基于 5G MEC 数据驱动模式的智慧工厂测试床

引言/导读

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”。

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。

关键词

工业互联网，数字化，智能化，互联化，价值流闭环。

测试床项目承接主体

发起公司和主要联系人联系方式

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

合作公司

无。

测试床项目目标

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，**逐步测试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。

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。

测试床方案架构

测试床应用场景

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。

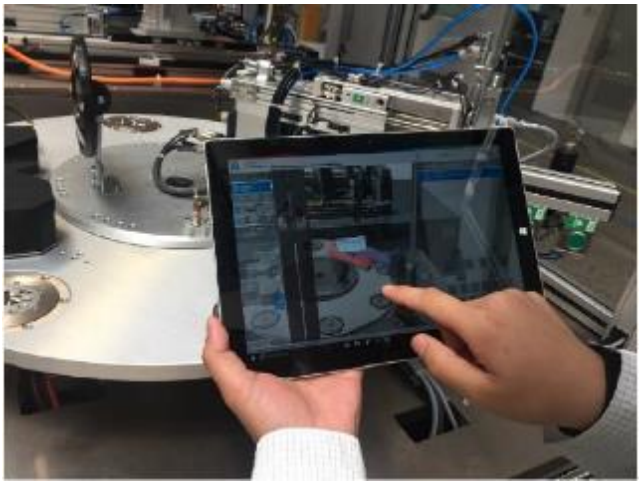
- 5G边缘云化AGV

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

测试床架构

测试床方案

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；

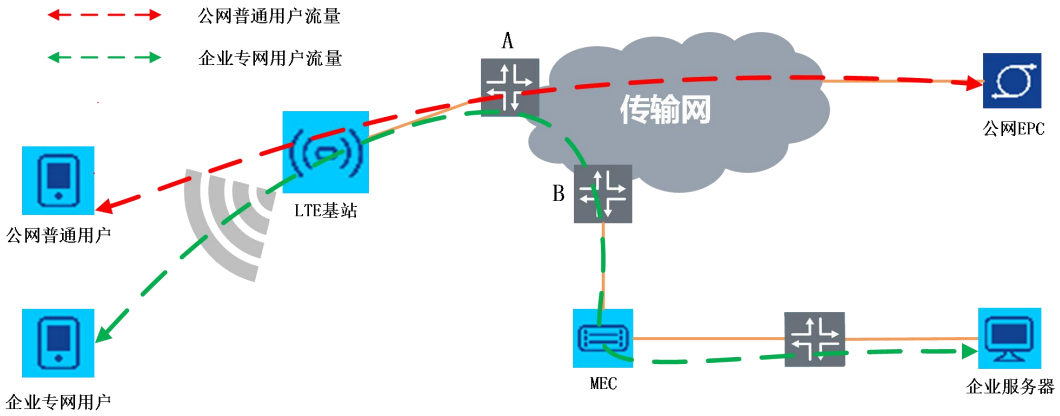
4、MEC 侧：在客户机房搭建热备方案，并和基站进行对接，建立 S1 链路；

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。

方案重点技术

