الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

Y.4102/Y.2074

(2015/01)

السلسلة Y: البنية التحتية العالمية للمعلومات، وجوانب بروتوكول الإنترنت، وشبكات الجيل التالي

شبكات الجيل التالي – الإطار العام والنماذج المعمارية الوظيفية

المتطلبات اللازمة لأجهزة إنترنت الأشياء (IoT) ولتشغيل تطبيقات إنترنت الأشياء أثناء وقوع كارثة

التوصية ITU-T Y.4102/Y.2074

الاتحاد الدولي للاتصالات

توصيات السلسلة Y الصادرة عن قطاع تقييس الاتصالات

البنية التحتية العالمية للمعلومات، وجوانب بروتوكول الإنترنت، وشبكات الجيل التالي

البنية التحتية العالمية للمعلومات	
اعتبارات عامة	Y.199–Y.100
الخدمات والتطبيقات، والبرمجيات الوسيطة	Y.299–Y.200
الجوانب الخاصة بالشبكات	Y.399–Y.300
السطوح البينية والبروتوكولات	Y.499–Y.400
الترقيم والعنونة والتسمية	Y.599–Y.500
التشغيل والإدارة والصيانة	Y.699–Y.600
الأمن	Y.799–Y.700
مستويات الأداء	Y.899–Y.800
جوانب متعلقة ببروتوكول الإنترنت	
اعتبارات عامة	Y.1099–Y.1000
الخدمات والتطبيقات	Y.1199–Y.1100
المعمارية والنفاذ وقدرات الشبكة وإدارة الموارد	Y.1299–Y.1200
النقل	Y.1399–Y.1300
التشغيل البيني	Y.1499–Y.1400
جودة الخدمة وأداء الشبكة	Y.1599–Y.1500
التشوير	Y.1699–Y.1600
التشغيل والإدارة والصيانة	Y.1799–Y.1700
الترسيم	Y.1899–Y.1800
تلفزيون بروتوكول الإنترنت عبر شبكات الجيل التالي	Y.1999–Y.1900
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	**Y.2099–Y.2000**
جودة الخدمة والأداء	Y.2199–Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249–Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات في شبكات الجيل التالي	Y.2299–Y.2250
تحسينات على شبكات الجيل التالي	Y.2399–Y.2300
إدارة الشبكة	Y.2499–Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599–Y.2500
الشبكات القائمة على الرزم	Y.2699–Y.2600
الأمن	Y.2799–Y.2700
التنقلية العامة	Y.2899–Y.2800
البيئة المفتوحة عالية الجودة	Y.2999–Y.2900
شبكات المستقبل	Y.3499–Y.3000
الحوسبة السحابية	Y.3999–Y.3500

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

التوصية ITU-T Y.4102/Y.2074

المتطلبات اللازمة لأجهزة إنترنت الأشياء (IoT) ولتشغيل تطبيقات إنترنت الأشياء أثناء وقوع كارثة

ملخص

تقدم التوصية ITU-T Y.2074 المتطلبات اللازمة لأجهزة وتطبيقات إنترنت الأشياء (IoT) التي تستعمل لتشغيل تطبيقات إنترنت الأشياء في سياق الكوارث إضافةً إلى المتطلبات العامة لإنترنت الأشياء الواردة في التوصية ITU T Y.2066. كما تقدم المتطلبات اللازمة لتشغيل التطبيقات في حالات الكوارث.

ومن الضروري تحديد هذه المتطلبات من أجل استعمال أجهزة وتطبيقات إنترنت الأشياء (IoT) في حالات الكوارث لعمليات الإخلاء والإنقاذ.

ويوضح التذييل I الطرق المتعلقة بضمان سلامة وموثوقية البيانات التي توفرها أجهزة IoT في حالات الكوارث.

وهذه التوصية مهمة لواضعي تطبيقات IoT ومقدمي خدمات IoT فضلاً عن مقدمي خدمات الطوارئ.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات	المعرف الوحيد*
1.0	ITU-T Y.4102/Y.2074	2015-01-13	13	11.1002/1000/12421

مصطلحات أساسية

كارثة، إنترنت الأشياء (IoT)، تطبيقات IoT، مقدمي خدمات IoT، متطلبات، أنظمة السلامة.

* للوصول إلى التوصية يرجى إدخال العنوان URL التالي: http://handle.itu.int/ في حقل العنوان في متصفح الويب الخاص بك ثم إدخال المعرف الوحيد للتوصية. على سبيل المثال: 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 رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد 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، 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 المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

© ITU 2016

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

1 مجال التطبيق 1
2 المراجع 1
3 التعاريف 1
1.3 مصطلحات معرفة في وثائق أخرى 1
2.3 المصطلحات المعرَّفة في هذه التوصية 2
4 الاختصارات والأسماء المختصرة 2
5 اصطلاحات 2
6 المتطلبات اللازمة لأجهزة إنترنت الأشياء (IoT) في سياق الكوارث 3
1.6 المتطلبات العامة بشأن الكوارث 3
2.6 المتطلبات اللازمة لأجهزة إنترنت الأشياء 3
7 المتطلبات اللازمة لتشغيل تطبيقات إنترنت الأشياء أثناء وقوع كارثة 3
1.7 تطبيقات إنترنت الأشياء بأسلوب التشغيل المخصص 4
2.7 تطبيقات إنترنت الأشياء التي تقدم مؤقتاً موارد لأنظمة السلامة الخارجية 4
3.7 تطبيقات إنترنت الأشياء ذات التحكُّم الخارجي في التشغيل أثناء وقوع كارثة 5
4.7 التبديل بين استراتيجيتي تشغيل أو أكثر خلال وقوع كارثة 6
التذييل I – الأساليب المتعلقة بضمان سلامة وموثوقية البيانات التي تنتجها أجهزة إنترنت الأشياء خلال وقوع كارثة 8
1.I نظرة عامة على مركز المراقبة والتحكم لأجهزة إنترنت الأشياء 8
2.I توزيع مسؤوليات مركز المراقبة والتحكم على المراكز المحلية 9
3.I سيناريوهات عمل مركز المراقبة والتحكم 9
1.3.I شبكة الاستشعار المستقلة ذاتياً 9
2.3.I المراقبة الذكية 10
4.I استخدام البيانات المخزنة 10
بيبليوغرافيا 11

