基于轻量化边缘计算平台的工业互联网场景安全测试床

引言/导读

华为创立于 1987 年，是全球领先的 ICT（信息与通信）基础设施和智能终端提供商，致力于把数字世界带入每个人、每个家庭、每个组织，构建万物互联的智能世界。目前华为有 19.4 万员工，业务遍及 170 多个国家和地区，服务 30 多亿人口。华为在通信网络、IT、智能终端和云服务等领域为客户提供有竞争力、安全可信赖的产品、解决方案与服务，与生态伙伴开放合作，持续为客户创造价值，释放个人潜能，丰富家庭生活，激发组织创新。华为坚持围绕客户需求持续创新，加大基础研究投入，厚积薄发，推动世界进步。

北京三联虹普新合纤技术服务股份有限公司（股票代码：300384）——国际一流的聚酰胺新材料工程技术服务公司。公司创立于 1999 年，是一家专注于合成纤维及其原料生产技术及装备领域的高新技术企业，公司集工艺技术开发、工程方案提供、主工艺设备制造及技术服务为一体，提供专业化“交钥匙”工程技术服务，是国内提供高品质锦纶聚合及纺丝整体技术解决方案的工程公司。公司于 2014 年 8 月 1 日在深交所挂牌上市。三联虹普数据科技有限公司为北京三联虹普新合纤技术服务股份有限公司与日本 TMT 机械株式会社成立的合资公司，其目的是以两家公司全面覆盖合成纤维行业聚酯、聚酰胺两大行业纤维及原材料领域具备技术壁垒的关键工艺技术，核心装备为基础，借助工业大数据、人工智能解决方案能力，构筑合成纤维工业互联网平台。

面向未来，客户差异化定制需求日益增多，对产品品质的一致性要求更高，但当前化纤行业生产过程中预测能力欠缺，人工抽检难度大，严重影响化纤产业高质量发展。随着人工智能、大数据、云计算、边缘计算、机器视觉等新兴技术蓬勃发展，业界亟需构建有预测能力的数字化基础设施支撑未来化纤行业的快速发展。通过工业技术（OT）与新一代信息通信技术（ICT）深度融合，推进化纤行业数字化转型——依托智能装备、工业互联网与大数据技术打造端-边-云协同智能化纤产线。

一、关键词

边缘计算、安全、化纤工业

二、发起公司和主要联系人联系方式

华为技术有限公司，联系人：朱锦涛，17791596167，jintao.zhu@huawei.com

三联虹普数据科技有限公司，联系人：沈晖，18610686310，shenhui@slhpcn.com

三、合作公司

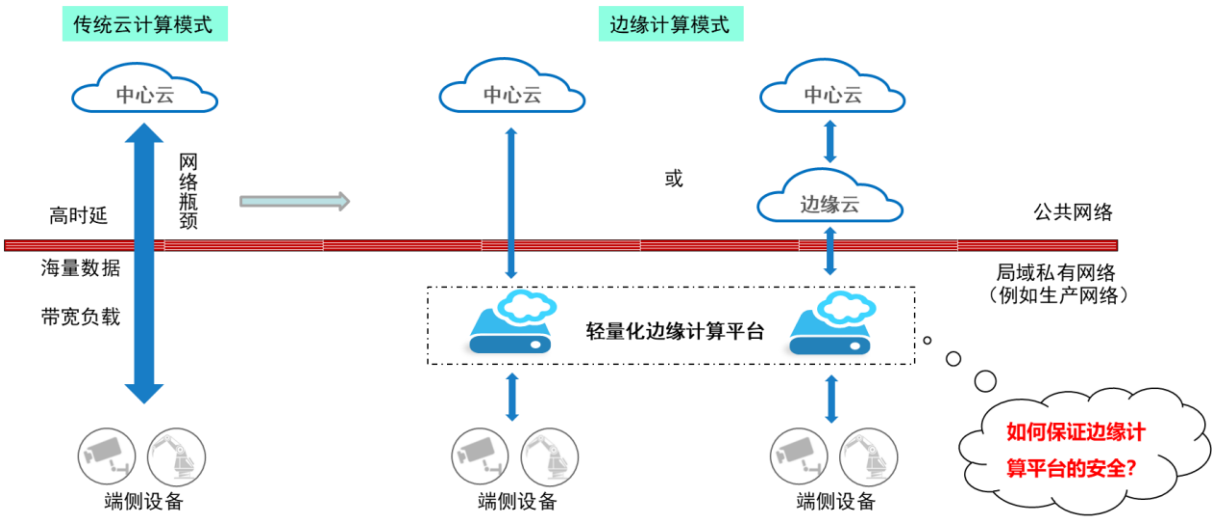
中国科学院沈阳自动化研究所，联系人：王挺，18204015560，wangting1@sia.cn

