**宁波路特斯机器人有限公司**

媒体：Lotus-Robotics.PR@lotuscars.com.cn
商务：bd_lr@lotuscars.com.cn
官网：http://lotus-robotics.lotuscars.com.cn

**中国智能网联汽车产业创新联盟**

地址：北京市北京经济技术开发区融兴北三街39号
电话：010-56760839
邮箱：daiyuanjie@china-icv.cn
官网：http://www.caicv.org.cn

May 2023

May 2023

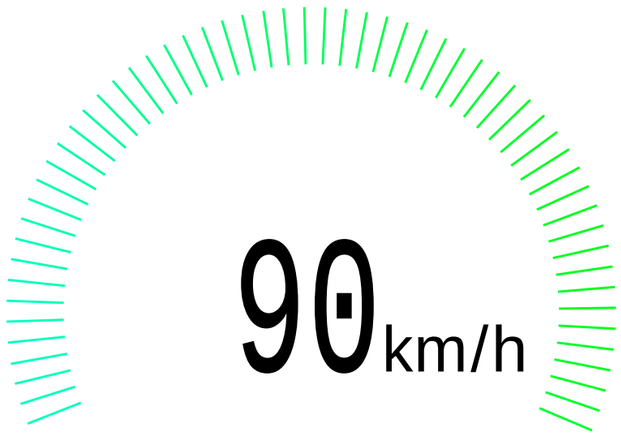
# 路特斯机器人信息安全白皮书

## 智能驾驶信息安全实践

ROBO

LOTUS ROBOTICS

中国智能网联汽车产业创新联盟
China Industry Innovation Alliance for the Intelligent and Connected Vehicles




# 智能驾驶信息安全实践

## AI DRIVING CYBERSECURITY PRACTICES

ROBO

# 专家评语

## AUTHORITARIAN EVALUATION



汽车产业正在经历百年未有之大变革，显著呈现电动化、智能化、网联化、共享化加速演进新特征。我国智能网联汽车基本与国际同步发展，我国率先提出并实践的车路云一体化协同技术路线得到全球认可，智能网联汽车市场表现远超预期，预计2025年，联网功能汽车将占汽车总销量的86%，具备辅助驾驶功能的智能网联汽车渗透率将超过50%。

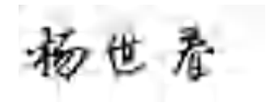
智能网联汽车“车路云一体化”中国方案落地，需要构建“计算、云控、高精地图、智能终端、信息安全”五大基础平台。其中信息安全基础平台是支撑智能网联汽车产业健康发展的重要环节和方向之一，也是未来汽车安全问题解决的重点和难点。国家多次出台网络安全相关政策法规和标准体系建设指南，支持企业开展信息安全实践。

路特斯机器人在国家政策法规的指引下，有序开展智能驾驶信息安全实践探索，符合我国智能网联汽车产业发展方向，是适合车路云一体化发展的有效实践。

北航交通科学与工程学院院长
中国智能网联汽车产业创新联盟信息安全工作组组长

智能网联汽车相较传统汽车的信息安全风险增加。 随着智能汽车软件和数据价值的提升，政府监管的紧密落地，信息安全成了真实的市场刚需。智能汽车信息安全需求来源于很多方面，比如满足合规需求、支撑业务运营、防范风险事件、保障企业自身发展、履行社会责任等。

信息安全是为智能网联汽车未来发展的关键布局，除了合规驱动外，更好的产品和信息安全保障，成为智能驾驶产品的新竞争力。同时面临如何落地的挑战。路特斯机器人从组织管理、队伍建设及技术架构等多方面布局建设信息安全企业能力，从设计阶段即建立全生命周期的体系化安全防护架构，应对智能网联汽车技术快速迭代，覆盖车端、路侧及云端，形成整体的安全治理和防护体系，可妥善保护汽车全生命周期中所赖以支撑的各项信息资产，提高企业信息安全风险的管控能力，是汽车智能驾驶信息安全领域的优秀做法。