مقدمة

يسعى كل جديد في تكنولوجيا المعلومات والاتصالات (ICT) لأن يكون معيناً ومفيداً للمستخدمين. وهذا يعني أن تكنولوجيا المعلومات والاتصالات ينبغي أن تهدف لتقديم الدعم، حتى أثناء وقوع الكوارث، من أجل إنقاذ مستخدمين في حالات خطرة. وفي الواقع، لا يتسع وقت المستخدمين في بعض الأحيان لانتظار قدوم فريق الإنقاذ أو مساعدة خارجية. وفي هذه الحالات، ليس للمستخدمين إلا الاعتماد على أنفسهم، والسعي لمغادرة منطقة الكارثة في أقرب وقت ممكن. ومن ثَم تقتضي الضرورة وضع متطلبات أجهزة إنترنت الأشياء (IoT) وكذلك متطلبات تشغيل تطبيقات إنترنت الأشياء خلال وقوع الكارثة بما يضمن التشغيل العادي لهذه التطبيقات. وفي الواقع، عادةً ما تصبح تطبيقات إنترنت الأشياء غير مجدية عملياً أثناء وقوع كارثة عندما تكون النجاة هي الهدف الأولى لمستخدمي إنترنت الأشياء. وبما أن البنية التحتية لإنترنت الأشياء منشورة بالفعل على نطاق واسع، يمكن أن تكون مواردها التقنية مفيدة جداً في إنقاذ الأرواح البشرية.

ومن الناحية العملية، يصعب جداً وضع نظام جديد للسلامة في حالات الطوارئ وتنفيذه بنجاح، نظراً لتعقيد إجراءات التقييس والاعتماد اللازمة لإدارة الكوارث. ولكن يكاد يسهل تعزيز الخواص الوظيفية لأنظمة السلامة القائمة بقدرات محسنة لدعم تطبيقات إنترنت الأشياء خلال وقوع كارثة. ويمكن الجمع أيضاً بين الخدمات المعتمِدة على إنترنت الأشياء وبين أنظمة السلامة القائمة كي تستخدمها أنظمة السلامة أثناء وقوع كارثة.

ومن المهم أن يُفهم أن أنظمة استعلامات إنترنت الأشياء الجديدة لن تحل أبداً محل أنظمة السلامة القائمة المختبَرة والمعتمَدة والمثبَتة على مدى سنوات عديدة؛ بيد أن أنظمة استعلامات إنترنت الأشياء الجديدة تدعم القدرة على التفاعل مع أنظمة السلامة القائمة. ومن شأن إدارة تطبيقات إنترنت الأشياء من مركز إدارة أنظمة السلامة القائمة أن تبقى ممكنة تقنياً أثناء وقوع كارثة.

وتُتوسم الفائدة من تفاعل تطبيقات إنترنت الأشياء المعززة هذه مع أنظمة السلامة القائمة في إجراءات الإنقاذ أثناء الكوارث، كالإنذار والإخلاء.

التوصية ITU-T Y.4102/Y.2074

المتطلبات اللازمة لأجهزة إنترنت الأشياء (IoT) ولتشغيل تطبيقات إنترنت الأشياء أثناء وقوع كارثة

1 مجال التطبيق

تقدم هذه التوصية المتطلبات اللازمة لأجهزة وتطبيقات إنترنت الأشياء (IoT) التي يمكن استخدامها لتشغيل تطبيقات إنترنت الأشياء في سياق الكوارث إضافةً إلى المتطلبات العامة لإنترنت الأشياء الواردة في التوصية [ITU-T Y.2066]. وهي تقدم أيضاً المتطلبات الخاصة اللازمة لتشغيل التطبيقات في حالات الكوارث.

ويشمل مجال تطبيق هذه التوصية متطلبات من أجل:

- أجهزة إنترنت الأشياء في سياق الكوارث؛
- تشغيل تطبيقات إنترنت الأشياء خلال وقوع كارثة (لكل من استراتيجيات التشغيل الثلاث المحددة)؛

ويوضح التذييل I الأساليب المتعلقة بضمان سلامة وموثوقية البيانات التي توفرها أجهزة IoT خلال وقوع كارثة.

وهذه التوصية مهمة لواضعي تطبيقات IoT ومقدمي خدمات IoT فضلاً عن مقدمي خدمات الطوارئ.

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.1303] التوصية ITU-T X.1303 (2007)، *بروتوكول الإنذار الموحد (CAP 1.1)*.

[ITU-T Y.1271] التوصية ITU-T Y.1271 (2004)، *إطار (أُطُر) متطلبات ومقدرات الشبكة اللازمة لتوفير اتصالات الطوارئ عبر الشبكات المتطورة بتبديل الرزم*.

[ITU-T Y.2066] التوصية ITU-T Y.2066 (2014)، *المتطلبات المشتركة لإنترنت الأشياء (IoT)*.

[ITU-T Y.2205] التوصية ITU-T Y.2205 (2011)، *شبكات الجيل التالي – اتصالات الطوارئ – اعتبارات تقنية*.

3 التعاريف

1.3 مصطلحات معرفة في وثائق أخرى

تستعمل هذه التوصية المصطلحات التالية المعرَّفة في مصادر أخرى:

1.1.3 تنبيه [b-ITU-T X.674]: رسالة تحذير أو إنذار بشأن خطر محدق أو مشكلة وشيكة.

2.1.3 الجهاز [b-ITU-T Y.2060]: فيما يتعلق بإنترنت الأشياء، هو جهاز يتسم بقدرات اتصالات إلزامية وقدرات اختيارية للاستشعار والتفعيل ونقل البيانات وتخزينها ومعالجتها.

