国 际 电 信 联 盟

ITU-T

国际电信联盟
电信标准化部门

Y.2074

(01/2015)

Y系列：全球信息基础设施，
互联网的协议问题和下一代网络

下一代网络 – 框架和功能结构模型

物联网设备应用在灾害条件下操作的需求

ITU-T Y.2074 建议书

国际电信联盟

ITU-T Y系列建议书

全球信息基础设施、互联网的协议问题和下一代网络

全球信息基础设施	
概要	Y.100–Y.199
业务、应用和中间件	Y.200–Y.299
网络方面	Y.300–Y.399
接口和协议	Y.400–Y.499
编号、寻址和命名	Y.500–Y.599
运营、管理和维护	Y.600–Y.699
安全	Y.700–Y.799
性能	Y.800–Y.899
互联网的协议问题	
概要	Y.1000–Y.1099
业务和应用	Y.1100–Y.1199
架构、接入、网络能力和资源管理	Y.1200–Y.1299
传输	Y.1300–Y.1399
互通	Y.1400–Y.1499
服务质量和网络性能	Y.1500–Y.1599
信令	Y.1600–Y.1699
运营、管理和维护	Y.1700–Y.1799
计费	Y.1800–Y.1899
下一代网络中的IPTV	Y.1900–Y.1999
下一代网络	
框架和功能体系模型	**Y.2000–Y.2099**
服务质量和性能	Y.2100–Y.2199
业务方面：业务能力和业务架构	Y.2200–Y.2249
业务方面：NGN中业务和网络的互操作性	Y.2250–Y.2299
编号、命名和寻址	Y.2300–Y.2399
网络管理	Y.2400–Y.2499
网络控制体系和协议	Y.2500–Y.2599
基于分组的网络	Y.2600–Y.2699
安全	Y.2700–Y.2799
通用移动性	Y.2800–Y.2899
运营商级别开放环境	Y.2900–Y.2999
未来网络	Y.3000–Y.3499
云计算	Y.3500–Y.3999

欲进一步了解详细信息，请查阅ITU-T建议书清单。

ITU-T Y.2074 建议书

物联网设备应用在灾害条件下操作的需求

摘要

不同于ITU-T Y.2066建议书中对物联网的普通需求，ITU-T Y.2074建议书提出了物联网设备应用在灾害条件下操作的需求。它也提出了物联网应用在灾害发生时的操作需求。

为了在灾害发生时使用物联网设备和物联网应用进行疏散和营救，必须制定这些需求。

附录I介绍了灾害条件下保证物联网设备产生的数据完整且可靠的相关方法。

本建议书与物联网应用开发者和物联网服务提供者以及应急服务提供者相关。

历史沿革

版本	建议书	批准日期	研究组	唯一标识*
1.0	ITU-T Y.2074	2015-01-13	13	11.1002/1000/12421

关键词

灾害、物联网、物联网应用、物联网设备、要求、安全系统。

* 如欲访问建议书，请在您的网络浏览器地址栏中输入URL http://handle.itu.int/，然后输入建议书的唯一标识。例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

引言

每种新的信息通信技术（ICT）均以为用户带来效用为诉求，故而，即使在发生灾害时，ICT亦应力求为抢险救人创造条件。事实上，用户有时根本无暇等待救援队伍或外部援助的到来。在此情况下，唯一的办法就是用户努力自救，以设法尽快离开灾区。因此，有必要针对灾害期间的物联网（IoT）设备以及物联网应用的操作制定相关要求，在此类应用正常操作的状态下亦概莫能外。实际的情况是，当灾害发生时，物联网应用通常变得毫无价值可言，此时物联网用户的迫切目标是实现自救。鉴于物联网基础设施已得到广泛部署，故其技术资源对挽救生命而言可能颇具价值。

从实用角度看，开发并顺利部署新的应急安全系统可谓相当为棘手，原因是灾害管理工作需要实施复杂的标准化和认证程序。然而，较易做到的是提高现有安全系统的能力及其在灾害中支撑物联网应用的能力。此外，物联网服务亦可与现有安全系统结合起来，并在灾害期间通过安全系统发挥作用。

须指出，新的物联网智能系统永远无法取代多年来经过数番测试和认证的现有安全系统；不过，新的物联网智能系统具备与现有安全系统交互的能力。在灾害期间，通过现有安全系统的管理中心来管理物联网应用在技术上仍然可行。