北航交通科学与工程学院院长
中国智能网联汽车产业创新联盟信息安全工作组组长

智能网联汽车信息安全是一个复杂系统问题，整个车联网信息安全问题主要萦绕在"云-管-端"三个层面。既包括硬件安全、固件安全、操作系统安全、应用安全等传统安全问题，还包括数据安全、人工智能算法安全、供应链安全等新型安全问题。从车端来看，智能驾驶系统、动力系统、车身控制系统以及信息娱乐系统都是智能网联汽车被攻击的对象。

路特斯作为高端汽车品牌，在智能驾驶领域严格按照ISO21434、ISO27001等标准体系搭建信息安全管理体系，成为汽车行业少数几家获得体系认证的企业之一。在产品层面，路特斯展开多轮安全测试和漏洞修复，其测试经验对于汽车企业具有参考和借鉴意义。

国汽（北京）智能网联汽车研究院有限公司信息安全部部长

# 目录

CONTENTS

# 前言
PREFACE

WE ARE FIRST,LAST AND ALWAYS FOR THE DRIVERS

当前智能网联从体验方面给汽车产业带来变革，智能网联汽车不断搭载更多智能化、网联化零部件和系统以提供更好的用户体验。根据预测，截至2025年，具备联网功能的汽车约将占据全球汽车市场销量的86%，车辆将开发更多富有个性化的功能配置。随着智能网联汽车技术与信息通信技术的高度融合，需同时支持车内、车与车、车与人、车与道路基础设施、车与云端等多种通信类型，汽车电子系统也将引入更多额外的漏洞和可攻击的入口，信息安全问题将愈发突出，信息安全逐渐成为必须落地的产业新基建。

面临智能网联汽车信息安全领域的严峻挑战，国内外积极开展智能网联汽车信息安全相关政策标准制订及实施，不断强化网络与信息安全保障体系建设，逐步规范智能网联汽车信息安全相关的管理工作，行业及企业持续探索可实施的管理模式及最佳实践。

路特斯机器人作为路特斯集团旗下在智能驾驶领域的重要布局，致力于打造安全的最佳智能驾驶平台。如何在愈加复杂严峻的形势下，与时间赛跑，打造最佳的信息安全实践，是一项巨大挑战。在深度解读国内外法律法规前提下，结合分析实际内外部安全威胁，路特斯机器人建立了覆盖车、云两端的信息安全管理体系。将信息安全融入智能驾驶平台全生命周期，通过对概念、设计、开发、生产、运维等各环节的安全管控，确保对所有信息安全风险可控。

本白皮书就以路特斯机器人的信息安全保护实践作为蓝本进行介绍，抛砖引玉，希望将路特斯机器人在智能驾驶方面的信息安全建设的思考和实践经验分享给行业各位，同时呼吁OEM、tier1、tier2、安全咨询等行业伙伴共建智能网联汽车安全生态。

# 信息安全是智能网联汽车产业链发展的护城河

CYBERSECURITY

汽车行业正在经历百年未有之大变局，智能化网联化的高速发展颠覆了传统产业模式，汽车产业链供应体系、分工合作方式、企业运营管理、消费价值链等不断变革，下一代通信技术、信息技术、人工智能技术在汽车产业应用逐渐深入，持续推动汽车从交通工具向智能移动终端进化，车企核心竞争力从传统的机械开发能力向软件开发与服务能力逐渐转化，信息安全成为车企必须落地的新基建。

信息是当下汽车产业数字化转型的基础，车企的变革和竞争即将进入全新的赛道，现阶段全球汽车产业格局分化加剧，优胜劣汰提速，产品品质与用户体验快速提升的同时，产品更加多元化、细分化，同时消费者对于车辆安全性的诉求愈发强烈，面临全面重构的产业格局及严峻的信息安全挑战，保障企业及产品的信息安全对于车企而言的必要性将愈发明显。

当前智能网联汽车产业链相关企业在信息安全相关流程管理层面，缺乏相关开发经验，仍未建立完善的管理机制及规划。大部分汽车企业开发人员并不熟悉公司信息安全的相关计划，缺乏应对汽车网络安全威胁的技能和措施，且未得到合理相关培训，开发人员并未掌握在系统底层开发过程中进行安全性建设的前沿技术和方法。针对车路云一体化智能网联汽车系统，产业链相关企业对于车-云协同的攻击防御和无线通信防护机制不足，贯通云、管、端的防护体系不完善，对云、管、端信息安全独立设计、协同设计机制不足。