3.1.3 اتصالات الطوارئ (ET) [ITU-T Y.2205]: أي خدمة متصلة بالطوارئ تتطلب من شبكة الجيل التالي (NGN) معالجة خاصة مقارنة بالخدمات الأخرى. ويشمل ذلك خدمات الطوارئ الحكومية المرخَّص بها وخدمات السلامة العامة.

4.1.3 إنترنت الأشياء (IoT) [b-ITU-T Y.2060]: بنية تحتية عالمية لمجتمع المعلومات، تمكّن الخدمات المتطورة عن طريق التوصيل البيني للأشياء (المادية والافتراضية) استناداً إلى تكنولوجيات المعلومات والاتصالات القابلة للتشغيل البيني القائمة والمتطورة.

الملاحظة 1 – من خلال استغلال إمكانيات تعرّف الهوية ونقل البيانات ومعالجتها واتصالاتها، تستخدم إنترنت الأشياء استخداماً كاملاً لإتاحة الخدمات لجميع أنواع التطبيقات، مع ضمان الحفاظ على الخصوصية المطلوبة.

الملاحظة 2 – يمكن النظر إلى إنترنت الأشياء، من منظور واسع، باعتبارها رؤية تنطوي على آثار تكنولوجية ومجتمعية.

5.1.3 شبكة الجيل التالي (NGN) [b-ITU-T Y.2001]: شبكة تقوم على أساس الرزمة ويمكنها تقديم خدمات الاتصالات للمستعملين ويمكنها الاستفادة من النطاق العريض المتعدد وتكنولوجيات النقل التي تتسم بجودة الخدمة وتكون فيها الوظائف المتصلة بالخدمة مستقلة عن التكنولوجيات الأساسية المتصلة بالنقل. وتتيح هذه الشبكة نفاذ المستعملين دون عوائق إلى الشبكات ومقدمي الخدمات المتنافسين و/أو الخدمات التي يختارونها. وهي تدعم التنقلية العامة التي تسمح بتقديم الخدمات إلى المستعملين بشكل متسق في كل مكان.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرف هذه التوصية المصطلحات التالية:

لا توجد.

4 الاختصارات والأسماء المختصرة

تستخدم هذه التوصية المختصرات التالية:

CAP بروتوكول التنبيه المشترك *(Common Alerting Protocol)*

ET اتصالات طوارئ *(Emergency Telecommunications)*

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

IoT إنترنت الأشياء *(Internet of Things)*

NGN شبكة الجيل التالي *(Next Generation Network)*

5 اصطلاحات

في هذه التوصية:

تدل الكلمات الرئيسية "يجب"، أو "يلزم"، أو "مطلوب" على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

وتدل كلمة "يوصَى" على متطلب يوصى به لكنه غير إلزامي بالمطلق. ومن ثم لا حاجة لتوفر هذا المتطلب لزعم المطابقة.

وتدل كلمات "يمكن اختيارياً" أو "يجوز" أو "من الجائز" أو "ربما" على مطلب خياري مسموح به دون أن ينطوي على أي توصية به. ولا ترمي هذه الكلمات إلى إلزام التطبيق بتوفير الجهة البائعة لهذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مقدم الخدمة خيارياً. بل يمكن للجهة البائعة إدراج هذا الخيار وزعم مطابقة المواصفة في نفس الوقت.

وتدل كلمة "كارثة" على أي نوع من الأوضاع أو الطوارئ الحرجة ذات المنشأ الطبيعي أو من صنع الإنسان.

وتدل العبارة الرئيسية "جهاز إنترنت الأشياء" على وجود جهاز في بيئة إنترنت الأشياء.

6 المتطلبات اللازمة لأجهزة إنترنت الأشياء (IoT) في سياق الكوارث

1.6 المتطلبات العامة بشأن الكوارث

تتناول التوصيات التالية الاتصالات المعنية بالكوارث:

- [ITU-T Y.1271] تقدم هذه التوصية متطلبات وقدرات الشبكة للاتصالات في حالات الطوارئ (ET).
- [ITU-T Y.2205] تحدد هذه التوصية الاعتبارات التقنية التي يمكن استخدامها اختيارياً في شبكات الجيل التالي (NGN) بهدف تمكين اتصالات الطوارئ (ET). كما تتناول بإيجاز المبادئ التقنية التي ينطوي عليها دعم هذه الاتصالات.

وتتناول هذه التوصيات المتطلبات والجوانب التقنية للاتصالات في حالات الطوارئ. وبافتراض أن تطبيقات إنترنت الأشياء ستستخدم شبكات الجيل التالي كبنية تحتية للاتصالات أثناء وقوع كارثة، فإن هذه المتطلبات تنطبق عليها تماماً.

ووفق التوصية [ITU-T Y.2205]، يوصى باستخدام بروتوكول التنبيه المشترك (CAP) المعرف في التوصية [ITU-T X.1303] لإتاحة تفاعل المعلومات بين أنظمة التنبيه.

2.6 المتطلبات اللازمة لأجهزة إنترنت الأشياء

يُتطلب من جميع أجهزة إنترنت الأشياء المصنَّعة اجتياز إجراءات اختبارية بنجاح.

وينبغي أن تتضمن هذه الإجراءات اختبار الأجهزة إنترنت الأشياء تحت ظروف تتجاوز المدى التشغيلي (كدرجة الحرارة والضغط والإشعاع) للتحقق من خلوها من المخاطر على البيئة والبشر أثناء وقوع الكوارث. فيجب ألا تتسبب أجهزة إنترنت الأشياء بمضاعفات أو بوقوع حالات الطوارئ من أنواع أخرى.

وينبغي اختيار ظروف الاختبار على أساس خصائص حالات الطوارئ المحتملة في منطقة النشر.