四、测试床项目目标和概述

化纤行业的传统实践是统一标准体系下的中心控制机制，但是这一机制在应对需求更加多变、细分的需求时已经显得困难。例如：

1. 客户定制化风格要求多：质量标准单一无法满足高端客户差异化需求；
2. 人工抽检负担重：产能规模大，用工多，检测效率低，无法在线检测；
3. 产品品质一致性要求高：化纤产品不同批次间质量波动不可控。

上述需求通过传统的中心化云计算模式难以妥善解决，因此通过引入端边云协同的“化纤工业智能体“来解决上述的需求。



本测试床基于“化纤工业智能体”业务相关的端-边-云协同总体架构，并且着重测试其中的轻量化边缘计算平台的安全性。本测试床使用的轻量化边缘计算平台为华为 Atlas500 智能小站。

Atlas 500 智能小站是一款性能强大，能在边缘进行实时处理的边缘计算产品，机顶盒大小的机身可以提供 16 TOPS INT8 的处理能力，同时功耗极低。Atlas 500 集成了 WIFI 和 LTE 两种无线数据接口，通过与私有云、公有云协同，云端推送应用、更新算法云端统一进行设备管理和固件升级。Atlas 500 在业界第一个在边缘计算产品中大规模应用 TEC（Thermo-electric Cooling）半导体制冷散热技术，使其支持严苛部署环境，在极端温度下，Atlas 500 都可以稳定运行。因此其对部署环境的要求极低，可以实现轻量化的部署与管理，同时满足了化纤行业场景下对于边缘计算的性能要求。

业界边缘计算方案提出了一段时间，但是对于边缘计算方案的安全如何保证，尤其是如何应用于化纤行业解决当前面临的安全挑战的业界实践是空白，因此本测试床的主要目标就是通过展示该边缘计算方案的安全能力，给化纤行业乃至流程制造的相关行业提供参考。

五、测试床解决方案架构

(一) 测试床应用场景

测试床的应用场景主要是面向化纤行业流程生产场景下端边云整体解决方案中轻量化边缘计算平台面临的安全风险，给出合理的安全保护方案，并给出测试床的测试建议。

安全风险主要可以将归纳为：

1. 安全性风险：边缘设备部署在产线旁，存在潜在的**生产敏感数据泄露、被篡改的风险。**
2. 可靠性风险：部署在物理环境中的边缘设备长期运行存在**业务失效的风险。**
3. 可用性风险：边缘计算平台被**恶意攻击**或自**运行出现故障时，存在业务中断的风险**。
4. 数据隐私风险：工厂内生产制造关键工艺参数、生产状态参数存在**被窃取风险**。