为保证智能网联汽车的信息安全，车企应加速建设网联安全防护体系，以抵御和减轻网络攻击引起的危害，此外对于全球化车企而已，符合各个国家及地区的信息安全法规标准将成为布局重心，信息安全已经成为智能网联汽车产业链发展的护城河。



# 信息安全组织建设是安全建设的首要保障

CYBERSECURITY ORGANIZATION DEVELOPMENT

信息安全工作的开展离不开组织全员的主动参与和责任义务的严格履行。路特斯机器人将信息安全定位为组织战略的重要工作之时，即启动信息安全组织建设工作。以原有公司架构为基础，设置虚拟组织，作为推动信息安全工作在组织内部成功执行并持续运转的首要保障。

如下图所示，信息安全委员会负责上层决策和管理。信息安全执行组作为其下设机构，负责独立的监督、评估、审计、考察工作，并指导、推动信息安全工作在各部门的落地实施。信息安全管理组牵头公司信息安全的建设，下设体系流程组、安全开发组、安全运营组进一步分解工作，确保职责清晰、权责对等、落实有力。项目管理部门、产品开发部门等配合管理组织，支撑信息安全具体工作的开展。

# 信息安全人才是企业发展的核心竞争力

## CYBERSECURITY TALENTS

专业的信息安全人员是信息安全建设的首要资源，人员能力建设也是当务之急。当前智能网联汽车信息安全产业人才体系与产业发展存在严重的供需矛盾，社会层面的人员招聘暂时难以满足公司紧迫的需求。路特斯机器人选择从人员能力入手，建立信息安全人员能力矩阵，同步搭建人才输送通道。

如下图所示，智能网联汽车信息安全人员通常需包含网络安全宏观概念、网络安全基础知识、网络安全措施、信息安全法律法规、网络安全测试5个维度能力。实际根据岗位定位的不同，对于五个维度的程度要求有所差异。

对于路特斯机器人来说，重点培养两类人才，信息安全经理和信息安全工程师。信息安全经理能力点在于信息安全需求的开发管理，以及与相关方（客户、供应商等）沟通协调。信息安全工程师能力点在于信息安全需求的实现和测试验证。截至目前，路特斯机器人信息安全团队已具备ISO/SAE　21434信息安全工程师资格10人，专业审核人员2人，并在持续建设扩充中。从实践经验来看，具备成熟的车辆知识的汽车工程师相对传统IT人员更具转型优势。


**内部人才能力建设**

- 制定内部人才成长计划
- 开展信息安全专项培训
- 采取分布式管理模式
- 搭建智能网联汽车信息安全实训平台

**外部校企协同培养**

- 以路特斯集团为桥梁，建立与武汉优秀高校合作的渠道
- 积极与武汉理工大学、华中科技大学等开展人才交流合作
- 建立产学研用闭环人才培养机制



# 安全管理体系是公司信息安全的保护伞

## CYBERSECURITY MANAGEMENT SYSTEM

信息安全体系的建立和实施一方面依据国内外法律法规、标准制度、行业监管等要求和指导，另一方面紧紧围绕路特斯机器人内部总方针总目标，确保搭建切合实际需求且行之有效的管理体系。如下图所示，路特斯机器人实际体系建设以路特斯集团建设为基础，在集团QMS、ISMS、CSMS、PIMS等体系赋能下，从智能驾驶业务出发，结合ISO21434、ISO27001等标准，针对车、云两端进一步制定和细化管理制度流程。总体制度依照传统的金字塔四层架构，由上至下，层层细化、层层落实。

路特斯机器人体系建设重点关注以下几点：

合规性：根据智能驾驶业务需求，明确公司应遵守的法律法规和行业标准，依照权威标准和最佳实践，进一步做解读和分析，在完成可靠差距分析的基础上再开展体系建设。

可落地性：为避免组织、管理、技术“三张皮”现象，最终导致体系成为“空中楼阁”，在建设前期首先对接个业务部门，做充分调研。完成建设后，加强宣贯、推动执行，并根据反馈不断持续优化。

可发展性：一个公司往往存在多个领域的体系建设，不同的体系再由不同负责部门主导开展，将导致内容重叠且繁琐，给体系管理、执行带来诸多不便和困扰。路特斯机器人体系建设往大质量、大合规、大融合的方向发展，在各体系之间做接口、做融合，实现体系的高质量建设和可持续发展。

