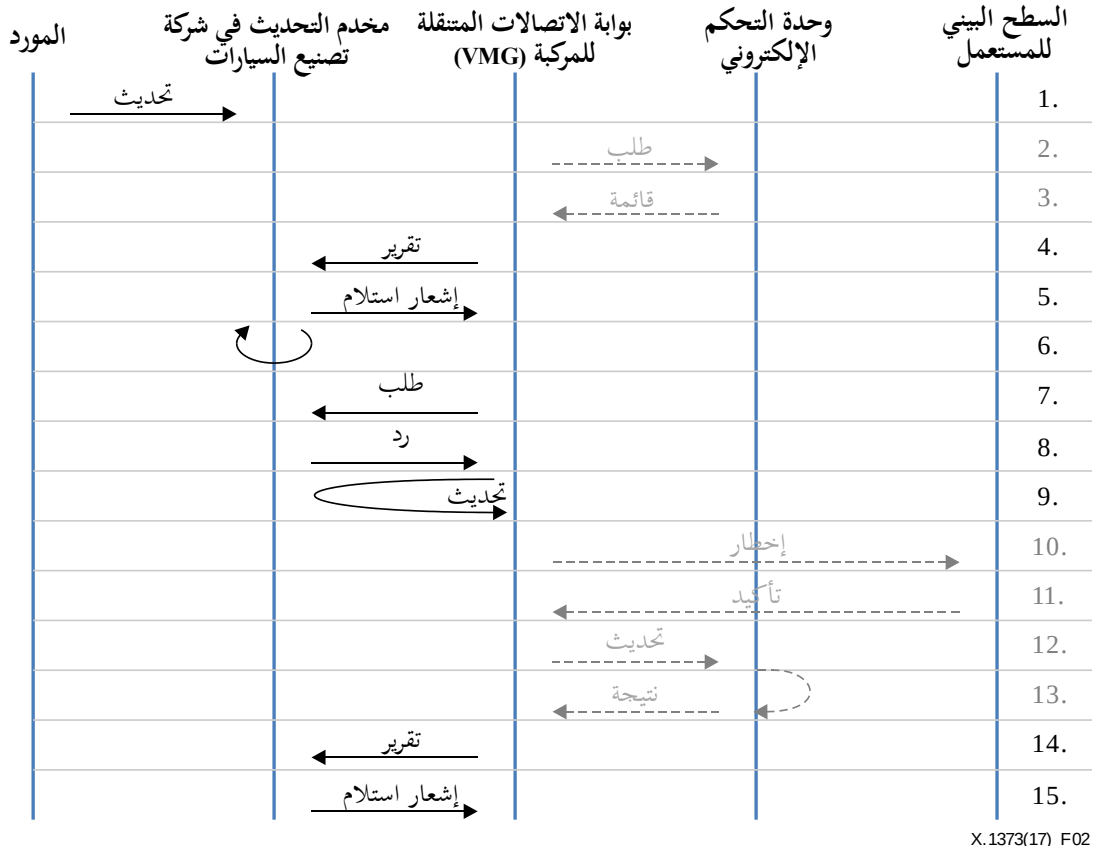
### 5.1.6 المورّد

المركبة عبارة عن تجميع لآلاف الأجزاء التي توفرها شركات توريد السيارات. وتوفر أجهزة الاتصالات ووحدات التحكم الإلكتروني الموجودة على المتن من جانب شركات التوريد هذه وتقوم شركات تصنيع السيارات بتجميعها مع مراعاة اعتماد الأجهزة المختلفة على بعضها البعض. وبالتالي، فإن وحدات التحديث الخاصة بأجهزة الاتصالات الموجودة على المتن لا تنتج بوجهٍ عام بواسطة شركة تصنيع السيارات، ولكن بواسطة مورد مناظر. وتوزع وحدات التحديث المقدمة من شركة تصنيع السيارات على المركبات بعد اختبارها وتقييمها بعناية في شركة تصنيع السيارات.

## 2.6 نموذج لإجراء تحديث البرمجيات

### 1.2.6 إجراء التحديث العام

يعرض الشكل 2 نموذجاً نمطياً لإجراء تحديث البرمجيات تستهله بوابة الاتصالات المتنقلة للمركبة من خلال التحقق من وجود التحديثات. وحيث إن الاتصالات داخل المركبة خارج مجال تطبيق هذه التوصية، فإن الخطوات المتعلقة بالاتصالات داخل المركبة الموضحة في الشكل 2 هي مجرد أمثلة إعلامية لكي يُرجع إليها عند تنفيذ إجراء تحديث آمن.




**الشكل 2 – نموذج لعملية تحديث البرمجيات**

يرد أدناه وصف الخطوات الخاصة بالتحديث، حيث تقدم الخطوات 2 و3 و10 إلى 13 (منسوخة بالخط المائل) لأغراض العلم:

1) في الخطوة الأولى من العملية، تقدم وحدة التحديث من أحد موردي مكونات السيارات، وهي خطوة تتم بصورة غير متزامنة مع الخطوات التالية.

2) *مع بداية تفعيل إجراء التحديث، تطلب بوابة الاتصالات المتنقلة للمركبة من وحدات التحكم الإلكتروني تقديم قائمة ببرمجياتها.*

3) *تقوم وحدة التحكم الإلكتروني بالتحقق من حالة برمجيتها وتعد قائمة بوحدات البرمجيات وتبلغ البوابة VMG بها.*

4) تقدم البوابة VMG القائمة المجمعة إلى مخدم التحديث للتحقق مما إذا كانت توجد تحديثات للمركبة.

5) يرسل مخدم التحديث إشعاراً باستلام القائمة المقدمة إلى البوابة VMG.

6) طبقاً للقائمة، يعاين مخدم التحديث حالة البرمجية المثبتة في المركبة ويحدد التحديثات الضرورية للبرمجية لوحدات التحكم الإلكتروني.

7) نظراً إلى أن المعاينة يمكن أن تستغرق وقتاً طويلاً، تقوم البوابة VMG دورياً بالتحقق من ضرورة إجراء تحديثات للمركبة.

8) إذا كان هناك تحديث ما، يرسل مخدم التحديث موقع موارد موحد (URL) للنفاذ من أجل التحديثات؛ أو خلاف ذلك، يرسل ثانية رسالة إخطار ليس إلا.

9) إذا كان هناك تحديث ما للمركبة، تتصل البوابة VMG بمخدم التحديث لتنزيل وحدات التحديث الخاصة بالمركبة.

10) *قبل تطبيق التحديثات على وحدات التحكم الإلكتروني، تخطر البوابة VMG قائد السيارة بأن يؤكد تطبيق التحديثات.*

11) *يؤكد قائد السيارة ويقبل تطبيق التحديثات.*

12) *توصل البوابة VMG ملفات التحديثات لوحدات التحكم الإلكتروني المقابلة وتطلب منها تطبيق التحديثات (انظر الفقرة 3.2.6).*

13) *تطبق كل وحدة من وحدات التحكم الإلكتروني التحديث وتبلغ البوابة VMG بنتائج التطبيق.*

14) تقدم البوابة VMG تقريراً بنتائج التطبيق لمخدم التحديث.

15) وفي النهاية، يرسل مخدم التحديث ثانية إشعار استلام بالمعلومات المحدثة. وإذا فشل تطبيق التحديث، أو في حالة وجود بعض التحديثات المتبقية، يكرر مخدم التحديث الخطوات من 6 إلى 14 حتى نجاح التطبيق (انظر الفقرة 2.2.6).

### 2.2.6 النظر في الإعادات غير المقيدة

طبقاً لوصف الإعادة حتى النجاح المذكور في الخطوة 15، يلاحظ أنه في بعض الحالات لن ينجح الإجراء مطلقاً، وبالتالي، يمكن أن يؤدي الوصف بالبوابة VMG إلى أن تعيد المحاولة لعدد غير محدد من المرات. ولتفادي ذلك، ينبغي تقييد عدد مرات الإعادة بعدد "N" يحدد طبقاً للسياسات الخاصة بإجراء التحديث. وكيفية تحديد السياسات الخاصة بالتحديث خارج مجال تطبيق هذه التوصية.

### 3.2.6 مراعاة قيود الموارد

حيث إنه بالنسبة للتطبيق العملي لبرمجية التحديث في المركبة (في الخطوة 12 الإعلامية الواردة في الفقرة 1.2.6)، هناك وحدات في المركبة لا تحتوي على موارد كافية من الذاكرة من أجل التخزين المؤقت لوحدة التحديث بالكامل مرة واحدة. وبالنسبة لهذه الوحدات، يلزم وجود تكنولوجيا تحديث البث المتقاطر بواسطة البث المتقاطر للبيانات المجزأة.

وبوجه عام، بالنسبة لأي وحدة في المركبة، أياً كان نظام التحديث، ينبغي أن تراعي بعناية قيود الموارد المحدودة للأجهزة مثل الذاكرة والتخزين وصبيب الشبكة.

# 7 مواصفة إجراء التحديث الآمن للبرمجيات

توصف هذه الفقرة إجراءً عملياً وأنساق رسائل تطبيقه بين مخدم التحديث والمركبة (البوابة VMG) من أجل تحديث برمجيات بوظائف أمنية. ويلاحظ أن هذه التوصية لا توصف وظائف سرية الرسائل. ويمكن توفير السرية ببروتوكولات طبقات أدنى (مثل أمن بروتوكول نقل النصوص الترابطية (HTTPS) وبروتوكول التمرير الآمن وما إلى ذلك).

ويتعين أن يراعى في الإجراء تنوع القدرات الأمنية بين المركبات. لذا، ففي هذه التوصية، تطبق المركبات ذات خوارزمية التجفير غير المتناظرة طريقة التوقيع الرقمي (في الفقرة 1.1.7)، في حين تطبق المركبات التي لا تستعمل خوارزمية تجفير غير متناظرة طريقة شفرة استيقان الرسالة (MAC) (في الفقرة 2.1.7).

## 1.7 نسق عام للرسالة مع الوظائف الأمنية

تطرح هذه الفقرة نسقاً عاماً للرسالة مع الوظائف الأمنية، بما في ذلك طريقة استيقان مرسل الرسالة والتحقق من سلامة الرسالة. وبالنسبة لتقنيات السلامة والاستيقان، يمكن تطبيق طريقة التوقيع الرقمي مع خوارزمية المفاتيح العمومية و/أو شفرة استيقان الرسالة مع خوارزمية مفاتيح مشتركة. وفي إجراء تحديث البرمجيات الآمن، ينبغي بناء كل رسالة بطريقة من الطرائق الأمنية، على النحو التالي.

### 1.1.7 طريقة التوقيع الرقمي

كطريقة من طرائق التنفيذ، يمكن تطبيق طريقة التوقيع الرقمي القائمة على التوصية [ITU-T X.509] من أجل استيقان الكيانات والتحقق من سلامة الرسالة بين المركبات ذات إمكانات التجفير غير المتناظر بواسطة وحدة أمن التجهيزات (HSM) (مثل وحدة منصة موثوقة (TPM)).

### 2.1.7 طريقة شفرة استيقان الرسالة

نظراً إلى أن خوارزمية المفاتيح المشتركة تتطلب حمل معالجة أقل من خوارزمية المفاتيح العمومية، فإن خوارزمية المفاتيح المشتركة تعتبر مناسبة للأجهزة ذات قدرات المعالجة الأقل. ولما كان المرسِل والمتلقي يستعملان نفس المفتاح في خوارزمية المفاتيح المشتركة، لذا، فإن نفس المفتاح يستعمله عدد كبير من الأجهزة. وتتطلب هذه العملية تحديث المفاتيح في جميع الأجهزة في النظام بمجرد تسرب المفتاح المشترك. وإلى جانب ذلك، نظراً إلى أن المفتاح المشترك نفسه لا يوفر استيقان المرسِل، يتعين أن تتضمن كل رسالة معرف هوية لجهاز المرسِل، وهو ما يفترض سلفاً أن معرف الهوية في الجهاز لم يتم التعامل معه بصورة غير سليمة.

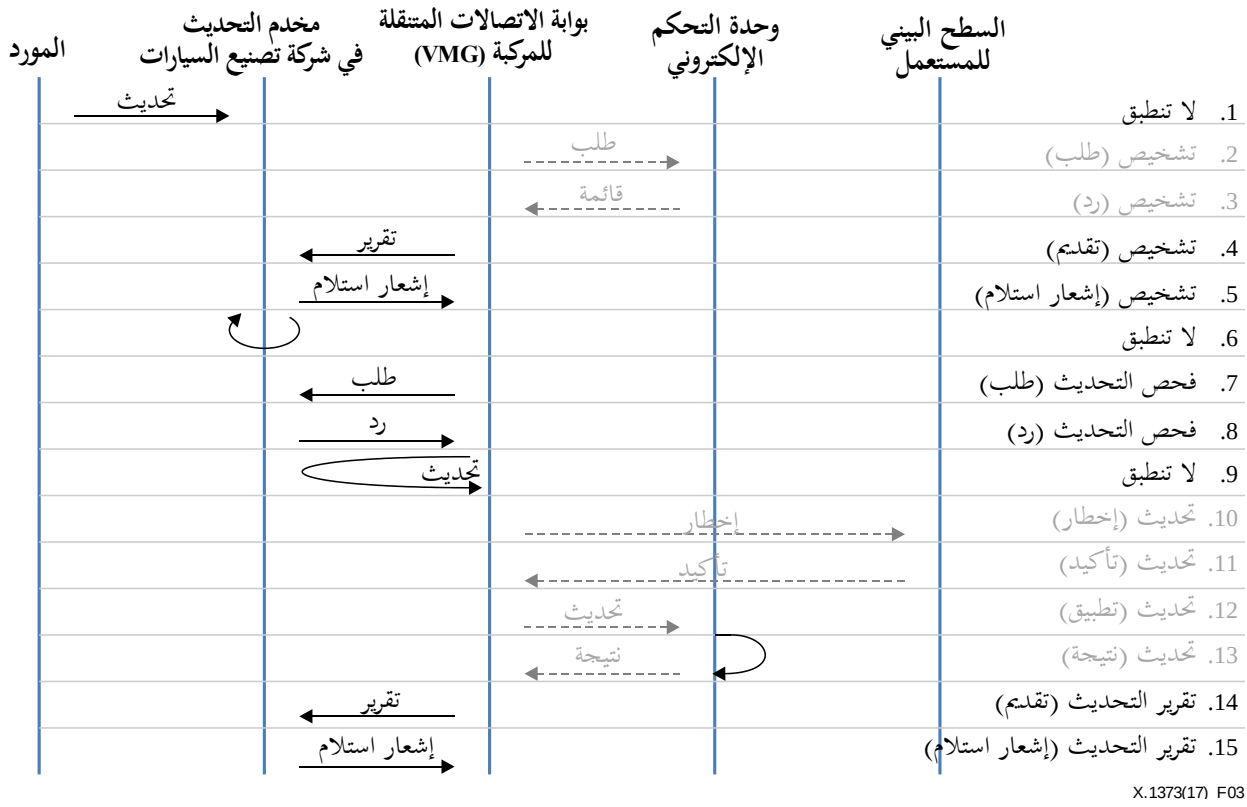
## 2.7 تعريف البروتوكول ونسق البيانات

يخصص نسق بيانات التطبيق لتوصيل الرسائل المتعلقة بتحديث البرمجيات فقط، المتضمن في نسق الرسالة العامة الموضح في الفقرة السابقة. وتعرف هذه الفقرة أولاً أنواع الرسائل المطبقة في إجراء تحديث البرمجيات، وتقدم ثانياً مواصفات أنواع الرسائل هذه. وترد أمثلة الرسائل بنسق لغة الوسم الموسعة (XML) للعلم.

