标题：博世汽车部件（苏州）有限公司基于 5G MEC 网络的“数据驱动”模式下的智慧工厂项目

引言/导读

【企业概况 XXX，项目建设的政策、业务创新等驱动因素等。】

（正文 小四 宋体。行距 1.5 倍行距）

在后疫情时代，挑战与机遇并存。除了要应对错综复杂的客户消费需求和市场的快速演变，生产企业还面临成本与质量进一步持续优化的考验，为了在利润空间日趋收窄，产品交期逐渐缩短，需求波动愈发频繁的情势下时刻保留一席之地，制造企业必须利用工业互联网技术，对自身进行数字化转型升级，赋能价值链，寻求新契机。基于此，博世汽车电子中国区开启了工厂的数字化转型。并同步启动了“数据驱动”模式下的智慧工厂项目。即：采用工业互联网技术实现价值流内闭环的智能管控，推动工厂从数字化，互联化向智能化的迈进。

博世汽车电子中国区立足于卓越运营，在生产智能方面，曾荣获江苏省智能制造突出贡献奖，拥有两座“江苏省智能车间”，分别为：汽车电子事业部传感器测试车间和防抱死系统九代电控单元生产车间。在 2019 年底被评选为工信部“智能制造标杆企业”。

图 1：工信部辛国斌部长为博世汽车部件（苏州）有限公司颁发荣誉证书

然而我们追求卓越的脚步并未停止。基于 5G 的超高速，超大连接及超低时延的关键

能力，和万物互联的应用场景，我们启动了 5G 在生产制造领域的试点。此举将极大地推动我们智能制造的实施，助力“数据驱动”模式下的智慧工厂的实现。为实现智能制造环节中的数据驱动，需花大力打造数据驱动模式下的工业互联网标杆工厂应用场景，力求业务与技术同步发展，依托工业互联网平台，综合运用数据采集与集成应用、建模分析与优化等技术，实现制造系统各层级优化，以及产品、工厂资产和商业的全流程优化。

该项目需求主要为了实现以下内容：生产调度和物料配送实现机器自动补料和 AGV 自动运输。实现车间内的生产执行系统与企业资源管理系统（ERP）互联，真正做到实物流与信息流的实时匹配。人工智能技术（AI）和大数据分析实现质量精进，实现信息共享，确保员工的标准化操作。工厂通过数字化转型在工厂各层级各领域的驱动，互联从供应商端到客户端的信息，在数据平台集成并储存生产过程中产生的数据，从而实现产品价值链的全流程透明化。此外，工厂还使用人工智能（AI）和大数据分析技术更好地实现了制程优化、问题排除和预测预警。全面的信息互通和共享保证工厂制程与生产工艺的全面优化。

一、 关键词

【测试床关键词，要求简练，不超过 20 字。】

（正文 小四 宋体。行距 1.5 倍行距）

工业互联网，数字化，智能化，互联化，价值流闭环。

二、 测试床项目承接主体

（正文 小四 宋体。行距 1.5 倍行距）

2.1. 发起公司和主要联系人联系方式

【说明测试床的发起公司（不限于一家）以及联系人信息。用于其他单位寻求合作。】

博世汽车（部件）苏州有限公司

中国电信股份有限公司苏州分公司

2.2. 合作公司

【说明以合作伙伴身份参与的公司。】

无。

三、 测试床项目目标

【说明建立测试床的目标，测试的是哪一方面？说明测试床提出的背景，用实际数据说明存在的难题和挑战，明确测试床计划解决哪些问题，价值点。】

（正文 小四 宋体。行距 1.5 倍行距）

自 2014 年始，博世集团就在调研 5G 的应用。在 2019 年，我们开始启动 5G 在生产制造领域的试点。在苏州工业园区管委会的大力支持和协调统筹下，博世汽车电子中国区和中国电信苏州于 2020 年 4 月双方达成合作协议，共同探索 5G 技术，助力智能制造，合力打造“数据驱动”下的智慧工厂。本项目主要围绕 5G 的增强宽带、海量连接、低延时、高可靠等特性，**逐步实现在量产模式下的全生产要素互联，实现产品全生命周期的实时数据跟踪和追溯。**

整个项目分三阶段实施，第一阶段基于中国电信高品质 5G 网络实现面向生产执行系统（MES）去中心化的接入功能；第二阶段将通过 5G+MEC 来完成 5G 和博世内网的融合；同步开展第三阶段，验证包括 PLC 及传感器数据回传、AR、VR、高清视频、大数据分析和边缘计算等场景在内的更多 5G+工业互联网在生产中的应用技术案例。

聚焦在"行业+技术+应用"的融合创新，博世将 5G 技术融合到智能制造的场景中，助力"智慧工厂"建设，最终实现"数据驱动工厂"的愿景。**即通过获取、分析、和应用企业内外部数据进行决策的过程，在实现产品价值链的全流程透明化的基础上，利用人工智能和大数据分析等技术更好地实现流程优化、问题解决和预测分析，全面的信息互通和共享保证人员始终在合适的时间确切的地点进行正确的操作。**作为博世集团汽车与智能交通技术业务领域首批步入 5G 时代的制造企业，博世苏州将成为率先在博世全球将 5G 融入实际量产的试点。

5G 助力的“数据驱动模式下”的智慧工厂项目，目前计划的主要应用包含：设备互

联，人员互联和产品互联。以及产品全生命周期的数据跟踪和追溯。利用基于 5G 的边缘计算来支持生产实时监控并动态优化制程的大数据分析。主要实现：

1. 生产线设备全互联。产品生命周期全追溯。
2. 扩大设备数据采集范围。利用 5G 技术，在不改动设备的情形下，加装物联传感器，采集更多设备信息来辅助数据分析，从而实现工艺优化。
3. 基于以上数据基础，对生产设备运行状态进行实时监控、进行故障自动报警和诊断分析。利用 5G 超带宽、低延迟特性，借助 AR、VR 技术实现人机互联快速问题解决。

根据博世汽车电子中国区的“数据驱动工厂”愿景，业务与技术需同步发展。依托 5G+工业互联网平台，综合运用数据采集与集成应用，实现在量产模式下的“数据驱动”智能制造。

图 2：博世汽车部件（苏州）有限公司汽车电子事业部数据驱动工厂战略

根据该战略，在量产中试点的 5G 应用项目应助力推动工厂从数字化，互联化向智能化的迈进。基于此，我们在试点的 5G 应用项目将聚焦在设备层面，并遵循以下设计理念：

1. 数字化：扩大设备数据采集范围。利用 5G 技术，在不改动设备的情形下，加装物联传感器，采集更多设备信息来辅助数据分析，从而实现工艺优化。

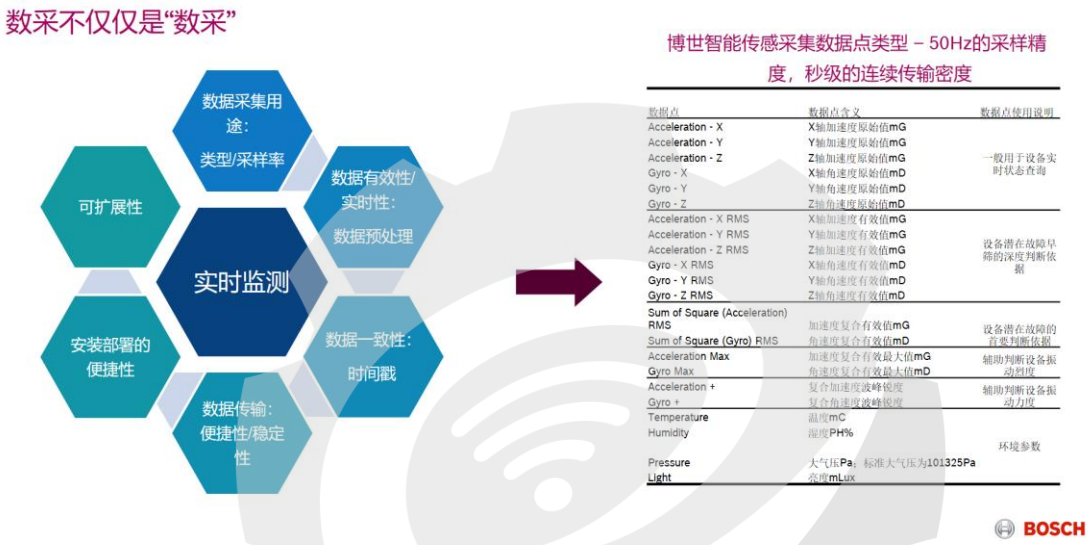


图 3：博世物联传感器采样精度

2. 互联化：首先，扩大设备互联范围，对生产线设备进行全互联。并基于现有博世生产执行系统（Nexeed MES），利用 5G 技术，实现去中心化的生产过程中各环节的数据集成和产品价值链的全流程数字化。其次，利用 5G 超带宽、低延迟特性，借助 AR、VR 技术实现人机互联快速问题解决。

图 4：博世 AR 远程专家在线辅助项目的体验

智能化：基于采集的数据，对生产设备运行状态进行实时监控、进行故障自动报警和诊断分析。通过 5G 技术接入设备，实现对加装的物联传感器、控制器等各类设备的数据采集，建立设备参数优化模型，实现参数智能配置。

