ICS 03.080

|  |
| --- |
| CCS A 16 |

DB21

辽宁省地方标准

DB21/T XXXX—XXXX

|  |
| --- |
|  |

基于蜂窝网络的工业无线通信安全

测评要求

（征求意见稿）

|  |
| --- |
| 在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。 |
|  |

XXXX - XX - XX发布

XXXX - XX - XX实施

辽宁省市场监督管理局　 发 布

目　次

[前言 III](#_Toc9868)

[1 范围 1](#_Toc30018)

[2 规范性引用文件 1](#_Toc17274)

[3 术语和定义 1](#_Toc22584)

[4 测评方法要求 2](#_Toc541)

[5 测评内容要求 2](#_Toc267)

[5.1 物理环境安全 2](#_Toc8084)

[5.2 通信网络安全 3](#_Toc22998)

[5.3 区域边界安全 5](#_Toc21542)

[5.4 计算环境安全 10](#_Toc20791)

[5.5 建设运维安全 18](#_Toc14312)

[6 测评结果判定要求 21](#_Toc27877)

前  言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由辽宁省工业和信息化厅提出并归口。

本文件起草单位：沈阳华睿博信息技术有限公司、东北大学、辽宁省信息安全与软件测测评认证中心、辽宁省先进装备制造业基地建设工程中心、沈阳鼓风机集团股份有限公司、辽宁艾特斯智能交通技术有限公司、中国烟草总公司辽宁省公司、辽宁省烟草公司沈阳市公司、济南大学、沈阳职业技术学院等。

本文件主要起草人：邵华、姚羽、郭剑峰、陈莹、刘奇、郝玉明、黄书鹏、王宇飞、袁辉、杨海涛、纪科、陈贞翔、吴丽萍、李慧玲、杨巍等。

本文件发布实施后，任何单位和个人如有问题和意见建议，均可以通过来电和来函等方式进行反馈，我们将及时答复并认真处理，根据实际情况依法进行评估及复审。

归口管理部门通信地址：辽宁省沈阳市皇姑区北陵大街45-2号

归口管理部门联系电话：024-86913384

标准起草单位通信地址：沈阳市和平区青年大街386号华阳国际大厦2396室

标准起草单位联系电话：18698849086

基于蜂窝网络的工业无线通信安全测评要求

1. 范围

本文件规定了基于蜂窝网络的工业无线通信安全测评要求。

本文件适用于安全测评服务机构、工业蜂窝网络运营使用单位及主管部门对工业蜂窝网络的安全状况进行安全测评并提供指南。

1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 35673-2017 工业通信网络 网络和系统安全 系统安全要求和安全等级

GB/T 36627-2018 信息安全技术 网络安全等级保护测试评估技术指南

GB/T 41780.1-2022 物联网 边缘计算 第1部分：通用要求

YD/T 2910-2015 LTE/SAE安全技术要求

1. 术语和定义

GB/T 22239-2019、GB/T 22240-2020、GB/T 35673-2017、GB/T 41780.1-2022界定的及以下术语和定义适用于本文件。