ويُتطلب إدراج نتائج الاختبار، والمخاطر المحتملة التي تسببها الأجهزة خارج المدى التشغيلي، ضمن الخصائص التقنية للأجهزة.

ويوصى بتزويد جديد أجهزة إنترنت الأشياء بمدى موسَّع للخصائص التشغيلية (كدرجة حرارة التشغيل والرطوبة والضغط). ويُعد تطلُّب توسيع مدى الخصائص التشغيلية لأجهزة إنترنت الأشياء ضرورياً لتطبيقات إنترنت الأشياء التي يحتمل أن تتعطل نظراً لعدم التيقن من سلوك البيئة ومن تأثيره على أجهزة إنترنت الأشياء خلال وقوع كارثة.

ويوصى بتعميم هذه الممارسة على أنماط أجهزة إنترنت الأشياء المستخدمة على نطاق واسع. ولعل تشغيل أجهزة إنترنت الأشياء التي تقوم بقياسات أثناء وقوع كارثة يوفر قاعدة بيانات لقياسات المعلمة البيئية أثناء وقوع الكوارث على اختلاف أنواعها. فمن شأن مثل هذه القياسات أن تساعد على التوصل إلى استنتاجات هامة عن مراحل وقوع الكارثة، وأن تتيح أخذها بعين الاعتبار في مرحلة تصميم جهاز إنترنت الأشياء.

7 المتطلبات اللازمة لتشغيل تطبيقات إنترنت الأشياء أثناء وقوع كارثة

تصف هذه الفقرة متطلبات تطبيقات إنترنت الأشياء المتعلقة بتشغيلها أثناء وقوع الكارثة. وعلى وجه الخصوص، تصف الفقرات من 1.7 إلى 3.7 متطلبات كل من استراتيجيات التشغيل الثلاث المحددة لتطبيقات إنترنت الأشياء ذات الصلة بالكوارث، فيما تصف الفقرة 4.7 التبديل بين استراتيجيتي تشغيل أو أكثر خلال وقوع كارثة.

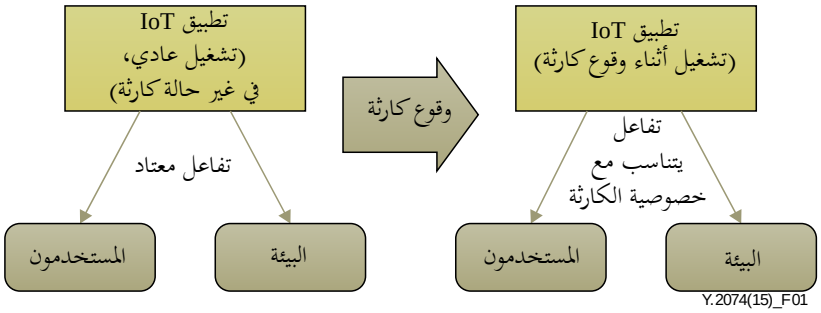
ولتحسين كفاءة موارد البنية التحتية المرتبطة بتشغيل تطبيقات إنترنت الأشياء، يوصى بأن تنفذ تطبيقات إنترنت الأشياء واحدة أو أكثر من استراتيجيات التشغيل التالية المتعلقة بالكوارث.

وتفترض جميع الاستراتيجيات أن تطبيقات إنترنت الأشياء لا تواصل التشغيل العادي أثناء وقوع كارثة، بل تكتفي بدلاً من ذلك بأداء المهام التي تهدف إلى إنقاذ الناس.

ويمكن أن تُطلَق تنبيهات طوارئ كاذبة: يجوز إلغاء حالة طوارئ (في حال اكتشاف حالة طوارئ كاذبة مثلاً)، وفي هذه الحالة، يعاود تطبيق إنترنت الأشياء تشغيله العادي. وتختلف المدة الزمنية المطلوبة لاتخاذ قرار بشأن حالة التنبيه الكاذب (استمرار التشغيل الحالي أو معاودة التشغيل العادي) لكل تطبيق حسب تعقيده.

1.7 تطبيقات إنترنت الأشياء بأسلوب التشغيل المخصص

إذا زُود تطبيق إنترنت الأشياء بأسلوب تشغيل مخصص يمكن تفعيله في حالات الطوارئ، أمكن استخدامه دون أي إجراء آخر أو تحكُّم خارجي. ويبين الشكل 1 تغير أسلوب تشغيل تطبيقات إنترنت الأشياء باتباع هذه الاستراتيجية.



الشكل 1 – تغير أسلوب تشغيل تطبيقات إنترنت الأشياء المزوَّدة بأسلوب تشغيل مخصص يفعَّل أثناء وقوع كارثة

إن التطبيقات القائمة على شبكة استشعار مصممة لتحديد مواضع المستخدمين في مبنى ومزودة بأساليب تشغيل مخصصة تفعَّل خلال وقوع كارثة، يمكن أن تكون فعالة للغاية في الإخلاء الذاتي من مبنى في حال نشوب الحرائق أو وقوع الزلازل أو غيرها من الكوارث.

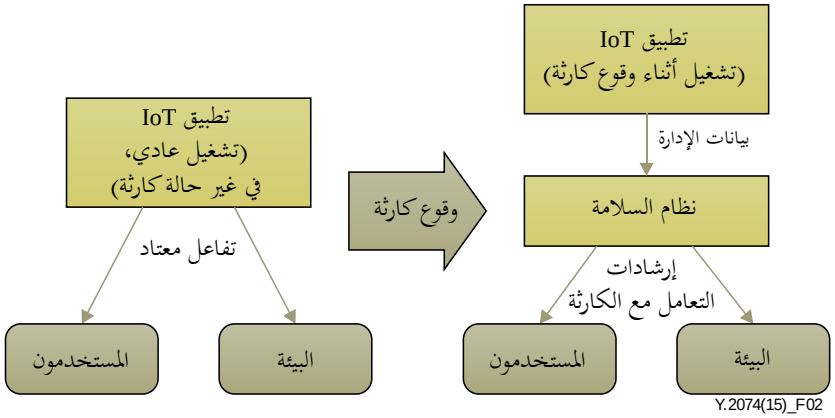
وثمة مثال آخر على هذه الاستراتيجية التشغيلية في إمكانية أن يقوم أحد تطبيقات إنترنت الأشياء بدور نظام السلامة.