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。



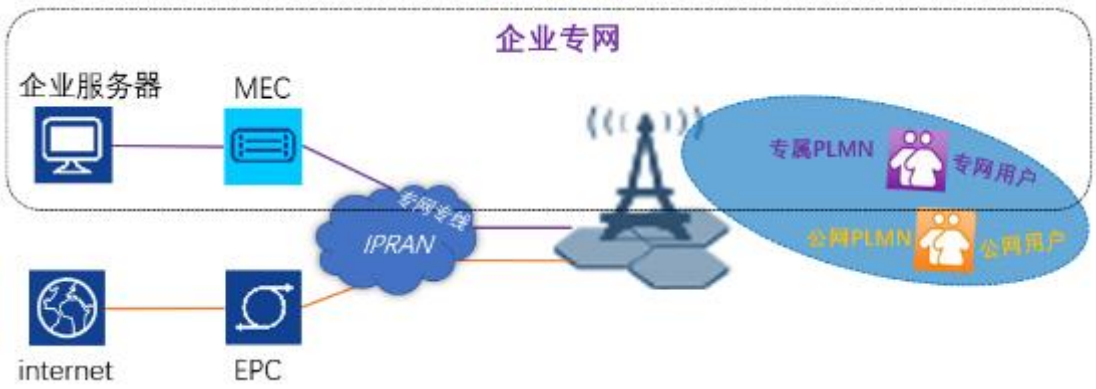
基于 5G MEC 的专网组网方案

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。

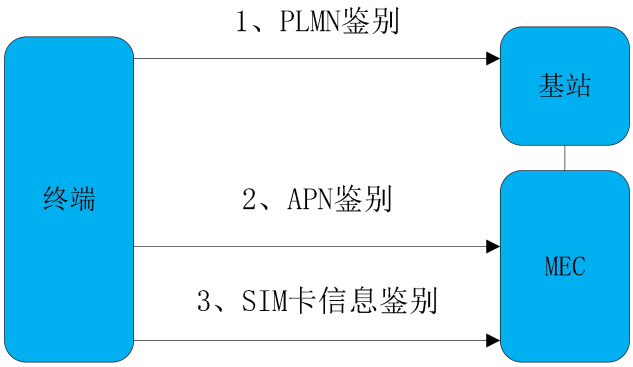
下行路由方案：从 MEC 往基站方向。

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。

方案自主研发性、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。

方案安全风险控制

- **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。

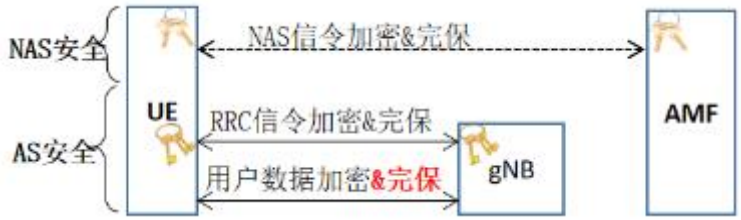
2、安全机制：终端和 MEC 双向认证，确保安全性。

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：

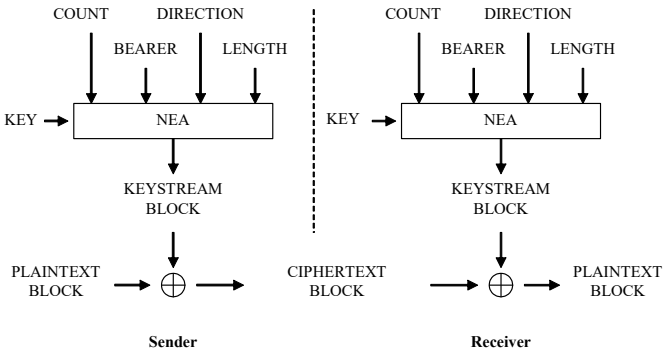


空口安全保护机制

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：**

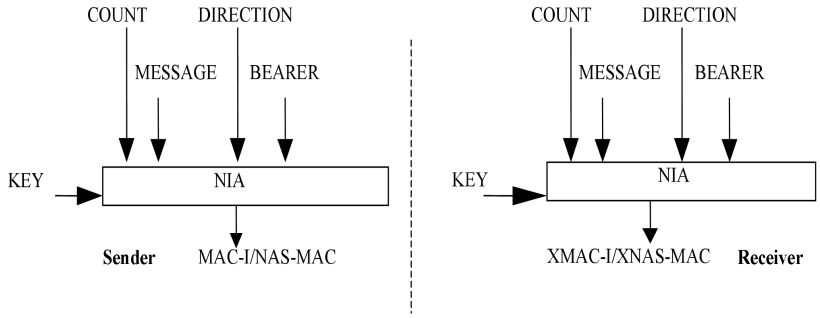
5G采用数据流加密机制，用算法和密钥一起产生一个随机秘钥流，再和数据流XOR一起产生加密后的数据流。解密方只要产生同样的随机秘钥流就可以了。用于生成伪随机密钥流(KEYSTREAM)的加密算法NEA包括：NEA0 空算法；128-NEA1 SNOW 3G算法；128-NEA2 AES算法；128-NEA3 ZUC算法。