四、 测试床方案架构

（正文 小四 宋体。行距 1.5 倍行距）

4.1. 测试床应用场景

【介绍测试床的应用场景。】

博世汽车部件（苏州）有限公司汽车电子事业部工厂生产车间内的所有设备都已百分之百连入网络。采用现场总线、以太网和分布式控制系统等信息技术和控制系统，建立了车间级工业互联网。博世汽车部件（苏州）有限公司汽车电子事业部还和苏州工业园区和中国电信江苏分公司合作进行生产区域中的 5G 试点。

本项目采用大数据、数据仓库、非关系型数据库等工厂的数据和 IT 架构战略在生产现场基于数据可视化管理、数据分析和数据建模对生产过程中工艺流程进行快速优化与调整。运用机器视觉，语音识别等人工智能技术完善产品质量、优化工艺及提升生产效率。

- 5G 网络下的产线数据采集

生产环节中，所有产品在生产第一个工艺由制造执行系统的序列号生成器生成一个唯一序列号并通过激光刻码机刻录一个二维码在产品规定的位置，所有生产工艺的生产数据和物料数据都链接到这个唯一的二维码信息并存储在制造执行系统里。所有生产设备工艺都由可编程逻辑控制器（PLC)或工业电脑（IPC)通过 5G 通讯连接到制造执行系统（MES),实现所有产品在所有工艺上的实时流程管控和质量管控，确保产品的完美质量和生产信息的透明，所有数据存储在制造执行系统的数据库里，定期归档，确保产品数据全程可追溯。

以电子线路板加工导通性测试设备为例，通过对测试机台的基于 5G 网络的数据采集后对后台文件进行解析，将解析出来的数据进行处理，并依据写入的正态规则自动完成

数据分析并预设预警值及控制极限。被处理过的数据，都保存在一个公共数据库中。通过可视化的数据界面开发，形成了根据需求定义的报告格式。与此同时，生产测试过程中产生的不良和偏差，也都可以透明化的呈现出来。因为对数据剖析的深刻，透明化的不良和偏差等级，不仅仅针对机台层面，更有针对每一个测试端点的实时偏差呈现。工程师和生产技术人员，能够获得实时的数据报告。

- 5G+AI AOI 视觉检测

本项目中基于 5G 技术同时引入人工智能技术，实现人工智能中图像识别在光学检测站的应用（AI@AOI）。由于汽车行业对产品安全性要求非常高，在汽车电子生产制造环节的末端，用自动光学检测设备（AOI）来检测产品的焊接质量，从而确保提供高品质产品给客户。由于设备是自动检测，为了降低质量风险，会对参数进行加严，在检测到真实不良的同时会产生误报-非真实不良产生，故每台光学检测设备（AOI）都会配备目检员对机器报警进行二次确认。由于员工本身存在技能的差异性和状态的不稳定性，我们也一直在探索新的方案对光学检测设备（AOI）报警进行确认。人工智能之图像识别在光学检测站的应用（AI@AOI）这个项目就是以大数据为基础（上百万张图片），采用神经网络深度学习，并制定专门的与之匹配数学逻辑，采用神经网络深度学习，并制定专门的与之匹配数学逻辑，使其具备预测性，由系统来自动判断 AOI 报警到底是好的产品还是不好的产品，代替人的作业，从而实现自动化智能化并且更精准的判断。同时，人工纠正后的信息会自动成为该人工智能（AI）系统的输入，进而做到神经网络深度学习模型的自优化，从而不断提升 AI 系统预判定的准确率。

- 5G 边缘云化 AGV

对于厂内物流优化，博世集团正在基于 5G 网络内部推行厂内物流执行系统（IES）。这是一套用于内部和外部客户的内部物流的互操作软件解决方案。该系统的主要重点是将所有内部物流运输工具（如牛奶车，叉车和自动引导车（AGV））集成到一个软件系统中。在拥有不同品牌，不同种类车辆的复杂环境中，通过 5G 网络形成低时延的快速响应，同时利用 IES 系统即时将运输订单分配到正确的车辆，以最大程度地提高流程效率。

- 5G+数字孪生

对于资产故障管理和优化，通过 5G 网络下的数据实时性采集，同时运用三维人机交互 3D-HMI 技术完成设备故障的在线诊断与预警。实现设备故障虚拟 3D 定位。即当设备

发生故障时，故障组件可以在虚拟 3D 中高亮并快速定位，缩短技术员排查故障的时间。采用远程真 3D 视角监控设备运动，掌握产线运行状态，实现虚拟现实动作同步。可以在虚拟组件上配置多种信息（组件文档，物料信息，工程信息），实现组件相关信息的快捷查看。我们还计划，在 2021 年底通过对历史运行数据的汇集与故障数据收集，训练故障预测模型，实现厂内设备的预测性维护。

利用三维人机交互 3D-HMI 进行在线诊断

4.2. 测试床架构

【说明测试床和 AII 总体架构的关系。说明本测试床重点测试的新技术/新架构，是 AII 总体架构中的哪一部分？如果 AII 总体架构中没有阐述本测试床中测试的部分，可以提取出来，作为对 AII 总体架构的补充。】

4.3. 测试床方案

【介绍测试床方案，主要测试要点，方案详细架构。如果本测试床是阶段性工作，需要给出更高层面的整体全景图。】

实施方案及周期

实施方案

1、进行业务需求的收集和分析，根据覆盖范围以及网络实际情况，设计和规划专网方案；

2、基站侧：开通 RAN sharing 功能，并配置基站共享参数；

3、传输侧：从传输机房拉线至客户机房，在 A/B 设备上为专网设置 VLAN 并配置路由；

4、MEC 侧：在客户机房搭建热备方案，并和基站进行对接，建立 S1 链路；

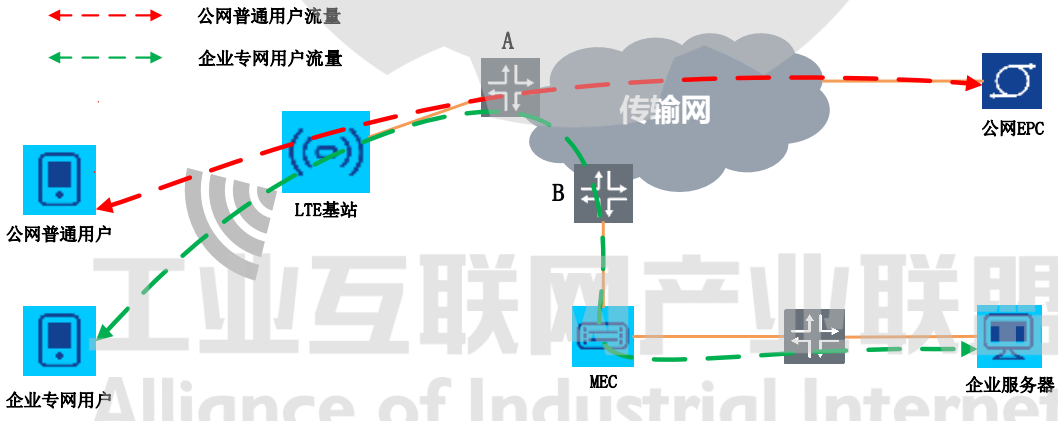
5、网络优化侧：在覆盖范围内进行测试优化，确保良好覆盖和合理的切换；

6、运行维护。

4.4. 方案重点技术

【介绍测试床方案的重点技术，与现有国内外技术对比。】

考虑到厂区应用所有数据需满足博世公司要求，所涉及所有数据需 5G 无线内网中传输，本项目网络方案采用 5G 专网+MEC 边缘计算方案，组网架构见下图。其中 MEC 位于 S1 接口靠近基站位置，采用通用的硬件设备和边缘云软件平台，连接博世（苏州）工厂多个宏基站及室分信号。

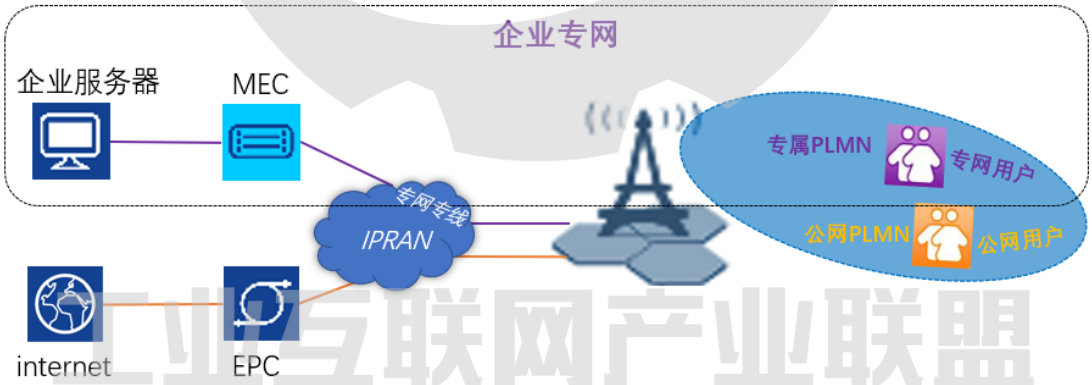


基于 5G MEC 的专网组网方案

其中 MEC 部署在苏州电信机房，作为网络边缘计算平台，和公网 EPC 共用基站资源，专网的控制面和业务面流量均与公网 EPC 隔离。公网用户接入 NR，S1 traffic 正常路由接入 EPC，不经过 MEC 设备。企业专网用户通过专属 PLMN，接入 MEC 设备，专网用户数据直接通过专网的传输链路到达 MEC 设备，传向企业服务器，专网数据不经过公网核心网。且 MEC 无需对 EPC 做任何的软件和硬件上的改动，仅需要本地修改基站部分路由的数据（如 TAC 参数）即可。