当上述能力得到强化的物联网应用与现有安全系统之间进行交互时，预计会有助于灾害期间救援程序（如告警和疏散）的实施。

ITU-T Y.2074 建议书

物联网设备应用在灾害条件下操作的需求

1 范围

除[ITU-T Y.2066]建议书在物联网方面的通用要求外，本建议书针对可在灾害情况下用来操作物联网应用的物联网设备提出了要求，此外亦针对灾害期间物联网应用的操作提出了特殊要求。

本建议书的范围包括以下要求：

- 灾害发生时的物联网设备；
- 灾害期间物联网应用的操作（针对三种已确定的操作策略）。

附录I介绍了在灾害发生时保障物联网设备产生的数据的完整性和可靠性的方法。

该建议书与物联网应用开发者和物联网服务提供者以及应急服务提供者相关。

2 参考文献

下列ITU-T建议书和其他参考文献的条款，因在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均可能被修订，本建议书的使用者应查证是否有可能使用下列建议书或其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用的文件自成一体时不具备建议书的地位。

[ITU-T X.1303] ITU-T X.1303建议书（2007），共同告警协议（CAP 1.1）。

[ITU-T Y.1271] ITU-T Y.1271建议书（2004），支持对不断变化的电路交换和分组交换网络的应急通信网络的网络要求和能力框架。

[ITU-T Y.2066] ITU-T Y.2066建议书（2014），物联网共同要求

[ITU-T Y.2205] ITU-T Y.2205建议书（2011），下一代网络 – 应急通信 – 技术设想

3 定义

3.1 其他地方定义的术语

本建议书使用以下其他地方定义的术语：

3.1.1 预警[ITU-T X.674]：有关即将发生的危险或问题的告警或警告信息。

3.1.2 设备[ITU-T Y.2060]：在物联网中，具有强制性通信能力和选择性传感、执行、数据捕获、数据存储和数据处理能力的设备。

3.1.3 应急通信（ET）[ITU-T Y.2205]：应急通信指任何相对于其他业务而言需要下一代（NGN）特别处理的与应急相关的服务。它包括政府授权的应急服务和公共安全服务。

3.1.4 物联网（IoT）[b-ITU-T Y.2060]：信息社会全球基础设施（通过物理和虚拟手段）将基于现有和正在出现的、信息互操作和通信技术的物质相互连接，以提供先进的服务。

注1 – 通过使用标识、数据捕获、处理和通信能力，IoT充分利用物体向各项应用提供服务，同时确保满足安全和隐私要求。

注2 – 从广义而言，IoT可被视为技术和社会影响方面的愿景。

3.1.5 下一代网络（NGN）[b-ITU-T Y.2001]：下一代网络（NGN）是能够利用多种宽带和具有服务质量（QoS）机制的、向用户提供电信业务的分组网络。该网络中提供的与业务相关的功能独立于底层与传输相关的技术。该网络允许用户不受限制地接入网络，可自由选择服务提供商或其业务。它支持一般移动性，允许向用户提供一致、普遍的服务。

3.2 本建议书定义的术语

本建议书定义了如下术语：

无。

4 缩略语和首字母缩略词

本建议书使用以下缩略语和首字母缩略词：

CAP 共同告警协议

ET 应急通信

ICT 信息通信技术

IoT 物联网

NGN 下一代网络

5 惯例

在本建议书中：

关键词“须”（is required to）指必须严格遵守的要求，如果宣称符合本文件，就不得违反。

关键词“建议”（is recommended）指建议但并非需要绝对遵守的要求。因此宣称符合本文件不需要说明已满足此要求。

关键词“选择性的”（optionally）可能和（may）指允许的选择性的要求、但并非建议遵守。该术语并非意在要求销售商实施该选项，网络运营商/业务提供商可选择性提供该功能。销售商选择性提供该项功能，同时仍根据宣称符合规范。

关键词“灾害”指因自然或人为原因引起的任何形式的危急或紧急情况。

关键词“物联网设备”指物联网环境中的设备。

6 灾害发生时对物联网设备的要求

6.1 关于灾害的一般要求

以下建议书与救灾通信有关：

– [ITU-T Y.1271]支持应急通信的网络要求和能力的基本框架

– [ITU-T Y.2205]本建议书对在下一代网络（NGN）内实现应急通信（ET）可能适用的技术设想做出规范。此外，本建议书还概括了支持应急通信的根本技术原则。