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。

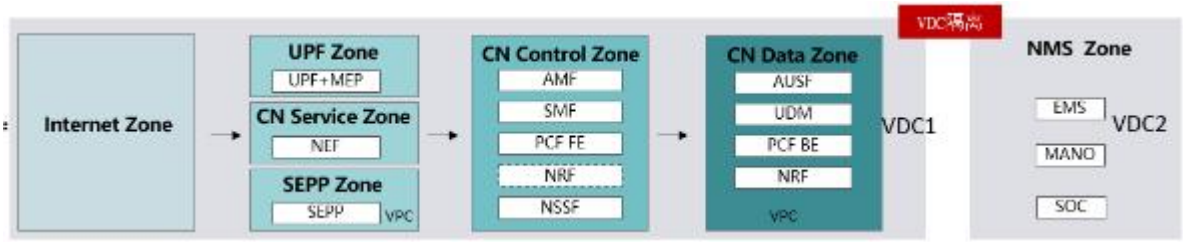


完整保护加密流程

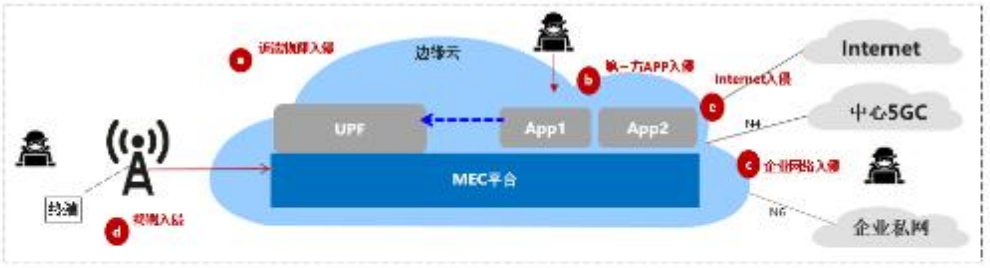
- 5G定制专网安全方面

安全解决方案框架如下图所示：

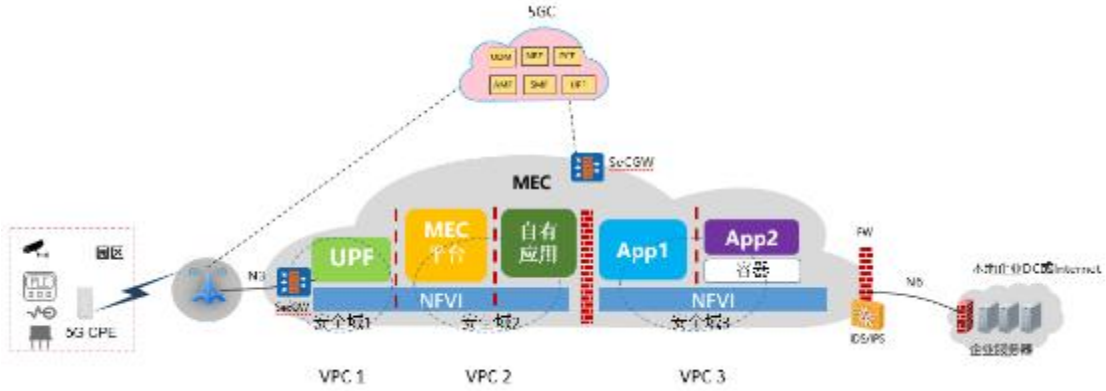
5GC安全防护策略如下图：核心网网元划分VPC，硬件独立，硬FW隔离。



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。

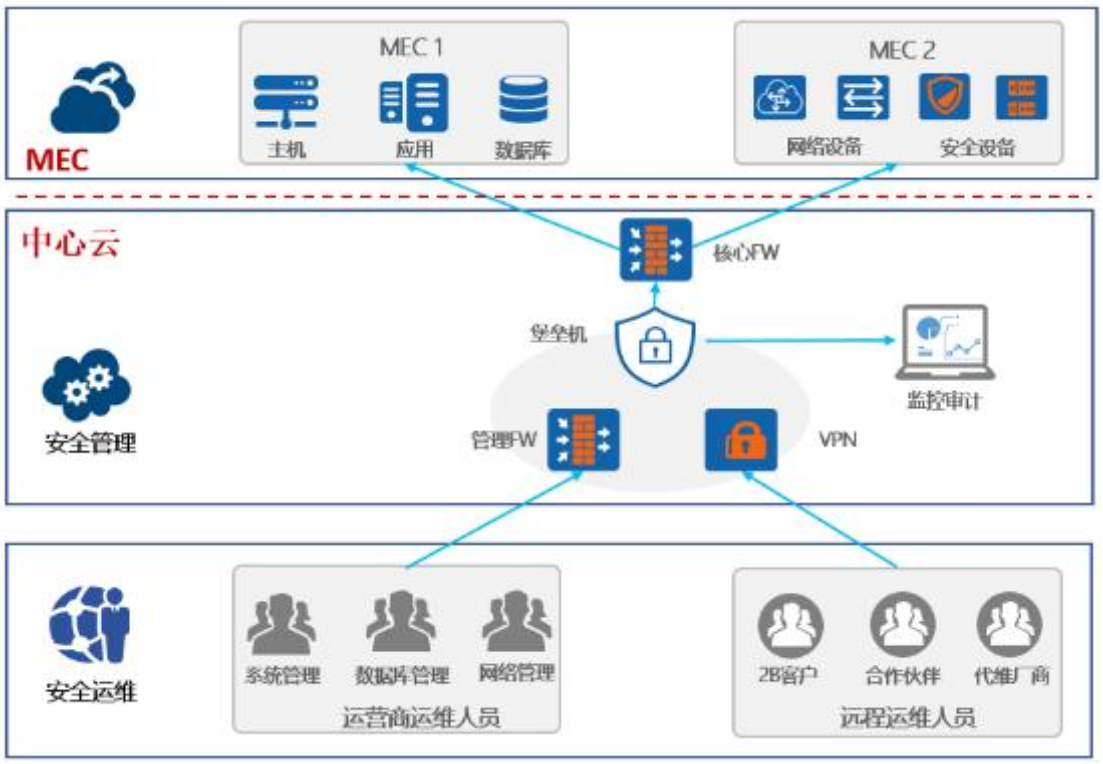
业务流程：

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。

测试床实施部署

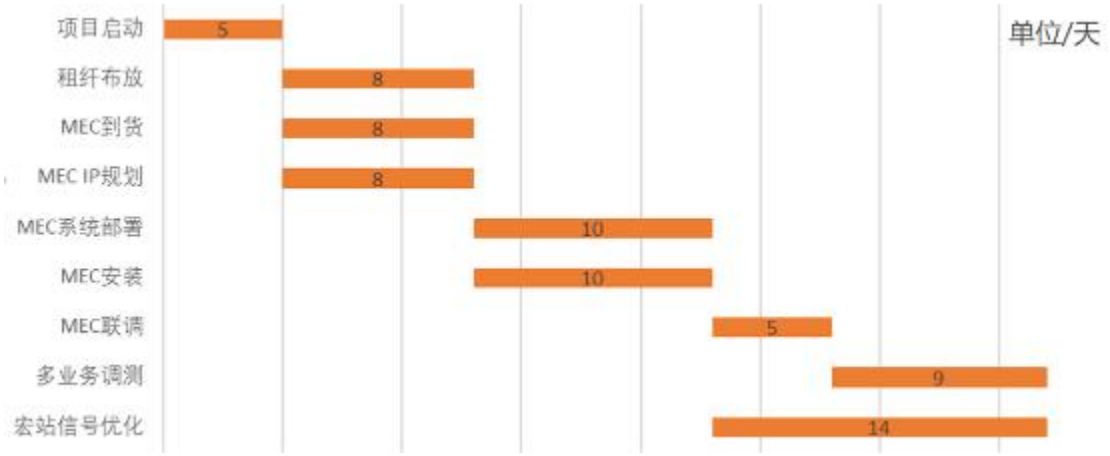
测试床实施规划

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	All
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



测试床实施的技术支撑及保障措施

1. 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。

2. 事件或故障处置原则

- 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；

- 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。

- 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；

测试床预期成果

测试床的预期可量化实施结果

- 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%。

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。