ملاحظة – هناك نماذج أولية من أنظمة السلامة تلك تعتمد على تكنولوجيات الاستشعار اللاسلكي (كالتي يرد وصفها في التوصية [b-ITU-T Y.2222])، ولكنها لا تُستخدم على نطاق واسع بسبب تعقيد إجراءات تقييس واعتماد معدات نظام السلامة والوقت الطويل الذي تستغرقه.

ويُتطلب من تطبيقات إنترنت الأشياء، المزودة بأسلوب تشغيل مخصص يفعَّل خلال وقوع كارثة، أن تلتزم بجميع القواعد التنظيمية المناسبة.

2.7 تطبيقات إنترنت الأشياء التي تقدم مؤقتاً موارد لأنظمة السلامة الخارجية

إن لتطبيقات إنترنت الأشياء أغراضاً محددة عادة، ولا يهدف جُلها إلى مساعدة أو إعانة المستخدمين أثناء وقوع كارثة. وبناء على ذلك، ينبغي لأنظمة السلامة الخارجية أن تساعد موارد تطبيقات إنترنت الأشياء من أجل تحسين كفاءة عملية إدارة الكوارث. ويبين الشكل 2 تغير أسلوب تشغيل تطبيقات إنترنت الأشياء باتباع هذه الاستراتيجية.



الشكل 2 – تغير أسلوب تشغيل تطبيقات إنترنت الأشياء
التي تقدم مؤقتاً موارد لأنظمة السلامة الخارجية

وينبغي لتطبيقات إنترنت الأشياء المصممة لمستخدمين داخل مبنى أو بيئة أخرى مجهزة بنظام سلامة أن تتشارك مؤقتاً مع نظام السلامة (خلال وقوع كارثة) بقدرة التحكم في تطبيقات إنترنت الأشياء وبجميع أنواع بيانات القياس. فقد يستفاد من هذه الموارد لتشغيل نظام السلامة، ومثال ذلك البيانات من مختلف أجهزة الاستشعار كبيانات درجة الحرارة والرطوبة في حالة نشوب حريق.

ولتبسيط تكامل تطبيقات إنترنت الأشياء مع أنظمة السلامة الخارجية، يوصى باستخدام التوصية [ITU-T X.1303] للتفاعل بين تطبيقات إنترنت الأشياء وأنظمة السلامة الخارجية. وCAP هو بروتوكول اتصالات في اتجاهين يمكنه أن يمكّن إرسال البيانات من تطبيقات إنترنت الأشياء إلى أنظمة السلامة وكذلك إرسال رسائل التنبيه من أنظمة السلامة إلى تطبيقات إنترنت الأشياء.

ويتمثل العيب الرئيسي لاستراتيجية التشغيل هذه في إمكانية وقوع أعطال في مكونات وظيفية للبنية التحتية لإنترنت الأشياء إن لم تصمَم هذه المكونات لتعمل بشكل صحيح أثناء وقوع كارثة. وقد تترتب نتائج سلبية على هذه الأعطال في حالة المكونات الوظيفية اللازمة أثناء عمليات إدارة الكوارث. ويمكن أن تقع هذه الأعطال جراء غياب إجراءات اعتماد خاصة للمكونات الوظيفية للبنية التحتية لإنترنت الأشياء من أجل ضمان التشغيل الصحيح أثناء وقوع الكوارث، على النقيض من الإجراءات المعتمدة لأنظمة السلامة.

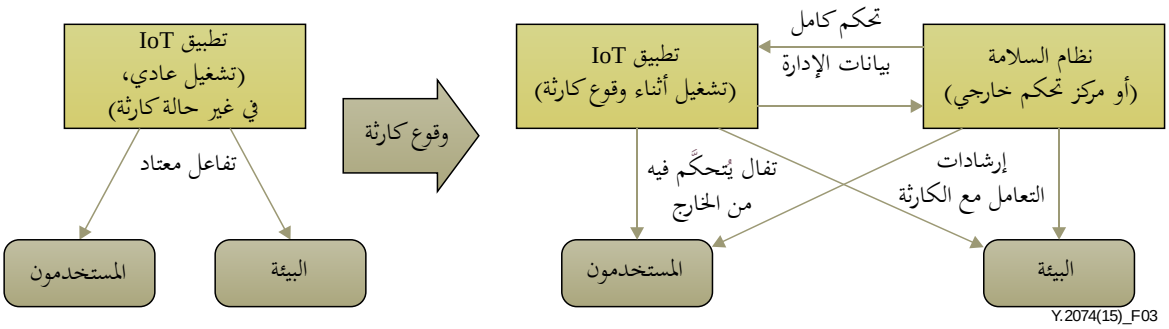
3.7 تطبيقات إنترنت الأشياء ذات التحكُّم الخارجي في التشغيل أثناء وقوع كارثة

وتنطوي استراتيجية التشغيل الثالثة لتطبيقات إنترنت الأشياء أثناء وقوع كارثة على نقل كامل لقدرات التحكم وبيانات القياس من تطبيقات إنترنت الأشياء إلى أنظمة سلامة خارجية أو مراكز تحكُّم خارجية.

الملاحظة 1 – إن النقل الكامل لقدرات التحكم يعني ضمناً إنهاء عملية إدارة الموارد من جانب تطبيق إنترنت الأشياء نفسه.

الملاحظة 2 – يمكن أن يكون مركز التحكم الخارجي، على سبيل المثال، منظمة أو وحدة وظيفية بمنظمة تتحمل المسؤولية القانونية والإدارية الكاملة عن الإدارة الصحيحة للكوارث في منطقة معينة.

