中国移动NB-IoT安全白皮书

中国移动

2017 年 11 月

目 录

1. 引言

在万物互联时代，人们期待借助物联网实现人与物和物与物之间的信息交互和通信，进而获得更为便捷的生活体验。物联网是互联网的延伸，其应用范围覆盖了个人穿戴、家庭安防、交通物流、智慧城市、工业制造、智慧金融、智能家居、环境监测等行业，为信息通信产业开拓了全新空间。

蜂窝物联网的主要应用场景有两类：一是智慧城市、智能家居、环境监测等行业应用，对速率要求不高，但需要待机时间长、模组成本低、覆盖能力强的物联网技术，NB-IoT 是此场景常用的技术。二是交通物流、个人穿戴等应用，对速率要求较高，需要支持移动性、支持语音的物联网技术，eMTC 是此场景常用的技术。此外，在 NB-IoT、eMTC 等低功耗物联网成熟之前，传统 2/3/4G 网络也常被用于接入各类物联网设备，实现通信需求。

在我国大力推进 NB-IoT 物联网基础设施建设之时，也应注意到网络信息安全问题给物联网的发展提出了全新的挑战。本白皮书基于物联网业务安全需求及应用场景，重点分析了当前正在大力建设的 NB-IoT 所面临的安全问题，提出了 NB-IoT 安全技术需求和安全架构，以期推动产业链在相关方面达成一致，尽快攻克核心技术难题，从而促进 NB-IoT 物联网健康持续发展。

1.1 业务简介

随着业务不断创新和快速发展，NB-IoT 在“云-管-端”模式的网

络体系结构之上，与各行业融合，衍生出了丰富多彩的物联网业务，共同形成“业务+云管端”的体系结构。其中，业务由物联网与传统行业融合而成，应用 NB-IoT 技术实现业务统一控制；“云”由开放平台组成，通常利用云计算技术实现数据统一传送、数据统一存储、设备连接统一管理；“管”即 NB-IoT 网络，提供各种网络接入和数据传输通道；“端”是各种类型的 NB-IoT 终端设备。

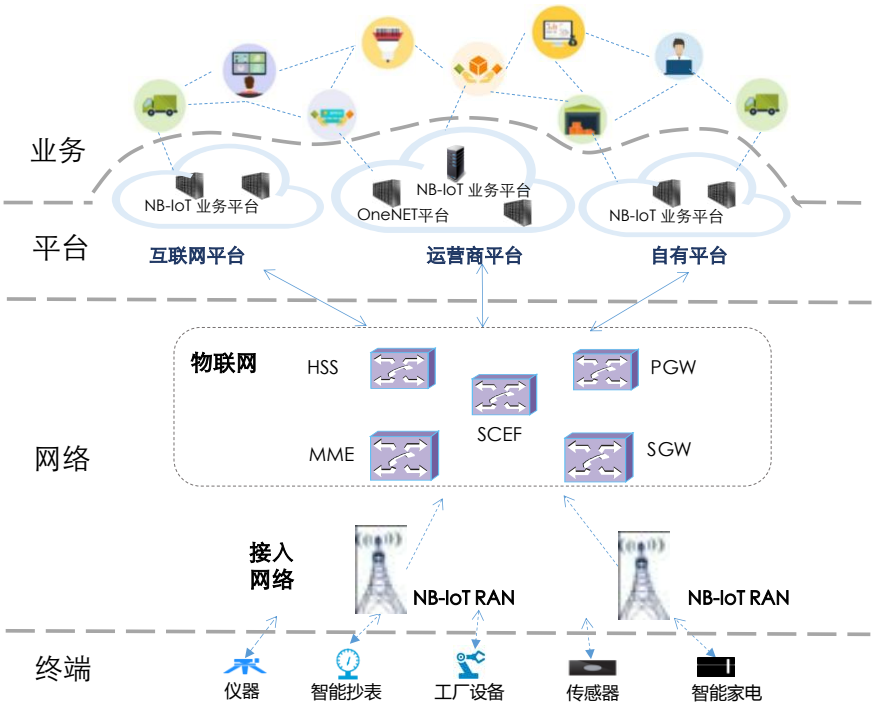

图 1 典型 NB-IoT 业务体系架构

1.2 特点分析

NB-IoT 业务的主要特点包括以下几点：

连接海量化。据 Gartner 预测，到 2020 年全球将有 260 亿物联网设备，市场价值超过 3000 亿美元，而 DHL 和思科联合发布的报告则预测到 2020 年物联网的连接数将达到 500 亿。中国移动十三五规划