上述建议书阐述了对应急通信的要求和相关技术问题。假设物联网应用在灾害期间将使用下一代网络作为电信基础设施，则对此类应用将可全面适用上述要求。

根据ITU-T Y.2205]，建议使用[ITU-T X.1303]建议书中定义的共同告警协议（CAP），以在告警系统之间实现信息交互。

6.2 对物联网设备的要求

所制造的各类物联网设备均须通过测试程序。

测试程序应包括在超出操作范围（如：温度、压力、辐射）的条件下对物联网设备进行的测试，以验证物联网设备在灾害期间相对于环境和人类的安全性。不得因使用物联网设备而造成灾情的复杂化或进而发生其他类型的灾情。

应根据物联网设备部署区域可能发生灾情的特性来选择相应的测试条件。

在设备的技术特性中需要介绍在超出设备操作范围后会导致哪些测试结果和潜在危险。

在开发新的物联网设备时，建议令其操作特性（如：工作温度、湿度、压力）具有扩展范围。对物联网应用而言，对物联网设备扩展操作特性范围的要求可谓至关重要。由于灾害期间环境行为的不确定性及其对物联网设备的影响，物联网应用可能会因此失效。

建议在广泛采用的各类物联网设备上普及上述做法。在灾害期间，通过操作物联网设备进行测量，则不同性质环境参数的测量结果便可汇集成库。此类测量结果将有助于就灾情的各个阶段做出重要结论，而在物联网设备的设计阶段亦可利用这些测量结果。

7 对灾害期间物联网应用的操作要求

本节介绍对灾害期间物联网应用的操作要求。应特别指出，第7.1至7.3节介绍针对灾害所涉物联网应用的三种已确定操作策略的要求，第7.4节则介绍灾害期间在两种或两种以上操作策略之间的切换情况。

为提高与物联网应用操作有关的基础设施资源的效率，建议物联网应用实施以下一种或多种与灾害有关的操作策略。

所有策略均假设在灾害期间物联网应用不会继续正常操作，而仅执行救人任务。

可能会发出假紧急告警，此时可能会取消紧急状态（如已检测到紧急情况为虚惊一场），而物联网应用亦会切换回正常操作。决定告警真假与否（继续目前的操作或切换回正常操作）所需的时长对所实施的每种特定策略而言不尽相同，这取决于相关策略的复杂程度。

7.1 具有专用操作模式的物联网应用

若物联网应用具有可在紧急情况下启动的专用操作模式，则可在没有任何进一步行动或外部控制的情况下使用此类操作模式。图1显示了采用这一策略的物联网应用在操作模式方面的变化情况。

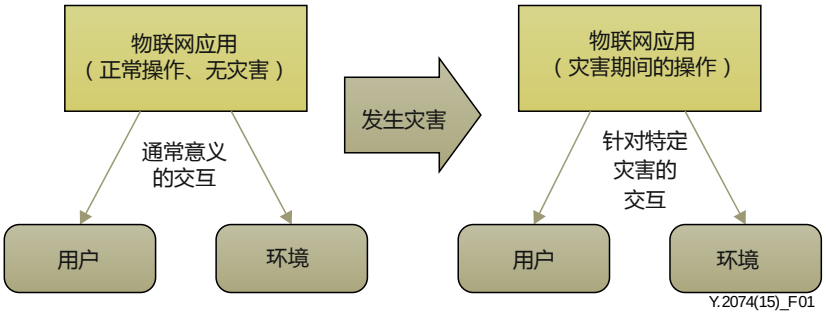

图1 – 具有在灾害时启动的专用操作模式的物联网应用操作模式的变化情况

传感器网络应用旨在实现楼宇内的用户定位，并具有在灾害时启动的专用操作模式。当发生火灾、地震或其他灾害时，此类应用对在楼宇里完成自行疏散可能颇具效用。

此操作策略的另一范例是：其中的一种物联网应用可作为安全系统使用。

注 – 目前已存在此类基于无线传感器技术的安全系统的原型（如[B-ITU-T Y.2222]所述），但这些系统并未得到广泛使用，原因是安全系统设备的标准化和认证程序旷日持久且错综复杂。

具有在灾害期间启动的专用操作模式的物联网应用须遵守各类相关监管规定。

7.2 暂时向外部安全系统提供资源的物联网应用

物联网应用一般均具有特定用途，且在多数情况下，其目标并非在灾害期间为用户提供协助或援助。因此，要利用物联网应用的资源，应由外部安全系统提供协助，以提高灾害管理工作的效率。图2显示了采用这一策略的物联网应用的操作模式的变化情况。