MEC 边缘计算结合 5G 网络的组网方案具有超带宽（本地服务，不受核心网带宽限制）、低时延（本地处理，适合工业自动化等重要通讯应用）、大连接（本地计算，内容汇整增强，减少传输负荷）、高可靠性（企业业务在本地处理，具有更高的安全性）的特点，可为移动终端提供更好的业务体验。充分解决 Wifi 干扰大、安全性低、容量低以及以太网移动性差的难题。

本方案中专网用户和公网用户通过 PLMN 实现业务隔离，MEC 会给用户分配专属 PLMN。专网用户业务面和控制面流量均指向 MEC，专网用户通过 MEC 建立专属连接，数据流量经传输专线直接路由至 MEC，并到企业内网。公网用户通过原链路连接到公网 EPC，不经过 MEC，正常访问公网业务。专网用户和公网用户互不干扰，业务完全隔离，MEC 为企业提供一个高度安全可靠的内网环境。基站设备通过光纤汇聚到传输设备上，通过传输专线接到 MEC 交换机上，MEC 通过专线连接企业核心汇聚节点设备，并打通企业服务器。MEC 会对终端周期性广播 PLMN、APN 等信息，允许专属 PLMN 的终端接入企业内网。



上行路由方案：从基站往 MEC 方向。

上行专网路由：专网用户接入基站，透过传输专线将业务 traffic 送达 MEC，最终到达企业服务器。

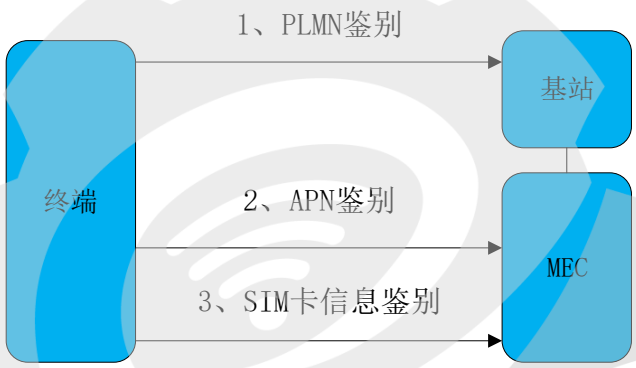
下行路由方案：从 MEC 往基站方向。

下行专网路由：企业服务器所有业务 traffic，会通过 MEC 及传输专线，到达基站。

为实现 MEC 和 EPC(公网)共享 LTE 载波，方案将公网用户和专网用户划分到不同的资源池内，通过基站资源智能调度算法，为公网和专网用户分配特定资源，保障专网用户业务体验。

另外，针对专网用户鉴权原理和实现方式，为确保只有企业内的特定用户才能使用专网业务，MEC 提供了对用户的多重鉴权方式。

专网用户只能通过专属 PLMN 和专属 APN 接入 MEC 设备。同时 MEC 设备会对想要登录的终端的 SIM 卡的 IMSI 进行鉴别，仅允许在 MEC 中被写入相应信息的终端登录。鉴权过程如下图。



专网数据鉴权过程

博世汽车（苏州）厂区内所有终端通过专属的 PLMN 来接入基站，当 PLMN 不正确时，基站将拒绝连接。当 PLMN 正确时，终端能够接入基站，此时终端将发送 APN 信息和 SIM 卡信息到 MEC 设备进行设备的鉴权。当 APN 和 SIM 卡信息符合 MEC 内设置的信息时，终端才能接入 MEC，进而接入企业内网。

数据备份方面，MEC 支持高可靠性硬件配置方式，透过两台相同硬件的服务器，提供热备份，一旦有任何问题发生即切换到另一台服务器，确保服务可靠性。主 MEC 故障时 1 秒内可以切换到备 MEC，当备用 MEC 上线后，基站和 MEC 重新建立链路，之后终端重连后网络端到端恢复。

4.5. 方案自主研发性、创新性及先进性

【介绍测试床方案的自主研发性、创新性及先进性。】

本项目中基于 5G+MEC 博世专属 5G 内网的优势：

优势一：低时延。内部数据传输通过 mec 智能判断，直连服务器平台，缩短路由，降低时

延，满足工业自动化要求。

优势二：超带宽。本地部署相关应用服务，不受其他应用及核心网带宽限制。

优势三：大连接。本地工业控制器、扫码枪、平板、摄像头等多种终端接入，汇聚 mec，内容汇整增强，减少传输负荷。

优势四：高可靠性。透过两台相同硬件的服务器，提供备份，一旦有任何问题发生即切换到另一台服务器，确保服务可靠性。

优势五：高安全性。所有专网用户内部机密数据皆无需经过公网，对于专网用户，核心网络进行鉴权和定义访问内部网络的权限，电信级别的网络防护，无需第三方平台，将网络受攻击的可能性降低到最低。

优势六：可控可管。宏微（站）结合，优选分布式室内皮站进行覆盖，故障定位易，灵活扩容，支持 5G 网络演进，同时可对企业接入终端用户进行个性化设置管理，减小设备故障概率、提高生产效率。

优势七：低成本。运营商提供独特的企业 LTE 接入解决方案， 快速、安全、优质覆盖，移动性好，摆脱传统有线、无线 WI-FI 等繁杂组网及后期维护困难问题，降低企业 TCO 成本。

4.6. 方案安全风险控制

【方案是否有安全风险应对模型？哪些是最关键部件？哪些是最脆弱的部件？最易受攻击的部件？】

- **系统安全方面**，分三个方面来保障博世汽车（苏州）数据安全：

1. 网络隔离：从终端，到基站，到传输网，到 MEC，公网业务与 MEC 业务高度隔离：专网终端与公网终端驻留不同的 PLMN 网络，相互之间不干扰；基站上联口公网业务与 MEC 业务通过 VLAN 隔离，使用不同网段；传输 B 设备到 MEC、B 设备到公网核心网使用的是不同 VLAN，不同网段；基站只将专网终端的数据转发到 MEC，公网数据不会流向 MEC，确保公网数据安全；MEC 反向访问不到公网业务相关的任何节点。

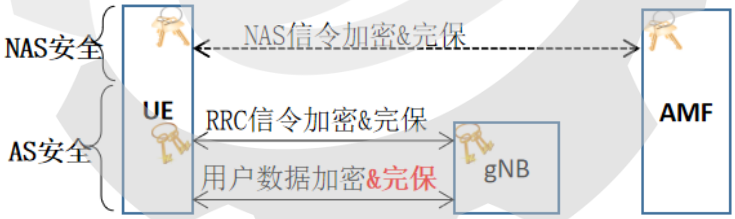
2、安全机制：终端和 MEC 双向认证，确保安全性。

3、NAT 和防火墙：MEC 与企业网之间有 NAT 与内置的 linux 防火墙,可根据需要添加过滤规则，或者部署其他安全软件。

同时，本套组网方案具备高可靠性保证。MEC 支持高可靠性硬件配置方式，透过两台相同硬件的服务器，提供热备份，一旦有任何问题发生即切换到另一台服务器，确保服务可靠性。当部署 MEC 热备份方案，主 MEC 故障时 1 秒内可以切换到备 MEC，当备用 MEC 上线后，基站和 MEC 重新建立链路，之后终端重连后网络端到端恢复。

- **5G 无线空口安全方面：**

5G 的空口安全包括两部分，无线接入层安全（AS）和非接入层安全（NAS）。5G 所采用的空口加密与完保机制如下图：

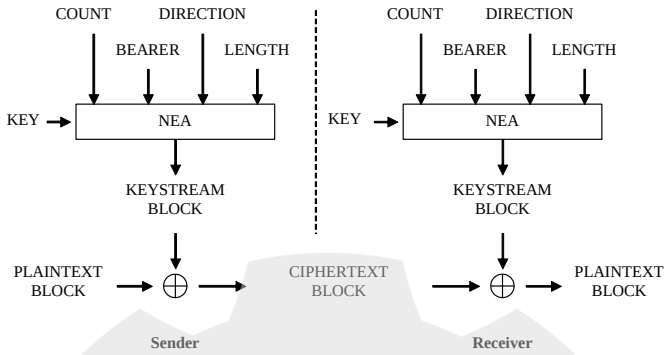


空口安全保护机制

整体加密机制采用的是对称密钥加密体制，即发送数据和接收数据的双方使用相同的密钥进行机密和解密运算。加密作用：为了保证数据安全、防窃听。完保作用：保证数据完整、防重攻击