提出到2020年蜂窝物联网连接规模超过5亿。

业务碎片化。NB-IoT与个人及家庭生活、工业生产深度融合，应用场景多，产业链中的终端、网络、芯片、操作系统、平台、业务等的具体实现各不相同，各类应用场景的业务规模、终端功能、数据种类也存在差异，“碎片化”现象严重。

服务开放化。NB-IoT业务平台既有运营商平台也有互联网或用户自建的平台，可满足各种业务需求；同时，部分业务需要运营商开放云计算、位置查询、设备状态查询、认证等必要能力，使得运营商网络更加开放。因此，NB-IoT 服务模式与传统的通信服务模式有较大不同，产业链将更长且不断产生各类新兴的商业模式，也相应地提出了新的网络信息安全需求。

1.3 行业现状

近年来,我国政府高度重视物联网发展，积极推进科技创新。2016年12月，工业和信息化部印发的《信息通信行业发展规划（2016－2020年）》中，提出要“建设完善窄带物联网（NB-IoT）基础设施，实现在城市运行管理和重点行业的规模应用”。

2017年6月，工业和信息化部办公厅发布的《关于全面推进移动物联网(NB-IoT)建设发展的通知》指出，建设广覆盖、大连接、低功耗的移动物联网基础设施，有助于推进网络强国和制造强国建设，同时要求，加快推进网络部署，构建NB-IoT网络基础设施，到2017年末，实现NB-IoT网络覆盖直辖市、省会城市等主要城市，基站规模

达到 40 万个；到 2020 年，NB-IoT 网络实现全国普遍覆盖，面向室内、交通路网、地下管网等应用场景实现深度覆盖，基站规模达到 150 万个。

在 NB-IoT 商用进程方面，中国移动已在全国 346 个城市启动移动物联网建设，2017 年底前实现部分重点城市商用。2017 年 5 月，在中国电信物联网发展政策恳谈会上，中国电信宣布在 6 月底建成全球首个全覆盖的 NB-IoT 商用网络，并率先开展 NB-IoT 商用放号；2017 年 8 月，在中国联通物联网大会上，中国联通宣布已在全国数十城市完成了 NB-IoT 试商用开通，全国 300 多个城市具备快速接入 NB-IoT 网络的能力。依托 NB-IoT 技术，物联网的规模化商用将全面提速。

在 NB-IoT 业务快速发展的同时，也存在着产业链发展不均衡的问题，例如芯片模组产业落后于网络设备产业及网络建设速度、终端入网测试进度与终端规模增长速度不一致等，这些问题也一定程度上会影响到 NB-IoT 的网络信息安全水平。

2. 风险分析

由于 NB-IoT 业务广泛涉及通信网络、大数据、云平台、移动 APP、WEB 等技术，其本身也沿袭了传统互联网的安全风险，加之 NB-IoT 终端规模十分巨大、升级困难，传统安全问题的危害在此环境下会被急剧放大。因此，作为一种全新的技术，NB-IoT 也面临着前所未有的安全风险。

2.1 业务风险分析

（1） 业务防护能力不足

物联网业务种类多，规模差别大，安全投入不均衡，部分业务防护能力不足，影响业务安全运行。

（2）业务漏洞风险大

NB-IoT 与各行业深度融合，业务逻辑复杂，应用协议多样，容易存在业务漏洞。

（3） 业务滥用风险高

NB-IoT 业务场景复杂，导致卡及终端形态多样，存在插拔式卡、嵌入式卡等形态，容易被恶意利用。例如使用插拔式卡的终端难以预防机卡分离，存在被用于发送垃圾短信等业务滥用的风险。

2.2 平台风险分析

（1）越权操作风险

大量 NB-IoT 应用运行在一个集中的平台上，如果没有进行有效的安全隔离和访问控制，容易引发不同应用之间的越权访问和操作。另外，如果没有对不同用户、设备进行有效隔离，也可能导致不同用户、设备之间的越权访问。