(二) 测试床重点技术

针对前述的化纤行业基于边缘计算平台工业互联网的不同测试床应用场景，本测试床项目提供的重点技术包括：安全性、数据隐私性、可用性和网关安全的相关关键技术及其测试项。

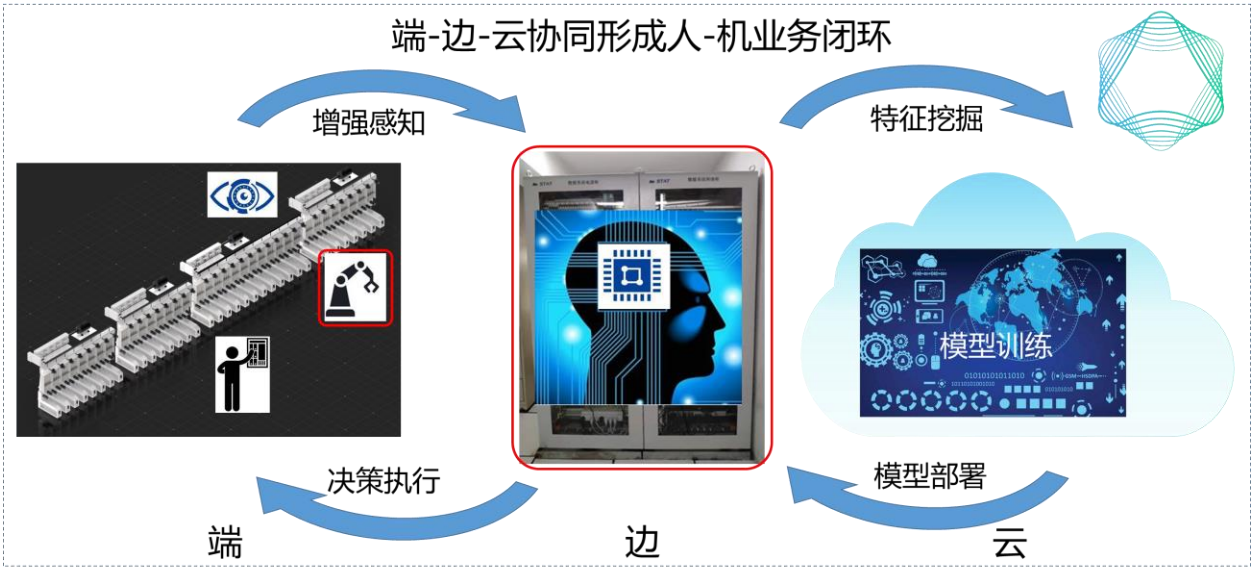
	创新点	**描述**
可用性	双机热备	双机热备，保证用户业务不中断；对外呈现只有一个 IP，上层业务平台不感知；
	无状态运维	更换设备，使用设备克隆技术，实现业务无感知。
安全性	数据加密	边缘侧业务数据加密，防数据丢失、防篡改
	安全启动	完善 Atlas 边缘产品的安全启动机制，支持客户自定义开发场景下的安全启动。
隐私性	联邦学习	产线与云端只传递模型参数，所有数据留在本地，保证数据隐私性
网关安全性	协议控制安全策略配置	南北向接口丰富，微服务灵活裁剪，安全可靠

(三) 技术创新性及先进性

本测试床的相关技术均为化纤行业端边云解决方案中的创新性解决方案。例如：为保障数据隐私性的联邦学习机制，目前已经申请专利（US62897808）。而其它测试床重点技术也

都是基于业界领先的安全可信的相关理念进行的特性设计，在业内的边缘计算平台防护上都属于较为先进的技术方案。

(四) 测试床解决方案架构



化纤行业基于轻量化边缘计算平台的工业互联网场景安全测试床解决方案总体架构核心是：一站式数据采集+全景可视化监控+人工智能分析应用。具体包括如下几个流程：

1. 自动化产线数据采集、传输与汇聚，包括纺丝、卷绕、落筒、质检、包装和仓储；
2. 网关收集产线数据，并进行协议转换，将转换后的数据发往边缘计算平台；
3. 边缘计算平台将产线数据安全上传至云端（特征提取、脱敏、加密）；
4. 云端对于产线数据进行大数据分析及模型训练；
5. 云端将训练优化后的模型推送至边缘计算平台；
6. 边缘计算平台基于训练模型对于本地数据处理进行进一步的处理；
7. 边缘计算平台将推理结果反推回产线，优化产线的决策。

六、预期成果

(一) 测试床的预期测试结果，针对测试项（重点）

本测试床针对基于化纤行业轻量化边缘计算平台的工业互联网的 4 大类安全场景安全性、可靠性、可用性、韧性进行测试，下表列举了本测试床项目的潜在测试项，但是具体的测试项可能随项目的实际进展和测试条件变动而有所调整。

1. 安全性

测试项	描述
安全启动	补齐边缘设备安全启动能力，系统启动全流程逐级校验，确保启动文件合法。
处理器提供加解密能力	• 硬件实现多种加解密算法、签名校验算法、防篡改算法和 HASH 算法 • 内部集成 32KBit OTP 存储空间和硬件随机数发生器 • 提供加解密引擎 API 应用接口
本地敏感数据保护	• Atlas 500 对涉及密码、密钥的所有敏感数据都进行了加密保护，防止敏感信息泄露。 • Atlas 500 支持升级包的签名保护，防止升级包内容被篡改，保证升级包的完整性。 • 除了加密保护，Atlas 500 对 Linux shell 进行了封装，用户通过 SSH 登录后无法直接访问文件系统中的文件，防止文件被破坏及文件信息泄露。 • Atlas 500 支持对关键数据文件进行备份及计算并保存文件校验和，并提供了文件校验失败的备份恢复机制，防止因系统异常掉电导致的数据文件破坏，保护数据文件的可用性和完整性。
密钥管理	Atlas 500 密钥管理采用“根密钥 + 工作密钥”的“两层密钥管理结构”，根密钥用来对工作密钥进行加密，工作密钥对被保护数据进行加密。 • 密钥生成：根密钥由安全随机数生成。工作密钥使用安全随机数生成。 • 密钥使用：密钥用途单一，每个密钥只用于一种用途。 • 密钥存储：根密钥分成多个组件分开保存，进行权限控制。工作密钥使用根密钥加密后保存。
传输安	外部接入访问默认使用 SSH、HTTPS 方式，传输通道通过使用安全协议进行加