加密算法：

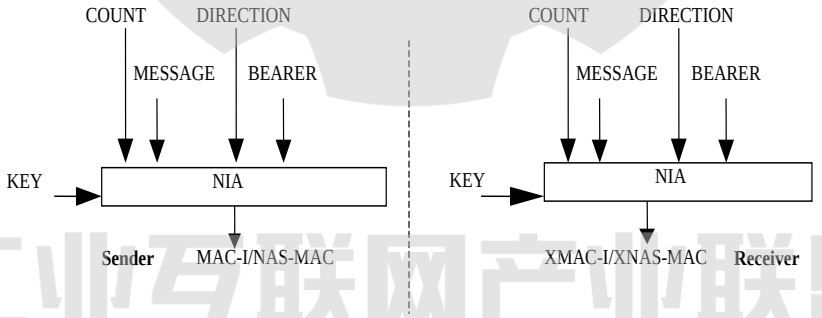
5G 采用数据流加密机制，用算法和密钥一起产生一个随机秘钥流，再和数据流 XOR 一起产生加密后的数据流。解密方只要产生同样的随机秘钥流就可以了。用于生成伪随机密钥流（KEYSTREAM）的加密算法 NEA 包括：NEA0 空算法；128-NEA1 SNOW 3G 算法；128-NEA2 AES 算法；128-NEA3 ZUC 算法。



加密流程图解

完整保护算法：

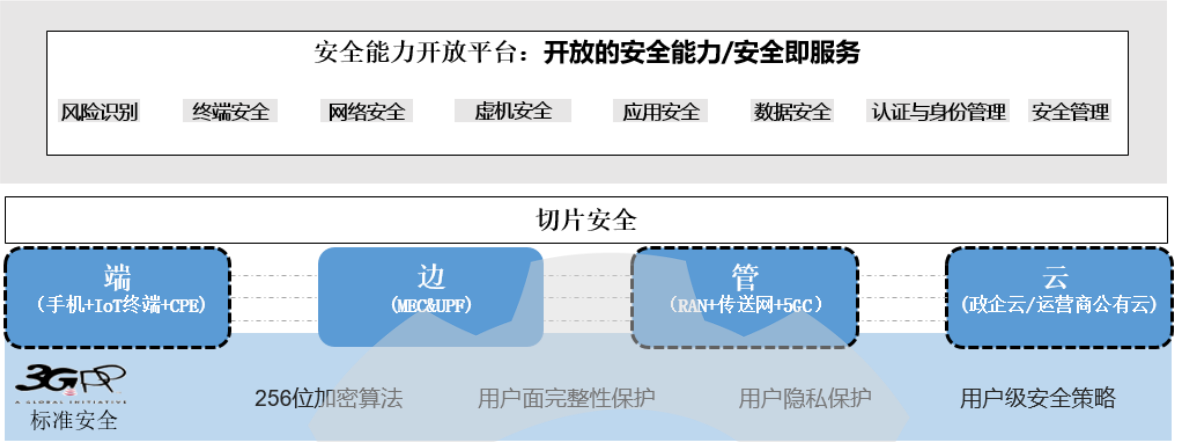
5G 无线安全保护在 PDCP 协议层实现：首先基于 PDCP PDU(header + data part)计算出 MAC-I(32bit)放在 PDU 尾部，然后对 PDCP PDU 的 data part 和 MAC-I 加密。5G 基于如下完保算法 NIA 生成 32bit 的消息认证码 MAC-I，所用算法包括：NIA0 空算法；128-NIA1 SNOW 3G 算法；128-NIA2 AES 算法；128-NIA3 ZUC 算法。



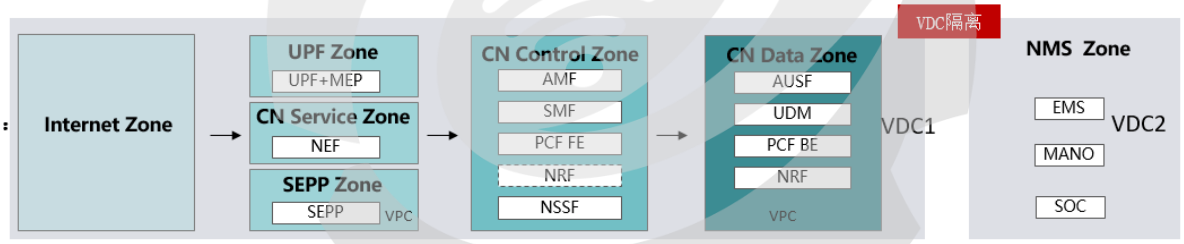
完整保护加密流程

- **5G 定制专网安全方面**

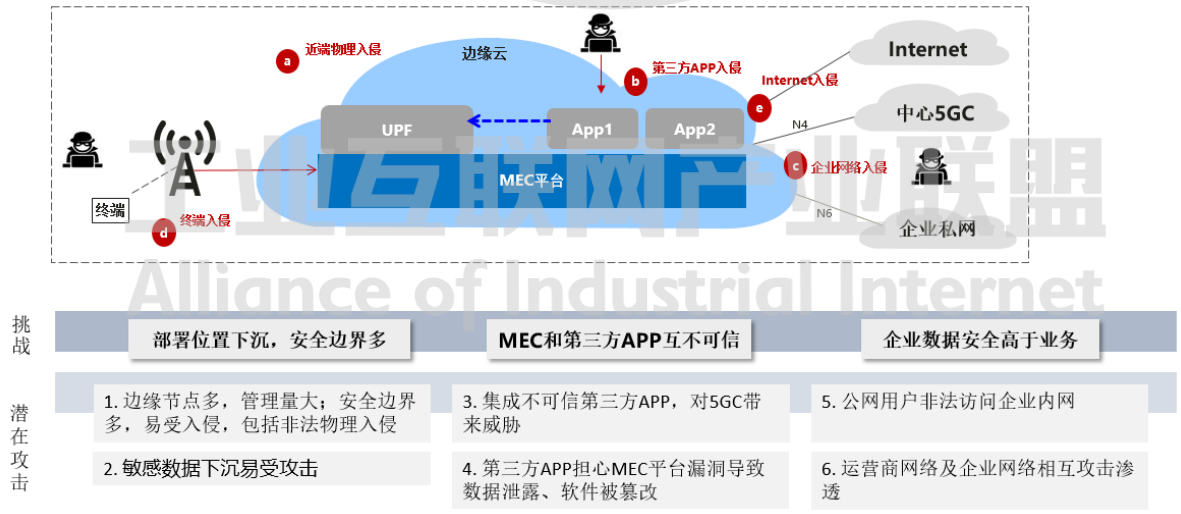
安全解决方案框架如下图所示：



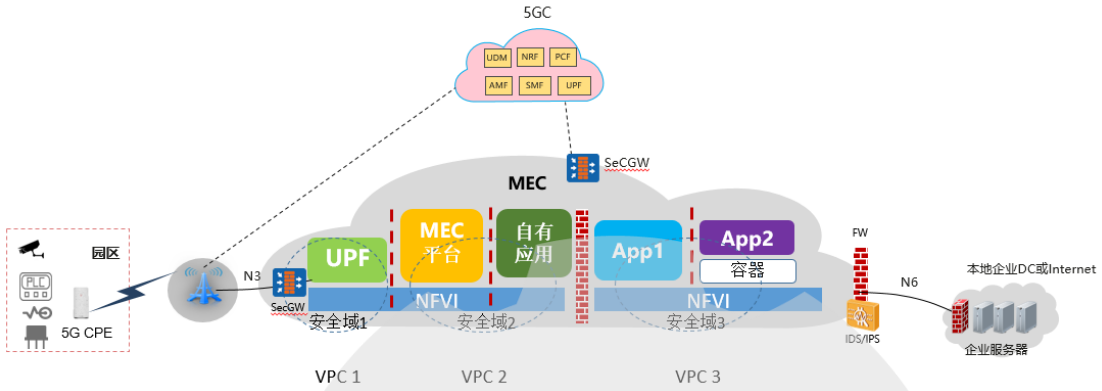
5GC 安全防护策略如下图：核心网网元划分 VPC，硬件独立，硬 FW 隔离。



2B MEC 的主要安全风险如下图所示：



针对风险 1：



分隔安全域、边界防护示意图

实现安全域分隔：MEC 分为三个安全域，同时采用 VPC 技术作安全域隔离，UPF 如基于规模或者流量的需要，可以做基于 I 层的硬件隔离；VPC 之间通过 vFW 或 FW 隔离。

- 安全域 1：承载 UPF，也就是与核心网边缘安全域
- 安全域 2：承载 MEC 平台与运营商自有应用；
- 安全域 3：第三方应用，VM 隔离；

实现边界防护：

- N6 口采用 FW+IPS 组合进行边界防护
- N3 部署 SecGW，与 RAN 实现 IPSec 加密通信
- 可选择 N4 部署 FW/SecGw，与 5GC 实现安全通信

针对风险 2：

配置 MEC 集中威胁监测处置：

- 建设针对 MEC 的 SOC：实现攻击行为、异常流量监测，支持自动化响应
- 构建 2B 客户视图的安全运营管理中心：支持对第三方 App、主机异常监控，能够对 MEC 内部的 VM、容器提供异常攻击行为的监测；