（2）数据泄露风险

多数 NB-IoT 应用的数据会集中存储在统一的物联网平台，并通过统一的平台对终端进行控制。若平台被恶意攻陷，就会导致大规模数据泄露，甚至大量终端设备被控制，进而影响工业生产及社会生活。

（3）边界模糊风险

NB-IoT 与工业制造等行业融合过程中，工业设备通过 NB-IoT 网络接入业务平台，重要生产数据通过公网传输，打破了传统工业网络封闭、隔离的安全边界，安全边界变得模糊，安全防护难度大大增加。

2.3 网络风险分析

（1）设备规模巨大易引发大规模网络攻击

NB-IoT 终端设备规模巨大，且分散安装、甚至位于户外，难以进行统一管理，一旦大量设备被恶意控制，就可能对其他网络系统发起大规模 DDoS 攻击，甚至导致大规模断网，传统安全问题的危害会被急剧放大。

（2）公网传输导致重要数据泄露风险

物联网应用的各类采集数据通过 NB-IoT 网络上传到对应的业务平台，传输过程跨越多个网络，经由大量网元进行处理，存在重要数据泄露的风险。

（3）应急管控不足造成危害难以及时消除

传统短信、数据、语音等通信功能管控依据单一设备、单一功能、单一用户进行，而 NB-IoT 终端规模大，且不同业务的短信、数据等通信功能组合较多，若不能在网络侧通过地域、业务、用户等多维度实施通信功能批量应急管控，则无法应对海量终端被控引发的风险。

（4）通信网络面临复杂攻击的风险

NB-IoT 核心网一般与互联网相对隔离，网元之间相互信任而没有

采取认证机制，随着网络更加开放化以及跨运营商网络之间的通信需求，NB-IoT 核心网也会面临信令伪造、篡改、重放攻击等风险，核心网与互联网接口也会面临来自互联网的各种攻击。同时，大量终端接入网络也可能对核心网络发起攻击，影响业务运行。

2.4 终端风险分析

（1）终端易被接触导致隐私泄露

NB-IoT 应用与人们的工作生活息息相关，而部分终端设备在户外部署，易被接触到，可能导致终端数据被非法获取而泄露用户隐私。另外，与业务安全紧密相关的密钥存储在终端，也容易被非法获取。

（2）计算能力受限导致易被恶意控制

NB-IoT 设备受成本限制，通常计算能力较弱，无法实现安全级别高的认证机制、安全算法，抵御暴力破解等攻击的能力差，容易被恶意控制。

（3）系统升级复杂导致设备“带病”运行

NB-IoT 终端操作系统及应用软件均可能存在安全漏洞，并且 NB-IoT 设备部署位置通常比较分散，现场系统升级方式不易实施，而远程升级一旦失败就会影响业务正常运营。同时，大部分安全漏洞并不影响终端用户的业务运行，因此，用户升级意愿较低，导致大量设备会长期“带病”运行，极容易被黑客恶意控制。

2.5 管理风险分析

（1）安全责任不清

NB-IoT 产业链包括设备制造商、网络运营商、平台运营商、用户等角色，发生安全事件时可能存在安全责任不清的问题。例如，终端设备在设备制造商出厂时就存在安全隐患，设备归用户所有，使用运营商的网络接入平台，而用户在使用时未及时升级，终端被恶意控制后产生了危害，产业链中各角色的安全责任不清晰。

（2）安全意识不足

NB-IoT 设备通常由用户进行管理，普通用户安全意识缺失容易导致弱口令、安全配置缺陷等问题，进而引发安全事件。

（3）安全分级缺失

涉及国家安全、国土资源、公共秩序等的重要物联网应用与个人普通物联网应用使用统一的网络和业务平台承载，若分级防护缺失，在受到攻击时，无法保障重要应用的安全。

（4）安全标准不统一

目前尚未形成全面的覆盖产业链的 NB-IoT 安全标准，平台、终端安全防护能力参差不齐，无法按照统一的标准进行体系化安全防护。

3. 总体目标

在大力推动 NB-IoT 发展与普及的同时，针对物联网面临的各种安全风险，应构建积极的安全风险防御体系，将安全防护措施贯穿于 NB-IoT 业务的全生命周期，实现 NB-IoT 全业务、全流程、端到端的