访谈 interview

测评人员通过引导测评对象相关人员进行有目的的（有针对性的）交流以及帮助测评人员理解、澄清或取得证据的过程。



核查 examine

测评人员通过对测评对象（如制度文档、各类设备及安全配置等）进行观察。以帮助测评人员理解、澄清或取得证据的过程。



测试 test

测评人员使用预定的方法/工具使测评对象（各类设备或安全配置）产生特定的结果，将运行结果与预期的结果进行对比的过程。



评估 evaluate

对测评对象可能存在的威胁及其可能产生的后果进行综合评价和预测的过程。



测评对象 target of testing and evaluation

测评过程中不同测评方法作用的对象，主要涉及相关配套制度文档、设备设施及人员等。

1. 测评方法要求

测评实施的基本方法是针对特定的测评对象，采用相关的测评手段，遵从一定的测评流程，获取需要的证据数据，给出是否达到特定的安全保护能力的评判。

本文件中针对每一个要求项的测评构成一个单项测评，针对某个要求项的所有具体测评内容构成测评实施。

1. 测评内容要求
   1. 物理环境安全
      1. 室外控制设备物理防护

室外控制设备物理防护应满足如下要求：

1. 室外控制设备应放置于采用铁板或其他防火材料制作的箱体或装置中并紧固。

测评对象：室外控制设备。

测评实施：应核查室外控制设备是否放置于采用铁板或其他防火材料制作的箱体或装置中并紧固。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求。

1. 箱体或装置具有透风、散热、防盗、防雨和防火能力等；

测评对象：室外控制设备箱体或装置。

测评实施：应核查室外控制设备箱体或装置是否具有透风、散热、防盗、防雨和防火能力。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求。

1. 室外控制设备放置应远离强电磁干扰、强热源等环境，如无法避免应及时做好应急处置及检修，保证设备正常运行。

测评对象：室外控制设备物理位置。

测评实施：应核查室外控制设备物理位置是否远离强电磁干扰、强热源等环境，如果无法避免是否及时做好应急处置及检修，保证设备正常运行。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求。

* + 1. 蜂窝网络接入节点的物理位置

应为蜂窝网络接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

测评对象：蜂窝网络接入设备物理位置。

测评实施：应核查蜂窝网络接入设备的物理位置是否能够避免过度覆盖和电磁干扰。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求。

* 1. 通信网络安全
     1. 网络架构

工业控制系统网络架构应满足如下要求：

1. 工业控制系统与企业其他系统之间应划分为不同区域，区域间应采用技术手段实现安全隔离；

测评对象：网闸、路由器、交换机和防火墙等提供访问控制功能的设备。

测评实施包括以下内容：

1. 应核查工业控制系统和企业其他系统之间是否部署单项隔离设备；
2. 应核查是否采用了有效的单项隔离策略实施访问控制；
3. 应核查使用无线通信的工业控制系统边界是否采用与企业其他系统隔离响度相同的措施。

单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

1. 工业控制系统内部应根据业务特点划分为不同的安全域，安全域之间应采用技术手段实现安全隔离；

测评对象：路由器、交换机和防火墙等提供访问控制功能的设备。

测评实施包括以下内容：

1. 应核查工业控制系统内部是否根据业务特点划分了不同的安全域；
2. 应核查各安全域之间访问控制设备是否配置了有效的访问控制策略。

单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

1. 涉及实时控制和数据传输的工业控制系统，应使用独立的网络设备组网，在物理层面上实现与其他数据网及外部公共信息网的安全隔离；

测评对象：工业控制系统网络。

测评实施：应核查涉及实时控制和数据传输的工业控制系统是否在物理层面上独立组网。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 对重要生产系统，应在无线蜂窝网络的边界采用屏蔽或干扰手段，隔离物理边界外对无线蜂窝网络的访问。

测评对象：无线蜂窝网络边界。

测评实施：应核查无线蜂窝网络边界是否采用屏蔽或干扰手段，隔离物理边界处对无线蜂窝网络的访问。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

* + 1. 通信传输

在工业控制系统内使用工业生产网络进行控制指令或相关数据交换的应采用加密技术手段实现身份认证、访问控制和数据加密传输。

测评对象：加密认证设备、路由器、交换机和防火墙等提供访问控制功能的设备。

测评实施：应核查工业控制系统中使用广域网传输的控制指令或相关数据是否采用加密认证技术实现身份认证、访问控制和数据加密传输。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

* 1. 区域边界安全
     1. 边界保护

应保证有线网络与蜂窝网络边界之间的访问和数据流通过无线接入网关设备。

测评对象：无线接入网关设备。

测评实施：应核查有线网络与无线网络边界之间是否部署无线接入网关设备。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