### 1.2.7 عرض مجمل للبروتوكول

استناداً إلى نموذج إجراء تحديث البرمجيات الموصوف في الفقرة 6، تصنف الرسائل إلى أنواع عديدة طبقاً لأهدافها، على النحو المعروض في الشكل 3. وتقع إجراءات الاتصالات داخل المركبة خارج مجال تطبيق هذه التوصية وترد بخط رمادي في الشكل 3.

**ملاحظة** – يمكن الاطلاع على الإجراء الخاص بالاتصالات داخل المركبة في المعيارين [b-ISO 14229] و[b-ISO 13440].




**الشكل 3 – تعريف أنواع الرسائل**

في الخطوات 2 و3 و4 و5، نظراً إلى أن الغرض من الرسائل هو طلب إجراء تشخيصات لحالة برمجيات كل وحدة ECU والإبلاغ عنها، تصنف الرسائل على أنها "تشخيص". وبنفس الطريقة، تصنف الرسائل في الخطوتين 7 و8 على أنها "فحص التحديث". والخطوات 10 و11 و12 و13 عبارة عن "تحديث"، حيث إنها رسائل لتأكيد التحديثات وتطبيقها. وفي نهاية المطاف، تقدم نتائج التحديثات عبر رسائل "تقرير التحديث" في الخطوتين 14 و15. وترد الأنواع والأنواع الفرعية للرسائل ورموزها في الجدول 1.

**الجدول 1 – أنواع الرسائل**

| النوع | النوع الفرعي | من | إلى | الغرض |
|---|---|---|---|---|
| تشخيص | *طلب* | *VMG* | *ECU* | *طلب تشخيص حالة البرمجيات* |
| | *تقرير* | *ECU* | *VMG* | *نتيجة التشخيص تشمل حالة البرمجيات* |
| | تقديم | VMG | Usvr | تقرير نتائج الوحدات ECU بالسيارة |
| | إشعار استلام | Usvr | VMG | إشعار استلام بتقديم تقرير التشخيص |
| فحص التحديث | طلب | VMG | Usvr | وحدة طلب التحديث |
| | رد | Usvr | VMG | تقديم وحدة التحديث |
| تحديث | *إخطار* | *VMG* | *UI* | *رسالة إخطار بتقديم تحديث للسائق* |
| | *تأكيد* | *UI* | *VMG* | *رسالة تأكيد من السائق بتطبيق التحديث* |
| | *تطبيق* | *VMG* | *ECU* | *رسالة طلب تضم وحدة التحديث* |
| | *نتيجة* | *ECU* | *VMG* | *نتائج تطبيق وحدة التحديث* |
| تقرير التحديث | تقديم | VMG | Usvr | تقرير تطبيق التحديث |
| | إشعار استلام | Usvr | VMG | إشعار باستلام التقرير |
| * Usvr: مخدم التحديث<br>* UI: السطح البيني للمستعمل | | | | |

**ملاحظة** – يستخدم النص بالخط المائل الرمادي في الجدول 1 للإشارة إلى العناصر التي تقع خارج نطاق هذه التوصية وهي مقدمة للعلم فقط.

### 2.2.7 رسائل التشخيص

حيث إن الغرض منها تحديد مدى ضرورة وحدات التحديث بالنسبة للمركبة، تستعمل رسائل التشخيص بين مخدم التحديث والبوابة VMG لتحميل معلومات البرمجيات من المركبات إلى مخدم التحديث.

#### 1.2.2.7 رسالة (تقديم) التشخيص

بعد جمع نتائج التشخيص من المركبة، تقدم البوابة VMG قائمة بمعلومات البرمجيات إلى مخدم التحديث في شركة التصنيع (أو مركز الخدمة). وتضم رسالة (تقديم) التشخيص هوية المركبة (vid) وقائمة بمعلومات البرمجيات المستخلصة من رسائل (تقرير) التشخيص.

X.1373(17)_F04

**الشكل 4 – هيكل رسالة (تقديم) التشخيص**

**الجدول 2 – عناصر رسالة (تقديم) التشخيص**

| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| **الرسالة** | – | حاوية الرسالة. |
| | بروتوكول | "1.0" دائماً. |
| | الصيغة | رقم صيغة مرسل الرسالة. |
| | النوع | نوع الرسالة ("تشخيص" دائماً). |
| | النوع الفرعي | النوع الفرعي للرسالة ("تقديم" دائماً). |
| | معرف هوية الدورة | معرف هوية الدورة عبارة عن معرف هوية عالمي للمستعمل (GUID) عشوائي مرتبط بدورة التشخيص. يستخدم معرف هوية واحد للدورة في مجموعة رسائل طلب وتقرير وتقديم والإشعار بالاستلام الخاصة بالتشخيص. |
| | مستوى الثقة | يحدد مستوى الثقة استناداً إلى قدرات الأمن ومتطلبات السلامة للجهاز الذي يولد هذه الرسالة. |
| | معرف هوية المالك | معرف هوية المالك المقدم من شركة تصنيع/توريد السيارة. |
| | معرف هوية الرسالة | معرف هوية الرسالة هو دليل عشوائي مصحوب برسالة فردية. |
| **المركبة** | – | حاوية معلومات المركبة. تحتوي على عناصر وحدات متعددة. |
| | الاسم | اسم المركبة، إن وجد. |
| | الطراز | اسم طراز المركبة المقدم من شركة تصنيع السيارة. |

**الجدول 2 – عناصر رسالة (تقديم) التشخيص *(تتمة)***

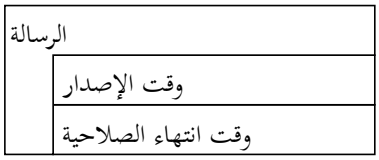
| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| | معرف هوية الطراز | اسم طراز المركبة. |
| | معرف هوية المركبة | معرف هوية المركبة المحدد من قبل شركة تصنيع/توريد السيارة. |
| | الموقع | معلومات موقع المركبة. |
| **الجهاز** | – | حاوية معلومات الجهاز. تحتوي على عناصر وحدات متعددة. |
| | الاسم | اسم الجهاز، إن وجد. |
| | النوع | اسم نوع الجهاز، مثل "الوحدة ECU لإدارة القدرة" و"الوحدة ECU للتحكم في حزام الأمان" وما إلى ذلك. |
| | الطراز | اسم طراز الجهاز. |
| | معرف هوية الجهاز | معرف هوية الجهاز المحدد من قبل شركة تصنيع/توريد السيارة. |
| | صيغة العتاد | صيغة وحدة العتاد هذه. |
| **الوحدة** | – | حاوية معلومات الوحدة والتي تضم عنصر اختزال. |
| | معرف هوية الوحدة | معرف هوية الوحدة معرف فريد يقدم من شركة تصنيع/توريد السيارة. |
| | الصيغة | صيغة وحدة البرمجية هذه. |
| | الصيغة التالية | صيغة تحديث الوحدة الجارية، والتي تستخدم بشكل أساسي لإرسال رسالة رد أثناء عملية التحديث. |
| **الاختزال** | – | Hash عبارة عن حاوية لقيمة ومعلومات الاختزال الخاصة بخوارزمية الاختزال الخاصة بها. |
| | الخوارزمية | خوارزمية دالة الاختزال (مثل SHA-3 وSHA-256 وغيرها). |
| **وقت الإصدار** | – | وقت توليد هذه الرسالة. |
| **وقت انتهاء الصلاحية** | – | وقت انتهاء صلاحية هذه الرسالة. |

**الجدول 3 – مثال لرسالة (تقديم) التشخيص**

```
<message protocol="1.0" version="1.0.2" type="diagnose" subtype="submit"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}" ownerid="oid987239487"
messageid="{BBCE3B0B-2A10-443A-97D0-EF4650457422}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{66E6F81E-F293-4531-B2FC-A93F177373AA }"
version="1.3.23.0" nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
    </Device>
    <Device name="device2" type="ECU" model="model1" id="did0987234"
hwversion=”HC-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion=""/>
            <Hash algorithm="SHA-256">hash data here</Hash>
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

### 2.2.2.7 رسالة (إشعار استلام) التشخيص

بعد تحميل معلومات البرمجية الخاصة بالمركبة برسالة (تقديم) التشخيص، يرسل مخدم التحديث إشعار استلام برسالة (إشعار استلام) التشخيص بحيث تدرك المركبة أن التقديم تم بنجاح وأنه يمكن للمركبة المضي قدماً إلى الحالة التالية (فحص التحديث).




X.1373(16)_F05

**شكل 5 – هيكل رسالة (إشعار استلام) التشخيص**

**الجدول 4 – عناصر رسالة (إشعار استلام) التشخيص**

| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| **الرسالة** | – | حاوية الرسالة. |
| | البروتوكول | "1.0" دائماً. |
| | الصيغة | رقم صيغة مرسل الرسالة. |
| | النوع | نوع الرسالة ("تشخيص" دائماً). |
| | النوع الفرعي | النوع الفرعي للرسالة ("إشعار استلام" دائماً). |
| | معرف هوية الدورة | معرف هوية الدورة عبارة عن دليل عشوائي مرتبط بدورة التشخيص. ويستخدم معرف هوية دورة واحد في مجموعة رسائل طلب وتقرير وتقديم والإشعار باستلام التشخيص. |
| | مستوى الثقة | يحدد مستوى الثقة استناداً إلى قدرات الأمن ومتطلبات السلامة للجهاز الذي يولد الرسالة. |
| | معرف هوية المالك | معرف هوية المالك المقدم من شركة تصنيع/توريد السيارة. |
| | معرف هوية الرسالة | معرف هوية الرسالة عبارة عن دليل عشوائي مرتبط برسالة فردية معينة. |
| | الحالة | إخطار استلام تقرير بشأن (تقديم) التشخيص. |
| **وقت الإصدار** | – | وقت توليد هذه الرسالة. |
| **وقت انتهاء الصلاحية** | – | وقت انتهاء صلاحية هذه الرسالة. |

**الجدول 5 – مثال لرسالة (إشعار استلام) التشخيص**

```
<message protocol="1.0" version="1.0.2" type="diagnose" subtype="receipt"
sessionid="{7316A97D-8C04-428B-B498-0F51087A1093}" ownerid="oid987239487"
messageid="{E313159C-2081-4A10-B61D-4F81D074D54F}" trustlevel="3"
status=”yes”>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

### 3.2.7 رسائل فحص التحديث

بعد تحميل معلومات البرمجية إلى مخدم التحديث عبر رسالة التشخيص، يبدأ مخدم التحديث التحليل من أجل تحديد وحدات التحديث اللازمة للمركبة، وهو ما قد يستغرق وقتاً طويلاً. وتستخدم رسالة فحص التحديث بصورة دورية للاستفسار عن قرار مخدم التحديث. وهناك نوعان فرعيان لرسالة فحص التحديث، الطلب والرد حيث يتم تبادلهما بين البوابة VMG ومخدم التحديث.

### 1.3.2.7 رسالة (طلب) فحص التحديث

تنقل رسالة (طلب) فحص التحديث من البوابة VMG إلى مخدم التحديث لفحص مدى الضرورة لإجراء التحديثات. وتشمل هذه الرسالة معلومات الوحدات التي ستخضع للمعاينة وهي مشابهة تماماً لرسالة (إشعار استلام) التشخيص.


