Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2074

(01/2015)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET, REDES DE PRÓXIMA GENERACIÓN, INTERNET DE LAS COSAS Y CIUDADES INTELIGENTES

Redes de la próxima generación – Marcos y modelos arquitecturales funcionales

Requisitos para dispositivos de Internet de las cosas y funcionamiento de aplicaciones de Internet de las cosas en caso de catástrofe

Recomendación UIT-T Y.2074

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET, REDES DE PRÓXIMA GENERACIÓN, INTERNET DE LAS COSAS Y CIUDADES INTELIGENTES

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	**Y.2000–Y.2099**
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Mejoras de las NGN	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Redes basadas en paquetes	Y.2600–Y.2699
Seguridad	Y.2700–Y.2799
Movilidad generalizada	Y.2800–Y.2899
Entorno abierto con calidad de operador	Y.2900–Y.2999
REDES FUTURAS	Y.3000–Y.3499
COMPUTACIÓN EN LA NUBE	Y.3500–Y.3999

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Y.2074

Requisitos para dispositivos de Internet de las cosas y funcionamiento de aplicaciones de Internet de las cosas en caso de catástrofe

Resumen

La Recomendación UIT-T Y.2074 proporciona requisitos para dispositivos de Internet de las cosas (IoT) que permiten el funcionamiento de aplicaciones IoT en el contexto de catástrofes, además de los requisitos comunes de IoT que figuran en la Recomendación UIT-T Y.2066. También proporciona requisitos para el funcionamiento de aplicaciones IoT durante catástrofes.

Es necesario especificar esos requisitos para poder utilizar dispositivos IoT y aplicaciones IoT en procesos de evacuación y rescate durante catástrofes.

El Apéndice I describe métodos relativos a la garantía de integridad y fiabilidad de datos generados en dispositivos IoT durante catástrofes.

La presente Recomendación es pertinente para desarrolladores de aplicaciones IoT y proveedores de servicios IoT, así como para proveedores de servicios de emergencia.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T Y.2074	2015-01-13	13	11.1002/1000/12421

Palabras clave

Aplicación IoT, catástrofe, dispositivo IoT, Internet de las cosas (IoT), requisitos, sistemas de seguridad.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Introducción

Cada nueva Tecnología de la Información y la Comunicación (TIC) persigue el objetivo de ser práctica y útil para el usuario. Esto significa que, aún en situaciones de catástrofe, las TIC deben servir para rescatar a los usuarios en circunstancias peligrosas. De hecho, en ciertas ocasiones los usuarios no pueden esperar al equipo de rescate o la ayuda externa. En estos casos, la única posibilidad es actuar de manera independiente e intentar alejarse de la zona de peligro cuanto antes. Por tal motivo, es necesario que se establezcan requisitos para dispositivos de Internet de las cosas (IoT) y requisitos para el funcionamiento de aplicaciones IoT en el contexto de catástrofes, más allá del funcionamiento normal de estas aplicaciones. De hecho, las aplicaciones IoT suelen ser prácticamente inservibles durante una catástrofe cuando el objetivo primordial de los usuarios IoT es recibir ayuda. Puesto que la infraestructura de IoT se encuentra ampliamente disponible, sus recursos técnicos podrían ser especialmente útiles para salvar vidas humanas.

Desde un punto de vista práctico, resulta extremadamente difícil diseñar y aplicar con éxito un nuevo sistema de seguridad para emergencias, debido a los complejos procedimientos de normalización y certificación que exige la gestión de catástrofes. Sin embargo, es bastante fácil mejorar las funciones de los sistemas existentes y dotarlos de mayor capacidad como para que puedan soportar las aplicaciones IoT durante catástrofes. Además, también existe la posibilidad de combinar los servicios basados en IoT con los sistemas de seguridad existentes, y así los sistemas de seguridad podrían utilizarlos durante la catástrofe.

Es importante comprender que los nuevos sistemas de inteligencia IoT nunca reemplazarán a los sistemas de seguridad probados y certificados que existen desde hace varios años. No obstante, los sistemas de inteligencia IoT pueden soportar la capacidad de interacción con los sistemas de seguridad existentes. Técnicamente, es posible gestionar las aplicaciones IoT desde el centro de administración de un sistema de seguridad durante una situación de catástrofe.