全	密。不安全协议 HTTP 默认关闭。 各种安全传输协议的特性如下： • SSH：支持用户密码认证。支持 SSH V2。 • HTTPS：默认开启 TLS1.2。支持安全的加密算法。
系统安全加固	• 系统最小化安装，Atlas 500 对嵌入式 Linux 系统进行裁剪，只安装系统必须的组件，不使用的组件和命令都被删除。 • 对 Linux shell 命令行进行了封装加固，屏蔽了一些 Linux 系统命令，只能执行白名单定义的命令，降低攻击风险。 • 对系统中 SSH、Restful 等服务端进行安全配置加固，只支持安全的算法，不安全的协议和端口默认关闭。 • 下行命令防护
账号安全	Atlas 500 支持 Web、Redfish、WebSocket 等管理接口，并提供了统一的用户管理功能。只支持 1 个外部可登录用户，不支持增加、删除用户。帐号安全措施包括：密码复杂度检查、密码有效期和帐号防暴力破解。
认证管理	用户通过 Web、CLI 访问时需要进行认证，支持“用户名 + 密码”的认证方式。认证通过后才能进行设备的管理配置和信息查询等操作。
证书管理	• 证书是指 SSL 证书，在建立 Web HTTPS 连接时使用，用于证明 Web 站点的身份。 • 证书管理就是指对 SSL 证书的各种管理操作，包括查看当前证书信息（证书的使用者、颁发者、有效期、序列号）、生成 CSR 文件、导入由 CSR 生成的签名证书、导入自定义证书，证书格式只支持 X.509 格式。 • Atlas 500 的 SSL 证书默认使用自签名 SSL 证书，证书的签名算法使用 SHA256 RSA（2048 位）。支持用户导入自己的证书来替换系统中默认的自定义证书，Atlas 500 支持两种替换自签名证书的方法
会话管理	• 会话标识使用安全随机数生成，禁止同一个用户同时建立多个会话。 • 对于 Web、SSH 等长连接会话实现了静默超时断连机制，超过超时时间没有操作则会自动断开会话。

	• 用户主动发起请求终止当前会话。 • 管理员可以主动终止其它会话。
用户权限控制	Atlas 500 系统内部创建了不可登录的普通用户帐号，用于运行非关键进程。管理员账号，默认只有普通用户权限，降低管理员账号泄露带来的安全风险。
双向认证	创建边缘节点时，边缘节点绑定唯一证书。与云上通信时，云端校验边缘节点证书，防止边缘节点被仿冒。同时边缘节点校验云上证书，防止云上应用被仿冒。即通过 HTTPS 双向证书认证，保证数据通道安全。（需边云联动测试，边缘侧单独无法完成）

2. 韧性

方案	描述
容器安全隔离	支持指定每个容器可使用的 CPU、内存等资源，限制每个容器可访问的磁盘空间，单个容器异常不影响系统整体功能。
系统重启	系统和关键进程异常都可被看门狗复位拉起。
边缘自治	中心网管中断不影响边缘软件继续运行；提供边缘 WEBUI 近端管理能力。

3. 可用性

方案	描述
双机备份	支持两台智能小站组成双机备份系统，提供双机软件平台，支持快速倒换（2s），支持主备仲裁，自动防双主、双备。
软硬件故障主动上报	提供丰富的故障检测功能，精确定位硬件故障，并支持发现容器服务异常，上报硬件/软件告警。
容器故障修复	当边缘部署的容器运行出现故障时，可以通过容器引擎重启该容器。
进程黑匣子	在芯片中保存关键日志，以便系统或设备意外宕机时远程获取黑匣子日志。
一键恢复出厂设置	提供一键恢复出厂设备功能，将系统固件、配置恢复到出厂状态。