X.1373(17) F06

**الشكل 6 – هيكل رسالة (طلب) فحص التحديث**

**الجدول 6 – عناصر رسالة (طلب) فحص التحديث**

| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| **الرسالة** | – | حاوية الرسالة. |
| | البروتوكول | "1.0" دائماً. |
| | الصيغة | رقم صيغة مرسل الرسالة. |
| | النوع | نوع الرسالة ("فحص التحديث" دائماً). |
| | النوع الفرعي | النوع الفرعي للرسالة ("طلب" دائماً). |
| | معرف هوية الدورة | معرف هوية الدورة عبارة عن دليل عشوائي يرتبط بدورة فحص التحديث. ويستخدم معرف واحد مع مجموعة رسائل طلب ورد فحص التحديث. |
| | مستوى الثقة | يحدد مستوى الثقة استناداً إلى قدرات الأمن ومتطلبات السلامة في الجهاز الذي يولد هذه الرسالة. |
| | معرف هوية المالك | معرف هوية المالك يقدم من قبل شركة تصنيع/توريد السيارة. |
| | معرف هوية الرسالة | معرف هوية الرسالة عبارة عن دليل عشوائي يرتبط برسالة فردية. |
| **المركبة** | – | حاوية معلومات المركبة. تضم عناصر وحدات متعددة. |
| | الاسم | اسم المركبة، إن وجد. |
| | الطراز | اسم طراز المركبة المقدم من شركة تصنيع السيارة. |
| | معرف هوية الطراز | اسم طراز المركبة. |
| | معرف هوية المركبة | معرف هوية المركبة المحدد من قبل شركة تصنيع/توريد السيارة. |
| | الموقع | معلومات موقع المركبة. |
| **الجهاز** | – | حاوية معلومات الجهاز. تضم عناصر الوحدات المتعددة. |
| | الاسم | اسم الجهاز، إن وجد. |
| | النوع | اسم النوع، مثل "الوحدة ECU لإدارة القدرة" و"الوحدة ECU للتحكم في حزام الأمان" وما إلى ذلك. |
| | الطراز | اسم طراز الجهاز. |
| | معرف هوية الجهاز | معرف هوية الجهاز المحدد من قبل شركة تصنيع/توريد السيارة. |
| | صيغة العتاد | صيغة وحدة العتاد هذه. |

**الجدول 6 – عناصر رسالة (طلب) فحص التحديث *(تتمة)***

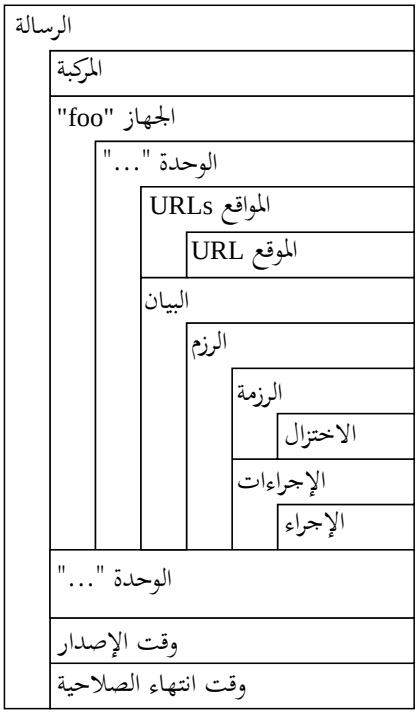
| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| **الوحدة** | – | حاوية معلومات الوحدة، والتي تتضمن عنصر الاختزال. |
| | معرف هوية الوحدة | معرف هوية الوحدة عبارة عن معرف فريد يقدم من جانب شركة تصنيع/توريد السيارة. |
| | الصيغة | صيغة وحدة البرمجية هذه. |
| | الصيغة التالية | صيغة تحديث الوحدة الجاري والذي يستخدم في الأساس لإرسال رسالة الرد أثناء التحديث. |
| **وقت الإصدار** | – | وقت توليد هذه الرسالة. |
| **وقت انتهاء الصلاحية** | – | وقت انتهاء صلاحية هذه الرسالة. |

**الجدول 7 – مثال لرسالة (طلب) فحص التحديث**

```
<message protocol="1.0" version="1.0.2" type="update_check" subtype="request"
sessionid="{19622672-A025-4500-B26A-BB626BC61C62}" ownerid="oid987239487"
messageid="{4604A6C9-F72F-452B-ABA5-94168CCD8FD6}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.3.23.0" nextversion=""/>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion=""/>
    </Device>
    <Device name="device2" type="ECU" model="model1" id="did0987234"
hwversion=”HC-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion=""/>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

#### 2.3.2.7 رسالة (رد) فحص التحديث

للرد على رسالة (طلب) فحص التحديث، يرد مخدم التحديث بإرسال نتائج المعاينة. فإذا كانت هناك تحديثات لازمة لأي وحدة من وحدات المركبة، تقوم رسالة (رد) فحص التحديث بتحميل المواقع الإلكترونية اللازمة للحصول منها على وحدات التحديث. ويلاحظ أن رسالة التحديث لا تتضمن ملفاً إثنينياً لوحدة التحديث ذاتها، بينما تقوم البوابة VMG بتحميلها بواسطة توصيلة أخرى استناداً إلى معلومات المورد في رسالة (رد) فحص التحديث.



X.1373(17)_F07

**الشكل 7 – هيكل رسالة (رد) فحص التحديث**

**الجدول 8 – عناصر رسالة (رد) فحص التحديث**

| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| **الرسالة** | – | حاوية الرسالة. |
| | البروتوكول | "1.0" دائماً. |
| | الصيغة | رقم صيغة مرسِل الرسالة. |
| | النوع | نوع الرسالة ("فحص التحديث" دائماً). |
| | النوع الفرعي | النوع الفرعي للرسالة ("رد" دائماً). |
| | معرف هوية الدورة | معرف هوية الدورة عبارة عن دليل عشوائي يرتبط بدورة فحص التحديث. ويستخدم معرف واحد مع مجموعة رسائل طلب ورد فحص التحديث. |
| | مستوى الثقة | يحدد مستوى الثقة استناداً إلى قدرات الأمن ومتطلبات السلامة في الجهاز الذي يولد هذه الرسالة. |
| | معرف هوية المالك | معرف هوية المالك يقدم من قبل شركة تصنيع/توريد السيارة. |
| | معرف هوية الرسالة | معرف هوية الرسالة عبارة عن دليل عشوائي يرتبط برسالة فردية. |
| **المركبة** | – | حاوية معلومات المركبة. تضم عناصر وحدات متعددة. |
| | الاسم | اسم المركبة، إن وجد. |
| | الطراز | اسم طراز المركبة المقدم من شركة تصنيع السيارة. |
| | معرف هوية الطراز | اسم طراز المركبة. |
| | معرف هوية المركبة | معرف هوية المركبة المحدد من قبل شركة تصنيع/توريد السيارة. |
| | الموقع | معلومات موقع المركبة. |

**الجدول 8 – عناصر رسالة (رد) فحص التحديث *(تتمة)***

| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| **الجهاز** | – | حاوية معلومات الجهاز. تضم عناصر الوحدات المتعددة. |
| | الاسم | اسم الجهاز، إن وجد. |
| | النوع | اسم النوع، مثل "الوحدة ECU لإدارة القدرة" و"الوحدة ECU للتحكم في حزام الأمان" وما إلى ذلك. |
| | الطراز | اسم طراز الجهاز. |
| | معرف هوية الجهاز | معرف هوية الجهاز المحدد من قبل شركة تصنيع/توريد السيارة. |
| | صيغة العتاد | صيغة وحدة العتاد هذه. |
| **الوحدة** | – | حاوية معلومات الوحدة، والتي تتضمن عنصر الاختزال. |
| | معرف هوية الوحدة | معرف هوية الوحدة عبارة عن معرف فريد يقدم من جانب شركة تصنيع/توريد السيارة. |
| | الصيغة | صيغة وحدة البرمجية هذه. |
| | الصيغة التالية | صيغة تحديث الوحدة الجارية والتي تستخدم في الأساس لإرسال رسالة الرد أثناء التحديث. |
| | الحالة | حالة معاينة التحديث. تظهر عبارة "لا يوجد تحديث" في حالة عدم وجود تحديثات، في حين تظهر كلمة "ok" في حالة وجود أي تحديثات لهذه الوحدة. |
| **المواقع URL** | – | حاوية عناصر لمواقع URL في حالة وجود أي تحديثات. ويرد هذا العنصر في عنصر الوحدة عندما تكون الحالة "ok". |
| **الموقع URL** | – | الموقع URL لملف التحديث. وينبغي إدراج عنصر الموقع URL مرتين على الأقل من أجل عمل نسخة احتياطية للموقع URL الأول (المخدم). وينبغي تحديد العدد الأقصى لعناصر المواقع URL بحذر مع مراعاة الموارد الحوسبية للبوابة VMG. |
| | قاعدة الشفرة | موقع ملف التحديث. |
| **البيان** | – | يصف الوحدة المطلوب تثبيتها والإجراءات المطلوب اتخاذها مع هذه الملفات. |
| | الصيغة | رقم صيغة أحدث محدد لوحدة البرمجية هذه. |
| **الرزم** | – | مجموعة الملفات التي يتعين تثبيتها. ولا تتضمن أي توزيع. وتتضمن عنصر حزمة تابع أو أكثر. |
| **الرزمة** | – | ملف وحيد يتعين تثبيته من أجل الوحدة. |
| | الاسم | يصف اسم ملف وحدة التحديث. |
| | الحجم | يحتوي على الحجم بالبايتات لوحدة التحديث. |
| | الوصف | وصف وحدة التحديث. |
| **الاختزال** | – | حاوية قيمة الاختزال ومعلومات خوارزمية الاختزال الخاصة بها. |
| | الخوارزمية | خوارزمية دالة الاختزال (مثل SHA-3 وSHA-256 وما إلى ذلك). |
| **الإجراءات** | – | الإجراءات التي يتعين اتخاذها لتثبيت الوحدة بعد التحميل الناجح لجميع الملفات المطلوبة في عنصر الرزم. |
| **الإجراء** | – | إجراء وحيد يتعين القيام به في إطار عملية التثبيت. |
| | الحدث | سلسة ثابتة تحدد الوقت الذي ينبغي فيه تنفيذ هذا الإجراء. وقيمة هذا العنصر تكون واحدة من "التثبيت المسبق" و"التثبيت" و"التثبيت اللاحق" و"التحديث". |
| | المبررات | مبررات الانتقال إلى عملية التثبيت. |
| **وقت الإصدار** | – | وقت توليد هذه الرسالة. |
| **وقت انتهاء الصلاحية** | – | وقت انتهاء صلاحية هذه الرسالة. |

**الجدول 9 – مثال لرسالة (رد) فحص التحديث**

```
<message protocol="1.0" version="1.0.2" type="update_check" subtype="response
" sessionid="{19622672-A025-4500-B26A-BB626BC61C62}" ownerid="oid987239487"
messageid="{4604A6C9-F72F-452B-ABA5-94168CCD8FD6}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale="CH"/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion="HB-01">
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.3.23.0" nextversion="" status="ok">
            <Urls>
                <Url
codebase="http://update1.server/this/is/an/example/url/"/>
                <Url
codebase="http://update2.server/this/is/an/example/url/"/>
                <Url
codebase="http://update3.server/this/is/an/example/url/"/>
            </Urls>
            <Manifest version="1.4.0">
                <Packages>
                    <Package name="module1.bin" size="589" description="This
update provides ...">
                        <Hash algorithm="SHA-256">hash data here</Hash>
                    </Package>
                </Packages>
                <Actions>
                    <Action arguments="--argument-for-installation"
event="install"/>
                </Actions>
            </Manifest>
        </Module>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="noupdate">
        </Module>
    </Device>
    <Device name="device2" type="ECU" model="model1" id="did0987234"
hwversion="HC-02">
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status="noupdate">
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

### 4.2.7 رسائل التحديثات

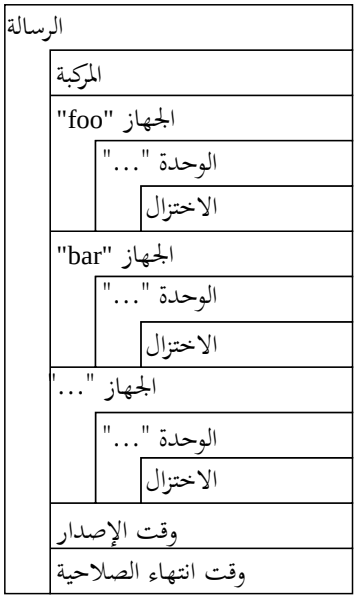
عملية التحديث التي تجري في المركبة خارج نطاق هذه التوصية. ولا يوجد تعريف أو مواصفة لرسائل التحديثات.

### 5.2.7 رسائل تقارير التحديثات

كخطوة أخيرة في تتابع إجراءات التحديث، تقدم البوابة VMG جميع التقارير المجمعة لأي تطبيق لتحديث في الأجهزة إلى مخدم التحديث بحيث يقوم مخدم التحديث بالتحكم في كل مركبة وإدارتها من موقع بعيد. وترسل البوابة VMG التقرير إلى مخدم التحديث عن طريق رسالة (تقديم) تقرير التحديث. وفي النهاية يرسل مخدم التحديث إشعاراً باستلام التقرير (رسالة (إشعار استلام) تقرير التحديث) إلى البوابة VMG بحيث يتسنى لها معرفة نهاية عملية التحديث بالكامل.

### 1.5.2.7 رسالة (تقديم) تقرير التحديث

بعد تجميع تقارير التطبيقات من الأجهزة، ترسل البوابة VMG رسالة (تقديم) تقرير التحديث إلى مخدم التحديث. وتتضمن هذه الرسالة نتائج التطبيقات فضلاً عن الحالة الراهنة للبرمجية مثل رسالة (تقديم) التشخيص.



X.1373(17)_F08

**الشكل 8 – هيكل رسالة (تقديم) تقرير التحديث**

**الجدول 10 – عناصر رسالة (تقديم) تقرير التحديث**

| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| **الرسالة** | – | حاوية الرسالة. |
| | البروتوكول | "1.0" دائماً. |
| | الصيغة | رقم صيغة مرسِل الرسالة. |
| | النوع | نوع الرسالة ("تقرير التحديث" دائماً). |
| | النوع الفرعي | النوع الفرعي للرسالة ("تقديم" دائماً). |
| | معرف هوية الدورة | معرف هوية الدورة عبارة عن دليل عشوائي يرتبط بدورة تقرير التحديث. ويستخدم معرف واحد مع مجموعة رسائل تقديم وإشعار استلام تقرير التحديث. |
| | مستوى الثقة | يحدد مستوى الثقة استناداً إلى قدرات الأمن ومتطلبات السلامة للجهاز الذي يولد هذه الرسالة. |
| | معرف هوية المالك | معرف هوية المالك المقدم من شركة تصنيع/توريد السيارة. |
| | معرف هوية الرسالة | معرف هوية الرسالة عبارة عن دليل عشوائي يرتبط برسالة فردية. |
| **المركبة** | – | حاوية معلومات المركبة. وتتضمن عناصر وحدات متعددة. |
| | الاسم | اسم المركبة، إن وجد. |
| | الطراز | اسم طراز المركبة المقدم من شركة تصنيع السيارة. |
| | معرف هوية الطراز | اسم طراز المركبة. |
| | معرف هوية المركبة | معرف هوية المركبة المحدد من قبل شركة تصنيع/توريد السيارة. |
| | الموقع | معلومات موقع المركبة. |