Se prevé que la interacción entre estas aplicaciones de IoT mejoradas y los sistemas de seguridad existentes resulte útil durante procedimientos de rescate en situaciones de catástrofe, en todo caso, en el marco de las alertas y la evacuación.

Recomendación UIT-T Y.2074

Requisitos para dispositivos de Internet de las cosas y funcionamiento de aplicaciones de Internet de las cosas en caso de catástrofe

1 Alcance

La presente Recomendación proporciona requisitos para dispositivos IoT que permiten el funcionamiento de aplicaciones IoT en el contexto de catástrofes, además de los requisitos comunes de IoT que figuran en la Recomendación [UIT-T Y.2066]. También proporciona requisitos especiales para el funcionamiento de aplicaciones IoT durante catástrofes.

El alcance de la presente Recomendación incluye requisitos para:

- dispositivos IoT en el contexto de catástrofes;
- el funcionamiento de aplicaciones IoT durante catástrofes (para cada una de las tres estrategias de funcionamiento identificadas).

El Apéndice I describe métodos relativos a la garantía de integridad y fiabilidad de datos generados por dispositivos IoT durante catástrofes.

La presente Recomendación es pertinente para desarrolladores de aplicaciones IoT y proveedores de servicios IoT así como proveedores de servicios de emergencia.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[UIT-T X.1303] Recomendación UIT-T X.1303 (2007), *Protocolo de alerta común (CAP 1.1)*.

[UIT-T Y.1271] Recomendación UIT-T Y.1271 (2004), *Requisitos y capacidades de red generales necesarios para soportar telecomunicaciones de emergencia en redes evolutivas con conmutación de circuitos y conmutación de paquetes*.

[UIT-T Y.2066] Recomendación UIT-T Y.2066 (2014), *Requisitos comunes de la Internet de las cosas*.

[UIT-T Y.2205] Recomendación UIT-T Y.2205 (2011), *Redes de próxima generación – telecomunicaciones de emergencia – Consideraciones técnicas*.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 alerta [b-UIT-T X.674]: Mensaje de alerta o alarma respecto de un problema o peligro inminente.

3.1.2 dispositivo [b-UIT-T Y.2060]: En el contexto de Internet de las cosas, se trata de un equipo con las capacidades obligatorias de comunicación y las capacidades opcionales para la detección, accionamiento y adquisición, almacenamiento y procesamiento de datos.

3.1.3 telecomunicaciones de emergencia (ET) [UIT-T Y.2205]: Todo servicio de emergencia que necesita de las NGN un tratamiento especial en comparación con otros servicios. Comprende los servicios de emergencia autorizados por el Estado y los servicios de seguridad pública.

3.1.4 Internet de las cosas (IoT) [b-UIT-T Y.2060]: Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperatividad de tecnologías de la información y la comunicación presentes y futuras.

NOTA 1 – Gracias a la identificación, la adquisición y el procesamiento de datos, y a las capacidades de comunicación, IoT hace pleno uso de los objetos para ofrecer servicios a todo tipo de aplicaciones, garantizando a su vez el cumplimiento íntegro de los requisitos de seguridad y privacidad.

NOTA 2 – Desde una perspectiva más amplia, IoT puede considerarse una noción con repercusiones tecnológicas y sociales.

3.1.5 red de la próxima generación (NGN) [b-UIT-T Y.2001]: Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha con garantías de QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Asimismo ofrece movilidad generalizada que permite la prestación coherente y ubicua de servicios a los usuarios.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se utilizan o definen los siguientes términos:

Ninguno.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas o acrónimos:

CAP Protocolo de alerta común (*common alerting protocol*)

ET Telecomunicaciones de emergencia (*emergency telecommunications*)

TIC Tecnología de la información y la comunicación (*information and communication technology*)

IoT Internet de las cosas (*Internet of things*)

NGN Red de la próxima generación (*next generation network*)

5 Convenios

En la presente Recomendación:

La expresión "se requiere" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con este documento.

La expresión "se recomienda" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

La expresión "se tiene la opción de" u "opcionalmente" indica que el requisito se permite, sin que ello signifique que se recomienda. No implica que el fabricante deba ofrecer esta opción y que el operador de red/proveedor de servicio tenga la posibilidad de activarla. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente especificación.