* + 1. 蜂窝网络使用控制

工业蜂窝网络使用控制应满足如下要求：

1. 应对所有参与蜂窝网络通信的用户（人员、软件进程或者设备）提供唯一性标识和鉴别；

测评对象：蜂窝通信网络及设备。

测评实施包括以下内容：

1. 应核查蜂窝通信的用户在登录时是否采用了身份鉴别措施；
2. 应核查用户身份标识是否具有唯一性。

单元判定：如果1）和2）均为为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 应对所有参与蜂窝网络通信的用户（人员、软件进程或者设备）进行授权以及执行使用进行限制；

测评对象：蜂窝通信网络及设备。

测评实施：应核查蜂窝通信过程中是否对用户进行授权，核查具体权限是否合理，核查未授权的使用是否可以被发现及告警。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 应对蜂窝网络通信采取传输加密的安全措施，实现传输报文的机密性保护；

测评对象：无线通信网络及设备。

测评实施：应核查无线通信传输是否采用加密措施保证传输报文的机密性。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 对采用蜂窝网络通信技术进行控制的工业控制系统，应能识别其物理环境中发射的未经授权的蜂窝网络设备，报告未经授权试图接入或干扰控制系统的行为。

测评对象：蜂窝通信网络及设备和监测设备。

测评实施：应核查工业控制系统是否可以实时检测其物理环境中发射的未经授权的无线设备，检测时被应及时发出告警并可以对视图接入的无线设备进行屏蔽。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

* + 1. 接入控制

应保证只有授权的终端节点可以接入。

测评对象：终端节点设备和设计文档。

测评实施包括以下内容：

1. 应核查终端节点设备接入机制设计文档是否包括防止非法的终端节点设备接入网络的机制以及身份鉴别机制的描述。
2. 应对边界和蜂窝网络进行渗透测试，测试是否不存在绕过白名单或相关接入控制措施以及身份鉴别机制的方法。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

* + 1. 入侵防范

工业网络入侵防范应满足如下要求：

1. 终端节点应能够限制与终端节点通信的目标地址，以避免对陌生环境的攻击行为；

测评对象：终端节点设备和设计文档。

测评实施包括以下内容：

1. 应核查终端节点设备安全设计文档，是否有对终端节点通信目标地址的控制措施的说明；
2. 应核查终端节点设备，是否配置了对终端节点通信目标地址的控制措施，相关参数配置是否符合设计要求；
3. 应对终端节点设备进行渗透测试，测试是否能够限制终端节点对违反访问控制策略的通信目标地址进行访问或攻击。

单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 终端节点应能够限制与网关节点通信的目标地址，以避免对陌生环境的攻击行为；

测评对象：终端节点设备和设计文档。

测评实施包括以下内容：

1. 应核查终端节点设备安全设计文档，是否有对终端节点通信目标地址的控制措施的说明；
2. 应核查终端节点设备，是否配置了对终端节点通信目标地址的控制措施，相关参数配置是否符合设计要求；
3. 应对终端节点设备进行渗透测试，测试是否能够限制终端节点对违反访问控制策略的通信目标地址进行访问或攻击。

单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 应能够检测到非授权蜂窝网络接入设备和非授权移动终端的接入行为；

测评对象：终端节点设备和设计文档。

测评实施包括以下内容：

1. 应核查终端节点设备安全设计文档，是否有对终端节点通信目标地址的控制措施的说明；
2. 应核查终端节点设备，是否配置了对终端节点通信目标地址的控制措施，相关参数配置是否符合设计要求；
3. 应对终端节点设备进行渗透测试，测试是否能够限制终端节点对违反访问控制策略的通信目标地址进行访问或攻击。

单元判定：如果1）～3）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 应能够检测到针对蜂窝网络接入设备的网络扫描、DDoS攻击、密钥破解、中间人攻击和欺骗攻击等行为；