**الجدول 10 – عناصر رسالة (تقديم) تقرير التحديث *(تتمة)***

| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| **الجهاز** | – | حاوية معلومات الجهاز. وتتضمن عناصر وحدات متعددة. |
| | الاسم | اسم الجهاز، إن وجد. |
| | النوع | اسم نوع الجهاز، مثل "الوحدة ECU لإدارة القدرة" و"الوحدة ECU للتحكم في حزام الأمان" وغيرها. |
| | الطراز | اسم طراز الجهاز. |
| | معرف هوية الجهاز | معرف هوية الجهاز المحدد من جانب شركة تصنيع/توريد السيارة. |
| | صيغة العتاد | صيغة وحدة العتاد هذه. |
| **الوحدة** | – | حاوية معلومات الوحدة، والتي تتضمن عنصر الاختزال. |
| | معرف هوية الوحدة | معرف هوية الوحدة هو معرف وحيد تقدمه شركة تصنيع/توريد السيارة. |
| | الصيغة | صيغة وحدة البرمجيات هذه. |
| | الصيغة التالية | صيغة تحديث الوحدة الجارية، والتي تستخدم بشكل أساسي لإرسال رسالة رد أثناء التحديث. |
| | الحالة | نتائج تطبيق هذه الوحدة. |
| **الاختزال** | – | Hash عبارة عن حاوية لقيمة الاختزال ومعلومات خوارزمية اختزالها. |
| | الخوارزمية | خوارزمية دالة الاختزال (مثل SHA-3 وSHA-256 وغيرها). |
| **وقت الإصدار** | – | وقت إصدار هذه الرسالة. |
| **وقت انتهاء الصلاحية** | – | وقت انتهاء صلاحية هذه الرسالة. |

**الجدول 11 – مثال لرسالة (تقديم) تقرير التحديث**

```
<message protocol="1.0" version="1.0.2" type="update_report" subtype="submit"
sessionid="{9AFFEB5A-F36B-4E05-819F-5BDCD3A0E3EC}" ownerid="oid987239487"
messageid="{3F7A6438-8306-447E-A1BB-99CED4C2B6AD}" trustlevel="3">
    <Vehicle name="vehicleName" modelid="mid34987130" type="ECU"
model="modelName" vid="vid0987234" locale=”CH”/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-01”>
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.4.0" nextversion="" status="ok">
            <Hash algorithm="SHA-256">hash data here</ModuleHash>
        </Module>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="ok">
            <Hash algorithm="SHA-256">hash data here</ModuleHash>
        </Module>
    </Device>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion=”HB-02”>
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status=”ok”>
            <Hash algorithm="SHA-256">hash data here</ModuleHash>
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

### 2.5.2.7 رسالة (إشعار استلام) تقرير التحديث

في نهاية التتابع، يرسل مخدم التحديث رسالة (إشعار استلام) تقرير التحديث إلى البوابة VMG بحيث تدرك المركبة انتهاء إجراء التحديث بأكمله. ويكاد نسق رسالة (إشعار استلام) تقرير التحديث يتطابق مع نظيره لرسالة (إشعار استلام) التشخيص.


X.1373(17) F09

**الشكل 9 – هيكل رسالة (إشعار استلام) تقرير التحديث**

**الجدول 12 – عناصر رسالة (إشعار استلام) تقرير التحديث**

| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| **الرسالة** | – | حاوية الرسالة. |
| | البروتوكول | "1.0" دائماً. |
| | الصيغة | رقم صيغة مرسِل الرسالة. |
| | النوع | نوع الرسالة ("تقرير التحديث" دائماً). |
| | النوع الفرعي | النوع الفرعي للرسالة ("إشعار استلام" دائماً). |
| | معرف هوية الدورة | معرف هوية الدورة عبارة عن دليل عشوائي يرتبط بدورة تقرير التحديث. ويستخدم معرف واحد للدورة لمجموعة رسائل تقديم وإشعار استلام تقرير التحديث. |
| | مستوى الثقة | يحدد مستوى الثقة استناداً إلى قدرات الأمن ومتطلبات السلامة للجهاز الذي يولد هذه الرسالة. |
| | معرف هوية المالك | معرف هوية المالك المقدم من شركة تصنيع/توريد السيارة. |
| | معرف هوية الرسالة | معرف هوية الرسالة عبارة عن دليل عشوائي يرتبط برسالة فردية. |
| **المركبة** | – | حاوية معلومات المركبة. وتضم عناصر وحدات متعددة. |
| | الاسم | اسم المركبة، إن وجد. |
| | الطراز | اسم طراز المركبة المقدم من شركة تصنيع السيارة. |
| | معرف هوية الطراز | اسم طراز المركبة. |
| | معرف هوية المركبة | معرف هوية المركبة المحدد من قبل شركة تصنيع/توريد السيارة. |
| | الموقع | معلومات موقع المركبة. |
| **الجهاز** | – | حاوية معلومات الجهاز. وهي تضم عناصر وحدات متعددة. |
| | الاسم | اسم الجهاز، إن وجد. |
| | النوع | اسم نوع الجهاز، مثل "الوحدة ECU لإدارة القدرة" و"الوحدة ECU للتحكم في حزام الأمان" وغيرها. |
| | الطراز | اسم طراز الجهاز. |
| | معرف هوية الجهاز | معرف هوية الجهاز المقدم من شركة تصنيع/توريد السيارة. |
| | صيغة العتاد | صيغة وحدة العتاد هذه. |

**الجدول 12 – عناصر رسالة (إشعار استلام) تقرير التحديث *(تتمة)***

| العنصر | النعت في العنصر | الوصف |
|---|---|---|
| **الوحدة** | – | حاوية معلومات الوحدة حيث تتضمن عنصر الاختزال. |
| | معرف هوية الوحدة | معرف هوية الوحدة هو معرف وحيد مقدم من شركة تصنيع/توريد السيارة. |
| | الصيغة | صيغة وحدة البرمجيات هذه. |
| | الصيغة التالية | صيغة تحديث الوحدة الجارية، والتي تستخدم بشكل أساسي لإرسال رسالة الرد أثناء التحديث. |
| | الحالة | إخطار استلام التقرير الخاص بهذه الوحدة. |
| **وقت الإصدار** | – | وقت توليد هذه الرسالة. |
| **وقت انتهاء الصلاحية** | – | وقت انتهاء صلاحية هذه الرسالة. |

**الجدول 13 – مثال لرسالة (إشعار استلام) تقرير التحديث**