La expresión "catástrofe" indica cualquier situación o emergencia crítica de origen natural o provocada por el hombre.

La expresión "dispositivo IoT" indica un dispositivo que funciona en un entorno IoT.

6 Requisitos para dispositivos IoT en el contexto de catástrofes

6.1 Requisitos generales para catástrofes

Las siguientes Recomendaciones tratan el tema de las telecomunicaciones en situaciones de catástrofe:

– [UIT-T Y.1271] la Recomendación proporciona requisitos y capacidades de red para soportar telecomunicaciones de emergencia (ET).

– [UIT-T Y.2205] la Recomendación especifica los aspectos técnicos que pueden incorporarse, de manera facultativa, en las redes de la próxima generación (NGN) para habilitar las telecomunicaciones de emergencia (ET). Se presentan asimismo los principios técnicos subyacentes para dar soporte a las ET.

Estas Recomendaciones se ocupan de los requisitos y los aspectos técnicos relativos a las telecomunicaciones de emergencia. Partiendo del principio que las aplicaciones IoT utilizarán las NGN durante una catástrofe, estos requisitos son plenamente aplicables a ellas.

De conformidad con la [UIT-T Y.2205], se recomienda el uso del protocolo de alerta común (CAP) definido en la [UIT-T X.1303] para facilitar el intercambio de información entre los sistemas de alerta.

6.2 Requisitos para dispositivos IoT

Todos los dispositivos IoT fabricados deben ser sometidos a procedimientos de prueba.

Entre dichos procedimientos se deben incluir pruebas que evalúen el funcionamiento de los dispositivos en condiciones que excedan su rango de operación normal (entre otras condiciones, la temperatura, la presión o la radiación) a fin de verificar su inocuidad para el medioambiente y su funcionamiento en situación de catástrofe. Los dispositivos IoT no deben causar complicaciones ni emergencias de otros tipos.

Las condiciones de prueba deben ser seleccionadas en base a las características de posibles emergencias en la zona de utilización.

Se requiere que los resultados de las pruebas y los posibles riesgos causados por los dispositivos cuando funcionan fuera de su rango de operación se incluyan en sus características técnicas.

Se recomienda que los nuevos dispositivos IoT cuenten con características de funcionamiento más amplias (entre otras cosas, mayor resistencia de funcionamiento a la temperatura, la humedad y la presión). Este requisito es fundamental porque las aplicaciones IoT pueden fallar a causa del imprevisible comportamiento medioambiental y sus repercusiones en los dispositivos IoT durante situaciones de catástrofe.

Se recomienda la difusión de esta práctica en dispositivos IoT ampliamente utilizados. Con las mediciones proporcionadas por los dispositivos IoT que logran funcionar durante situaciones de catástrofe se puede crear una basa de datos de mediciones de parámetros medioambientales durante catástrofes de distinta naturaleza. Estas mediciones ayudarían a sacar importantes conclusiones

sobre las diferentes etapas en una situación de catástrofe que luego se podrían tener en cuenta durante la fase de diseño de un dispositivo IoT.

7 Requisitos para el funcionamiento de aplicaciones IoT durante situaciones de catástrofe

Esta cláusula describe los requisitos que necesitan las aplicaciones IoT para funcionar durante catástrofes. Las cláusulas 7.1 a 7.3 describen en detalle los requisitos para cada una de las estrategias de funcionamiento de las aplicaciones IoT relacionadas con catástrofes, y la cláusula 7.4 describe la manera de intercambiar estrategias de funcionamiento durante la catástrofe.

A fin de mejorar la eficacia de los recursos de infraestructura asociados con el funcionamiento de aplicaciones IoT, se recomienda que estas aplicaciones empleen una o más de las siguientes estrategias de funcionamiento relacionadas con catástrofes.

Todas las estrategias parten del principio que las aplicaciones IoT no funcionan de manera normal durante situaciones de catástrofe, sino que se limitan a llevar a cabo tareas destinadas a salvar vidas.