设备安全威胁及策略：

将数据下沉遭受攻击的情况分为以下两种情况，设备安全威胁及解决策略下表所示：

a) 从近端攻击：物理近端接触，破坏、窃取或更换 MEC 部件进行攻击

b) 从外部接口发起攻击

分类	主要威胁	风险	解决方案
物理保护	• 部署于室外或边缘机房，恶意损坏、盗取设备	中	• 机房安全 • 机柜门锁、磁告警；地理容灾
存储数据保护	• 恶意人员可能拆解设备，恶意替换设备器件，运行恶意软件包 • 非法接入存储设备，窃取数据	高	• 加密敏感数据（密钥，口令）；密钥分层管理； • UPF/MEP无IMSI/MSISDN等用户标识信息；UPF实时上报核心网计费信息本地不存储 • 基于硬件的安全启动、可信启动；
端口安全	• 物理端口接入系统	高	• 默认关闭本地维护端口 • 接入认证和授权
软件安全	攻击者或者恶意操作人员利用运维通道、设备近端接口、应用通信协议、软件实现漏洞等 • 利用缓冲区溢出漏洞攻击 • 对软件包或配置进行篡改，如篡改操作系统内核对系统资源的恶意访问和控制	高	• 安全加固：去root化、安全编译选项等， • 内部网络平面隔离 • 安装时的软件安装包完整性校验； • 基于硬件的安全启动、可信启动； • 主机入侵检测HIDS • 关键文件完整性检查
容器安全	• 裸机容器部署，资源共享，部分容器被攻击后存在攻击Host OS后，进一步攻击其他容器	中	• UPF/MEP独占物理主机资源，APP独占物理主机资源 • 容器安全加固 • 基于SeLinux强制访问控制； • 容器安全监控平台

MEC 对外接口安全威胁及策略：

分类	主要威胁	风险	解决方案
控制面接口：N4	• 非法访问 • 信息伪造、明文信息泄露	中	• IPSec（内置或SeGW） • ACL,网络平面隔离
管理面接口：O&M, Mm4, Mm5, Mm6	• 非法访问 • 伪造或篡改管理信息导致恶意操作	中	• 安全协议（HTTPS, SNMPv3,ssh） • 认证授权,集中日志审计 • ACL,网络平面隔离
用户面接口：N3, N9, N6	• 数据被拦截 • 伪造恶意数据，畸形报文攻击 • N6口流量攻击	高	• 可选的IPSec（内置或SeGW） • N6接口内置或外置防火墙 • 防UE IP假冒，基于接口的ACL，基于UE的ACL；对畸形报文检测防攻击；对UE QoS进行控制 • ACL,网络平面隔离 • 恶意UE检测

针对风险 3、4：

分类	主要威胁	风险	解决方案
MEP和APP之间的Mp1接口，O&M接口	威胁来源：APP安全性不足导致被攻击后成为跳板；恶意APP攻击 • API调用未授权 • APP发起拒绝服务攻击 • 通过OM接口发起拒绝服务、命令注入攻击 • 外部攻击导致APP利用率过高	高	• APP独立刀片服务器部署； • APP部署时的软件包签名校验；APP安全认证 • APP与MEP之前内置或外置FW，实现隔离和访问控制 • API认证授权、API流控、API调用加密 • 主机入侵检测HIDS • 资源KPI监控 • 内部隔离：MEP对接APP的微服务独立容器部署；
MEP与UPF的内部Mp2接口	• MEP被入侵后，通过MEP访问UPF的接口 • MEP被入侵后，通过容器、虚拟机逃逸后再攻击UPF	低	• UPF/MEP不同微服务使用不同容器隔离 • UPF模块与MEP模块为微服务框架，服务间支持认证加密
Vn-Nf虚拟化接口	• APP所在虚拟机\容器利用系统漏洞逃逸到APP所在HostOS • 通过该Host OS横向攻击其他Host	低	• 安全加固，虚拟资源隔离 • APP独立刀片服务器部署 • 安全容器 • 主机入侵检测HIDS

针对风险 5，6：

构建企业 5G 私网：

- 通过 APN/DNN 等方案组成企业子网，只允许无线侧接入；
- 人，卡，机多因子鉴权；机卡绑定；企业 AAA 二次鉴权，仅特定终端可以访问；
- 配置基站白名单，基站仅允许专网用户接入（需额外配置）：

规划建设独立 DNN，本地 MEC 作为边缘 UPF，为园区区域规划独立 TA 区，规划独立 MEC DNN。省份专网 AMF 上配置指定 TA 表和号段（号码）关联，并配置接入限制白名单，用户从指定基站接入后，AMF 根据用户接入的 TA 和号码匹配白名单，通过白名单匹配的用户，可以接入，白名单号码在 UDM 中签约区域漫游限制，不允许从其他 TA 下接入。

企业内部用户签约独立 DNN，可以正常使用；企业外用户，也会接入到独立 DNN，但是会被拒绝认证，导致无法使用 5G。企业内网用户附着激活后由 SMF 根据独立 DNN 选择本地 MEC UPF，对边缘业务进行本地流量卸载，实现业务流量不出园区。

业务流程：

1. 企业用户终端（白名单用户）进行 5G 激活附着；

2. AMF 配置根据 TAI+DNN 选择 SMF；

3. SMF 通过 DNN 选择 UPF；企业用户使用特定行业 DNN，选择 MEC UPF 根据数据报文的用户面路由转发。

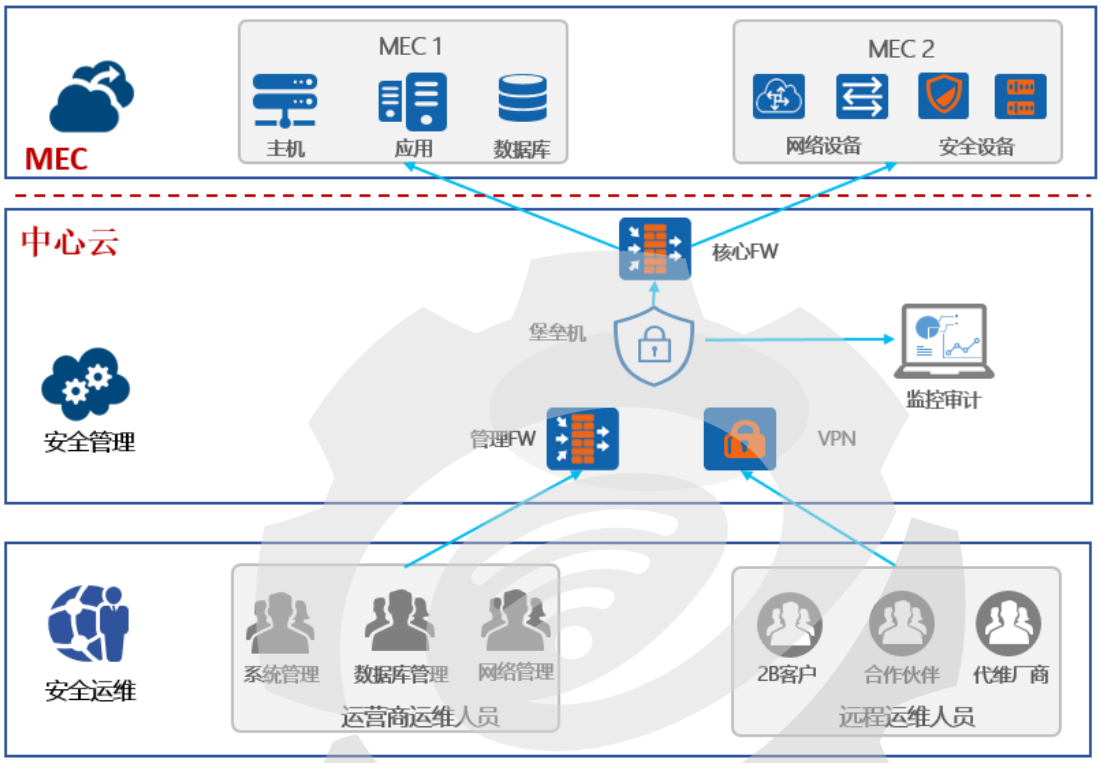
4. 企业用户移动到企业园区外，AMF 中断终端会话，强制用户下线。

5. 企业外用户（非白名单用户）无法激活，在园区内无法正常使用 5G。

确保网络数据机密性和完整性：

- 建立数据传输加密管道，包括空口加密完保、基站与 MEC IPSec 加密、MEC 与企业云 IPSec 加密传输；
- 企业应用层自身加密、CPE 安全隧道；

保障 MEC 运维安全：在中心云构建统一的 MEC 运维堡垒机。



管理区域部署堡垒机，对运维人员进行统一认证、单点登录、授权、操作审计等，主帐号过双因素动态口令认证加强安全性堡垒机部署在管理维护区，部署位置灵活，路由可达即可核心交换机旁挂 VPN，外网运维人员、2B 客户应用维护人员通过 VPN 隧道安全接入内网，登录堡垒机系统进行统一运维操作；禁止直接登录设备和云平台。