4. 可靠性

方案	描述
审计日志自动备份	Atlas 500 日志保存在 Flash 文件系统中，当日志文件达到指定大小后会自动进行日志文件备份。

固件、系统双备份	支持 uboot、MCU 固件双备份，以及操作系统、驱动软件双备份，固件、系统损坏情况下自动切换备区运行，并保持原有配置不丢失。

(二) 商业价值

本项目研究成果可提高基于边缘计算平台的纺丝工业互联网生产系统安全运行的可靠性，降低安全事件造成的经济损失。本项目成果为边缘计算平台在化纤行业的应用提供综合的安全防护方案，增强纺丝工业互联网系统防范网络安全攻击的能力，保障生产系统的安全稳定运行并减少安全事件造成的损失，为用户带来显著的经济效益。

(三) 经济效益

本安全测试床项目研究成果可做为纺丝工业智能体产品的重要组成部分，为基于边缘计算平台的纺丝工业互联网产线提供安全防护。

在实际生产环境中，每套纺丝工业智能体产品可为约 40 条卷绕机位产线提供服务，每条卷绕机位产线价值约 10 万美元，因此本项目研究成果每套可为价值约 400 万美元的产线提供安全防护，保障生产系统的安全稳定运行。

方案可在合成纤维行业、纺织行业推广使用。

(四) 社会价值

本项目的设计思想、核心技术、相关成果不仅适用于化纤行业的工业互联网场景，对其他行业和相关系统也具有示范作用。通过本项目积累高等级工业互联网生产系统安全防护体系的建设经验，可供其他行业参考借鉴，对工业互联网整体数字化水平的提升具有重要意义，满足国家高质量发展的需求，也为国家网络空间安全战略提供支撑。

七、测试床技术可行性

(一) 物理平台

本次测试床所涉及的边缘计算平台硬件基于华为 Atlas 500 智能小站。Atlas 500 是一款性能强大，能在边缘进行实时处理的边缘计算产品，单台可提供 16 TOPS INT8 的处理能力，

同时功耗极低，每天耗能小于一度电。Atlas 500 集成了 WIFI 和 LTE 两种无线数据接口，提供灵活的网络接入和数据传输方案。Atlas500 小站大小与电视机顶盒相近，免风扇设计，通过业界第一个在边缘计算产品中大规模应用 TEC 散热技术，使其可以在-40℃~70℃稳定运行。

(二) 软件平台

本次测试床所涉及的边缘计算平台 Atals500 智能小站软件基于 EulerOS。EulerOS 是基于开源技术的开放的企业级 Linux 操作系统软件，具备高安全性、高可扩展性、高性能等技术特性，能够满足客户 IT 基础设施和云计算服务等多业务场景需求。

通过部署于 Atlas500 小站上的智能边缘平台 IEF（Intelligent EdgeFabric ）满足客户对边缘计算资源的远程管控、数据处理、分析决策、智能化的诉求， 为用户提供完整的边缘和云协同的一体化服务。实现隐私数据本地化、业务处理低时延、数据智能化，驱动企业数字化转型。IEF 提供海量边缘节点安全接入、边缘应用生命周期管理、安全可靠的边云数据通道、丰富的边缘 AI 算法等关键能力。