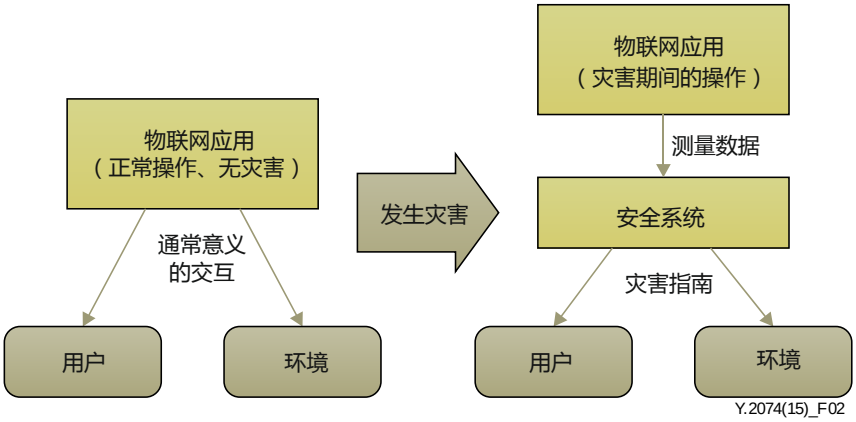

图2 – 在灾害期间暂时向外部安全系统提供资源的物联网应用操作模式的变化情况

对为配有安全系统的楼宇或其他环境中的用户而设计的物联网应用而言，应能（在灾害期间）暂时与安全系统共享物联网应用控制能力和各种测量数据。上述资源可能有助于安全系统的操作，如火灾时的温度和湿度等来自各种传感器的数据。

为简化物联网应用与外部安全系统的集成工作，建议使用CAP [ITU-T X.1303]来实现物联网应用与外部安全系统之间的交互。CAP是一种双向通信协议，可实现从物联网应用到安全系统的数据传输，以及从安全系统到物联网应用的告警消息传输。

此操作策略的主要缺点是：若在设计时不支持在灾害期间正确操作，在物联网基础设施的功能组件或会发生故障。对灾害管理工作所需的功能组件而言，此类故障可能会造成负面影响，而发生此类故障的可能性却的确存在，原因是：在确保在灾害期间的正确操作方面，针对物联网基础设施的功能组件没有任何特殊认证程序，而针对安全系统却具有经认证的程序。