ويبين الشكل 3 تغير أسلوب تشغيل تطبيقات إنترنت الأشياء باتباع استراتيجية التشغيل هذه.



الشكل 3 – تغير أسلوب تشغيل تطبيقات إنترنت الأشياء بالتحكُّم الخارجي في التشغيل أثناء وقوع كارثة

في استراتيجية التشغيل هذه، تتحكم أنظمة سلامة وتنبيهات خارجية بالكامل في سلوك المستخدمين أثناء وقوع كارثة فيما يتعلق بتطبيقات إنترنت الأشياء المتبِّعة لأسلوب التشغيل الموصوف في الفقرة 1.7.

والغرض الرئيسي من استراتيجية التشغيل هذه هو ضمان الاستخدام الأكثر فعالية لجميع موارد تطبيقات إنترنت الأشياء المتاحة، عن طريق إدارة سليمة التي تنفذها أنظمة السلامة أو مراكز تحكُّم خارجية.

ويصف التذييل I الأساليب المتعلقة بضمان سلامة وموثوقية البيانات التي تنتجها أجهزة إنترنت الأشياء. ويمكن لمركز مراقبة أجهزة إنترنت الأشياء والتحكم فيها، على النحو الموضح في التذييل الأول، أن يكون بمثابة مركز التحكم الخارجي لتطبيقات إنترنت الأشياء في استراتيجية التشغيل هذه.

وعلى غرار استراتيجية التشغيل التي ورد وصفها في الفقرة 2.7، يوصى باستخدام بروتوكول التنبيه المشترك (CAP) [ITU-T X.1303] للتفاعل بين تطبيقات إنترنت الأشياء وأنظمة السلامة خارجية أو مراكز التحكُّم الخارجية في استراتيجية التشغيل هذه.

4.7 التبديل بين استراتيجيتي تشغيل أو أكثر خلال وقوع كارثة

تبعاً للغرض من تطبيق إنترنت الأشياء وقدراته، يمكن تنفيذ توليفة من استراتيجية تشغيل واحدة أو أكثر في تطبيق إنترنت الأشياء. وهذا ينطوي على انتقال قدرة تطبيق إنترنت الأشياء بين استراتيجيات التشغيل إذا طرأت بعض الظروف الخارجية، مثل استقبال إشارات تحكم، أو زيادة الدرجة المقررة في قراءات أجهزة الاستشعار، وما إلى ذلك.

وكمثال على ذلك، يمكن أن يتحقق تشغيل تطبيق إنترنت الأشياء على النحو التالي:

وبالنظر في تطبيق إنترنت الأشياء (ضمن منطقة جغرافية) مجهز بنظام سلامة (خارجي فيما يتعلق بتطبيق إنترنت الأشياء)؛ إذا أظهرت مراقبة بيانات جهاز إنترنت الأشياء وقوع حالة طوارئ أثناء التشغيل العادي، ينتقل تطبيق إنترنت الأشياء تلقائياً إلى أسلوب التشغيل المخصص للتشغيل أثناء وقوع كارثة وينفذ الاستراتيجية المذكورة في الفقرة 1.7.

وفي نهاية وقت اتخاذ قرار بشأن تنبيه كاذب، يستمر تطبيق إنترنت الأشياء في التشغيل بأسلوب تشغيل مخصص أو يعود إلى أسلوب التشغيل العادي (في حالة تنبيه كاذب). وإذا استمر التشغيل بأسلوب التشغيل المخصص، قبل مرحلة الكارثة المدمرة، يولد تطبيق إنترنت الأشياء معلومات على مقاس كل شخص تضربه الكارثة لإدارة انقاذه.

وعند وقوع المرحلة المدمرة، متى يعجز تطبيق إنترنت الأشياء عن إدارة عمليات الإنقاذ بسبب تراجع القدرات، ينتقل تطبيق إنترنت الأشياء إلى استراتيجية التشغيل التي يرد وصفها في الفقرة 2.7 (مراقبة وإرسال البيانات التي جُمعت إلى نظام السلامة الخارجي). وقد يساعد على إنقاذ الأرواح خلال مرحلة الإنقاذ اللاحقة في حالات الطوارئ وسيراقب تطور الكارثة.

التذييل I

الأساليب المتعلقة بضمان سلامة وموثوقية البيانات التي تنتجها أجهزة إنترنت الأشياء خلال وقوع كارثة

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يمكن أن تؤدي أجهزة إنترنت الأشياء في كل مكان دوراً هاماً في الحياة اليومية للناس، وأن تؤثر على قراراتهم وأفعالهم. وبالتالي، قد يعتمد الناس على أجهزة إنترنت الأشياء الخاصة بهم، ولا سيما بشأن قراءات المعلومات وأجهزة الاستشعار الخاصة بهم، فضلاً عن الإجراءات المستمدة من هذه القراءات التي تؤثر على البيئة. ولذلك، فإن سلامة وموثوقية البيانات التي تنتجها أجهزة إنترنت الأشياء هي قضايا مهمة جداً لإنترنت الأشياء بشكل عام.

وتصبح المشكلة المحيطة بسلامة وموثوقية البيانات التي تنتجها أجهزة إنترنت الأشياء ذات صلة خاصة أثناء وقوع الكوارث الطبيعية والكوارث من صنع الإنسان، حيث قد يتعذر ضمان سلامة أجهزة إنترنت الأشياء نفسها.