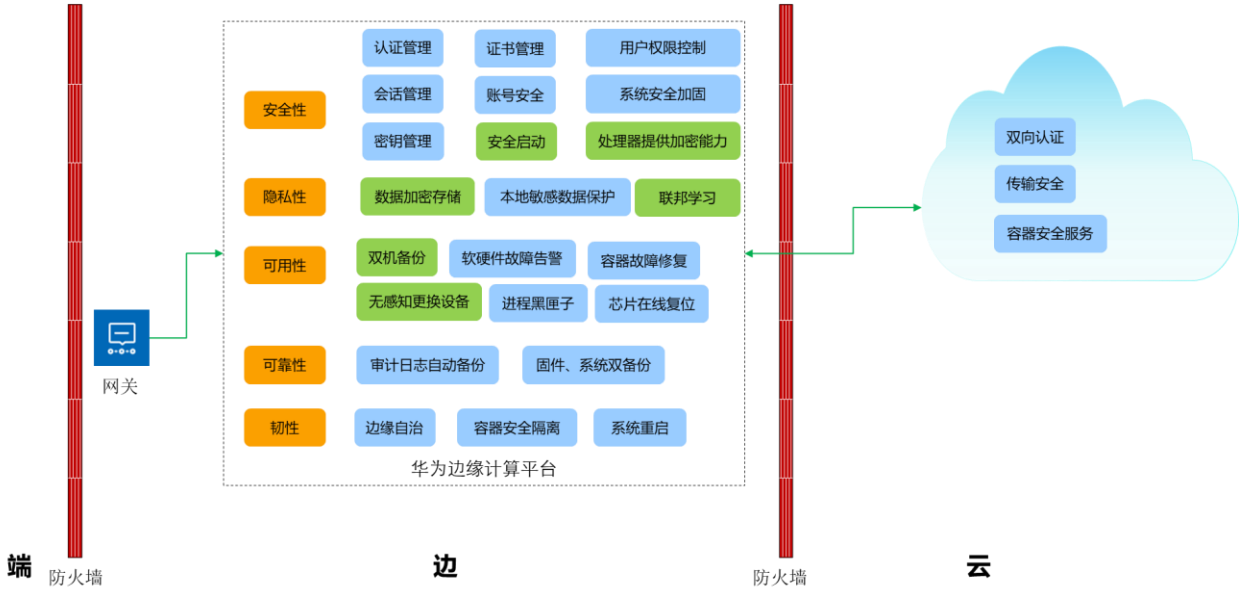
八、和 AII 技术的关系

(一) 与 AII 总体架构的关系

本测试床符合 AII 总体架构，主要验证内容属于边缘计算特设组与安全组工作范畴。

(二) AII 安全（可选）

本测试床项目将化纤行业生产过程中边缘计算面临的安全问题作为核心测试因素，因而设计了基于边缘计算平台的整体安全能力解决方案，包括安全性、隐私性、可用性、可靠性和韧性等多种特性，如下图所示：



(三) 详细清单（可选）

参与方	物料信息
华为	提供边缘计算平台； 提供公有云训练平台； 完成边缘安全技术的创新。
沈自所	提供工业网关，完成工业私有协议的向上转换。
三联虹普	提出业务安全需求； 提供测试床相关生产检测环境。
日本 TMT	提供卷绕机等生产设备。

(四) 安全联系人

华为技术有限公司，联系人：朱锦涛，17791596167，jintao.zhu@huawei.com

(五) 与已存在 AII 测试床的关系

本测试床定位面向工业互联网流程中的边缘计算平台的安全能力测试，与现有其他测试床之间存在一定互补关系，暂未见到在应用领域上存在重复的情况。

九、交付件

测试床交付物包括前述包含边缘计算平台的安全解决方案以及“预期成果”中的相关测试项测试结果报告。

十、测试床使用者

本测试床欢迎更多合作伙伴加入安源安全测试验证。非发起方的参与者可以使用验证示范平台的所有操作功能，但仅限于功能的操作使用，禁止泄露给同行业的第三方。

十一、 知识产权说明

项目合作过程中产生的全部开发成果及其知识产权，包括但不限于申请专利的权利、专利申请权、专利权、版权、商业秘密，均归发起方共有；未经一方书面同意，另一方不可将本协议项目合作过程中产生的任何知识产权转让、许可给任何第三方。

十二、 部署，操作和访问使用

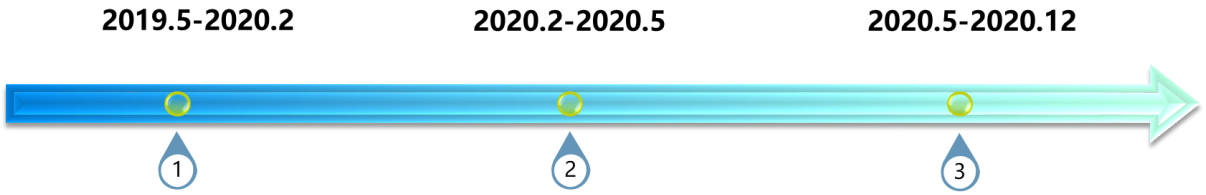
本次测试部署于三联虹普数据科技有限公司的纺丝智能试点产线，测试床资源由三联虹普数据科技有限公司负责运营。

十三、 资金

本安全测试床项目总投资 xxx 万元人民币，全部由参与单位自筹。其中，科研投资约 60%，试点示范单位工程费用投资估算 40%。

十四、 时间轴

本方案验证分为三个阶段：



十五、 附加信息

本测试床成果将不仅应用于化纤行业的工业互联网场景，未来测试床还可以广泛复制到各种对边缘计算有需求的行业的工业互联网场景中，具备规模复制性。在提升其流程建模分析效率，找出降低生产质量的因素，进而提升良品率的基础之上，保障了其生产过程中的安全性。