测评对象：抗APT攻击系统、网络回溯系统、威胁情报检测系统、抗DDos攻击系统和入侵保护系统或相关组件。

测评实施包括以下内容：

1. 应核查是否能够通过网络扫描、DDos攻击、秘钥破解、中间人攻击和欺骗攻击等行为进行检测；
2. 应核查规则库版本是否及时更新。

单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 应能够阻断非授权蜂窝接入设备或非授权移动终端；

测评对象：终端准入控制系统、移动终端管理系统或相关组件。

测评实施包括以下内容：

1. 应核查是否能够阻断非授权无线接入设备或非授权移动终端接入；
2. 应测试验证是否能够阻断非授权无线接入设备或非授权移动终端接入。

单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 对重要生产系统应采用探针和异常检测技术对网络行为进行实时检测；

测评对象：探针、异常检测技术。

测评实施：应核查是否对重要生产系统采用探针和异常检测技术对网络行为进行实时检测。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 对重要生产系统宜部署态势感知及蜜罐系统进行持续监控，并对网络攻击行为进行捕获。

测评对象：态势感知及蜜罐系统。

测评实施：应核查是否对重要生产系统部署态势感知及蜜罐系统进行持续监控，对网络攻击行为进行捕获。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

* + 1. 安全审计

工业蜂窝网络区域边界安全审计应满足如下要求:

1. 应在网络边界、重要网络节点进行安全审计,审计覆盖到每个用户,对重要的用户行为和重要安全事件进行审计；

测评对象：综合安全审计系统等。

测评实施包括以下内容：

1. 应核查是否部署了综合安全审计系统或类似功能的系统平台。
2. 应核查安全审计范围是否覆盖到每个用户。
3. 应核查是否对重要的用户行为和重要安全事件进行了审计。

结果判定：如果1）～3）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

1. 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

测评对象：综合安全审计系统等。

测评实施：应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

结果判定：如果以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

1. 应对审计记录进行保护,定期备份，避免受到未预期的删除、修改或覆盖等；

测评对象：综合安全审计系统等。

测评实施包括以下内容：

1. 应核查是否采取了技术措施对审计记录进行保护。
2. 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。

结果判定：如果1）和2）均为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

1. 应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。

测评对象：综合安全审计系统等。

测评实施：应核查是否对远程访问用户及互联网访问用户行为单独进行审计分析。

结果判定：如果以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

* 1. 计算环境安全
     1. 工业蜂窝网络控制设备安全

工业蜂窝网络控制设备应满足如下要求：

1. 控制设备自身应实现相应级别安全通用要求提出的身份鉴别、访问控制和安全审计等安全要求，如受条件限制控制设备无法实现上述要求，应由其上位控制或管理设备实现同等功能或通过管理手段控制；

测评对象：控制设备。

测评实施应包括以下内容：

1. 应核查控制设备是否具有身份鉴别、访问控制和安全审计功能；
2. 如控制设备不具备上述功能，则核查是否由其尚未控制或管理设备实现同等功能或者通过管理手段控制。

单元判定：如果1）或2）为肯定，则符合本测评单元的指标要求，否则不符合或部分符合本测评单元的指标要求。

1. 应在经过充分测试评估后，在不影响系统安全稳定运行的情况下对控制设备进行补丁更新、固件更新等工作；

测评对象：控制设备。

测评实施包括以下内容：

1. 应核查是否有测试报告和测试评估记录；
2. 应核查控制设备版本、补丁及固件是否经过充分测试后进行了更新。

单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

1. 应关闭或拆除控制设备的软盘驱动、光盘驱动、USB接口、串行口或多余网口等，确需保留的应通过相关的技术措施实施严格的监控管理；

测评对象：控制设备。

测评实施包括以下内容：

1. 应核查控制设备是否关闭或拆除设备的软盘驱动、光盘驱动、USB接口、串行口或多余网口等；
2. 应核查保留的软盘驱动、光盘驱动、USB接口、串行口或多余网口等是否通过相关的措施严格的监控管理。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 应使用专用设备和专用软件对控制设备进行更新；