安全管控。

NB-IoT 是互联网的延伸，其业务涉及 WEB、移动 APP、云平台、大数据相关技术，需要实现对业务、平台、网络、终端各层的安全防护:

1、 **业务防滥用。**对不同行业的 NB-IoT 应用都能提供有效的安全保障，减少业务滥用及业务攻击带来的危害。

2、 **平台防入侵。**平台应具备检测及阻止入侵的安全措施，以防止发生大规模数据泄露以及通过平台恶意控制设备等事件。

3、 **网络防攻击。**NB-IoT 网络需具备强度较高的身份认证机制，防止设备认证绕过等攻击；同时，需要防止大量终端设备被控制引发的 DDoS 等网络攻击。

4、 **终端防被控。**NB-IoT 终端需要防止被盗窃、被控制，进而防止终端用户隐私数据被窃取、终端被篡改仿冒。

4. 安全框架

NB-IoT 安全框架包括终端安全、网络安全、平台安全和业务安全四个部分，四部分安全能力结合，实现业务端到端安全，如图 2 所示。

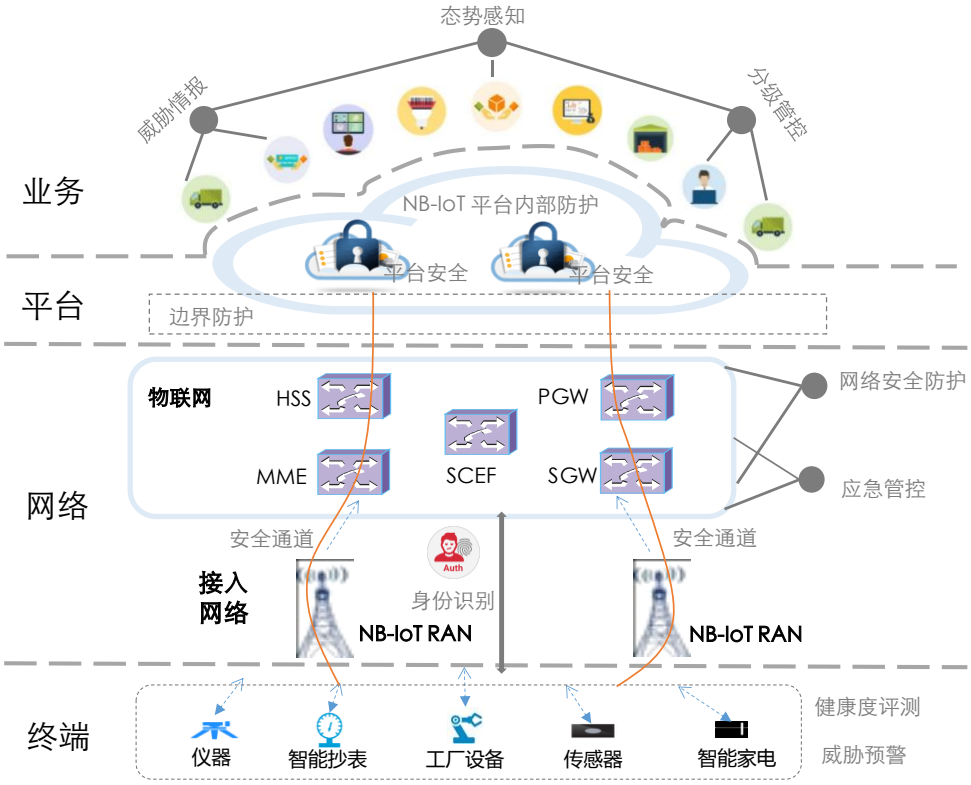

图 2 NB-IoT 安全技术架构

- **业务安全：**具备业务分级管控能力，满足不同业务的安全需求，并能基于终端、网络、平台的安全状态及业务运行情况，打造 NB-IoT 业务安全态势感知能力。同时，能够基于威胁情报交换、共享，预防业务安全事件。
- **平台安全：**包括边界防护、平台自身安全防护等能力，并能够为大规模数据在存储、传输、使用等各个环节提供安全防护。
- **网络安全：**提供身份保护和数据安全通道能力；同时，具备应急管控和网络安全防护能力以抵御来自互联网的攻击，并能及时消除物联网设备被控引发的危害。
- **终端安全：**能够提供物理安全、数据存储安全、系统安全更新、用户隐私等安全保护能力。