```
<message protocol="1.0" version="1.0.2" type="update_report" subtype="receipt"
sessionid="{9AFFEB5A-F36B-4E05-819F-5BDCD3A0E3EC}" ownerid="oid987239487"
messageid="{B5585708-6BDA-4B07-B2CB-5E9241F63271}" trustlevel="3">
    <Vehicle name="vehicleName" model="modelName" modelid="mid34987130"
vehicleid="vid0987234" locale="CH"/>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion="HB-01">
        <Module moduleid="{1F6EDD6C-17D4-461B-8403-1E240E26464E}"
version="1.4.0" nextversion="" status="ok"/>
        <Module moduleid="{4D168B58-26FA-4157-9703-A431D99C8438}"
version="2.4.34.0" nextversion="" status="ok"/>
    </Device>
    <Device name="device1" type="ECU" model="model1" id="did0987234"
hwversion="HB-02">
        <Module moduleid="{70628FDC-2282-4B2F-8A36-13445DED587A}"
version="3.5.45.0" nextversion="" status="ok"/>
        </Module>
    </Device>
    <IssuedTime "1903-07-01T00:00:00Z"/>
    <ExpirationTime "1903-07-01T00:00:00Z"/>
</message>
```

# التذييل I

# منهجية بشأن تحليل المخاطر

(لا يشكل هذا التذييل جزءاً من هذه التوصية)

## 1.I منهجية بشأن تحليل المخاطر استناداً إلى المعيار [b-JASO TP15002]

يقدم هذا التذييل معلومات مفصلة بشأن التذييل II. وتستند هذه المعلومات إلى المبادئ التوجيهية المتعلقة بأمن معلومات السيارات [المعيار b-JASO TP15002].

وقد أصبح أمن المعلومات من الأمور الهامة عند تصميم النظام المدمج. وهناك أمثلة للهجمات الأمنية المختلفة المعروفة بالنسبة لنظام تكنولوجيا المعلومات حتى هذه اللحظة وتتراكم الدراية الفنية لتقييم أي مخاطر من خلال تصميم أنظمة تكنولوجيا المعلومات. وترد مفاهيم الأمن الأساسية الضرورية لتقييم منتجات تكنولوجيا المعلومات في المعيار [ISO/IEC 15408-1]. وفي سياق التقييم، يستخدم المعيار [ISO/IEC 15408-1] المصطلح "هدف التقييم" (TOE). وهناك أصول تتمثل في الكيانات التي يفترض أن يضيف إليها مالك الهدف TOE قيمة. ويرمي المعيار [ISO/IEC 15408-1] إلى تحديد أهداف أمنية لأي هدف TOE تمثل بياناً بالعزم على مكافحة تهديدات محددة و/أو تنفيذ سياسات و/أو افتراضات أمنية محددة للمنظمة. وتفضي التهديدات إلى مخاطر بالنسبة للأصول، طبقاً لأرجحية تحقق التهديد وآثاره على الأصول عندما يقع. ومع ذلك لا يوصف المعيار [ISO/IEC 15408-1] كيفية إجراء عمليات استخلاص التهديدات وتحليل المخاطر.

وفيما يتعلق بالنظام المدمج، يشرح هذا التذييل التهديدات المستخلصة ويجري تحليلاً للمخاطر طبقاً لإطار المعيار [ISO/IEC 15408-1]. ويستهدف هنا، ألا يعتمد تحليل المخاطر على الدراية الفنية بتصميم الأمن. لذا، فإن طريقة تحليل المخاطر CRSS [b-JASO TP15002] في هذه التوصية تقوم بحساب مستوى مخاطر التهديد للنظام المدمج. وتتسم هذه الطريقة بما يلي: (1) صياغة الخرج في خطوة تعريف نموذج النظام وفي خطوة تحليل التهديد؛ (2) وضع قيمة للمعلمة باستعمال المعلومات التي تتاح من إجراء الخطوة السابقة.

وتتألف عملية تقييم الأمن الواردة في المعيار [b-JASO TP15002] من المراحل التالية:

المرحلة 1: تعريف هدف التقييم؛

المرحلة 2: تحديد التهديدات؛

المرحلة 3: تحليل المخاطر.

ويرد أدناه شرح كل مرحلة من هذه المراحل.

### 1.1.I المرحلة 1: تعريف هدف التقييم

يوضح هدف تحديد التهديدات في المرحلة التالية.

وتجرى الخطوات الأربع التالية في المرحلة 1:

#### الخطوة 1: وضع إدراك مشترك

استناداً إلى وثيقة الاستعراض الشامل للنظام ومن أجل تمكين جميع أعضاء المشروع من وضع إدراك مشترك لدورة حياة النظام المستهدف وبناء النظام، يتم إعداد معلومات مثل شكل بناء النظام ووظيفة النظام وبيانات النظام المستخدمة.

### الخطوة 2: بناء شكل النموذج لهدف التقييم

يتم بناء "شكل نموذج لهدف التقييم" يوضح مكونات النظام وتدفق المعلومات بين هذه المكونات.

### الخطوة 3: تعريف نظرة عامة لوظائف الوحدات

لكل وحدة بنائية موضحة في شكل نموذج هدف التقييم، توضح الوظائف المتاحة وأصولها المحمية. وبهذه الطريقة، يتم بناء جدول من أجل "نظرة عامة لوظائف الوحدات".

ويمكن وصف التهديدات الأمنية من منظور: "ما هي عوامل التهديدات الموجودة وما هي الإجراءات الضارة التي تقوم بتنفيذها وعلى أي من الأصول" في النظام المستهدف بالتقييم. وإلى جانب المعلومات التي تعالج تقليدياً كأحد الأصول التي يتعين حمايتها، تضم الأصول في الأنظمة المدمجة للمركبات برمجيات الأنظمة المدمجة والوظائف التي تتحكم في أجزاء ميكانيكية مثل المحرك أو الفرامل.

ويتولد نموذج النظام من طبيعة الأصول ومن مخططات تدفق البيانات التي توصف تدفقات البيانات فيما يتعلق بهذه الأصول.

وفيما يتعلق بالإجراءات الضارة التي تنفذ (التهديدات)، تدرس جميع الأشياء التي يمكن أن تحدث بالنسبة لكل نقطة من نقاط المدخلات وينظر في ذلك أيضاً من منظور أنواع الأعطال المسماة السرية أو السلامة أو التيسر التي يمكن أن تحدث لكل نوع من أنواع الأصول. فعلى سبيل المثال، من المهم أن تعمل وظائف أي نظام لتكنولوجيا المعلومات في مركبة بالشكل السليم المتوقع مع ضرورة منع أعطال السلامة أو التيسر. وبالمثل، من المهم حماية المعلومات المتبادلة بين المخدمات المركزية وأجهزة أنظمة النقل الذكية (ITS) المثبتة على المركبات من الاطلاع عليها وتعديلها ويجب أيضاً منع أعطال السرية أو السلامة. ويعرض الجدول 1.I أمثلة للمعلومات والأصول الأخرى التي ينبغي للمركبات أن تحميها.

**الجدول 1.I – أمثلة على المعلومات والأصول الأخرى التي ينبغي للمركبات أن تحميها (أمن معلومات المركبات)**

| الأشياء التي ينبغي حمايتها | الوصف |
|---|---|
| تشغيل "وظائف التحكم الأساسية" | تماسك وتيسر "وظائف التحكم الأساسية" وبيئة تنفيذها واتصالات التشغيل. |
| معلومات خاصة بالمركبة حصراً | المعلومات الخاصة ببدن السيارة حصراً (معرف هوية المركبة ومعرف هوية الجهاز وما إلى ذلك) وشفرة الاستيقان والمعلومات المتراكمة مثل تاريخ السير وتاريخ التشغيل. |
| معلومات حالة المركبة | البيانات التي تمثل حالة المركبة مثل الموقع وسرعة السير والوجهة. |
| معلومات المستعمل | معلومات شخصية ومعلومات الاستيقان ومعلومات الفوترة وتاريخ الاستعمال وتاريخ التشغيل الخاص بالمستعمل (سائق/ركاب) |
| البرمجيات | البرمجيات التي تتعلق "بوظائف التحكم الأساسية" للمركبة و"الوظائف الموسعة". وتشمل الأمثلة برمجيات وحدة التحكم الإلكتروني. |
| المحتويات | بيانات من أجل التطبيقات مثل الفيديو والموسيقى والخرائط وغيرها. |
| معلومات التشكيل | بيانات التشكيل من أجل سلوك العتاد والبرمجيات وما إلى ذلك. |

### الخطوة 4: تعريف نطاق دورة حياة الهدف

يتم بناء "جدول دورة حياة" يوضح دورات الحياة بالكامل للنظام المستهدف.

وعوامل التهديدات هي كل الأشخاص المشاركين في أي نقطة عبر دورة حياة المركبة وتشمل شركة التصنيع وهل اشتراها المالك جديدة أم مستعملة وفي النهاية انتهاء خدمتها. ويرجع ذلك إلى أن المعلومات السرية الموجودة في الأنظمة المدمجة في المركبات تخزن ويتم النفاذ إليها ليس فقط أثناء مرحلة الاستعمال العادي ولكن أيضاً خلال المراحل الأخرى، أثناء التصنيع أو التسليم أو الصيانة والإصلاح، مثلاً. ويعرض في الجدول 2.I تفاصيل دورة حياة هدف التقييم.

**الجدول I.2 – دورة حياة هدف التقييم**

| المرحلة | المرحلة الفرعية | نظرة عامة | الأشخاص المعنيون |
|---|---|---|---|
| التشغيل | النقل | يقوم أحد موظفي شركة تصنيع المعدات الأصلية (OEM) بنقل المركبة المصنعة إلى تاجر المركبات. ويطلب من مشغل شركة النقل القيام بذلك. | • موظف الشركة OEM<br>• مشغل شركة النقل<br>• موظف تاجر المركبات<br>• طرف ثالث |
| | توصيل المركبة | يقوم أحد موظفي تاجر المركبات بتوصيل المركبة إلى المالك. | • موظف تاجر المركبات<br>• المالك<br>• طرف ثالث |
| | التشغيل/ الاستعمال العادي | يقوم المالك أو المستعمل باستخدام المركبة. ويشترك مدير المخدم بوصفه مديراً لمخدم التحديث الذي يوفر البرمجيات. وتشترك شركة الاتصالات لتوفير شبكة الاتصالات. | • المالك أو المستعمل<br>• مدير المخدم<br>• شركة الاتصالات<br>• طرف ثالث |
| | التشغيل/ الاستعمال العادي<br>تحميل برمجيات | للإعداد لتحديث البرمجيات عبر مخدم التحديث، تحمل المركبة البرمجيات من مخدم التحديث. | • موظف الشركة OEM<br>• موظف المورد<br>• مدير المخدم<br>• شركة الاتصالات<br>• طرف ثالث |
| | الصيانة (تحديث البرمجيات عبر مخدم التحديث)<br>تحديث البرمجيات | عندما تكون السيارة في المرأب، يتم تحديث البرمجيات. ويشترك مدير المخدم بوصفه مديراً لمخدم التحديث.<br>وتشترك شركة الاتصالات بوصفها مورداً لشبكة الاتصالات. ويشترك موظف توريد بوصفه مورد خدمة باستعمال شبكة الاتصالات. | • موظف الشركة OEM<br>• موظف المورد<br>• مدير المخدم<br>• شركة الاتصالات<br>• طرف ثالث |
| | الصيانة (تحديث البرمجيات عبر موصل عمليات التشخيص من على المتن (OBD) | يقوم موظف تاجر المركبات أو موظف شركة الصيانة بتحديث البرمجيات عبر الموصل OBD وقت معاينة المركبة. | • موظف تاجر المركبات<br>• موظف شركة الصيانة<br>• المالك أو المستعمل<br>• طرف ثالث |

### I.2.1 المرحلة 2: تحديد التهديدات

تحدد المشكلات الأمنية المتعلقة بهدف التقييم المعرف في المرحلة 1.

وتجرى الخطوات الثلاث التالية في المرحلة 2.

#### الخطوة 1: وضع الافتراضات

من أجل توضيح النطاق الذي تحدد فيه التهديدات، تعرف الافتراضات استناداً إلى شكل نموذج هدف التقييم، والاستعراض الشامل لوظائف الوحدات وجدول دورة الحياة. ويتسم النطاق الذي تحدد فيه التهديدات في المرحلة 2 بالمحدودية. وتعرف الافتراضات بشأن بيئة هدف التقييم. ويخصص معرف هوية بسابقة "A" لكل تهديد محدد. وبهذه الطريقة، يتم بناء "جدول الافتراضات".

ويتم تشغيل هدف التقييم طبقاً للافتراضات التالية:

**A.Reliability_OfficeStaff (موثوقية موظف الشركة OEM/موظف التوريد/موظف تاجر المركبات/موظف شركة الصيانة)**

لا ينفذ موظف الشركة OEM أو موظف التوريد مادياً إلى المركبة المستهدفة بالهجمات. وعلاوة على ذلك لا ينفذ موظف تاجر المركبات/موظف شركة الصيانة مادياً إلى المركبة في مرحلة التشغيل/الاستعمال العادي.

**A.Reliability_ServiceProvider (موثوقية مدير المخدم/شركة الاتصالات)**

لا ينفذ مدير مخدم التحديث/شركة الاتصالات مادياً إلى المركبة. وعلاوة على ذلك، لا يتسبب مدير مخدم التطبيق/شركة الاتصالات في تهديدات عن عمد.

**A.Reliability_User (موثوقية المالك/المستعمل)**

لا ينفذ المالك/المستعمل مادياً إلى المركبة المستهدفة بالهجمات، خلال مرحلة الصيانة.

ولا ينفذ المالك/المستعمل مادياً إلى المركبة، خلال مرحلة الصيانة. وعلاوة على ذلك، يقوم المالك/المستعمل بالغلق المحكم للأبواب في مرحلة التشغيل/الاستعمال العادي. وعلاوة على ذلك، لا يسمح المالك/المستعمل للأشخاص غير المخولين المعنيين بالولوج إلى المركبة في مرحلة التشغيل/الاستعمال العادي.

**A.Operation_Server (حماية المخدم خارج هدف التقييم)**

يتم تشغيل مخدم التحديث بشكل جيد وهو ما يعني أنه لن يسمح للأشخاص المعنيين بالحصول على/التلاعب في المعلومات المخزنة في المخدم.

**A.Control_OBD-Tool (حماية جهاز القياس، وما شابه، خارج هدف التقييم)**

يتم تشغيل جهاز القياس بشكل جيد وهو ما يعني عدم السماح للأشخاص المعنيين بالحصول على/التلاعب في المعلومات المخزنة في جهاز القياس.

**الخطوة 2: تحديد التهديدات**

استناداً إلى شكل نموذج هدف التقييم، والاستعراض الشامل لوظائف الوحدات وجدول دورة الحياة لكل مكون من مكونات النظام، تعرض في الجدول 3.I، هوية التهديدات من منظور المكان (نقاط الدخول) والجهة الفاعلة (عامل التهديد) والتوقيت (المرحلة من دورة الحياة) والدواعي (الأسباب) والماهية (الإجراءات الضارة). ويخصص لكل تهديد محدد معرف هوية بالسابقة "T". وبهذه الطريقة، يتم بناء "جدول التهديدات".

وبتطبيق هذه الرؤى على نموذج النظام وعلى دورة الحياة وعلى الإجراءات الضارة التي تتم دراستها عند تعريف النظام المستهدف بالتقييم الموصوف في الفقرة 1.I، يمكن، بشكلٍ كامل، تحديد عوامل التهديدات القائمة والإجراءات الضارة التي تقوم بتنفيذها وعلى أي من الأصول وفي أي مرحلة من المراحل.