测评对象：控制设备。

测评实施：应核查是否使用专用设备和专用软件对控制设备进行更新。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 应保证控制设备在上线前经过安全性检测，避免控制设备固件中存在恶意代码程序。避免设备中存在未授权的无线网络通信模块。

测评对象：控制设备。

测评实施：应核查由相关部门出具或认可的控制设备的检测报告，明确控制设备固件中是否不存在恶意代码程序。

单元判定：如果以上测评实施内容为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

* + 1. 终端节点设备安全

工业蜂窝网络终端节点设备应满足如下要求：

1. 终端节点设备应保证只有授权的用户可以对终端节点设备上的软件应用进行配置或变更；

测评对象：终端节点设备。

测评实施包括以下内容：

1. 应核查终端节点设备是否采取了一定的技术手段防止非授权用户对设备上的软件应用进行配置或变更；
2. 应通过试图接入和控制传感网访问未授权的资源，测试验证感知节点设备的访问控制措施对非法使用感知节点设备资源的行为控制是否有效。

单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合本测评单元指标要求。

1. 终端节点设备应具有对其连接的网关节点设备进行身份标识和鉴别的能力；

测评对象：网关节点设备（包括读卡器）。

测评实施包括以下内容：

1. 应核查是否对连接的网关节点设备（包括读卡器）进行身份标识与鉴别，是否配置了符合安全策略的参数；
2. 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

1. 终端节点设备应具有对其连接的其他终端节点设备进行身份标识和鉴别的能力；

测评对象：其他终端节点设备（包括路由节点）。

测评实施包括以下内容：

1. 应核查是否对连接的其他终端节点设备（包括路由节点）进行身份标识与鉴别，是否配置了符合安全策略的参数；
2. 应测试验证是否不存在绕过身份标识与鉴别功能的方法。

单元判定：如果1）和2）均为肯定，则符合本测评单元指标要求，否则不符合或部分符合本测评单元指标要求。

1. 对重要生产系统，当终端节点设备通过非可信网络访问（例如远程访问）控制系统时，控制系统应为其提供多因子认证的能力；

测评对象：控制系统。

测评实施：应核查控制系统是否具有对通过非可信网络访问系统的多因子认证的能力。

结果判定：如果以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

1. 控制系统应具备对经由不可信网络访问控制系统的访问控制限制的方法，例如可限制未授权的IP地址接入。

测评对象：控制系统。

测评实施：应核查控制系统是否具有对经由不可信网络访问系统的限制方法。

结果判定：如果以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

* + 1. 网关节点设备安全

工业蜂窝网络网关节点设备应满足如下要求:

1. 网关节点设备应具备对合法连接设备进行标识和鉴别的能力；

测评对象：网关节点设备。

测评实施：

1. 应检查网关节点设备是否能够对连接设备（包括终端节点设备、路由节点、数据处理中心进行标识并配置了鉴别功能。
2. 应测试认证是否不存在绕过身份标识与鉴别功能的方法。