Es posible que ocurran falsas alarmas de emergencia. De hecho, se puede cancelar el estado de emergencia (por ejemplo, si se detecta una falsa emergencia) y, en ese caso, la aplicación IoT vuelve a retomar su funcionamiento normal. El plazo para decidir si se trata de una falsa alarma (es decir, si se continúa el funcionamiento en curso o se vuelve al funcionamiento normal de la aplicación) es diferente para cada caso, depende de su complejidad.

7.1 Aplicaciones IoT con modos de funcionamiento especializados

Si una aplicación IoT tiene un modo de funcionamiento especializado, capaz de ser activado en casos de emergencia, la aplicación puede ser utilizada sin ninguna acción posterior, ni control externo. En la Figura 1 se observa el cambio en el modo de funcionamiento que se produce en las aplicaciones que siguen esta estrategia.

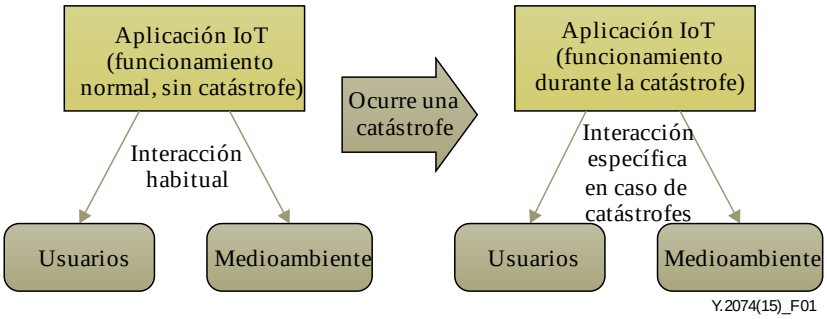

Figura 1 – Cambio de modo de funcionamiento para aplicaciones IoT con modo de funcionamiento especializado en situación de catástrofe

Las aplicaciones basadas en redes de sensores diseñadas con el fin de determinar la posición del usuario en un edificio, que además cuentan con un modo de funcionamiento especializado capaz de activarse en situaciones de catástrofe, resultan ser sumamente eficaces para la evacuación de edificios en caso de incendios, terremotos u otras catástrofes.

Otro ejemplo de esta estrategia de funcionamiento es que una de las aplicaciones IoT actúe como sistema de seguridad.

NOTA – Existen prototipos de estos sistemas de seguridad basados en tecnologías de sensores inalámbricas (como se describe en la [b-ITU-T Y.2222]), pero no se utilizan mucho debido a los complejos procedimientos de normalización y certificación que exigen los equipos de seguridad.

Se requiere que las aplicaciones IoT con modo de funcionamiento especializado activado durante situaciones de catástrofe cumplan con toda la reglamentación correspondiente.

7.2 Aplicaciones IoT que proporcionan recursos temporales a sistemas de seguridad externos

En general, las aplicaciones IoT tienen una finalidad específica y la mayoría no está pensada para asistir o ayudar a los usuarios durante una catástrofe. Como consecuencia, los recursos de las aplicaciones IoT deben recibir asistencia de los sistemas de seguridad externos a fin de mejorar la eficiencia de sus procesos de gestión de catástrofes. En la Figura 2 se observa el cambio en el modo de funcionamiento que se produce en las aplicaciones que siguen esta estrategia.

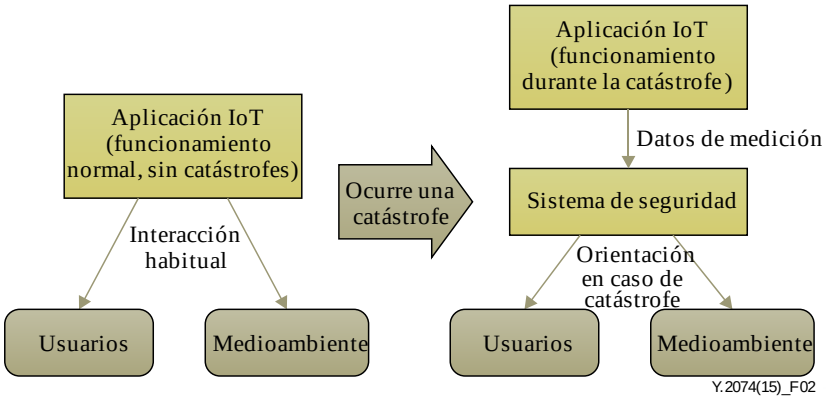

Figura 2 – Cambio de modo de funcionamiento para aplicaciones IoT que proporcionan recursos temporales a sistemas de seguridad externos durante catástrofes