# 安全管理体系是公司信息安全的保护伞

## CYBERSECURITY MANAGEMENT SYSTEM

2022年10月，路特斯机器人ISO21434流程体系也正式顺利通过国际权威认证机构之一的DNV审核，同月正式获得了其颁发的认证证书。

11月，路特斯机器人智能驾驶系统顺利完成公安系统备案，获得等级保护三级认证。





# 信息安全架构是实现产品安全的基础

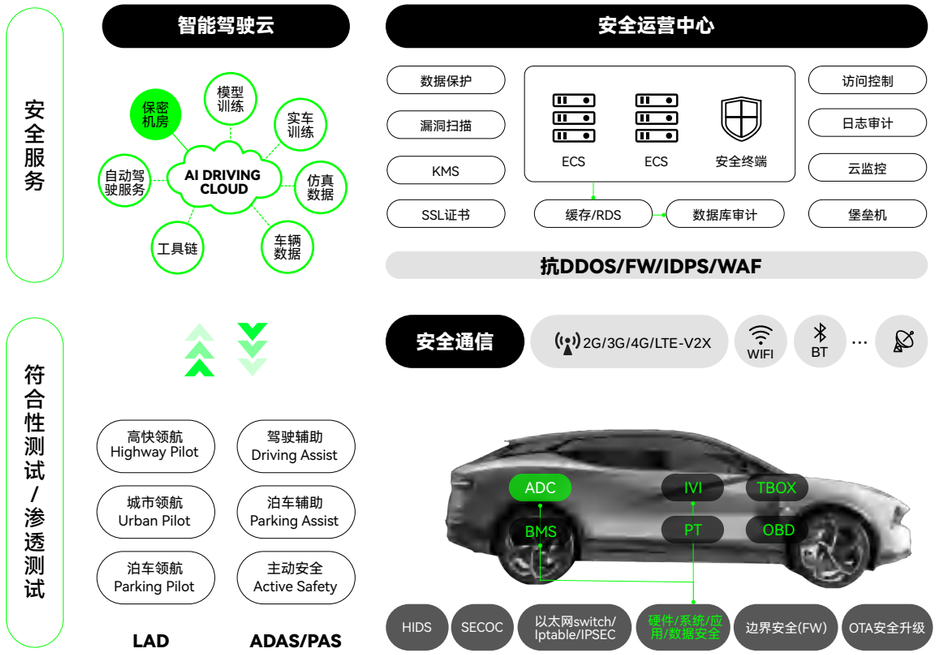
## CYBERSECURITY ARCHITECTURE

基于智能网联汽车“车”、“云”两端架构设计架构，路特斯机器人智能驾驶平台信息安全架构搭建如下图所示。

车端通过智能驾驶信息安全架构的设计，进一步采用TARA方法论，分析硬件、系统、应用（服务）、通信、数据相关资产所受威胁及风险，在5个维度落实信息安全措施，实现其安全保障。

智能驾驶云参照等保三级最佳实践，在云平台原生安全能力的基础上，结合企业自建，部署云防火墙、WAF、抗DDOS、堡垒机、数据库审计、漏洞管理、云安全中心等设备和系统，建设贯穿南北东西的纵深防御体系。

另外，数据安全作为智能驾驶信息安全的重要内容之一。路特斯机器人建设保密机房，将海量的车辆重要数据进行安全隔离，并将数据安全的保护贯穿于采集、传输、存储、销毁等生命周期各个环节。