结果判定：如果1）和2）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

1. 网关节点设备应具备过滤非法节点和伪造节点所发送的数据的能力；

测评对象：网关节点设备。

测评实施：

1. 应核查是否具备过滤非法节点和伪造节点发送数据的功能。
2. 应测试验证是否能够过滤非法节点和伪造节点发送的数据。

结果判定：如果1）和2）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

1. 授权用户应能够在设备使用过程中对关键密钥进行在线更新；

测评对象：网关节点设备。

测评实施：应核查网关节点设备是否对其关键密钥进行在线更新及在线更新方式是否有效。

结果判定：如果以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

1. 授权用户应能够在设备使用过程中对关键配置参数进行在线更新；

测评对象：网关节点设备。

测评实施：应核查网关节点设备是否支持对其关键配置参数进行在线更新及在线更新方式是否有效。

结果判定：如果以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

1. 网关节点设备的电磁兼容性应满足 GB/T 17626 (所有部分) 、GB/T 17799.1-2017、GB/T17799.2-2003、GB 17799.3-2012、GB 17799.4-2012、GB/T 17799.5-2012、GB/T 18268.1-2010.GB/T 19286-2015、GB/T 19287-2016、GB/T 22451-2008、CISPR 16-1-1、CISPR 16-2-1、IEC61000-4-1、IEC 61000-4-2、IEC 61000-4-3、IEC 61000-4-4、IEC 61000-4-5、IEC 61000-4-6.IEC 61000-4-7、IEC 61000-4-8、IEC 61000-4-9、IEC 61000-4-10、IEC 61000-4-11、IEC61000-4-12、IEC 61000-6-1、IEC 61000-6-2、IEC 61000-6-3、IEC 61000-6-4等标准中的要求。

测评对象：网关节点设备。

测评实施：应核查网关节点设备的电磁兼容性是否满足 GB/T 17626 (所有部分)、GB/T 17799.1-2017、GB/T17799.2-2003、17799.3-2012、GB 17799.4-2012、GB/T 17799.5-2012、GB/T 18268.1-2010.GB/T 19286-2015、GB/T 19287-2016、GB/T 22451-2008、CISPR 16-1-1、CISPR 16-2-1、IEC61000-4-1、IEC 61000-4-2、IEC 61000-4-3、IEC 61000-4-4、IEC 61000-4-5、IEC 61000-4-6.IEC 61000-4-7、IEC 61000-4-8、IEC 61000-4-9、IEC 61000-4-10、IEC 61000-4-11、IEC61000-4-12、IEC 61000-6-1、IEC 61000-6-2、IEC 61000-6-3、IEC 61000-6-4等标准中的要求。。

结果判定：如果以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

* + 1. 抗数据重放

工业蜂窝网络终端节点设备抗数据重放应满足如下要求:

1. 终端节点设备应能够鉴别数据的时效性，避免历史数据的重放攻击；

测评对象：终端节点设备。

测评实施：

1. 应核查终端节点设备鉴别数据时效性的措施，是否能够避免历史数据重放。
2. 应进行终端节点设备历史数据重放测试，验证其保护措施是否生效。

结果判定：如果1）和2）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

1. 终端节点设备应能够鉴别对历史数据的非法修改，避免数据的修改重放攻击。

测评对象：终端节点设备。

测评实施：应测试验证终端设备是否能够检测到历史数据的非法修改，避免数据的修改重放攻击。

结果判定：如果以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

* + 1. 边缘计算

边缘计算节点的设计、开发和应用应满足GB/T 41780.1-2022中的要求。

测评对象：边缘计算节点。

测评实施：应检查边缘计算节点的设计、开发和应用是否满足GB/T 41780.1-2022中的要求。

结果判定：如果以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

* + 1. 安全审计

工业蜂窝网络计算环境安全审计应满足如下要求：

1. 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

测评实施包括以下内容：

1. 应核查是否开启了安全审计功能。
2. 应核查安全审计范围是否覆盖到每个用户。
3. 应核查是否对重要的用户行为和重要安全事件进行审计。

结果判定：如果1）～3）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

1. 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

测评实施：应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、时间是否成功及其他与审计相关的信息。

结果判定：如果以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

1. 应对审计记录进行保护，定期备份，避免收到未预期的删除、修改或覆盖等；

测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

测评实施包括以下内容：

1. 应核查是否采取了保护措施对审计记录进行保护；
2. 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。

结果判定：如果1）和2）均为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

1. 应对审计进程进行保护，防止未经授权的中断。

测评对象：终端和服务器等设备中的操作系统（包括宿主机和虚拟机操作系统）、网络设备（包括虚拟网络设备）、安全设备（包括虚拟安全设备）、移动终端、移动终端管理系统、移动终端管理客户端、感知节点设备、网关节点设备、控制设备、业务应用系统、数据库管理系统、中间件和系统管理软件及系统设计文档等。