تقتضي الضرورة إنشاء بيئة موثوقة لتشغيل أجهزة إنترنت الأشياء. ولهذا الغرض، وللحفاظ على سلامة وموثوقية البيانات التي تنتجها أجهزة إنترنت الأشياء، من المهم تحديد نطاق المسؤولية عن سلوك أجهزة إنترنت الأشياء بشكل عام، كالمسؤولية عن أي قراءات غير صحيحة لأجهزة الاستشعار. وهناك طريقتان لتحقيق هذا الهدف:

1 تولّي الجهة الشركة المصنعة لأجهزة إنترنت الأشياء مسؤولية كاملة عن أي خلل في جهاز إنترنت الأشياء المنتج وضمانها للسلوك المناسب لجهاز إنترنت الأشياء؛

2 تولّي مركز مخوَّل مستقل مسؤولية كاملة عن أي خلل في جهاز إنترنت الأشياء تحت سيطرته (أي يخضع لولايته)، وضمانه للسلوك المناسب لجهاز إنترنت الأشياء.

والطريقة الأولى أقل فعالية من الثانية بسبب التفاعل المعقد بين المستخدمين والجهات المصنعة المسؤولة عن أجهزة إنترنت الأشياء لدى المستخدم، ويعود ذلك إلى إمكانية اختلاف أجهزة إنترنت الأشياء الموردة من جهات مصنعة مختلفة والمستخدمة داخل منطقة النشر نفسها. وتصبح هذه المشكلة ذات صلة خاصة أثناء وقوع كارثة، عندما تصبح سلامة وموثوقية البيانات التي تنتجها أجهزة إنترنت الأشياء شأناً يخص حماية الأرواح البشرية. فأثناء وقوع كارثة، لن يتمكن المستخدمون ولا خدمات الإنقاذ ولا أجهزة إنترنت الأشياء من الاتصال بالجهة المصنعة لكل جهاز معيَّن من أجهزة إنترنت الأشياء لتأكيد سلامة وموثوقية البيانات الخاصة به.

أما الطريقة الثانية فهي أكثر واقعية بكثير من حيث أنها تنطوي على إنشاء مراكز مراقبة وتحكم لأجهزة إنترنت الأشياء. وستتولى هذه المراكز المسؤولية عن التشغيل الصحيح لأجهزة إنترنت الأشياء الخاضعة لولايتها.

1.I نظرة عامة على مركز المراقبة والتحكم لأجهزة إنترنت الأشياء

إن مركز المراقبة والتحكم (المركز) لأجهزة إنترنت الأشياء هو منظمة، أو وحدة وظيفية للمنظمة، تتحمل المسؤولية القانونية والإدارية الكاملة عن التشغيل الصحيح لأجهزة إنترنت الأشياء التي تخضع لولايتها. وهو أيضاً يراقب أجهزة إنترنت الأشياء ويخزن المعلومات عن العمليات أثناء الكوارث. ويتمثل الهدف الرئيسي لمركز المراقبة والتحكم لأجهزة إنترنت الأشياء في التحقق من سلامة وموثوقية المعلومات التي تقدمها أجهزة إنترنت الأشياء التي تخضع لولايته. وبالإضافة إلى ذلك، المركز هو المسؤول عن إخطار مستخدمي و/أو مالكي أجهزة إنترنت الأشياء فور اكتشاف أعطال في أي من أجهزة إنترنت الأشياء.

وإذا لاح خطر وقوع كارثة أو أثناء وقوع كارثة، يتولى المركز المسؤولية عما يلي:

- مراقبة حالة أجهزة إنترنت الأشياء التي تخضع لولايته وبيانات مخرجاتها (من قبيل قراءات أجهزة الاستشعار)؛
- تحديد أجهزة إنترنت الأشياء العاملة بشكل غير صحيح وإخطار مستخدميها و/أو مالكيها بالأعطال على الفور؛
- تحديد منطقة الكارثة وطبيعة ومعلمات الكارثة، مع الأخذ بعين الاعتبار المعلومات المحصَّلة من أجهزة إنترنت الأشياء التي تخضع لولايته والمصادر الخارجية للمعلومات (كالوكالات المعنية بحالات الطوارئ)؛
- إدارة أجهزة إنترنت الأشياء التي تخضع لولايته من أجل الإجلاء الآمن للسكان من منطقة الكارثة؛
- تسجيل وتخزين المعلومات المحصَّلة أثناء وقوع كارثة والسجل الزمني للعمليات خلال وقوع كارثة.

2.I توزيع مسؤوليات مركز المراقبة والتحكم على المراكز المحلية

توجد أجهزة إنترنت الأشياء في كل مكان بكميات كبيرة ضمن الشقق والبيوت والمؤسسات والشوارع والأماكن العامة، وما إلى ذلك.

وفي حالة مركز المراقبة والتحكم لأجهزة إنترنت الأشياء، يمكن أن تقع جميع أجهزة إنترنت الأشياء في منزل أو مبنى معين تحت ولاية مركز محلي واحد. وبالمثل، يمكن أن تدير المراكز المحلية الأخرى جميع أجهزة إنترنت الأشياء في مناطق أخرى، في الشارع نفسه، على سبيل المثال. ويمكن دمج جميع هذه المراكز المحلية في البنية التحتية للمركز الجذر.

ويمكن تنظيم البنية التحتية للمركز الجذر ضمن تراتبية متعددة المستويات تحتوي على عُقَد مراقبة وتحكُّم على عدة مستويات مسؤولة عن أجهزة إنترنت الأشياء في مختلف: المباني (المراكز المحلية) والمدن (مراكز البلدية)، والأقاليم (المراكز الإقليمية) والبلدان (المراكز الاتحادية).

بالإضافة إلى ذلك، يمكن أن تتوزع مسؤولية المراكز المحلية على أساس الغرض من جهاز إنترنت الأشياء. فعلى سبيل المثال، يمكن لمركز إدارة العديد من المراكز المحلية، فيتولى أحدها المسؤولية عن أجهزة إنترنت الأشياء للأغراض المنزلية، وآخر عن أجهزة إنترنت الأشياء لأغراض إدارة الحركة، وثالث عن أجهزة إنترنت الأشياء لأغراض نظام الأمن، وما إلى ذلك.

وتصف الفقرات التالية سيناريوهات العمل الممكنة لمركز المراقبة والتحكم.