Las aplicaciones IoT destinadas a usuarios que se encuentran en un edificio o en otro entorno equipado con un sistema de seguridad deben compartir temporalmente (durante la catástrofe) la capacidad de control de la aplicación IoT y todo tipo de datos de medición con el sistema de seguridad. Estos recursos pueden ser de utilidad para el funcionamiento del sistema de seguridad, entre otras cosas, los datos provenientes de diversos sensores como la temperatura y la humedad en casos de incendio.

Para simplificar la integración de las aplicaciones IoT con los sistemas de seguridad externos, se recomienda el uso del protocolo de alerta común (CAP) [ITU-T X.1303] para la interacción entre las aplicaciones IoT y los sistemas de seguridad externos. El CAP es un protocolo de comunicación bidireccional que permite la transmisión de datos de las aplicaciones IoT a los sistemas de seguridad, y la transmisión de mensajes de alerta de los sistemas de seguridad a las aplicaciones IoT.

La principal desventaja de esta estrategia de funcionamiento es la posibilidad de que falle un componente funcional de la infraestructura IoT si no está diseñado para funcionar correctamente en situaciones de catástrofe. Este tipo de fallos, en el caso de los componentes funcionales que se necesitan durante los procesos de gestión de catástrofes, puede acarrear consecuencias negativas. Estos fallos se producen debido a que no existen procedimientos de certificación específicos para los componentes funcionales de la infraestructura IoT que garanticen su funcionamiento correcto durante situaciones de catástrofe, contrariamente a los sistemas de seguridad.

7.3 Aplicaciones IoT con control de funcionamiento externo durante situaciones de catástrofe

La tercera estrategia de funcionamiento para aplicaciones IoT durante catástrofes comprende una transferencia total de las capacidades de funcionamiento y los datos de medición de las aplicaciones IoT a los sistemas de seguridad o centros de control externos.

NOTA 1 – La transferencia total de las capacidades de control significa que la propia aplicación IoT pierde el proceso de gestión de recursos.

NOTA 2 – Un centro de control externo puede ser, por ejemplo, una organización o una unidad funcional dentro de una organización que asume la plena responsabilidad jurídica y administrativa de la gestión adecuada de catástrofes en un área en particular.

En la Figura 3 se observa el cambio en el modo de funcionamiento que se produce en las aplicaciones que siguen esta estrategia.

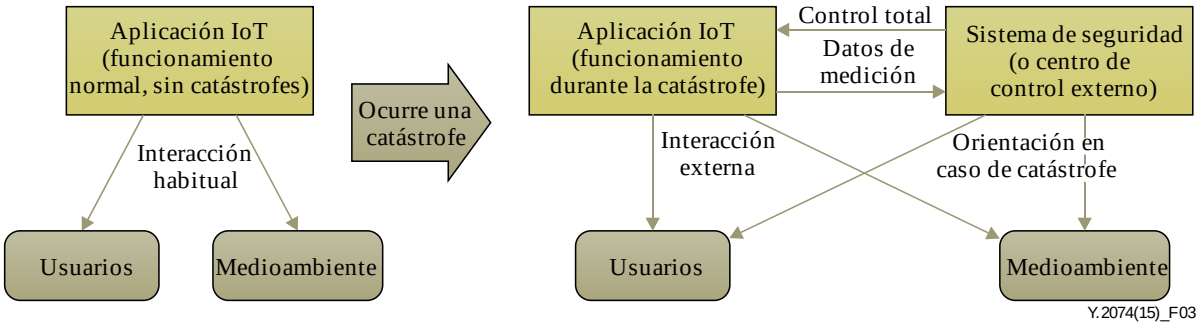

Figura 3 – Cambio de modo de funcionamiento para aplicaciones IoT con control externo durante situaciones de catástrofe

Si se compara esta estrategia de funcionamiento con el modo descrito en la cláusula 7.1, en este caso las actividades del usuario durante la catástrofe están totalmente controladas por sistemas de seguridad externos y alertas.