测评实施包括以下内容：

1. 应核查是否采取了保护措施对审计记录进行保护；
2. 应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。

结果判定：如果1）和2）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

* + 1. 数据完整性保护

工业蜂窝网络计算环境数据完整性保护应满足如下要求:

1. 应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；

测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。

测评实施包括以下内容：

1. 应核查系统设计文档,鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性。
2. 应测试验证在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改，是否能够检测到数据在传输过程中的完整性受到破坏并能够及时恢复。

结果判定：如果1）和2）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

1. 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

测评对象：业务应用系统、数据库管理系统、中间件、系统管理软件及系统设计文档、数据安全保护系统、终端和服务器等设备中的操作系统及网络设备和安全设备等。

测评实施包括以下内容：

1. 应核查设计文档,是否采用了校验技术或密码技术保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；
2. 应核查是否采用技术措施(如数据安全保护系统等)保证鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在存储过程中的完整性；
3. 应测试验证在存储过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等进行篡改,是否能够检测到数据在存储过程中的完整性受到破坏并能够及时恢复。

结果判定：如果1）～3）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

* 1. 建设运维安全
     1. 产品采购和使用

工业控制系统重要设备应通过专业机构的安全性检测后方可采购使用。

测评对象：工业控制系统重要设备检测报告类文档。

测评实施：

1. 应访谈安全管理员系统使用的工业控制系统重要设备及网络安全专用产品是否通过专业机构的安全性检测。
2. 应核查工业控制系统是否具有通过专业机构出具的安全性检测报告。

结果判定：如果1）和2）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

* + 1. 外包软件开发

应在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专业等方面的内容。

测评对象：外包软件开发合同

测评实施：应核查是否在外包开发合同中规定针对开发单位、供应商的约束条款，包括设备及系统在生命周期内有关保密、禁止关键技术扩散和设备行业专业等方面的内容。

结果判定：如果1）和2）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

* + 1. 运维

运维应满足如下要求：

1. 应指定人员定期巡视终端节点设备、网关节点设备的部署环境，对可能影响终端节点设备、网关节点设备正常工作的环境异常进行记录和推护；

测评对象：设备运行维护记录

测评实施：

1. 应访谈系统运维负责人是否有专门的人员对终端节点设备、网关节电设备进行定期维护，由何部门或何人负责，维护周期多长。
2. 应核查终端节点设备、网关节点设备部署环境维护记录是否包含维护日期、维护人、维护设备、故障原因、维护结果等方面的内容。

结果判定：如果1）和2）均为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

1. 应对终端节点设备、网关节点设备入库、存储、部署、携带、维修、丢失和报废等过程作出明确规定，并进行全程管理；

测评对象：终端节点、网关节点设备安全管理文档

测评实施：应核查终端节点和网关节点设备安全管理文档是否覆盖终端节点、网关节点设备入库、存储、部署、携带、维修、丢失和报废等方面。

结果判定：如以上测评实施内容为肯定，则符合本测评项指标要求，否则不符合本测评项指标要求。

1. 应加强对终端节点设备、网关节点设备部署的保密性管理，包括负责检查和维护的人员调离工作岗位应立即交还相关检查工具和检查维护记录等。

测评对象：终端节点、网关节点设备部署环境的管理制度

测评实施：

1. 应核查终端节点和网关节点设备部署环境管理文档是否包括负责核查和维护的人员调离工作岗位立即交还相关核查工具和检查维护记录等方面的内容。
2. 应核查是否具有终端节点设备、网关节点设备部署环境的相关保密性管理记录。