五、 测试床实施部署

（正文 小四 宋体。行距 1.5 倍行距）

5.1. 测试床实施规划

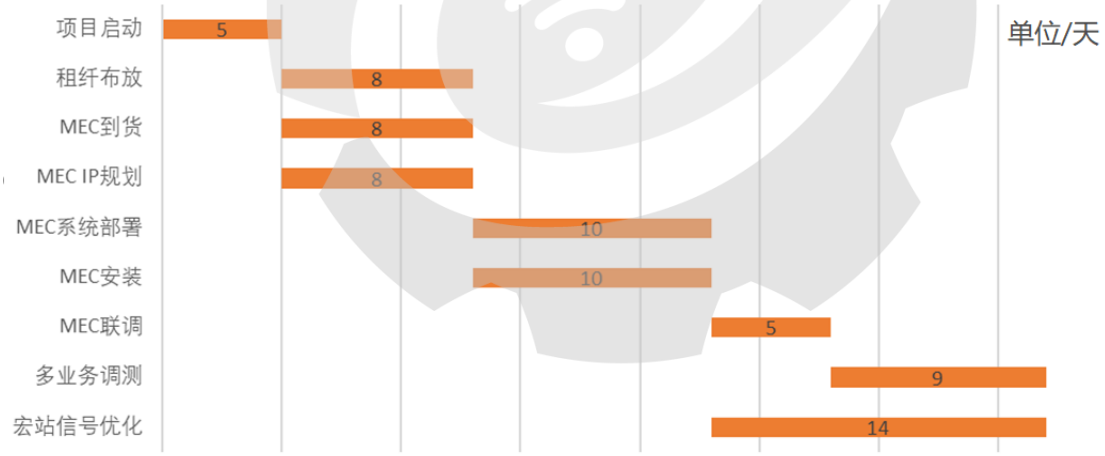
【明确测试床实施的时间规划。】

实施规划周期

从实施周期仅供参考，根据实际情况调整。

各阶段任务	工作内容	部门
项目启动	项目启动，职责分工	A11

租纤布放	MEC 至传输设备专线布放	电信
MEC 到货	MEC 硬件设备到货	诺基亚
MEC 安装	MEC 设备安装	电信
IP 规划	MEC 至企业、基站、传输 B 设备的 IP/VLAN 规划	电信/企业
MEC 部署	MEC 软件部署和调测	诺基亚
MEC 联调	MEC 与企业/基站 IP 路由调测，实现终端 ping 通企业服务器	诺基亚/电信/企业
多业务调测	企业业务测试及时延优化	电信/企业/诺基亚



5.2. 测试床实施的技术支撑及保障措施

【说明测试床实施的技术支撑及保障措施。】

项目维护和服务方案如下：

事件或故障定义和描述

- 事件或故障定义和描述

  该大客户发生影响业务的网络故障或重要业务阻断障碍。

- 事件或故障的影响面分析

  影响大客户网络或重要业务的通信。

1.2、事件或故障处置原则

- 处理原则

1、障碍申告

1）在客户端现场的故障修复过程中，要求现场维护人员每 30 分钟向客户调度中心汇报障碍处理的情况和进展；

2）并根据重要大客户业务故障处理的问题升级制度，将故障情况逐级向上报告；

2、障碍处理

1）客户端现场维护人员在接到用户障碍申告后，应迅速作出响应；

2）对客户端的故障处理应严格遵守大客户故障处理流程（或与客户签订的差异化服务协议或 SLA 服务协议）；

3）本着“对客户负责到底”的原则，并遵循“先抢通，后排障”的原则在规定的时间内恢复业务。

3、处理结束

1）应认真听取并记录用户的意见和建议，耐心解答用户提出的问题；同时详细记录故障现象及故障处理过程，并向客户调度中心反馈处理结果与情况；

2）故障处理完毕后，应在客户端继续观察 10 分钟（重复发生的故障应适当延长时间），确认故障已经彻底排除，业务恢复稳定后，方能离开；

- 业务领导关系

  服从客户调度中心大客户受理岗的调度。

1.3、应急处置组织体系

- 组织构成

  团队组成部门：客调中心，政支中心，网维中心，无线中心，厂家团队，江苏电信支撑团队，天翼物联支撑团队。

- 各层、各级职责分工

中国电信苏州分公司大客户服务支撑团队，由网络管理部统一组织和协调，由客户调度中心统一匝口负责大客户障碍接应保障和应急调度工作，政企客户支撑中心负责用户现场维护，网络监控中心负责相关专业技术支撑工作，无线维护中心负责基站的日常维护和

信号优化，江苏公司网络操作维护中心负责用户信令流的对接分析工作，电信天翼物联公司负责进行物联网卡的数据制作。

苏州电信分公司客户调度中心职责包括：作为大客户售后服务统一接口，负责承担向客户提交维护障碍故障报告，设置报障电话如 10000+9 单独专席服务电话接应用户障碍申告，对障碍进行有效预处理及应急启动响应预案等。

苏州电信分公司政企支撑中心职责包括：大客户现场服务，提供 7×24 小时的网络技术支持以及设备的维护服务；对客调中心派发的故障单进行及时有效的闭环操作和现场应急抢修调度。向客调中心提交配置变更、问题总结、性能优化方案以及常规维护报告；按照差异化服务标准开展大客户主动性巡检工作。

苏州电信分公司无线维护中心职责包括：对博世厂区内部信号优化，基站的日常维护巡检和升级，基站网管的后台支撑及现场障碍处理。

苏州电信分公司网络操作维护中心职责包括：作为电信后端技术管控支撑部门，负责大客户网络设备核心监控及障碍抢修的技术支撑职责。

江苏电信网络操作维护中心职责包括：对博世卡信令流的监控和对于疑难终端上线问题的定位抓包。

中国电信天翼物联公司职责包括：物联网卡的数据制作，提供 CMP 卡管理平台，监控卡流量等信息。

人员

序号	保障部门	保障地点	职责
1	客户调度服务中心	局端	障碍调度管控、启动应急预案
2	政企客户支撑中心	用户机房	客户端现场保障、执行应急预案具体操作
3	无线维护中心	基站	无线信号优化，基站障碍分析
4	苏州网络操作维护中心	局端	传输网络、交换网络核心层保障。

5	省网络操作维护中心	局端	核心网信令流跟踪抓取
6	天翼物联公司	局端	物联网卡管控，数据监测

1.4、应急调度或处置方案

用户重大业务中断解释为用户中心机用户核心业务全阻故障，影响用户生产作业，需启动应急预案：博世无论从线路保护、设备单板保护等保护措施，安全性都较高，为防万一，我们特制定更为完善的应急方案如下

- 局端设备应急保障预案

1）定期进行局端核心网元及用户端设备的备份和检查，确保备份的网元数据和实际运行数据相一致，并在软件故障发生后能通过备份数据迅速恢复故障。

2）在全程路由的核心节点，对主要硬件板卡进行热备份和冷备份。

3）EMS 网管平台 UPF 进行性能监测，对业务进行 24 小时不间断的性能检测，做好主动性维护工作。

4）对设备出现不可逆的障碍，将由苏州电信客调中心立即调度政企客户支撑中心现场支撑工程师在最短时间内赶至用户现场，并调度相关设备厂家驻苏人员一并前往，进行抢修，网络操作维护中心支撑人员负责提供技术支撑，首先恢复受阻业务。在业务恢复正常后，再着手进行故障原因的排查，其间，电信客调中心将负责与现场支撑工程师的联系，并按重大障碍汇报流程逐级汇报上级部门。

5）障碍定位到长途核心层和对端局点故障的，由客调中心负责启动集团一站式系统派发障碍处理单，通过集团公司管控相关本地网进行障碍的应急抢修和调度。

- 基站故障应急调度预案

1）设置障碍监控岗位负责 7×24 小时的故障监控工作，在发现疑似重大障碍现象的 10 分钟内将故障派各代维管理人员；

2）障碍监控人员在障碍开始的 15 分钟内将障碍时间、影响基站数量、基站大致所属范围（区域）短信通知部门领导及无线重大障碍支撑岗，障碍支撑人员在障碍开始的 20 分钟内，根据资料梳理基站对应传输设备、光路资料，提供无线重大障碍支撑岗，将监控岗梳理的传输、光缆信息，告知其他专业障碍协调人，要求调度抢修。

3）现场代维处理人员在接障后 5 分钟内初步判断障碍性质、大致影响范围、预计修复时间，并通知监控岗；短时间无法定位的障碍需在接障后 20 分钟内将定位信息反馈监控岗。

4)处理人员每 30 分钟与监控岗进行沟通，汇报障碍处理进度，如其他专业（如光缆、传输）处理中，了解告警及业务恢复情况，并将信息反馈监控岗。

5)为满足无线障碍应急处理需求，无线维护中心设立了无线设备应急仓库，应急设备包括 2G/3G/4G/5G 的所有设备及板卡，7*24 可领取，确保应急备件需求发起后快速将备件送达现场。

6)光缆障碍确认断纤情况后，优先发起调纤流程，无法调纤的按照重大障碍处理流程升级至区局、接入维护中心、网络操作维护中心和网络部，确定抢修时间后跟踪处理进度；

- 专线故障应急调度预案

1）当苏州电信客户调度中心综合各方情况，确认为用户接入光缆中断的极端情况，影响用户业务的，由客户调度中心立即启动紧急预案，通过电话，保持同客户的沟通，尽可能利用未断光缆先恢复故障光缆所承载的重要业务，未影响用户业务的，客调中心仍需直接联系现场维护工程师，并派发障碍单进行障碍管控。

2）调度中心值班人员在与两端用户沟通的同时，立即通过调度系统派发障碍单，调度抢修人员前往用户端进行抢修。必要时 VIP 中心“兵分两路”，前往用户端及相应光交接箱，协调处理，重点是先恢复中断的业务。调度中心值班人员做好相应联络配合工作，并提供一切必要的方案、资料数据，协助现场维护人员抢修障碍。