3.I سيناريوهات عمل مركز المراقبة والتحكم

يتمثل الهدف الرئيسي للمركز في التحقق من سلامة وموثوقية المعلومات التي تقدمها أجهزة إنترنت الأشياء التي تخضع لولايته. ويمكن أن يتحقق هذا الهدف من خلال الطرق التالية:

1 مقارنة قراءات الاستشعار من أجهزة إنترنت الأشياء الواقعة تحت ولاية المركز، مع قراءات من شبكات الاستشعار المستقلة ذاتياً (المستنسخة)؛

2 المراقبة الذكية لقراءات أجهزة الاستشعار الواقعة تحت ولاية المركز، وهي تنطوي على جمع البيانات والتحليل الرياضي (استخراج البيانات) من المعلومات المحصَّلة، مما يتيح تحديد أعطال جهاز إنترنت الأشياء.

ويمكن تنفيذ كلا الطريقتين واستخدامهما في توليفة بنسبة ملائمة.

ويرد وصف الطريقتين المذكورتين أعلاه بمزيد من التفصيل في الفقرتين 1.3.I و2.3.I.

1.3.I شبكة الاستشعار المستقلة ذاتياً

وينشر المركز شبكات استشعار مستقلة تحتوي على أجهزة استشعار لمختلف المعلمات الفيزيائية وهي تستنسخ مستشعرات أجهزة إنترنت الأشياء الواقعة تحت ولاية المركز.

ويُتطلب من شبكة الاستشعار المستقلة ذاتياً تغطية كامل المنطقة الواقعة تحت ولاية المركز. فعلى سبيل المثال، ينبغي أن ينشر مركز محلي داخل مبنى شبكة استشعار تغطي المنطقة داخل مبنى التي تحتوي على أجهزة إنترنت الأشياء الواقعة تحت تحكُّم المركز.

وتُعتبر أجهزة الاستشعار، في شبكة الاستشعار المستقلة ذاتياً هذه، أجهزة الاستشعار المرجعية، أي تؤخذ قراءاتها كقيم المعلمات الفيزيائية المرجعية في هذه المنطقة. ويُتوقع أن تعتمد منظمة موثوقة ومعتمَدة أجهزة الاستشعار المرجعية حسب الأصول.

ويجمع المركز البيانات من أجهزة إنترنت الأشياء التي تخضع لولايته، ويقارنها مع القيم المرجعية. وعلى أساس هذه المقارنة، يتخذ المركز قرارات بشأن سلامة وموثوقية البيانات التي تنتجها أجهزة إنترنت الأشياء.

وتتمثل ميزة هذه الطريقة فيما تنطوي عليه من أجهزة الاستشعار المرجعية عالية الموثوقية بمعزل عن أجهزة إنترنت الأشياء. وبالتالي، تحدَد أعطال أجهزة إنترنت الأشياء بدقة عالية.

وتتمثل مساوئ هذه الطريقة في تكلفة وتعقيد نشر شبكات الاستشعار المستقلة ذاتياً وفي الأعطال التي قد تصيب أجهزة الاستشعار المرجعية أثناء وقوع كارثة.

2.3.I المراقبة الذكية

تتعلق المراقبة الذكية بجمع معلومات الأجهزة وقراءات الاستشعار المحصَّلة من أجهزة إنترنت الأشياء الواقعة تحت ولاية المركز، ومن التحليل الرياضي لهذه المعلومات. وهذا يشمل، على سبيل الذكر لا الحصر، أساليب التحليل الإحصائي ومعالجة إشارة الارتباط.

وتتيح المراقبة الذكية تحديد اختلال أجهزة إنترنت الأشياء أو أجهزة الاستشعار ضمن مجموعة من الأجهزة المماثلة.

وتظهر ميزة هذه الطريقة في استقلال المعلمات الخارجية التام عن البيئة، مما يسمح بالتشغيل في كل حالة من الحالات أثناء وقوع كارثة.

ويعاب على هذه الطريقة حاجتها إلى وجود مجموعة من أجهزة إنترنت الأشياء المتماثلة لتحديد الأعطال بموثوقية أعلى.

4.I استخدام البيانات المخزنة

ينفذ المركز المراقبة ويقوم بتسجيل وتخزين معلومات الأجهزة وقراءات الاستشعار المحصَّلة من أجهزة إنترنت الأشياء الواقعة تحت ولاية المركز، بما فيها تلك المحصَّلة قبل وقوع الكارثة مباشرةً وخلالها.

وتتيح هذه الخاصية الوظيفية للمركز أن يعمل "كصندوق أسود" في حالات الطوارئ. ويُفترض أن المركز يساعد في تحديد أسباب حالات الطوارئ، بطريقة مشابهة لما يقوم به الصندوق الأسود في الطائرات.

ويمكن استخدام البيانات التاريخية التي جُمعت في مخزن بيانات المركز لتحسين طرق المراقبة الذكية وتطوير طرق إدارة جهاز إنترنت الأشياء والتحكُّم فيه، إذا لاح خطر وقوع كارثة أو أثناء وقوع كارثة، من أجل تحقيق أوسع إخلاء ممكن للناس، بأمان، من منطقة الكارثة.

بيبليوغرافيا

[b-ITU-T X.674] التوصية ITU-T X.674 (2011)، *إجراءات تسجيل التفرعات في إطار تفرع معرّف الكائن المنبه.*

[b-ITU-T Y.2001] التوصية ITU-T Y.2001 (2004)، *نظرة عامة على شبكات الجيل التالي.*

[b-ITU-T Y.2060] التوصية ITU-T Y.2060 (2012)، *نظرة عامة على إنترنت الأشياء.*

[b-ITU-T Y.2222] التوصية ITU-T Y.2222 (2013)، *شبكات التحكم في أجهزة الاستشعار والتطبيقات ذات الصلة في بيئة شبكات الجيل التالي.*

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
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	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
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، وجوانب بروتوكول الإنترنت وشبكات الجيل التالي**
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2016