结果判定：如以1）和2）均为为肯定，则符合本测评项指标要求，否则不符合或部分符合本测评项指标要求。

* + 1. 安全检查及响应措施

安全检查及响应措施应满足如下要求：

1. 应定期进行常规安全检查，检查内容包括系统运行、系统漏洞和数据备份等情况；

测评对象:信息/网络安全主管和记录表单类文档。

测评实施包括以下内容:

1. 应访谈信息/网络安全主管是否定期进行了常规安全检查；
2. 应核查常规安全检查记录是否包括了系统日常运行、系统漏洞和数据备份等情况。

结果判定；如果1)和2)均为肯定，则符合本测评单元指标要求否则不符合或部分符合本测评单元指标要求

1. 应定期进行全面的安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

测评对象:信息/网络安全主管和记录表单类文档。

测评实施包括以下内容：

1. 应访谈信息/网络安全主管是否定期进行了全面安全检查；
2. 应核查全面安全检查记录是否包括了现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

结果判定：如果1)和2)均为肯定，则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

1. 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；

测评对象：记录表单类文档。

测评实施：应核查是否具有安全检查表格、安全检查记录、安全检查报告、安全检查结果通报记录。

结果判定：如果以上测评实施内容肯定，则符合本测评单元指标要求,否则不符合本测评单元指标要求。

1. 应及时向安全管理部门报告所发现的安全弱点和可疑事件；

测评对象:运维负责人和记录表单类文档。

测评实施包括以下内容:

1. 应访谈运维负责人是否告知用户在发现安全弱点和可疑事件时及时向安全管理部门报告；
2. 应核查在发现安全弱点和可疑事件后是否具备对应的报告或相关文档。

结果判定:如果1)和2)均为肯定，则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

1. 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；

测评对象:管理制度类文档。

测评实施包括以下内容:

1. 应核查是否建立了安全事件报告和处置管理制度；
2. 应核查安全事件报告和处置管理制度是否明确了与安全事件有关的工作职责、不同安全事件的报告、处置和响应流程等。

结果判定:如果1)和2)均为肯定，则符合本测评单元指标要求,否则不符合或部分符合本测评单元指标要求。

1. 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因、收集证据、记录处理过程总结经验教训。

测评对象:记录表单类文档。

测评实施:应核查安全事件报告和响应处置记录是否记录引发安全事件的原因、证据、处置过程、经验教训、补救措施等内容。

结果判定:如果以上测评实施内容为肯定，则符合本测评单元指标要求,否则不符合本测评单元指标要求。

1. 测评结果判定要求

本项要求如下：

1. 针对整体测评后的单项测评结果中部分符合项或不符合项所产生的安全问题，结合关联测评对象和威胁,分析可能对定级对象、单位、社会及国家造成的安全危害。
2. 结合安全问题所影响业务的重要程度、相关系统组件的重要程度、安全问题严重程度以及安全事件影响范围等综合分析可能造成的安全危害中的最大安全危害（损失）结果。
3. 根据最大安全危害严重程度进一步确定定级对象面临的风险等级，结果为“高”“中”或“低”。
4. 对测所有测评项的单项测评结果进行统计，计算出综合得分，具体要求如下：
5. 符合项记1分；
6. 部分符合记0.5分；
7. 不符合记0分。
8. 结合测评结果中所有测评项的单项测评结果中部分符合和不符合项的统计结果、安全问题导致测评对象面临的风险情况、以及测评综合得分情况，形成测评结论，测评结论分为三种情况：
9. 符合：测评对象中未发现安全问题,测评结果中所有测评项的单项测评结果中部分符合和不符合项的统计结果全为0,综合得分为61分；
10. 基本符合：测评对象中存在安全问题,部分符合和不符合项的统计结果不全为0,但存在的安全问题不会导致定级对象面临高等级安全风险，且综合得分不低于36.6分；
11. 不符合：测评对象中存在安全问题,部分符合项和不符合项的统计结果不全为0,而且存在的安全问题会导致定级对象面临高等级安全风险，或者综合得分低于36.6分。