3)当通过调度备份路由纤芯，经用户确认业务、告警恢复后，调度人员依此作为障碍结单的依据进行结单，但现场抢修人员仍应继续查修故障的光纤纤芯，可利用 OTDR 或光功率计等光纤测试仪表全程测试租纤的各项性能参数，精确判断纤芯障碍具体断点。如障碍点发生在光交接箱内，现场抢修人员应立即前往所在障碍点光交，在局端及用户端抢修人员的配合下完成调度空纤或更换法兰盘的工作。

- 客户侧设备故障应急调度预案

对于客户侧设备故障引起的故障，如客户核心防火墙等，由苏州电信政企客户支撑中心全力配合客户完成修复，提供与 UPF 对接的 ip 信息和相关配置备份，必要时可以赶至用户现场协助

2.1 维护基本条件

古话说的好，“巧妇难为无米之炊”，对各系统的维护来说也是一样的道理，对系统进行正常的设备维护所需的基本维护条件，即做到“四齐”，即备件齐、配件齐、工具齐、仪器齐。

维护注意事项

在对系统设备进行维护过程中，应对一些情况加以防范，尽可能使设备的运行正常，主要需做好防潮、防尘、防腐、防雷、防干扰的工作。

1)防潮、防尘、防腐

对于系统的各种采集设备来说，由于设备直接置于有灰尘的环境中，对设备的运行会产生直接的影响，需要重点做好防潮、防尘、防腐的维护工作。如摄像机长期悬挂于棚端，防护罩及防尘玻璃上会很快被蒙上一层灰尘、碳灰等的混合物，又脏又黑，还具有腐蚀性，严重影响收视效果，也给设备带来损坏，因此必须做好摄像机的防尘、防腐维护工作。在某些湿气较重的地方，则必须在维护过程中就安装位置、设备的防护进行调整以提高设备本身的防潮能力，同时对高湿度地带要经常采取除湿措施来解决防潮问题。

2)防雷、防干扰

只要从事过机电系统的维护工作的人都知道，雷雨天气一来，设备遭雷击是常事，给设备正常的运行造成很大的安全隐患，因此，设备在维护过程中必须对防雷问题高度重视。防雷的措施主要是要做好设备接地的防雷地网，应按等电位体方案做好独立的地阻小于 1 欧的综合接地网，杜绝弱电系统的防雷接地与电力防雷接地网混在一起的做法，以防止电力接地网杂波对设备产生干扰。防干扰则主要做到布线时应坚持强弱电分开原则，把电力线缆跟通讯线缆和视频线缆分开，严格按通信和电力行业的布线规范施工。

2.2 常规服务、日常运营巡检计划

维护要求：

1、定期对网络、硬件设备、软件系统、存储数据进行巡检、保养；

2、每月对所有外场设备进行巡检、保养；

3、每年对所有外场设备的金属部件进行防锈保养；

4、每次巡检、保养必须进行详细记录并报确认，每月向采购方报送巡检、保养报表；

机房巡检内容如下：

<table>
<tr><td>客户名称</td><td colspan="2"></td><td>联系人</td><td colspan="2"></td></tr>
<tr><td></td><td colspan="2"></td><td>电 话</td><td colspan="2"></td></tr>
<tr><td>客户地址</td><td colspan="2"></td><td>巡 检 时 间</td><td colspan="2">年 月 日</td></tr>
<tr><td>巡检部门</td><td>中国电信苏州分公司</td><td>巡检人员</td><td></td><td>联 系 电 话</td><td></td></tr>
<tr><td colspan="6">机房环境检查</td></tr>
<tr><td>机房环境</td><td colspan="3">机房温度 20 度 湿度 40 %</td><td colspan="2">☐ 正常 ☐ 异常</td></tr>
<tr><td rowspan="2">机柜检查</td><td colspan="3">机柜防尘防鼠</td><td colspan="2">☐ 正常 ☐ 异常</td></tr>
<tr><td colspan="3">机柜接地情况</td><td colspan="2">☐ 正常 ☐ 异常</td></tr>
<tr><td colspan="6">设备运行状况检查</td></tr>
</table>

网上运行受理服务器运行状况	☐ 正常 ☐ 异常	网上运行统计服务器运行情况	☐ 正常 ☐ 异常
网上运行处理服务器运行状况	☐ 正常 ☐ 异常	网上运行统计数据库运行情况	☐ 正常 ☐ 异常
短信网关运行状况	☐ 正常 ☐ 异常	MQ 前置机运行情况	☐ 正常 ☐ 异常
录音及软电话数据库服务器运行状况	☐ 正常 ☐ 异常	服务器运行状况	☐ 正常 ☐ 异常
设备的连接情况检查			
专线连接是否正常	☐ 正常 ☐ 异常	走线是否整洁、规范，标识是否清晰	☐ 正常 ☐ 异常
网线连接是否正常	☐ 正常 ☐ 异常	走线是否整洁、规范，标识是否清晰	☐ 正常 ☐ 异常
巡检人员签字			
客户意见或建议：			
客户签字		电信签字	

基站巡检内容如下：

主设备网管上可监控，状态异常时直接短信派发工单到维护人员手机，正常情况每 3 月巡检一次，巡检要求如下：		
巡检模块	巡检子项	巡检要求
信源设备	主设备是否正常	检查信源主设备是否运行正常

检查	电源线及接电器是否正常	检查电源线和接电器是否正常
	光缆及接口是否正常	检查现场线缆走线是否整齐、规范，线缆接头是否紧固
	接地是否正常	检查室分系统是否正确接地
	天馈接头是否正常	检查天馈接头是否紧固，是否包扎完好
直放站远端机检查	直放站远端机检查	检查检查直放站远端机是否运行正常
信号测试	信号测试 1	天线一测试
	信号测试 2	天线二测试
	信号测试 3	天线三测试
	信号测试 4	一层的中心
	信号测试 5	顶层的窗口
	信号测试 6	地下室测试
	信号测试 7	电梯
	信号测试 8	入口
现场环境检查	温湿度检查	检查室分信源所处环境的温湿度符合要求
	环境检查	检查室分信源所处环境是否清洁，有无堆积物，定期进行保洁和堆积物清理
	安全隐患检查	检查室分信源所处环境有无水浸或火灾隐患
	标签检查	检查室分系统各标签和标识是否清晰，正确，完整
资料更新	地址信息和图纸检查	系统图、平面图、接电系统图更新
无源设备检查	合路器是否正常	检查合路器是否正常
	主干部分是否正常	检查主干部分是否正常
	天线是否正常	检查天线是否正常

2.3 特殊服务计划

I. 每季度一次设备的除尘、清理，扫净设备显露的尘土。

II. 根据系统各部份设备的使用说明，每季度检测其各项技术参数及系统传输线路质量，处理故障隐患，协助主管设定使用级别等各种数据，确保各部份设备各项功能良好，能够正常运行。

III. 对容易老化的设备部件每季度一次进行全面检查，一旦发现老化现象应及时更换、维修。

我方中标后，将根据招标方要求对所有招标项目涉及的系统项目的设备现状生成报表提交给招标方确认，在此之前如果检查出有设备损坏，更换设备所产生的费用经审计后由招标方负责。

（如与招标文件有冲突的，以招标文件时间为准）

2.4 产品的技术服务和售后服务的内容、措施和承诺

- 对所有已经出保的设备提供至合同到期的设备硬件维护服务，设备的正常损坏所造成的更换、维修费用由招标方承担，但我方将免费提供设备的拆卸及安装调试服务。
- 派遣技术人员中心进行日常服务，排除系统故障，保障整个系统的正常运行。
- 对整个系统进行定期巡检服务，及时发现设备的损坏或系统的功能异常。
- 对整个系统所有设备进行必要的定期保养服务。
- 负责视频综合应用平台软件的功能维护及软件版本升级。
- 对招标方的重大事件和重大活动进行技术支持和现场保障服务。
- 对室外设备进行巡检并承担由于非正常因素引起的设备损坏、偷盗而无法索赔的风险。

2.5 备品备件

维护过程中，我方会提供一定比例的备品备件，以方便设备损坏后的维护工作，我方对这些设备的维护标准等同于运行设备。若我方在故障维修中用备品备件顶替原设备运行，则换下的故障设备应在最短时间内送修后作为备品备件。 因本次项目重点为设备的搬迁，