El objetivo principal de esta estrategia de funcionamiento es que los sistemas de seguridad o los centros de control externos utilicen de la manera más eficiente posible todos los recursos disponibles de las aplicaciones IoT, a través de una buena gestión de recursos.

En el Apéndice I se describen métodos relativos a la garantía de integridad y fiabilidad de los datos generados por los dispositivos IoT. Además, como se observa en el Apéndice I, un centro de control y supervisión de dispositivos IoT podría actuar como centro de control externo para aplicaciones IoT en esta estrategia de funcionamiento.

De manera similar a la estrategia de funcionamiento que se describe en la cláusula 7.2, se recomienda utilizar el CAP para la interacción entre las aplicaciones IoT y los sistemas de seguridad o centros de control externos en esta estrategia de funcionamiento.

7.4 Cambiar entre dos o tres estrategias de funcionamiento durante la catástrofe

En función del objetivo de la aplicación IoT y de sus capacidades, se pueden aplicar una o más estrategias de funcionamiento. Esto significa que la aplicación IoT debe contar con la capacidad de cambiar de estrategia de funcionamiento según las condiciones externas, por ejemplo, en caso de recibir señales de control o de sobrepasar los grados previstos en la lectura del sensor, entre otras cosas.

El funcionamiento de la aplicación IoT puede ser el siguiente:

En el caso de una aplicación IoT (que se encuentra en una zona geográfica determinada) y cuenta con un sistema de seguridad (externo en relación con la aplicación). Si el seguimiento de los datos del dispositivo IoT muestra que está ocurriendo una catástrofe durante el modo de funcionamiento normal, la aplicación IoT cambia automáticamente al modo especializado para situaciones de catástrofe y pone en marcha la estrategia descrita en la cláusula 7.1.

Una vez que se decide si se trata o no de una falsa alarma, la aplicación IoT puede continuar en modo especializado o volver a su funcionamiento normal (si se verifica la falsa alarma). Si continúa el modo de funcionamiento especializado, antes de que comience la etapa crítica de la catástrofe, la aplicación IoT es capaz de generar información personalizada para cada uno de los usuarios en peligro a fin de que preparen su propio rescate.

Una vez ocurrida la etapa crítica, cuando la aplicación IoT ya no puede gestionar rescates a causa de su capacidad reducida, la aplicación cambia a la estrategia de funcionamiento descrita en la cláusula 7.2 (seguimiento y transmisión de datos al sistema de seguridad externo). Esto puede ayudar a salvar vidas en la siguiente etapa de rescate de emergencia, además de supervisar el desarrollo de la catástrofe.

Apéndice I

Métodos relacionados con la garantía de integridad y fiabilidad de los datos generados por dispositivos IoT durante catástrofes

(El presente apéndice no forma parte integrante de esta Recomendación.)

Los dispositivos ubicuos IoT pueden desempeñar una función importante en la vida cotidiana e influir en las decisiones y acciones de los usuarios. De este modo, la gente puede depender de sus dispositivos IoT, sobre todo en su información y lectura de sensores, y en las acciones derivadas que repercuten en el entorno. Por consiguiente, la integridad y fiabilidad de los datos generados por los dispositivos IoT son temas de suma importancia para la IoT en general.

El problema de la integridad y la fiabilidad de los datos generados por dispositivos IoT cobra especial relevancia durante catástrofes naturales o provocadas por el hombre, cuando la integridad de los propios dispositivos IoT no está garantizada.

A fin de preservar la integridad y fiabilidad de los datos generados por los dispositivos IoT, es preciso establecer un entorno de confianza para el funcionamiento de estos dispositivos. En ese sentido, es importante determinar el grado de fiabilidad del comportamiento de los dispositivos IoT en general, por ejemplo, evitar una lectura de sensores incorrecta. Existen dos métodos para lograr este objetivo:

1) el fabricante de los dispositivos IoT es plenamente responsable de cualquier defecto en el dispositivo y garantiza su funcionamiento adecuado;
2) un centro autorizado independiente es plenamente responsable de cualquier defecto en los dispositivos que se encuentran bajo su control (su jurisdicción) y garantiza su funcionamiento adecuado;