**الجدول 3.I – مظاهر تحديد التهديدات**

| المظهر | الشرح |
|---|---|
| المكان | تحديد نقاط دخول الهجمات. |
| الجهة الفاعلة | تحديد عوامل التهديدات. |
| التوقيت | تحديد مراحل دورة حياة الهجمات. |
| الدواعي | تحديد الأسباب وراء الهجمات. |
| الماهية | تحديد الإجراءات الضارة. |

## الخطوة 3 – وضع السياسات الأمنية للمنظمة

تعرف السياسات الأمنية للمنظمة المتطلبات التي تستوجب وجود تدابير أمنية مضادة نتيجة لأسباب أخرى خلاف التهديدات. ومن الأمثلة على ذلك القوانين والمبادئ التوجيهية للصناعة التي يتعين اتباعها عند تطوير هدف للتقييم وفي بيئة التشغيل. وتحدد القوانين أو قواعد الشركة المتعلقة بتطوير النظام والتي ينبغي تعريفها بوصفها مشكلات أمنية لهدف التقييم. ويخصص لكل سياسة أمنية معرف هوية بالسابقة "O". وبهذه الطريقة، يتم بناء "جدول السياسات الأمنية للمنظمة".

ولا توجد سياسات أمنية للمنظمة تطبق على هدف التقييم.

### 3.1.I المرحلة 3: تحليل المخاطر

توصف هذه الخطوة درجات المخاطر لجميع التهديدات التي تحددت.

وتحسب درجة الأولوية لكل تهديد في جدول التهديدات.

وتجرى الخطوتان التاليتان في المرحلة 3.

## الخطوة 1: تقييم المخاطر

تقيم المخاطر التي تنشأ عن التهديدات على أي نظام لتكنولوجيا المعلومات عادة باشتقاقها من قيمة الأصول وتكلفة الهجمات واللتين تعتمدان على كيفية تنفيذ التهديد. ويعد هذا النهج فعالاً عندما تكون هناك أمثلة عديدة من الهجمات وإمكانية التوصل إلى توافق بشأن تكلفة طريقة الهجمات، بما في ذلك عوامل من شاكلة وقت التنفيذ اللازم لتنفيذ الهجمة وقدرات الشخص الذي يطلقها. وفي حالة الأنظمة المدمجة في المركبات، فعلى الرغم من أن عدد أمثلة الهجمات قد تم تحديده على مستوى البحث، فإنه لا توجد مجموعة واسعة من تغايرات طريقة الهجمة الموجودة بالنسبة لأنظمة تكنولوجيا المعلومات. ونتيجة لذلك، يصعب تقدير تكلفة طرائق الهجمات.

#### 1.3.1.I نظام تحديد درجات المخاطر القائم على نظام تحديد درجات مواطن الضعف الشائعة (CRSS)

النظام CRSS عبارة عن طريقة لتقييم مخاطر التهديدات تقوم على نظام تحديد درجات مواطن الضعف الشائعة (CVSS)، أي نظام تحديد درجات المخاطر (RSS) للتوصية [ITU-T X.1521]، والذي يستخدم لتحديد درجات لمدى خطورة مواطن الضعف الخاصة بأنظمة تكنولوجيا المعلومات [المعيار b-JASO TP15002]. ويتألف النظام CVSS من ثلاث مجموعات للمقاييس: الأساسية والزمنية والبيئية، حيث تتكون كل منها من مجموعة من المقاييس. ويرد أدناه شرح لمجموعات المقاييس هذه:

- الأساسية: تمثل الخصائص المتأصلة والأساسية لمواطن الضعف الثابتة مع الزمن ومع بيئات المستعملين.
- الزمنية: تمثل خصائص مواطن الضعف التي تتغير مع الزمن ولكنها لا تتغير بين بيئات المستعملين.
- البيئية: تمثل خصائص مواطن الضعف التي ترتبط وتختص حصراً ببيئة معينة من بيئات المستعملين.

ويقيم النظام CRSS درجات المخاطر بواسطة *مجموعة المقاييس الأساسية* في نظام تحديد الدرجات CVSS. وتتناول هذه المجموعة من المقاييس خصائص مواطن الضعف الثابتة مع الزمن وعبر بيئات المستعملين المختلفة. وتقوم مقاييس متجه النفاذ وتعقد النفاذ والاستيقان بتناول الكيفية التي يتم بها النفاذ إلى مواطن الضعف وما إذا كانت هناك شروط إضافية مطلوبة من أجل استغلاله.

وتخصص طريقة النظام CRSS قيمة لكل أصل من الأصول من منظور السرية والسلامة والتيسر ثم تقوم بحساب درجات المخاطر من درجة سهولة إطلاق الهجمات ومن مستوى الأثر.

وتشتق درجة سهولة إطلاق الهجمات من مقياس يعكس إلى أي مدى تحتاج عوامل التهديدات أن تكون قريبة من الأصول ومن وجود عوائق تقوم بتذليلها للنفاذ إلى هذه الأصول. ويعرض في الجدول 4.I مثال على التصنيف فيما يتعلق بدرجة سهولة إطلاق الهجمات.

ويقيس مستوى الأثر كيفية تأثير مواطن الضعف، في حالة استغلالها بشكل مباشر على الأصول، حيث تحدد الآثار بشكل مستقل كدرجة لفقدان السرية والسلامة والتيسر. فعلى سبيل المثال، يمكن لموطن من مواطن الضعف أن يتسبب في فقدان جزئي للسلامة والتيسر ولكنه لا يؤدي إلى أي فقدان للسرية. ويعرض في الجدول 5.I مثال على التصنيف فيما يتعلق بمستوى الأثر.

**الجدول 4.I – مثال على التصنيف فيما يتعلق بدرجة سهولة إطلاق الهجمات**
**(الجدول 2.D من المعيار [b-JASO TP15002])**

| المعلمة | مبدأ البحث | التصنيف | أمثلة |
|---|---|---|---|
| متجه النفاذ (AV): تصنيف منشأ الهجمة | التصنيف فيما يتعلق بالمنشأ (مكان) الهجمة المؤدية إلى التهديد. | محلية (L) | الذاكرة USB |
| | | شبكة مجاورة (A) | جهاز توصيل Wi-Fi |
| | | شبكة (N) | خط هاتف محمول |
| تعقد النفاذ (AC): درجة تعقيد شروط الهجمة | التصنيف فيما يتعلق بعدد المهارات والمعارف المطلوبة للهجمة | عالية (H) | مهارات ومعارف الهجمة مطلوبة |
| | | متوسطة (M) | معارف الهجمة مطلوبة |
| | | منخفضة (L) | لا توجد حاجة إلى مهارات ومعارف الهجمة (أو قدر يسير) |
| الاستيقان (Au): عدد عمليات الاستيقان الضرورية قبل الهجمة | التصنيف فيما يتعلق بعدد عمليات الاستيقان بين الأصل وعامل التهديد | متعددة (M) | متعددة |
| | | فريدة (S) | فريدة |
| | | لا توجد (N) | لا توجد ضرورة |

**الجدول 5.I – مثال للتصنيف فيما يتعلق بمستوى الأثر**
**(الجدول 3.D من المعيار [b-JASO TP15002])**

| الأصل | التصنيف | C: الأثر على السرية | | | I: الأثر على السلامة | | | A: الأثر على التيسر | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | لا يوجد | جزئي | كامل | لا يوجد | جزئي | كامل | لا يوجد | جزئي | كامل |
| وظيفة الاتصالات المتنقلة | خدمة التحديث | Y | | | | | Y | | | Y |
| معلومات استيقان الاتصالات المتنقلة | | | | Y | | | Y | Y | | |
| وظيفة الحصول على البرمجيات | | Y | | | | | Y | | | Y |
| البرمجيات | | | | Y | | | Y | Y | | |
| وظيفة تحديث البرمجيات عن بُعد | | Y | | | | | Y | | | Y |
| البرمجيات | | | | Y | | | Y | Y | | |
| وظيفة استقبال النظام GPS | معالجة المعلومات | Y | | | | Y | | | Y | |
| وظيفة توصيل Wi-Fi | | Y | | | | Y | | | Y | |
| معلومات استيقان التوصيل Wi-Fi | | | Y | | | Y | | Y | | |
| وظيفة التوصيل USB | | Y | | | | Y | | | Y | |
| وظيفة الاتصالات CAN | التحكم في المركبة | Y | | | | | Y | | | Y |
| وظيفة بوابة الشبكة CAN | | Y | | | | | Y | | | Y |
| جدول التسيير | | | | Y | | | Y | Y | | |
| وظيفة توصيل التشخيصات OBD | | Y | | | | | Y | | | Y |

ويمكن حساب درجة المخاطر لكل تهديد موصوف بالنسق 5W (where، who، when، why، what) (المكان، الجهة الفاعلة، التوقيت، الدواعي، الماهية).

ويقدم الجدول 6.I مثالاً لعملية تقييم درجة المخاطر.

**الجدول 6.I – مثال على تقييم درجات المخاطر**
**(الجدول 4.D من المعيار [b-JASO TP15002])**

| # | التهديدات | AV | AC | Au | درجة سهولة الهجمة | C | I | A | مستوى الأثر | قيمة المخاطر |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | T.control_fcn_Mobile_3rd_ opearation_on_purpose of interfere-function | شبكة | متوسط | فريد | | غير ضرورية | كبيرة | كبيرة | | |
| | | 1 | 0,61 | 0,56 | 6,83 | 0 | 0,66 | 0,66 | 9,20 | 7,95 |
| 2 | T.vehicle_status_WiFi_dealer_main_purpose_forge | شبكة مجاورة | فريد (فريدة) | فريد | | صغيرة | صغيرة | لا توجد | | |
| | | 0,646 | 0,71 | 0,56 | 5,14 | 0,275 | 0,275 | 0 | 4,94 | 4,14 |
| 3 | T. info_transfer_USB_3rd_operation_pursuse_misop | محلي | منخفض | لا يوجد | | لا توجد | صغيرة | لا توجد | | |
| | | 0,395 | 0,71 | 0,704 | 3,95 | 0 | 0,275 | 0 | 2,86 | 2,11 |

وحتى في الحالات التي على غرار الأنظمة المدمجة في المركبات والتي لا توجد فيها دراية متراكمة بشأن التهديدات الأمنية، يمكن لطريقة النظام CRSS أن تحسب قيمة المخاطر تحليلياً من تعاريف التهديدات ومن نظام التقييم. ويمكن أيضاً إضافة اعتبار لعوامل مثل المخاطر على الأرواح ضمن تقييم المخاطر من خلال التعامل مع الوظائف على أنها أصول وذلك بغرض التقييم وزيادة القيمة المقدرة للأصول في حالة الوظائف التي ينطوي فيها فقدان السلامة أو التيسر على تبعات خطيرة.

### الخطوة 2: تحديد مسببات التهديدات

لكل تهديد له درجة مخاطر تزيد عن قيمة معينة، تحلل المسببات منطقياً بواسطة شجرة الأعطال (FT).

#### 2.I التحقق من البيانات باستخدام خوارزميات الشفرة MAC

لخوارزميات الشفرة MAC أدوار هامة في التجفير والأمن من خلال تحقيق السلامة للرسائل (الاستيقان). وبالنسبة للشفرات MAC، توصلت المنظمة الدولية للتوحيد القياس (ISO)/اللجنة الكهرتقنية الدولية (IEC) إلى نواتج هامة مثل المعيار [b-ISO/IEC 9797-1] (آليات استعمال شفرة المجموعات) والمعيار [b-ISO/IEC 9797-2] (آليات استعمال دالة اختزال مخصصة) والمعيار [b-ISO/IEC 9797-3] (آليات استعمال دالة اختزال عالمية).

وبالنظر إلى موارد التنفيذ المحدودة في أي مركبة، فإن من المناسب استعمال معايير تجفير بسيطة. ومن هذا المنظور، هناك نوعان من الشفرة MAC. والنوع الأول عبارة عن شفرة MAC قائمة على شفرة المجموعات تستخدم المعايرين المذكورين [b-ISO/IEC 9797-1] و[b-ISO/IEC 29192-2] (شفرة مجموعات بسيطة). والنوع الثاني عبارة عن شفرة MAC قائمة على دالة الاختزال تستخدم المعيارين المذكورين [b-ISO/IEC 9797-2] و[b-ISO/IEC 29192-5] (دالة اختزال بسيطة).

ومن أجل اختيار الخوارزميات المرشحة المحتملة من أجل أمن المركبات، قد يكون على الخوارزميات MAC أن توفر مزايا أمنية أو مزايا تتعلق بالأداء واضحة بالمقارنة مع خوارزميات MAC القياسية القائمة. ويمكن للهدف الرئيسي للشفرة MAC أن يفضي إلى عمليات تنفيذ مدمجة وسريعة للبرمجيات على وسائل التحكم الصغرية مع توفير الأمن الكافي الذي تتطلبه التطبيقات المستهدفة. ويمكن أن يكون مرغوباً بوجه خاص توفير خوارزمية MAC ذات كفاءة عالية جداً.

# التذييل II

# التهديدات ومتطلبات الأمن وضوابط الأمن

(لا يشكل هذا التذييل جزءاً من التوصية)

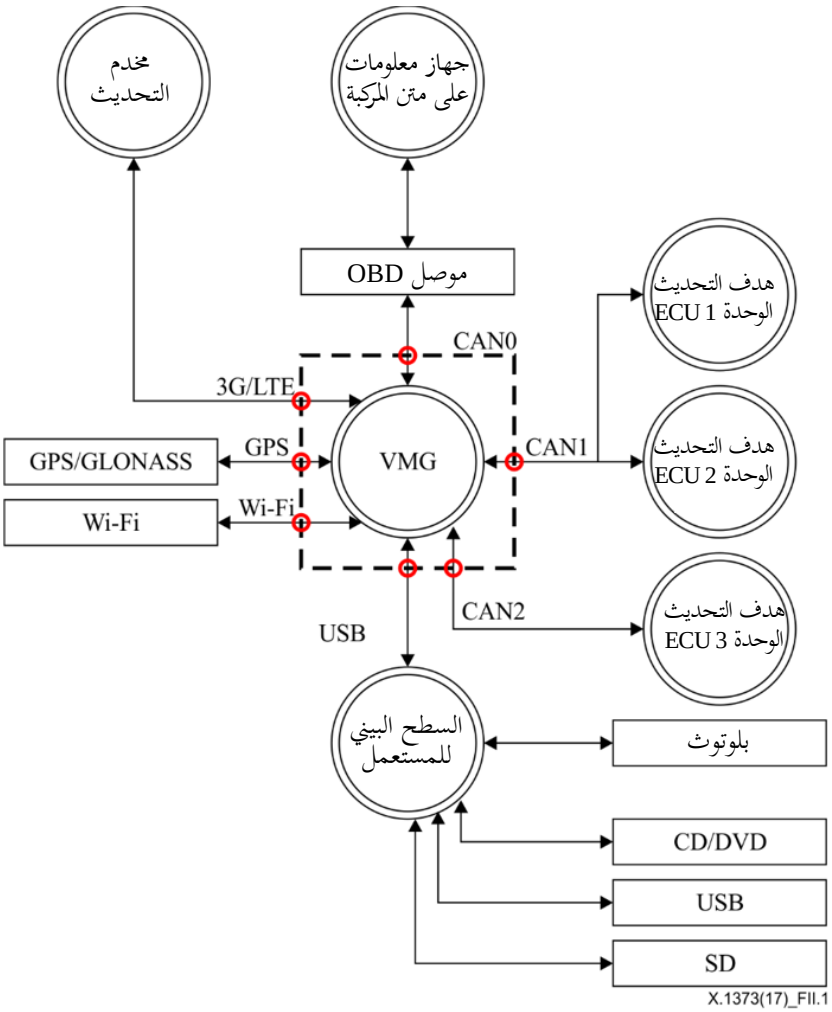
هناك أمثلة للهجمات/التهديدات الأمنية المختلفة المعروفة بالنسبة لنظام تكنولوجيا المعلومات حتى هذه اللحظة وتتراكم الدراية الفنية لتقييم أي مخاطر من خلال تصميم أنظمة تكنولوجيا المعلومات. وترد مفاهيم الأمن الأساسية الضرورية لتقييم منتجات تكنولوجيا المعلومات في المعيار [ISO/IEC 15408-1]. وفي سياق التقييم، يستخدم المعيار [ISO/IEC 15408-1] المصطلح "هدف التقييم" (TOE). وهناك أصول تتمثل في الكيانات التي يفترض أن يضيف إليها مالك الهدف TOE قيمة. ويرمي المعيار [ISO/IEC 15408-1] إلى تحديد أهداف أمنية لأي هدف TOE تمثل بياناً بالعزم على مكافحة تهديدات محددة و/أو تنفيذ سياسات أمنية محددة للمنظمة. وتفضي التهديدات إلى مخاطر بالنسبة للأصول، طبقاً لأرجحية تحقق التهديد وآثاره على الأصول عندما يقع. ومع ذلك لا يوصف المعيار [ISO/IEC 15408-1] كيفية إجراء عمليات تحديد التهديدات وتحليل المخاطر. ومن جهة أخرى، هناك عدد من الطرائق المعروفة لتحديد التهديدات وتحليل المخاطر. وفي هذه الفقرة، وبعد تعريف هدف التقييم (TOE) للبوابة VMG الذي يدرك بالنسبة لمكون رئيسي من مكونات التحديث المؤمن للبرمجيات، يتم القيام بتحديد التهديدات الرئيسية وينظر في المتطلبات الأمنية المتعلقة بالتهديدات الرئيسية. وفي النهاية، تُوفر ضوابط أمنية رفيعة المستوى من أجل تحقيق المتطلبات الأمنية.

## 1.II تعريف هدف التقييم

تعرف هذه الفقرة هدف التقييم (TOE) للبوابة VMG الذي يدرك بالنسبة لمكون رئيسي وأساسي من مكونات التحديث المؤمن للبرمجيات في هذه التوصية.

ويوجد كسطح بيني مع الخارج، موصل OBD ووحدة اتصالات متنقلة وجهاز استقبال لإشارة النظام العالمي لتحديد الموقع (GPS)/النظام العالمي للملاحة الساتلية (GLONASS) والتكنولوجيا Wi-Fi وتوصيل بلوتوث من أجل الراديو/التلفزيون وتوصيل CAN0/1 وسطح بيني للمستعمل مع قرص مدمج (CD)/قرص رقمي متعدد الاستعمالات (DVD) وموصل الناقل التسلسلي العالمي (USB) وموصل رقمي مؤمن (SD). وعلى الرغم من استخدام موصل الشبكة CAN كأحد وسائل النقل داخل المركبة في هذه الفقرة، فإنه يمكن تطبيق تحليلات مماثلة على الأنواع الأخرى لوسائل النقل داخل المركبة، مثل نقل الأنظمة المتمحورة حول الوسائط (MOST) والشبكة المحلية للتوصيل البيني (LIN) والبروتوكول FlexRay وغيرها.