7.3 在灾害期间具有外部操作控制的物联网应用

灾害期间物联网应用的第三种操作策略涉及控制能力和测量数据从物联网应用到外部安全系统或外部控制中心的完整传输。

注1 – 控制能力的完整传输意味着物联网应用本身已终止资源管理过程。

注2 – 例如，外部控制中心可能是为在某一领域进行正确灾害管理而承担全面法律和行政责任的机构或机构的功能单位。

图3显示了采用此操作策略的物联网应用的操作模式的变化情况。

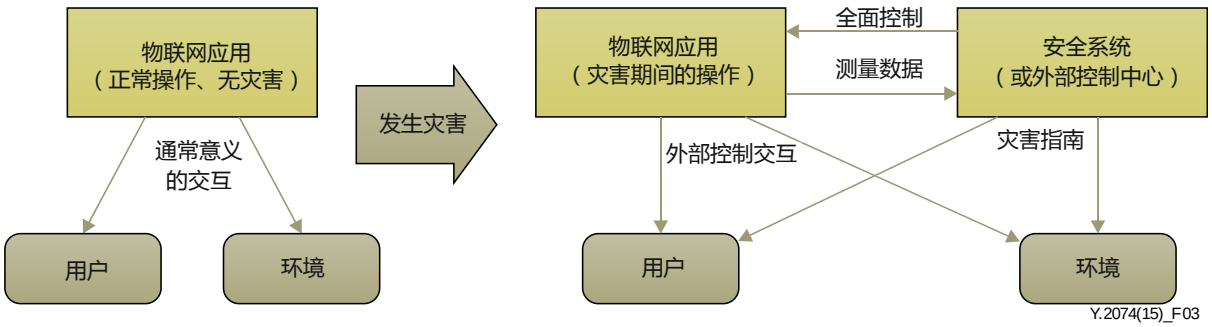

图3 – 在灾害期间具有外部操作控制的物联网应用操作模式的变化情况

在此操作策略中，对采用第7.1节所述操作模式的物联网应用而言，灾害期间的用户行为完全由外部安全系统和告警进行控制。

此操作策略的主要目的是：通过适当的资源管理，经由安全系统或外部控制中心来确保物联网应用的各类可利用资源均可得到最有效的利用。

附录I介绍了保障物联网设备所产生数据的完整性和可靠性的方法。附录I所述的物联网设备监控中心亦可用作采用此操作策略的物联网应用的外部控制中心。

与第7.2节所述的操作策略类似，建议使用CAP [ITU-T X.1303]来实现物联网应用和此操作策略中的外部安全系统或外部控制中心之间的交互。

7.4 灾害期间两种或两种以上操作策略之间的切换

根据物联网应用的目的及其能力，可在物联网应用中部署一种或多种操作策略的组合。这涉及物联网应用在出现某些外部条件（如接收控制信号、传感器读数超过规定量级等）的情况下在操作策略之间进行切换的能力。

例如，可通过如下方式来实现物联网应用的操作：

在此考虑的是配有（相对于物联网应用而言的外部）安全系统的（某一地理区域内的）某一物联网应用。若物联网设备的数据监测显示在正常操作期间出现了紧急情况，则物联网应用将自动切换到在灾害期间操作的专用操作模式，并实施第7.1节所述的策略。

在假告警决策时间结束后，物联网应用继续在专用操作模式下操作或切换回正常操作模式（在假告警情况下）。若物联网应用继续在专用操作模式下操作，则在灾害具有破坏力的阶段到来之前，物联网应用将为灾害波及的所有人生成量身定制的信息，以对他或她的救援工作进行管理。

一旦灾害进入了具有破坏力的阶段，则当物联网应用因能力下降而无法管理救援工作时，物联网应用将切换到第7.2节（监控收集到的数据并将其传输到外部安全系统）所述的操作策略。这可能有助于在随后的应急救援阶段拯救生命，并对灾情的进展进行监控。

附录I

保障灾害期间物联网设备所产生数据的完整性和可靠性的方法

（本附录不构成本建议书的组成部分）

无处不在的物联网设备可在人们的日常生活中发挥重要作用，并对人们的决策和行动产生影响。因此，人们可能会对物联网设备形成依赖性，这一点在物联网设备所提供的信息和传感器读数及其影响环境的衍生行动方面体现得尤其明显。因此，对宏观意义上的物联网而言，物联网设备所产生数据的完整性和可靠性是非常重要的问题。

在自然和人为灾害期间，物联网设备的完整性本身可能无法得到保障，这凸显了物联网设备所产生数据的完整性和可靠性问题的现实意义。

为确保物联网设备所产生数据的完整性和可靠性，必须为物联网设备的操作营造可信环境。为此，须就物联网设备确定一般行为责任的范围，（如在不正确的传感器读数方面）。为实现此目标，可采用两种方法：

1. 物联网设备制造商对物联网设备发生的任何故障负全责，并保证物联网设备行为的适当性；
2. 经授权的独立中心对其控制下（其管辖下）的物联网设备的故障负全责，并保证物联网设备行为的适当性。

第一种方法不如第二种方法有效，原因是在用户和对用户物联网设备负责的制造商之间存在复杂的交互关系，且在同一部署区域可能会使用来自不同制造商的各种物联网设备。在灾害期间，这一问题变得尤为重要，原因是此时物联网设备所产生数据的完整性和可靠性会成为攸关人类生命的问题。在灾害期间，为确认设备数据的完整性和可靠性，用户、救援服务或物联网设备均无法与每种特定物联网设备的制造商取得联系。

第二种方法更加具体，原因是其要求建立物联网设备监控中心。此类中心将负责其管辖下的物联网设备的正确操作。

I.1 物联网设备监控中心的总体概述

物联网设备监控中心（中心）是对其管辖下的物联网设备的正确操作承担全部法律和行政责任的机构或机构的功能单位，此类中心负责在灾害期间监测物联网设备及存储与操作有关的信息。物联网设备监控中心的主要目的是检查其管辖下的物联网设备所提供信息的完整性和可靠性。此外，若识别到有物联网设备出现故障，则中心亦将负责将有关情况及时通知物联网设备的用户和/或所有者。

在出现灾害威胁的情况下或在灾害期间，中心的职责是：

- 监测其管辖的物联网设备的状态及其输出数据（如传感器读数）；
- 识别操作不当的物联网设备，并将故障及时通知用户和/或所有者；

- 确定灾害方位及灾害的性质和参数，同时考虑到其管辖的物联网设备获得的信息和外部信息源（如应急机构）；
- 管理其管辖的物联网设备，以使受灾民众安全撤离灾区；
- 记录并存储灾害期间获得的信息以及灾害期间的操作历史。