5. 能力要求

为保障 NB-IoT 端到端安全，需要从业务安全、平台安全、网络安全、终端安全四方面打造 NB-IoT 的核心安全能力。

5.1 业务安全

业务安全是 NB-IoT 的生命线。业务安全防护能力决定了安全事件发生时对国计民生的影响程度，也是 NB-IoT 健康发展的核心要素。业务防护措施需要能够深度解析智能抄表、环境监测等各种应用协议，具有识别业务应用层面的身份冒用、资源消耗、业务滥用等攻击行为的能力，同时，NB-IoT 关键防护能力是能阻断业务层面的各种攻击。

5.1.1 业务行为监测

根据业务需求，对物联网终端的短信、流量等进行总量、峰值等多个维度的监测，及时发现业务运行的异常情况。在业务运营过程中，根据设备 IMEI 变化等特征，监测设备机卡分离等业务滥用情况。同时，能够以物联网终端行为大数据为基础，从全局视角提升对 NB-IoT 安全威胁的识别发现、分析和处置能力。

5.1.2 业务威胁防范

具备与产业链上下游各方进行威胁情报交换、共享、分析的能力，及时发现影响 NB-IoT 安全的终端、网络、平台、业务等各层面的威胁，为攻击检测、安全防护、联动处置、信息共享提供一个决策信息

平台，从而开展积极防御，保障业务健康运行。

5.1.3 业务分级管理

业务应具备分级管控的能力，重要业务与普通业务在安全方面进行区分防护，不同级别的业务采取不同防护及管控措施，避免重要业务的安全水平受到其他业务影响。

5.2 平台安全

5.2.1 访问控制

平台应面向不同业务场景中的用户、设备、应用提供访问控制能力，防止用户、设备、应用越权操作。对接入系统的用户、设备、应用进行分组，根据不同分组授予不同的访问权限，只有获得授权的用户、设备、应用才能访问指定的数据，调用相应的业务能力，执行相应的业务操作。

5.2.2 边界防护

业务平台在边界应具备防护来自传统互联网安全攻击的能力，重点应对大数据、云计算、WEB 等技术带来的安全风险，具有防 DDOS 攻击、防篡改、防入侵、防病毒的能力，保障业务平台安全稳定运行。

5.2.3 平台内部防护

开展安全域划分，将平台网络划分成管理区、业务区、接口区等，

不同功能设备位于不同安全域。安全域之间具备入侵检测、访问控制能力，结合平台边界防护，实现平台纵深安全防御。同时，业务平台需具有不同用户安全隔离的能力，在大规模用户接入时，确保用户按权限按需要访问资源，避免越权访问等问题。此外，业务平台应具备常见安全监测、安全审计等能力，确保平台自身安全运行。

5.2.4 数据安全

平台能够为数据的存储、传输、使用等各环节提供安全防护，定期备份关键业务数据，并对销毁、恢复等过程进行保护，保障数据的机密性、完整性和可用性。在逻辑上隔离敏感信息，严格控制系统文件及日志的操作权限，并提供数据新鲜性保护。同时，应保障密钥完整性，支持复杂密钥并定期更新，提高抵抗恶意攻击的能力。