وفي الشكل 1.II، يعرف هدف التقييم (TOE) بالمنطقة المحاطة بالخط المتقطع وهو يحقق تحكم مؤمن في الاتصالات كسطح بيني للتوصيل بخارج المركبة.




**الشكل 1.II – نموذج لهدف التقييم (TOE)**

ويعرض في الجدول 1.II استعراض شامل لوظائف الوحدات في الهدف TOE. ويعرض هذا الجدول أيضاً العلاقة بين الوظيفة المشروحة في الهدف TOE والسمات الأمنية الرئيسية للسرية (C) و/أو السلامة (I) و/أو التيسر (A) من أجل توفير المتطلبات الأمنية استناداً إلى الهدف TOE الوارد في الفقرة 3.II.

**الجدول 1.II – استعراض شامل لوظائف وحدات الهدف TOE**

| # | الوحدة | الوظيفة | | الأصل | C | I | A |
|---|---|---|---|---|---|---|---|
| 1 | بوابة الاتصالات المتنقلة للمركبة | وظيفة الاتصالات المتنقلة | تتواصل مع المخدم عبر توصيلة للاتصالات المتنقلة. | وظيفة الاتصالات المتنقلة | | Y | Y |
| | | | تستخدم معلومات الاستيقان للاستيقان من المخدم. | معلومات الاستيقان | Y | Y | |
| | | وظيفة الحصول على البرمجيات | تحصل على البرمجيات عن بُعد عن طريق توصيل متنقل أو موصل OBD. | وظيفة الحصول على البرمجيات | | Y | Y |
| | | | | معلومات البرمجيات | Y | Y | |
| | | وظيفة تحديث البرمجيات عن بُعد | تحدث البرمجيات عن بُعد عن طريق توصيل متنقل أو موصل OBD. وإذا تم تحديث البرمجيات عن بُعد، تستخدم المعلومات الأمنية للتحديث من أجل استيقان المخدم. | وظيفة تحديث البرمجيات عن بُعد | | Y | Y |
| | | | | معلومات أمنية للتحديث | Y | Y | |
| | | | | معلومات البرمجيات | Y | Y | |
| | | وظيفة استقبال إشارة النظام GPS | تستقبل البيانات من ساتل النظام GPS. | وظيفة استقبال إشارة النظام GPS | | Y | Y |
| | | وظيفة التوصيل Wi-Fi | تنشئ توصيلة للأجهزة بالإنترنت عبر توصيل Wi-Fi. تستعمل معلومات الاستيقان عبر توصيل Wi-Fi. | وظيفة التوصيل Wi-Fi | | Y | Y |
| | | | | معلومات الاستيقان | Y | Y | |
| | | وظيفة التوصيل USB | تتواصل مع السطح البيني للمستعمل عبر كبل USB. | وظيفة التوصيل USB | | Y | Y |
| | | وظيفة الاتصالات CAN | ترسل/تستقبل البيانات CAN إلى/من الوحدة ECU | وظيفة الاتصالات CAN | | Y | Y |
| | | وظيفة البوابة CAN | تسير الاتصالات CAN بالعودة إلى جدول التسيير. جدول التسيير. | وظيفة البوابة CAN | | Y | Y |
| | | | | جدول التسيير | Y | Y | |
| | | وظيفة التوصيل OBD | ترسل البيانات في الشبكة CAN عبر موصل OBD. | وظيفة التوصيل OBD | | Y | Y |

## 2.II تحديد التهديدات الرئيسية

استناداً إلى تعريف الهدف TOE من أجل تحديث البرمجيات في الفقرة 1.II، تحدد هذه الفقرة التهديدات الرئيسية الموجودة في الهدف TOE طبقاً لإطار المعيار [ISO/IEC 15408-1].

وفيما يتعلق بطريقة تحديد التهديدات الرئيسية استناداً إلى نموذج الهدف TOE هذا، تستخدم هذه التوصية طريقة تحليل المخاطر الواردة في التذييل I (إعلامي).

**الجدول 2.II – –التهديدات الرئيسة استناداً إلى نموذج الهدف TOE**

| # | الوسم | من | متى (المرحلة) | لماذا | أين/ما |
|---|---|---|---|---|---|
| 1 | T.DoS-Functions-From-OBD-Device | طرف ثالث<br>موظف شركة الصيانة | التشغيل العادي<br>الصيانة | عن عمد | بالنسبة لوظائف أصول البوابة VMG، ينتحل صفة جهاز توصيل موصل OBD ويرسل كم ضخم من البيانات ويتداخل مع هذه الوظيفة. |
| 2 | T.Malfunction-Functions-From-OBD-Device | طرف ثالث<br>موظف شركة الصيانة | التشغيل/الاستعمال/ الصيانة في الظروف الاعتيادية<br>الصيانة | عن عمد | بالنسبة لوظائف أصول البوابة VMG، ينتحل صفة جهاز توصيل موصل OBD ويرسل بيانات غير مرخصة ويتسبب في عطل لهذه الوظيفة. |
| 3 | T.MissDoS-Functions-From-OBD-Device | موظف تاجر المركبات<br>موظف شركة الصيانة | الصيانة | عرضياً | بالنسبة لوظائف أصول البوابة VMG، يرسل كم ضخم من البيانات أو بيانات غير مرخصة من جهاز توصيل توصيلة OBD بالخطأ ويتسبب في عطل لهذه الوظيفة. |
| 4 | T.DoS-Functions-From-ECU | طرف ثالث<br>موظف شركة الصيانة | التشغيل/الاستعمال/ الصيانة في الظروف الاعتيادية<br>الصيانة | عن عمد | بالنسبة لوظائف أصول البوابة VMG، يستعمل الهندسة العكسية لنفس المنتج مثل البرمجيات الثابتة للوحدات ECU الموصولة بالسطح CAN0-2 ويعدلها إلى برمجيات ثابتة غير مرخصة من هذا النوع؛ وبهذه الطريقة، يرسل كم ضخم من البيانات من الوحدة ECU الموصولة بالسطح CAN1-5 ويتداخل مع هذه الوظيفة. |
| 5 | T.Malfunction-Functions-From-ECU | طرف ثالث<br>موظف شركة الصيانة | التشغيل/الاستعمال/ الصيانة في الظروف الاعتيادية<br>الصيانة | عن عمد | بالنسبة لوظائف أصول البوابة VMG، يستعمل الهندسة العكسية لنفس المنتج مثل البرمجيات الثابتة للوحدات ECU الموصولة بالسطح CAN1-5 ويعدلها إلى برمجيات ثابتة غير مرخصة من هذا النوع؛ وبهذه الطريقة، يرسل كم ضخم من البيانات من الوحدة ECU الموصولة بالسطح CAN1-5 ويتداخل مع هذه الوظيفة. |
| 6 | T.DoS-Functions-From-Mobile-Device | طرف ثالث | التشغيل/الاستعمال/ الصيانة في الظروف الاعتيادية | عن عمد | بالنسبة لوظائف أصول البوابة VMG، ينتحل صفة مخدم ويرسل كم ضخم من البيانات إلى البوابة VMG من جهاز توصيل متنقل ويتداخل مع هذه الوظيفة. |
| 7 | T.Spoofing-Server_ToGet-Data | طرف ثالث | التشغيل/الاستعمال/ الصيانة في الظروف الاعتيادية | عن عمد | بالنسبة لمعلومات أصول البوابة VMG، يرسل أمراً للحصول على معلومات أصول البوابة VMG من جهاز توصيل متنقل عن طريق اعتراض قناة الاتصال أو انتحال صفة جهاز توصيل متنقل. وبهذه الطريقة، يستقبل معلومات أصول البوابة VMG. |
| 8 | T.MissDoS-Functions-From-mobile-Device | مدير المخدم | التشغيل/الاستعمال/ الصيانة في الظروف الاعتيادية | عرضياً | بالنسبة لوظائف أصول البوابة VMG، يرسل المخدم عن طريق سوء التشغيل كم ضخم من البيانات أو البيانات غير المرخصة من جهاز توصيل متنقل ويتداخل مع هذه الوظيفة ويتسبب في عطل بها. |

**الجدول 2.II – –التهديدات الرئيسة استناداً إلى نموذج الهدف TOE *(تابع)***

| # | الوسم | من | متى (المرحلة) | لماذا | أين/ما |
|---|---|---|---|---|---|
| 9 | T.Leaking-Mobile-Information-From-Mobile-Device | المالك/المستعمل<br>مدير المخدم/<br>موظف تاجر المركبات<br>مدير المخدم | التشغيل/الاستعمال العادي/توصيل المركبة<br>التشغيل/الاستعمال/<br>الصيانة في الظروف الاعتيادية | عرضياً | بالنسبة لمعلومات أصول البوابة VMG، يرسل عن طريق سوء التشغيل من جهاز توصيل متنقل أمراً إلى البوابة VMG للحصول على أصول حماية البوابة VMG (معلومات) ويتحصل على هذه الأصول (المعلومات) ويسربها. |
| 10 | T.MissUpdate-Mobile-Information-From-Mobile-Device | المالك/المستعمل<br>مدير المخدم/<br>موظف تاجر المركبات<br>مدير المخدم | التشغيل/<br>الاستعمال العادي<br>توصيل المركبة<br>التشغيل/الاستعمال/<br>الصيانة في الظروف الاعتيادية | عرضياً | بالنسبة لمعلومات أصول البوابة VMG، يرسل عن طريق سوء التشغيل أو عن طريق الخطأ من جهاز توصيل متنقل أمراً إلى البوابة VMG لتحديث أصول حماية البوابة (معلومات) ويعدل هذه الأصول (المعلومات). |
| 11 | T.Malfunction-Functions-From-mobile-Device | طرف ثالث | التشغيل/الاستعمال/<br>الصيانة في الظروف الاعتيادية | عن عمد | بالنسبة لوظائف أصول البوابة VMG، ينتحل صفة مخدم، من جهاز توصيل متنقل، ويرسل بيانات غير مرخصة ويتسبب في عطل لهذه الوظيفة. |
| 12 | T.Spoofing-Server_ToRewrite-Data | طرف ثالث | التشغيل/<br>الاستعمال العادي | عن عمد | بالنسبة لأصول حماية (معلومات) البوابة (VMG)، ينتحل صفة جهاز توصيل متنقل ويقوم من جهاز كهذا بإرسال أمر بإعادة كتابة أصول (معلومات) حماية البوابة VMG (معلومات). |
| 13 | T.DoS-Functions-From-Wi-Fi-Device | طرف ثالث | التشغيل/الاستعمال/<br>الصيانة في الظروف الاعتيادية | عن عمد | بالنسبة لوظيفة التوصيل Wi-Fi، ينتحل صفة جهاز توصيل Wi-Fi ويرسل كم ضخم من البيانات ويتداخل مع هذه الوظيفة. |
| 14 | T.Malfunction-Functions-From-Wi-Fi-Device | طرف ثالث | التشغيل/الاستعمال/<br>الصيانة في الظروف الاعتيادية | عن عمد | بالنسبة لوظيفة التوصيل Wi-Fi، ينتحل صفة جهاز توصيل Wi-Fi ويرسل بيانات غير مرخصة ويتسبب في عطل لهذه الوظيفة. |
| 15 | T.MissDoS-Functions-From-Wi-Fi-Device | المالك/المستعمل | التشغيل/<br>الاستعمال العادي | عرضياً | بالنسبة لوظيفة التوصيل Wi-Fi، يقوم من خلال سوء تشغيل جهاز التوصيل Wi-Fi أو إصابة جهاز التوصيل Wi-Fi ببرمجيات ضارة، بإرسال كم ضخم من البيانات أو بيانات غير مرخصة ويتداخل مع هذه الوظيفة ويتسبب في عطل لها. |
| 16 | T.Spoofing-Wi-Fi-Device_ToGet-Wi-Fi-Information | طرف ثالث | التشغيل/الاستعمال/<br>الصيانة في الظروف الاعتيادية | عن عمد | بالنسبة لوظيفة التوصيل Wi-Fi، ينتحل صفة جهاز توصيل Wi-Fi ويرسل أمراً للحصول على معلومات استيقان التوصيل Wi-Fi ويستغل معلومات الاستيقان هذه. |
| 17 | T.Spoofing-Wi-Fi-Device_ToRewrite-Wi-Fi-Information | طرف ثالث | التشغيل/الاستعمال/<br>الصيانة في الظروف الاعتيادية | عن عمد | بالنسبة لوظيفة التوصيل Wi-Fi، ينتحل صفة جهاز توصيل Wi-Fi ويرسل أمراً بإعادة كتابة معلومات استيقان التوصيل Wi-Fi ويعيد كتابة معلومات الاستيقان هذه. |

**الجدول 2.II – –التهديدات الرئيسة استناداً إلى نموذج الهدف TOE** *(تتمة)*

| # | الوسم | من | متى (المرحلة) | لماذا | أين/ما |
|---|---|---|---|---|---|
| 18 | T.Leaking-Wi-Fi-Information-From-Wi-Fi-Device | موظف<br>تاجر المركبات<br>المالك/المستعمل | توصيل المركبة<br>التشغيل/<br>الاستعمال العادي | عرضياً | بالنسبة لمعلومات استيقان التوصيل Wi-Fi، يرسل أمراً للحصول على معلومات استيقان التوصيل Wi-Fi ويحصل على معلومات الاستيقان هذه ويسربها. |
| 19 | T.MissUpdate-Wi-Fi-Information-From-Wi-Fi-Device | موظف<br>تاجر المركبات<br>المالك/المستعمل | توصيل المركبة<br>التشغيل/<br>الاستعمال العادي | عرضياً | بالنسبة لمعلومات استيقان التوصيل Wi-Fi، يرسل أمراً بإعادة كتابة معلومات استيقان التوصيل Wi-Fi ويعيد كتابة معلومات الاستيقان هذه. |

## 3.II المتطلبات الأمنية في الهدف TOE

استناداً إلى التهديدات المحددة في الفقرة 2.II، تستخلص ثلاثة مكونات للمتطلبات الأمنية من نموذج الهدف TOE في الفقرات الفرعية التالية. ويشتق كل متطلب من المتطلبات الأمنية من التهديدات المحددة في الفقرة 2.II. وترفق بكل متطلب من المتطلبات الأمنية في الفقرة 3.II مجموعة من معرفات هوية التهديدات (#) والتي يمكن الرجوع إليها من الجدول 2.II.

### 1.3.II المتطلبات الأمنية للهدف TOE

#### 1.1.3.II SR.حماية السلامة/التيسر لوظائف البوابة VMG من خلال اتصالات CAN

يتعين ضمان سلامة وظائف البوابة VMG وتيسرها إزاء هجمات رفض الخدمة (DoS) وهجمات الإعطاب من الوحدات ECU من خلال اتصال CAN0-CAN2 (انظر التهديدين 4 و5).

**الوصف**

في الاتصالات CAN لا تسير إلا البيانات CAN المخصص لها معرفات الهوية CAN المحددة. وإذا ما استقبلت البوابة VMG كم ضخم من رزم الاتصالات و/أو أكدت نفاذ مخططات غير عادية من أجهزة توصيل CAN0-CAN2، لا يتعين عليها إجراء عمليات تشغيل غير عادية.

#### 2.1.3.II SR.حماية سرية بيانات البوابة VMG

يتعين حماية محتويات الاتصالات بين البوابة VMG والمخدم من منظور السرية بطريقة تحول دون قراءة أي طرف ثالث لهذه المحتويات (انظر التهديدات 7 و16 و17).

#### 3.1.3.II SR.حماية سلامة/تيسر وظائف البوابة VMG عبر الاتصالات المتنقلة

يتعين ضمان سلامة وظائف البوابة VMG وتيسرها إزاء هجمات رفض الخدمة وهجمات الإعطاب من الأجهزة المتنقلة عبر الاتصالات المتنقلة (انظر التهديدات 6 و7 و8 و9 و10 و11 و12).

**الوصف**

عند الاتصال مع جهاز توصيل متنقل، تحتاج البوابة VMG إلى التأكد مما إذا كان الطرف المتصل جهاز توصيل متنقل مخولاً. ويتعين حماية البوابة VMG من انتحال المخدم عند تلقي بيانات غير مرخصة/غير عادية عبر اتصالات متنقلة. وإذا استقبلت البوابة VMG كماً ضخماً من رزم الاتصالات من أجهزة توصيل متنقل و/أو تحققت من نفاذ مخططات غير عادية من جهاز توصيل متنقل، لا يتعين عليها أن تجري أي عمليات تشغيل غير عادية. وعلاوة على ذلك، يتعين أن تتحقق البوابة VMG من اتساق ووتيرة الإرسال بين الأوامر المرسلة من أجهزة التوصيل المتنقل.