El primer método es menos eficaz que el segundo debido a la compleja interacción que existe entre los usuarios y los fabricantes de los dispositivos IoT, por la posible variedad de dispositivos IoT provenientes de diferentes fabricantes que funcionan en una misma zona. Este problema cobra especial relevancia durante catástrofes, cuando la protección de vidas depende de la integridad y fiabilidad de los datos generados por los dispositivos IoT. Durante la catástrofe, ni los usuarios, ni los servicios de rescate, ni los dispositivos IoT podrán contactar al fabricante de cada dispositivo IoT para confirmar la integridad y fiabilidad de sus datos.

El segundo método es mucho más concreto ya que consiste en establecer centros de seguimiento y control de los dispositivos IoT. Estos centros serán responsables del buen funcionamiento de los dispositivos IoT que se encuentren bajo su jurisdicción.

I.1 Aspectos generales de un centro de seguimiento y control para dispositivos IoT

Un centro de seguimiento y control (en adelante, el Centro) para dispositivos IoT es una organización o una unidad funcional dentro de una organización que asume la plena responsabilidad jurídica y administrativa del buen funcionamiento de los dispositivos IoT que se encuentran bajo su jurisdicción. También supervisa los dispositivos IoT y almacena información sobre su funcionamiento durante situaciones de catástrofe. El objetivo principal del centro de seguimiento y control de dispositivos IoT es comprobar la integridad y fiabilidad de la información proporcionada por los dispositivos bajo su jurisdicción.

Además, el Centro es responsable de notificar rápidamente a los usuarios o dueños de los dispositivos si se identifican fallos en cualquiera de ellos.

En caso de peligro de catástrofe o durante la misma, el Centro es responsable de:

- supervisar el estado de los dispositivos IoT bajo su jurisdicción y sus datos de salida (por ejemplo, las lecturas de sensores);
- identificar aquellos dispositivos IoT que no están funcionando correctamente y notificar rápidamente a sus usuarios o dueños acerca de los fallos;
- determinar la zona, la naturaleza y los parámetros de la catástrofe, tomando en cuenta la información obtenida a partir de los dispositivos IoT bajo su jurisdicción y de fuentes de información externas (por ejemplo, agencias de emergencia);
- gestionar los dispositivos IoT bajo su jurisdicción con el objetivo de evacuar a las personas de manera segura de la zona afectada;
- registrar y almacenar la información obtenida durante la catástrofe y el historial de funcionamiento durante la catástrofe.

I.2 Traspaso de responsabilidades del centro de seguimiento y control a los centros locales

Existen grandes cantidades de dispositivos ubicuos IoT en apartamentos, casas, organizaciones, calles y lugares públicos, entre otros sitios.

En el caso de un centro de seguimiento y control para dispositivos IoT, es posible que todos los dispositivos en una misma casa o edificio se encuentren bajo la jurisdicción de un centro local. De manera similar, todos los dispositivos IoT de otra zona, por ejemplo, la misma calle, pueden ser gestionados por otros centros locales. Todos estos centros pueden ser integrados a la infraestructura del Centro principal.

La infraestructura del Centro principal se puede organizar como una pirámide de varios niveles jerárquicos con nodos de seguimiento y control responsables por los dispositivos IoT que se encuentran en diferentes edificios (centros locales), ciudades (centros municipales), regiones (centros regionales) y países (centros federales).

Además, la responsabilidad de los centros locales se puede repartir según la finalidad del dispositivo IoT. Por ejemplo, el Centro puede gestionar diversos centros locales, uno que se encargue de dispositivos IoT para el hogar, otro, de dispositivos IoT destinados a la gestión del tráfico, y un tercero, de dispositivos IoT para sistemas de seguridad, y así sucesivamente.

Las siguientes cláusulas describen diferentes hipótesis de trabajo de los centros de seguimiento y control.