5.3 网络安全

5.3.1 身份识别及通道安全

NB-IoT网络需要提供用户与网络之间的双向身份识别和安全通道，实现信令和用户数据的安全传输，如图3所示。

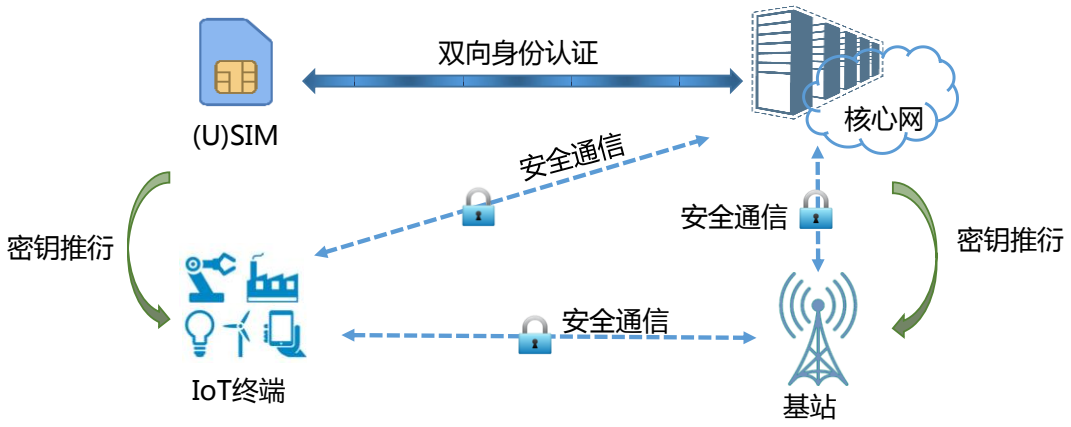

图 3 网络安全能力

NB-IoT 网还可基于网络接入认证功能进行安全能力开放，即业务应用直接使用网络层认证结果或认证参数，不再对终端进行单独认证，降低因设备双层认证而带来的消耗。

5.3.2 应急管控能力

在大规模终端被恶意控制发起网络攻击时，NB-IoT 网络需要具备应急管控能力，能够迅速关停被控设备的通信功能，停止设备的网络接入服务，及时阻断大规模攻击，迅速降低危害的影响范围。

5.3.3 网络安全防护

NB-IoT 应具备应对各类网络攻击的能力，尤其是能够防御互联网发起的 DDoS 攻击，确保网络的安全性与可靠性，避免因网络瘫痪造成严重影响。同时，NB-IoT 还应提供近源防护能力，在网内恶意终端发起网络攻击时，进行及时处理，确保 NB-IoT 及连接终端不被作为攻击“肉鸡”。

此外，NB-IoT 核心网应具备应对信令伪造、篡改、重放攻击的能力，避免核心网网元暴露在互联网上，增强网元之间访问控制能力，减少网络开放、跨网络通信等带来的风险。

5.4 终端安全

5.4.1 用户隐私安全

终端应能根据业务需求，灵活设置隐私保护范围，同时应满足企业客户的隐私保护策略，依据用户授权原则来处理终端设备数据，确保不采集业务需求外的联网设备数据。此外，还应为终端用户敏感数据访问、存储、传输、转移、备份及恢复等各个环节提供全方位安全防护。

5.4.2 升级安全

终端设备的系统/固件及应用等软件应具备升级能力，能够及时安装厂商安全补丁，并在升级完成后加以验证，确保系统及应用安全运行。同时，在升级时考虑利用加密传输机制保障升级数据的安全性，保证升级文件不被破坏和篡改。最后，在系统升级失败时能够回退到升级前的版本。对于分散部署的终端设备，考虑支持远程升级方式，便于集中管理和防止危害范围扩大。

5.4.3 物理安全

终端设备应对接口和芯片提供物理保护，使得攻击者即使获得硬

件设备也难以获得数据。除此之外，终端应具备针对不同接口的认证授权能力。另外，建议采用具有例如 TEE 安全内核的芯片，提供对终端内部闪存和基带的安全保护，实现安全启动、调试权限甄别、应用及数据安全存储等，确保芯片内系统程序、终端参数、配置文件数据、用户数据不被篡改或非法获取。

5.4.4 系统安全

终端应遵循“最小权限原则”，保持系统权限和服务的最小化运行，采用访问控制、身份认证、权限限制等机制提高系统的可靠性和完整性，缩小攻击面。其次，应严格限制调试进程在操作系统中的权限，提高调试功能可控性。另外，应尽量避免设备缺省密码固化等硬编码问题。最后，终端系统还应保证终端配置文件等数据存储的安全性。

6. 中国移动安全实践

中国移动将致力于推动 NB-IoT 发展与普及，通过加强源头管控，建立闭环、可控的安全保障体系，发挥运营商管道侧安全管控能力优势，助力打造和谐共生的 NB-IoT 安全生态环境。