#### 4.1.3.II SR.تحمل وظائف البوابة VMG للأعطال

يتعين على وظائف البوابة VMG الاستمرار في أداء عملياتها المحددة، ويمكن أن يكون هذا الأداء على مستوى منخفض في حالة وجود أي شيء غير عادي نتيجة للهجمات (انظر التهديدات 1 و2 و3 و4 و5 و6 و8 و11 و15).

#### 5.1.3.II SR.حماية سلامة/تيسر وظائف البوابة VMG عبر موصل OBD

يتعين ضمان سلامة وظائف البوابة VMG وتيسرها إزاء هجمات رفض الخدمة وهجمات الإعطاب من أجهزة توصيل OBD عبر موصل OBD (انظر التهديدات 1 و2 و3).

**الوصف**

فيما يتعلق بالتوصيل CAN عبر موصل OBD، لا يسمح بالنفاذ إلى الوحدات ECU إلا للأجهزة المحددة. ويتعين حماية البوابة VMG من انتحال أجهزة توصيل OBD عند تلقي بيانات غير مرخصة/غير عادية من موصل OBD. وإذا ما استقبلت البوابة VMG كماً ضخماً من الاتصالات أو الأوامر غير المرخصة من أجهزة توصيل OBD، لا يتعين عليها إجراء أي عمليات تشغيل غير عادية.

#### 6.1.3.II SR.حماية السرية/السلامة/التيسر للبوابة VMG عبر اتصالات Wi-Fi

يتعين حماية البوابة VMG من انتحال صفة أجهزة اتصالات Wi-Fi عند تلقي بيانات غير مرخصة/غير عادية عبر اتصالات Wi-Fi (انظر التهديدات 13 و14 و15 و16 و17 و18 و19).

**الوصف**

في الاتصالات باستخدام جهاز Wi-Fi يتعين أن تتحقق البوابة VMG مما إذا كان الجهاز مسجلاً من قبل. فإذا تلقت البوابة VMG كماً ضخماً من رزم الاتصالات من أجهزة Wi-Fi و/أو تحققت من نفاذ أنماط غير عادية من أي جهاز Wi-Fi، يجب ألا تقوم بإجراء أي عمليات غير عادية.

### 2.3.II المتطلبات الأمنية للبيئة التشغيلية للهدف TOE من منظور تكنولوجيا المعلومات

#### 1.2.3.II SRE.حماية الوحدات ECU

يتعين حماية الوحدة النمطية ECU إزاء تحليل برمجياتها الثابتة عن طريق عمل تمويه للوحدة. ويتعين حماية الوحدات ECU من الهجمات التي تستعمل بيانات أجهزة استشعار غير مرخصة. ويتعين حماية الوحدات ECU مادياً من الهجمات التي تتم من خلال الاستبدال غير المرخص لها (انظر التهديدين 4 و5).

#### 2.2.3.II SRE.حماية الاتصالات CAN

يتعين حماية الاتصالات CAN من تحليل بروتوكول الاتصالات CAN بواسطة عمليات التخليط (العمليات البسيطة مثل تخليط البتات وما شابهها) على بيانات الحمولة النافعة CAN. ويتعين حماية الشبكة CAN مادياً من الهجمات التي تتم من خلال قيام طرف ثالث ضار بقص كبلات الشبكة CAN (انظر التهديدين 4 و5).

#### 3.2.3.II SRE.حماية شبكة الاتصالات المتنقلة

يتعين حماية شبكة الاتصالات المتنقلة التي تستخدمها البوابة VMG للاتصالات بالمخدم من الهجمات الصادرة عن أجهزة غير مرخصة. ويتعين حماية معلومات تشكيلة الشبكة من منظور السرية. ويتعين مراقبة الشبكة لاكتشاف الهجمات (انظر التهديدات 6 و7 و11 و12).

#### 4.2.3.II SRE.حماية الاتصالات اللاسلكية

يتعين حماية الاتصالات اللاسلكية من تحليل البروتوكول الخاص بها عن طريق تخزين أدنى قدر من البيانات فقط في الحمولة النافعة لرزمة الاتصالات أو عن طريق تخليط بيانات الحمولة النافعة بواسطة عمليات بسيطة مثل تخليط البتات وما شابهها (انظر التهديدات 7 و12 و16 و17).

### 3.3.II المتطلبات الأمنية لبيئة التشغيل من منظور التشغيل/الإدارة خلاف تكنولوجيا المعلومات

#### 1.3.3.II SREN.الاحتراس

من المعلوم أن أي هجمة على النظام المدمج بالمركبة تعد عملاً إجرامياً. وعلاوة على ذلك، يتعين تقييد بيع المنتج للأغراض التي تساعد على الجريمة (انظر التهديدات 1 و2 و4 و5 و6 و7 و11 و12 و13 و14 و16 و17).

#### 2.3.3.II SREN.مقدمو الخدمات الشبكية

يجب أن يحول مدير المخدم دون تسرب البيانات المخزنة أو التلاعب بها من خلال إدارة غير ملائمة للمخدم (انظر التهديدين 7 و8).

#### 3.3.3.II SREN.حماية الأداة OBD

يتعين حماية الأدوات OBD الموصولة بأي مركبة من الاستعمال غير المرخص عن طريق الإدارة المؤمنة. وإلى جانب ذلك، يتعين التحقق من طرائق تشغيل هذه الأدوات قبل التشغيل (انظر التهديد 3).

#### 4.3.3.II SREN.المستعمل

عندما يستخدم المستعملون المركبة، يتعين إحاطتهم علماً بالاحتياطات المطلوبة.

**الوصف**

يتعين إحكام غلق المركبة لمنع غزوات الأطراف الثالثة عندما يكون المستعمل بعيداً عنها. ويجب أن توقف المركبة في مكان لا يسمح لأي طرف ثالث من الوصول إليها بسهولة، إذا لم تكن قيد الاستخدام. ويجب أن يتأكد المستعمل من عدم وجود أي جهاز غير محدد قبل استعمال المركبة. ويجب أن يتوخى المستعمل الحذر عند توصيل منتجات تجارية بالموصل OBD ليكون واجهة للصيانة (انظر التهديدات 1 و2 و4 و5 و13 و14 و16 و17).

#### 5.3.3.II SREN.المسح للكشف عن الفيروسات

يتعين مسح الأجهزة الموصولة بالنظام عبر توصيلات متنقلة/Wi-Fi بانتظام (انظر التهديدات 9 و10 و15 و18 و19).

#### 6.3.3.II SREN.حماية الأجهزة اللاسلكية

يتعين على الشخص المعني التأكد من كيفية تشغيل الجهاز الموصول عبر توصيلات متنقلة/Wi-Fi قبل التشغيل. وإضافة إلى ذلك، يتعين عليه توخي الحذر لمنع تسرب كلمة المرور الخاصة بالأجهزة الموصولة بتوصيلات Wi-Fi والأوامر (انظر التهديدات 9 و10 و12 و13 و14 و16 و17 و18 و19).

#### 7.3.3.II SREN.شاشة العرض اللاسلكية

يتعين على المستعملين الذين يستخدمون جهاز توصيل Wi-Fi/متنقل التأكد من إرسال أو عدم إرسال أوامر "الحصول على/كتابة" معلومات أصول البوابة VMG بتحديد اختيار على شاشة عرض الجهاز (انظر التهديدات 9 و10 و18 و19).

### 4.II الضوابط الأمنية

استناداً إلى المتطلبات الأمنية الواردة في الفقرة 3.II، تقدم هذه الفقرة الضوابط الأمنية التي تفي بهذه المتطلبات الأمنية، خاصة من منظور تكنولوجيا المعلومات.

### 1.4.II SC.التحميل الموثوق

كإجراء مضاد لتحليل (مثل التلاعب في) الوحدة النمطية للبرنامج الأصلي في الوحدة ECU، يوصى بأن تنفذ الوحدة ECU آليات الفحص الذاتي لبرمجياتها باستعمال آلية حماية أمن التحميل الخاصة بوحدة أمن التجهيزات (HSM) في كل تتابع تحميل للوحدة ECU.

#### المتطلب الأمني المقابل

- SRE.حماية الوحدة ECU في الفقرة 1.2.3.II.

### 2.4.II SC.التحقق من الرسائل

تعد طريقة التحقق من الرسالة طريقة فعالة في الحفاظ على استيقان الكيانات وسلامة الرسائل ضد هجمات التلاعب والتنصت وإعادة التشغيل.

وهناك طريقتان تلائمان هذا الغرض: الأولى باستخدام التوقيع الرقمي (طريقة التوقيع الرقمي)، والثانية باستخدام شفرة استيقان الرسالة (MAC).

وفي نفس الوقت، ولأغراض عمليات التنفيذ العملية للوحدات ECU في المركبة، تختلف قدرات تجفير الأجهزة باختلاف المركبات. فعلى سبيل المثال، قد تكون هناك وحدات HSM لجميع الوحدات ECU في المركبات الفخمة، بينما قد لا تكون هناك وحدات HSM في المركبات الشعبية إلا لجزء من الوحدات ECU. وإضافة إلى ذلك، هناك فوارق في قدرات التجفير طبقاً لأنواع الوحدات HSM المستخدمة.

لذا، يتعين أن تراعي المعمارية الأمنية فوارق القدرات الأمنية بين المركبات. وتستخدم هذه التوصية تحديداً طريقة التوقيع الرقمي استناداً إلى التوصية [ITU-T X.509] للتحقق من رسائل المركبات مع خوارزمية تجفير غير متناظرة (مثل وحدة المنصة الموثوقة (TPM)) ومن جهة أخرى بالنسبة للمركبات التي لا تستخدم خوارزمية تجفير غير متناظرة (مثل الوحدة HSM والبطاقة الذكية)، تستخدم هذه التوصية الشفرة MAC للتحقق من الرسائل. وللاطلاع على تفاصيل بروتوكول الاتصالات، بما في ذلك التحقق من الرسائل، انظر الفقرة 7. وهذا الضابط الأمني من التدابير الضرورية في تحديث البرمجيات عن بُعد من أجل التحقق من الرسائل في هذه التوصية.

#### المتطلبات الأمنية المقابلة

- SR.حماية سرية بيانات البوابة VMG في الفقرة 2.1.3.II؛
- SR.حماية السرية/السلامة/التيسر للبوابة VMG عبر اتصالات Wi-Fi في الفقرة 6.1.3.II؛
- SRE.حماية شبكة الاتصالات المتنقلة في الفقرة 3.2.3.II؛
- SRE.حماية الاتصالات اللاسلكية في الفقرة 4.2.3.II.

### 3.4.II SC.استيقان كيان الاتصالات

لتفادي انتحال صفة كيانات الاتصالات (أي انتحال صفة وحدة ECU أو بوابة VMG أو مخدم تحديث)، يوصى بأن تستيقن هذه الكيانات عن بعضها البعض في بداية كل اتصال. وينبغي تنفيذ هذا الضابط الأمني في إطار طبقة النقل وينبغي تأمين إجراءات التحديث المؤمن للبرمجيات المحددة في هذه التوصية من خلال وظيفة الطبقة الأدنى. وكتدبير مضاد محدد لاستيقان كيانات الاتصالات، يعد استيقان العميل والمخدم على السواء باستخدام طبقة توصيل آمنة (SSL)/أمن طبقة النقل (TLS) فعالاً في إطار سلطة إصدار شهادات (CA) طرف ثالث.

#### المتطلبات الأمنية المقابلة

- SR.حماية السرية/السلامة/التيسر للبوابة VMG عبر اتصالات Wi-Fi في الفقرة 6.1.3.II؛
- SRE.حماية شبكة الاتصالات المتنقلة في الفقرة 3.2.3.II؛
- SRE.حماية الاتصالات اللاسلكية في الفقرة 4.2.3.II.

### 4.4.II SC.ترشيح الرسائل

كمثال لهجمات رفض الخدمة ضد البوابة VMG، تنتهك أي وحدة ECU من قبل مهاجم ويرسل بشكل كثيف رسائل مزيفة إلى البوابة VMG لاستهلاك قدراتها الحاسوبية بشكل غير سليم. وللحد من الأثر الأمني لهجمات رفض الخدمة هذه، تعد تقنية ترشيح الرسائل واحدة من الطرائق الفعالة في هذا الصدد. ويوصى بأن ترشح البوابة VMG الرسائل غير ذات الصلة طبقاً لمعرف هوية المرسل أو نوع الرسالة أو حجمها أو تواترها وما إلى ذلك أو توليفة منها جميعاً.

#### المتطلبات الأمنية المقابلة

- SR.حماية سلامة/تيسر وظائف البوابة VMG عبر اتصالات CAN في الفقرة 1.1.3.II؛
- SR.حماية سلامة/تيسر وظائف البوابة VMG عبر اتصالات متنقلة في الفقرة 3.1.3.II؛
- SR.حماية سلامة/تيسر وظائف البوابة VMG عبر وصلة OBD في الفقرة 5.1.3.II.

### 5.4.II SC. تحمل وظائف البوابة VMG للأعطال

يوصى موردو البوابات VMG بشدة بتنفيذ برمجيات VMG ذات تصميم آمن إزاء الأعطال بحيث يمكن للبوابة VMG مواصلة عملياتها المحددة في ظل وجود شيء ما غير عادي من جراء بعض الهجمات. وتقوم البوابة VMG تحديداً بمراقبة حالة التشغيل وعند اكتشاف أي شيء غير عادي، يتخذ إجراء (إعادة التحميل وما شابه) من أجل استعادة الحالة العادية. وإذا تعذرت استعادة الحالة العادية، تخطر البوابة VMG السائق بالأمر وتعلق التشغيل بأمان.

#### المتطلب الأمني المقابل

- SR.تحمل وظائف البوابة VMG للأعطال في الفقرة 4.1.3.II.

# بيبليوغرافيا


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

[b-ISO/IEC 9797-1] ISO/IEC 9797-1:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50375>

[b-ISO/IEC 9797-2] ISO/IEC 9797-2:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function*.
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51618>

[b-ISO/IEC 9797-3] ISO/IEC 9797-3:2011, *Information technology – Security techniques – Message Authentication Codes (MACs) – Part 3: Mechanisms using a universal hash-function.*
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51619>

[b-ISO/IEC 29192-2] ISO/IEC 29192-2:2012, *Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers*.
<http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56552>

[b-ISO/IEC 29192-5] ISO/IEC 29192-5:2016, *Information technology – Security techniques – Lightweight cryptography – Part 5: Hash-functions.*
<http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67173>

[b-JASO TP15002] JASO TP15002:2015, *Guideline for automotive information security analysis.*

[b-FIPS-202] Federal Information Processing Standards Publication-202 (2015), *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.* National Institute of Standards and Technology,
<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>

[b-ISO 14229] ISO 14229-1:2013, Road vehicles –Unified diagnostic services (UDS) – Part 1: Specification and requirements

[b-ISO 13400] Road vehicles – Diagnostic communication over Internet Protocol (DoIP) – Part 1: General information and use case definition

## 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، 2018