多数设备为利旧设备，新增设备较少且都是不需要提供备件的设备，所有我方提供的备品备件重点考虑了系统组成中较多的、较易发生损坏的设备。

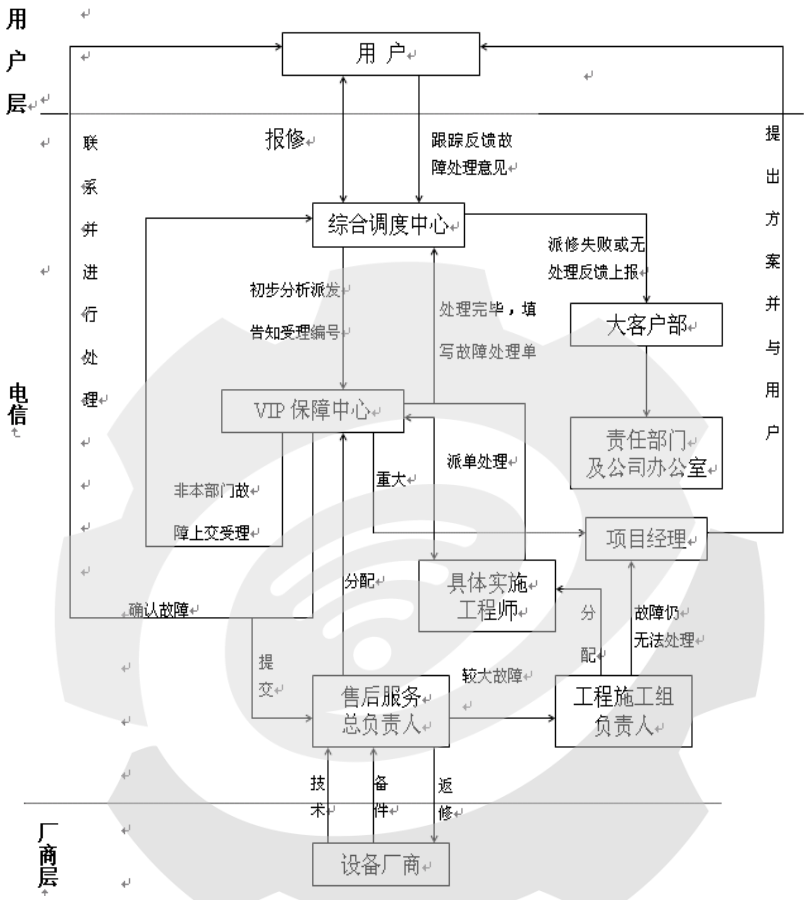
2.6 维护档案、服务建议等

平时在巡检或者维修的过程中我方会及时更新档案的数据资料，为用户提供一手的档案信息，建议用户配备相关专业的 IT 人员，达到事半功倍的效果。

- 为确保本项目中涉及的传输网络电路安全、稳定安全，特制定以下应急方案及保护措施。
- 本应急保障方案同时适用吴中区政务外网出口光纤租赁项目主用电路租赁服务和备用电路租赁服务。

2.7 售后服务体系

经过多年的建设和运营，苏州电信不仅建立了一支高水平、高素质的专业技术支持队伍，同时还建立了一套完善的支持售后服务体系。



5.3. 测试床实施的自主可控性

【说明测试床实施的自主可控性。】

自主可控。

六、 测试床预期成果

（正文 小四 宋体。行距 1.5 倍行距）

6.1. 测试床的预期可量化实施结果

【明确测试床的预期可量化实施结果，针对测试项。】

- 物料拿取和放置自动化。实现动态化多区域无人物流：减少 50%厂内物流管理成本和 30%在线物料库存。

- 利用数据分析进行的工艺监控和优化要求的样本完整性提高接近真实场景，确保分析结果的准确度，为机器学习和深度学习打下良好基础：基于此目的 IT 基建成本减少 50%；实现生产线“无感”改造和快速部署。
- 量产情况下，实现实时 AI 算法结果反馈，确保缺陷产品的实时在线自动分流：同工艺，AI 视觉检测的比例达到 99%；光学检测的工艺成本降低 50%。

6.2. 测试床的商业价值、经济效益

【说明测试床的商业价值、经济效益。】

随着智能制造和工业互联网技术的成熟，制造型企业对于设备的连接数量，生产布局的灵活程度以及更灵活的通讯模式都有了越来越高的要求。基于有线和 wifi 的网络架构在连接数、数据传输等方面存在诸多的限制。5G 技术的发展正好契合了工业化 4.0 的进程需要。

连接数的大量提升：随着各类 IOT 技术的使用在生产设备上需要用来采集的数据越来越多，5G 对客户端连接能力的提升解除了这一类限制。

网络连接的灵活性：90%的工业生产的设备是基于有线网络，这样的模式限制了设备模块化和产线的灵活再组的期望，5G 让生产线的布局更加的灵活。

端对端的通讯模式：在工业生产信息化后，数据中心化的 IT 架构使得每台设备必须经过数据机房的服务器进行数据交互，服务器的性能在很大程度上制约着生产进程。5G 的 D2D 技术可以让生产回归到真实，实现去数据中心化。

6.3. 测试床的社会价值

【说明测试床的社会价值。】

博世与中国电信签约共建 5G 智慧工厂，是苏州工业园区 5G+工业互联网先行先试的典范，是园区聚力创新、推进产业升级进程中，需要重点发展的模式。以本次共建 5G 智慧工厂为契机，持续打造园区 5G+工业互联网标杆项目，形成可复制可推广的经验，拉动园区整体产业发展，成为园区"金字招牌"。

6.4. 测试床初步推广应用案例

【证明测试床的对外服务性。】

七、 测试床成果验证

（正文 小四 宋体。行距 1.5 倍行距）

7.1. 测试床成果验证计划

【明确测试床成果的验证计划。】

主要验证项目 5G 网络覆盖、5G 网络特性和 5G 行业应用效果。

5G 应用测试的基本程序：

收集资料-----现场踏勘------编制测试方案----测试前的设备调试（调试至正常工作状态）-----现场测试并采集影像资料-----影像判读与编辑------数据总结及测试报告-----编写技术总结报告-----提交评估测试报告。

7.2. 测试床成果验证方案

【明确测试床成果的验证方案，涉及对设备单元、信息系统、关键技术、多样场景等的全面验证。】

- **标准依据**

1. 3GPP TS 38.521 Release 15
2. 具体应用场景的相关行业规范（若有）

对 5G 网络性能需求：

根据工厂量产应用的要求，对 5G 网络的关键指标要求如下：

编号	应用名称	上行带宽（Mbps）	下行带宽（Mbps）	最大时延（ms）	可靠性
1	MES@Edge	10	500	10	99.999%
2	AI 辅助图像质检	50	10	8	99.999%
3	Sensor 数据采集	5	10	8	99.999%

- **仪器和方法**

本次测试仪器采用 5G 商用终端或专用测试设备，具体型号如下：

编号	终端型号	版本号
1	华为 Mate20X	
2	CMCC FR01	
3	专用设备（若有）	

通过测试，5G“101 车间”覆盖情况为：5G 信号强度-80.98dbm，最大下行速率 964Mbps，平均下行速率 950.12Mbps，最大上行速率 116Mbps，平均上行速率 92Mbps，平均时延 9ms。上述 5G 网络覆盖测试结果表明，该项目的被测区域 5G 网络覆盖水平达到行业应用的关键指标要求。

实际测试结果表明，MES 生产数据采集应用场景每条通讯报文的时长都在 20ms 以内，收发率 100%，可以满足 MES 生产系统的通讯要求。

通过检测，AI 辅助图像质检到 MEC 的平均时延为 8 ms，上行带宽平均 92 Mbps，满足每秒 20 张照片的处理需求。

通过检测，Sensor 传感器数据采集的线路时延为 7 ms，带宽为 100 M，满足应用要求。

八、 与已存在 AII 测试床的关系

【请说明测试床和之前已经审批的测试床的关联关系，以防重复申请。并考虑互操作性。】（正文 小四 宋体。行距 1.5 倍行距）

九、 测试床成果交付

（正文 小四 宋体。行距 1.5 倍行距）

9.1. 测试床成果交付件

【请确定测试床需要提供的交付件：阶段目标及阶段交付件、最终交付件、测试床成功标准。测试床成果需包含至少一项知识产权，包括专利、商标、版权等。】

项目主要设备清单（例）

编号	名称	规格	单位	数量	备注
1	华力建设、星港变电站、北环东路与苏嘉杭交叉西北基站	AAU5613	个	3	华为
2	博世汽车室分系统	PRRU5936	套	4	华为
3	MEC 边缘计算设备	AirFrame RM19 DC Compute	套	1	诺基亚
4	AOI 内置工业相机	TRI	套	1	Type7500
5	PLC	倍福，力士乐	台	5	Opcon Plus
6	Sensor 传感器	Keyence；力士乐	套	2	LK-H080；CS 系列
7	CPE	NR100	台	3	四信

9.2. 测试床可复制性

【明确测试床可复制于哪些行业、哪些场景。】

博世汽车电子中国区的 5G 应用试点，是基于量产的环境，在实际生产线上运行的应用。一旦试点完成，就可直接复制。

9.3. 测试床开放性

【证明同行企业或者上下游企业的共同参与度。】

十、 其他信息

（正文 小四 宋体。行距 1.5 倍行距）

10.1. 测试床使用者

【明确非发起方的公司可以使用测试床程度，以及相关的要求和限制条件。】

10.2. 测试床知识产权说明

【请清晰说明谁对测试床的建设、运营以及使用拥有产权。】

10.3. 测试床运营及访问使用

【请说明测试床如何部署、运营以及访问使用。】

10.4. 测试床资金

【请列出预估的资金需求和资金来源。】

10.5. 测试床时间轴

【请列出测试床的建设、部署和运行时间段。预估关键的时间点。标明是短期项目还是需要多年的研究项目。】

10.6. 附加信息

【请列出其他有价值的信息以便委员会更好的对测试床提案申请进行评估和决策，如可应用复制的行业等。】