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"。

测试床成果验证

测试床成果验证计划

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。

测试床成果验证方案

- **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	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。

测试床成果交付

测试床成果交付件

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	
2	博世汽车室分系统	R8149 M182135	套	4	中兴
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

项目主要设备清单（例）

测试床可复制性

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。

测试床最新进度

测试床时间轴

测试床进度说明

博世测试床项目已经完成第一、二阶段建设，整体进度完成70%左右。第三阶段验证主要包括生产设备PLC及传感器数据回传、复合AGV自动上下料及运输、AI视觉检测集群运算等场景在5G网络环境下的应用情况。

第三阶段场景：

设备 PLC 及传感器数据采集

复合 AGV 自动上下料及运输

AI 视觉检测集群运算

第三阶段测试完成情况：

- 设备PLC及传感器数据采集：已完成多条产线设备传感器加装和关键参数采集，基本实现基于AR&3D-HMI的设备远程诊断和控制，下一步开始设备预测性维护平台搭建，整体已完成80%的测试；
- 复合AGV自动上下料及运：5G环境下的AGV物料搬运已正式上线，博世计划将部分AGV通过加装机械手改装成复合机器人，这部分工作还在进行中，整体已完成60%的测试；

AI 视觉检测集群运算:已完成单台检测设备高精度照片实时上传至 AI 处理集群验证,下一步要测试量产情况下多台检测设备同时上传至处理集群的网络传输和集群处理能力, 整体已完成 30%的测试。