I.2 将监控中心的职责分配到地方中心

在公寓、住宅、机构、街道、公共场所等都遍布着大量的物联网设备。

对物联网设备监控中心而言，一栋特定住宅或楼宇内的所有物联网设备可能受一个地方中心的管辖。同样，在其他区域（如：在同一条街上）的所有物联网设备可由其他地方中心进行管理。所有这些地方中心均可整合至根中心的基础设施。

根中心的基础设施可被组织成包含负责不同楼宇（地方中心）、城市（市中心）、区域（区域中心）和国家（联邦中心）内的物联网设备的多层面监控节点的多层次结构。

此外，地方中心承担的职责可在物联网设备用途的基础上进行分配。例如，中心可管理多个地方中心，其中一个地方中心负责家庭用途的物联网设备，另一个地方中心负责交通管理用途的物联网设备，第三个地方中心则负责安全系统用途的物联网设备等。

以下各节介绍了监控中心的可能工作场景。

I.3 监控中心的工作场景

中心的主要目的是检查其管辖的物联网设备所提供信息的完整性和可靠性。此目标可通过以下方式来实现：

1. 将中心管辖的物联网设备的传感器读数与自主（经复制）传感器网络的读数进行比较；
2. 对中心管辖的传感器读数进行智能监控，其中包括对所获得信息进行的数据收集和数学分析（数据挖掘），以对物联网设备发生的故障加以识别。

这两种方法可以适当比例结合起来加以实施和使用。

关于上述方法的更详细介绍见第I.3.1和I.3.2节。

I.3.1 自主传感器网络

中心将部署包含具有各种物理参数的传感器的自主传感器网络，该网络可对中心管辖的物联网设备的传感器进行复制。

自主传感器网络须覆盖中心管辖的整个区域。例如，一个地方室内中心应部署覆盖包含中心控制下的物联网设备的室内面积的传感器网络。

此自主传感器网络的传感器被视作参考传感器，即：其读数将被作为此区域物理参数的参考值。参考传感器预计会得到经适当认证的可信机构的认证。

中心从其管辖的物联网设备收集数据，并将此类数据与参考值进行比较。根据上述比较结果，中心将就物联网设备所产生数据的完整性和可靠性做出决定。

这种方法的优点是独立于物联网设备的参考传感器可能会具有较高的可靠性，故其在识别物联网设备的故障方面具有较高的准确性。

这种方法的缺点是在灾害期间部署自主传感器网络的成本较高，且部署过程较为复杂，同时，参考传感器亦可能会发生故障。

I.3.2 智能监控

智能监控包括收集从中心管辖的物联网设备获得的设备信息和传感器读数，以及对这些信息进行数学分析。这包括但不限于：统计分析和相干信号处理方法。

智能监控允许在一组类似的设备内识别乱序的物联网设备或其传感器。

这种方法的优点是完全独立于环境的外部参数，且在灾害期间可在各种情况下进行操作。

这种方法的缺点是需要一组类似的物联网设备，以对故障进行更可靠的判断。

I.4 所存储数据的使用

中心对从其管辖的物联网设备获取的设备信息和传感器读数进行监控、记录和存储，其中包括在灾害发生前夕和灾害期间获得的信息和读数。

此功能允许中心在紧急情况下作为“黑匣子”进行操作，即假定中心可帮助确定紧急情况发生的原因，这与飞机黑匣子的作用类似。

在出现灾害威胁的情况下或在灾害期间，中心数据库收集的历史数据可用于改进智能监控方法及开发物联网设备管理和控制方法，以竭尽所能地将人群疏散到安全地区。

参考书目

[b-ITU-T X.674] ITU-T X.674 (2011)建议书，告警对象标识符弧下的弧登记程序。

[b-ITU-T Y.2001] ITU-T Y.2001 (2004) 建议书，下一代网络的总体概述。

[b-ITU-T Y.2060] ITU-T Y.2060 (2012) 建议书，物联网概述。

[b-ITU-T Y.2222] ITU-T Y.2222 (2013) 建议书，下一代网络环境中的传感器控制网络和相关应用。

ITU-T 系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络操作、电话业务、业务操作和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听和多媒体系统
I系列	综合业务数字网
J系列	有线网和电视、声音节目和其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话设备、本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	**全球信息基础设施、互联网的协议问题和下一代网络**
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2016年，日内瓦