I.3 Hipótesis de trabajo de los centros de seguimiento y control

El objetivo principal del Centro es comprobar la integridad y la fiabilidad de la información proporcionada por los dispositivos IoT bajo su jurisdicción. Dicho objetivo puede alcanzarse de las siguientes maneras:

1) comparar las lecturas de los sensores de los dispositivos IoT que se encuentran bajo la jurisdicción del Centro con las lecturas de redes de sensores autónomas (superposición);
2) realizar un seguimiento inteligente de las lecturas de los sensores que se encuentran bajo la jurisdicción del Centro, es decir reunir datos y realizar un análisis matemático (minería de datos) a partir de la información recibida, permitiendo así la identificación de fallos en los dispositivos IoT.

Se pueden aplicar ambos métodos y combinarlos en una proporción adecuada.

Los métodos antes mencionados se describen con mayor detalle en las cláusulas I.3.1 y I.3.2.

I.3.1 Red de sensores autónoma

El Centro utiliza redes de sensores autónomos dotadas de sensores que detectan diversos parámetros físicos que se superponen a los sensores de los dispositivos IoT bajo la jurisdicción del Centro.

La red de sensores autónomos debe cubrir toda la zona que se encuentra bajo la jurisdicción del Centro. Por ejemplo, un centro local responsable de espacios interiores debe utilizar una red de sensores que comprenda todos los dispositivos IoT ubicados en los espacios interiores dentro de la zona bajo el control del Centro.

A los sensores de esta red se los considera como sensores de referencia, es decir que sus lecturas se utilizan como valores de referencia de parámetros físicos en la zona. Se prevé que los sensores de referencia estén validados por una organización seria y adecuadamente certificada.

El Centro reúne datos a partir de los dispositivos IoT bajo su jurisdicción, y los compara con los valores de referencia. Sobre la base de esta comparación, el Centro toma sus decisiones respecto de la integridad y la fiabilidad de los datos generados por los dispositivos IoT.

La ventaja de este método es la fiabilidad potencialmente alta de los sensores de referencia que es independiente de los dispositivos IoT. Por tanto, se identifican muy precisamente los fallos de los dispositivos IoT.

En cambio, sus desventajas son el coste y la complejidad de utilizar redes de sensores autónomos y los posibles fallos de los sensores de referencia durante situaciones de catástrofe.

I.3.2 Seguimiento inteligente

El seguimiento inteligente es la compilación de la información del dispositivo y de las lecturas de sensores obtenidas a partir de los dispositivos IoT que se encuentran bajo la jurisdicción del Centro, junto con el análisis matemático de dicha información. Esto incluye, entre otras cosas, métodos de análisis estadístico y de procesamiento de señales por correlación.

El seguimiento inteligente permite identificar aquellos dispositivos IoT, o sus sensores, que se encuentran fuera de servicio dentro de un grupo de dispositivos similares.

La ventaja de este método es la independencia total de los parámetros externos del entorno, lo que permite un funcionamiento normal en cualquier situación durante la catástrofe.

La desventaja es la necesidad de contar con un grupo similar de dispositivos IoT para determinar los fallos de manera más fiable.

I.4 Uso de datos almacenados

El Centro supervisa, registra y almacena la información del dispositivo y las lecturas de sensores obtenidas a partir de los dispositivos IoT que se encuentran bajo su jurisdicción, incluidos los datos obtenidos inmediatamente antes de la catástrofe.

Esta función permite que el Centro actúe como una "caja negra" durante situaciones de emergencia. Se prevé que el Centro ayude a identificar las causas de las emergencias, igual que la caja negra en los aviones.

El historial de datos almacenado por el Centro puede ser utilizado para mejorar los métodos de seguimiento inteligente y crear métodos de gestión y control de dispositivos IoT que se encuentren en peligro de catástrofe o en una situación de catástrofe a fin de evacuar de manera segura a la mayor cantidad de gente de la zona afectada.

Bibliografía

[b-ITU-T X.674] Recomendación UIT-T X.674 (2011), *Procedimientos para el registro de arcos dentro del arco de aviso de identificador de objeto*.

[b-ITU-T Y.2001] Recomendación UIT-T Y.2001 (2004), *Visión general de las redes de próxima generación*.

[b-ITU-T Y.2060] Recomendación UIT-T Y.2060 (2012), *Visión general de la Internet de las cosas*.

[b-ITU-T Y.2222] Recomendación UIT-T Y.2222 (2013), *Redes de control de sensores y aplicaciones conexas en el contexto de las redes de próxima generación*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	**Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2017