中国移动将采取如下举措，确保 NB-IoT 网络和业务可管可控。一是建立物联网安全保障体系，制定物联网业务、终端、运营等方面的管理制度，及智能硬件、NB-IoT 网络、平台安全等方面的技术规范，将安全要求融入业务全生命周期运营。二是构建安全态势感知和重点业务安全保障两方面能力，通过构建态势感知、威胁情报分析能力，

开展主动防御，同时关注重点业务的安全，由点及面，推广到 NB-IoT 各类业务。三是开展业务安全评估、终端入网评测与日常运营安全检测三方面评估，及时发现业务滥用等安全问题，减少终端安全隐患，防范源头风险。具体工作如下:

在业务安全方面，中国移动坚持物联网专卡专号的管理模式，针对不同应用场景开展分类管理,严格限制不同业务种类物联网卡的通信功能，基于“最小、必要、可控”的原则仅开通物联网应用场景需要的通信功能，严格控制物联网与公众通信网络的互通。

在平台安全方面,基于云计算技术建设了集中的开放平台 OneNET,部署了安全防护手段实现全网集中安全防护，重点防范数据泄漏、网络攻击等风险。

在网络安全方面，做到网络集中建设、专网专用，实现“一点接入、全网服务”，在专网出入口进行集中安全防护，严格限制专网与互联网的互通。针对重点业务，提供基于 APN 的安全通道。基于网络与终端的双向认证能力，向应用开放网络认证等安全能力。

在终端安全方面，一方面开展终端入网安全测评，从源头避免终端“带病入网”;另一方面基于网络流量、外部情报源等多维度信息，开展终端安全大数据分析，及时发现终端异常行为，从源头防范终端安全风险。

7. 推进建议

NB-IoT 业务爆发式增长，对安全提出了越来越高的要求，应从以下五方面推进 NB-IoT 安全体系建设:

1） **推动业务分级保护**。NB-IoT 业务类型众多，一旦发生信息窃取或伪造，可能对国家安全、社会秩序、公众利益造成不同程度的侵害。建议根据业务涉及的数据、对象以及对国家、社会和个人的影响程度，建立业务分级制度，制定不同等级业务的安全防护技术要求和管理要求。

2） **加快安全标准体系建设**。制定符合我国国情的技术标准，进一步完善国家及行业安全标准体系。积极推动和参与安全国际标准的编制，扩大我国在国际上的话语权。

3） **健全入网安全测评**。尽快建立国家及行业覆盖系统、终端、设备及业务安全评估的测评体系，制定 NB-IoT 系统、终端、设备及业务平台安全准入机制，防止设备和系统“带病入网”。

4） **深化安全法制建设**。目前国家已出台《网络安全法》等信息安全法规，在信息安全、个人隐私保护等方面进一步加强了安全保护要求。建议针对 NB-IoT 业务应用场景，细化法律法规相关条款。针对产业发展过程中出现的典型案例，制定防范和应对措施，在全社会进行广泛宣传和教育，强化全民安全意识。

5） **建立安全生态联盟**。物联网产业链已初具规模，应尽快建立联合上下游合作伙伴的安全生态联盟。一方面围绕具体业务场景，建立以终端、网络、平台和业务安全为支撑的安全生态体系，明确终端厂商、运营商、平台系统厂商等物联网生态参与者的安全责任；另一方面发挥产业链各个角色的优势，推动产业合作伙伴不断提升安全能力（例如运营商可开放基于网络的身份认证等安全能力提升不同应

用的认证安全等），共同建设安全、健康、有序的物联网业务生态环境。

8. 总结展望

NB-IoT 是互联网向真实世界的全面延伸，必将为整个人类社会带来更加深刻的革新，其技术的复杂与嬗变不可避免地会引入新的安全风险和挑战。为有效应对风险和挑战，产业链需要紧紧围绕 “业务+云管端”开展安全防护，将安全要求落实到业务全生命周期、云服务、数据传输通道、终端运营等各个环节。

NB-IoT 的发展与普及，需要有和谐共生的 NB-IoT 安全生态环境。中国移动将秉承创新、协调、绿色、开放、共享的发展理念，与产业界各方通力合作，共同建设可信的 NB-IoT 安全防护体系，为促进物联网的持续健康发展做出积极贡献。