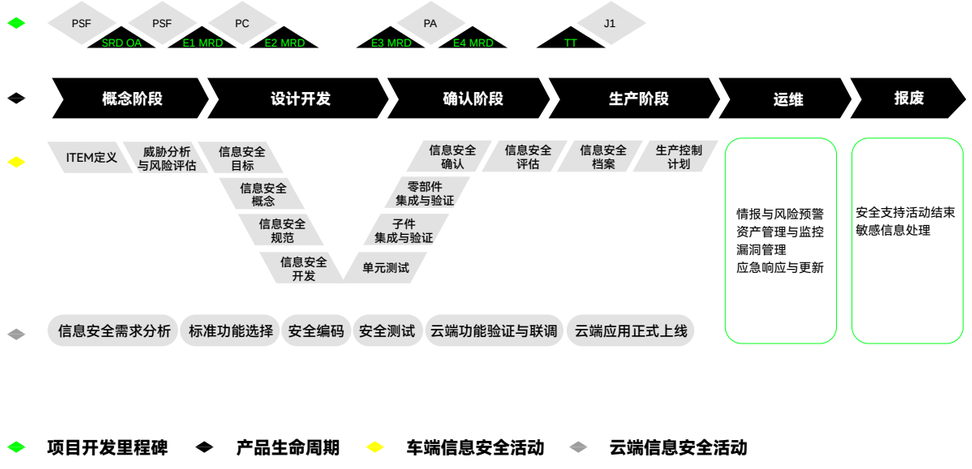
# 实现产品全生命周期安全管理是核心目标

## PRODUCT LIFECYCLE SECURITY

**路特斯产品生命周期信息安全管理**

为能实现对安全要求，对标项目开发里程碑，路特斯机器人将信息安全嵌入概念、设计开发、确认、生产、运维、报废等生命周期各个环节，明确各环节中需要开展的信息安全活动。通过对各环节信息安全活动的监控和管理，保障智能驾驶系统的交付满足信息安全要求。

作为Tier1厂商，在概念阶段需承接OEM在整车层面的信息安全需求，在完成智能驾驶域的信息安全实现与验证后，也需及时跟进OEM在整车层面的确认，才能确保成功验收交付。对于开发后的持续运维，与OEM建立联系及时的沟通渠道是关键，在提供主动提供信息安全支持工作的同时，保持联络，以及时响应OEM需求，特别是开展安全风险与事件的联动处置。





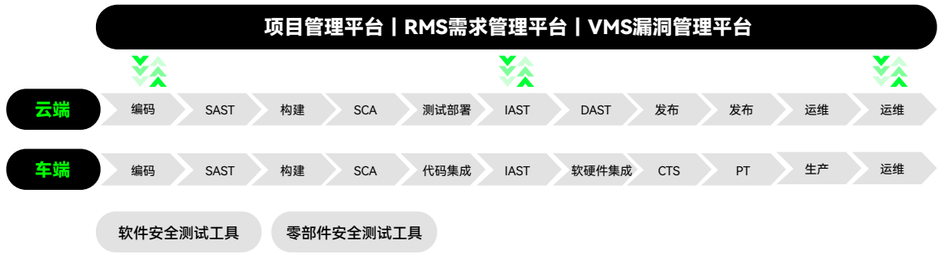

**安全工具链建设**

安全工具是安全开发的实现基础，在具有完备工具的前提下，推动信息安全工具与CI/CD黄金管道融合，向高度集成化、自动化方向建设，形成覆盖软硬件的自动化安全工具平台是路特斯机器人的最终目标。

如下图所示，路特斯机器人已建立覆盖车、云两端软件安全开发的自动化工具平台，其中包括静态代码扫描、开源组件管理、灰盒测试及渗透测试等相关工具。车端软硬件集成后的安全测试后续将通过车联网安全实验室的建设来进行补足和实现。

自动化工具平台同步对接项目协同管理、缺陷管理、需求管理、漏洞管理等系统，实现测试进度查看、安全红线控制、漏洞关联分析、测试覆盖评估、综合安全测试报告输出等能力，进一步降低人工占比，提高测试和管理效率。

目前，智能驾驶系统的安全测试调用了内外部多个渗透测试团队，针对车端硬件、系统、通讯、应用、数据和安全机制强度等多个维度，以及云端所有基础设施和应用资产，展开了多轮安全测试，并跟踪完成漏洞修复，确保安全风险可管、可控。



# 车载终端安全基线
## CYBERSECURITY BASELINE

| 安全维度 | 安全项 | 基线数 |
|---|---|---|
| 硬件安全 | 硬件安全 | 7 |
| | 调试接口安全 | 2 |
| | 最小攻击面 | 4 |
| 系统安全 | 安全启动 | 3 |
| | 操作系统安全 | 6 |
| | 系统代码安全 | 3 |
| | 系统安全漏洞 | 2 |
| | 系统安全刷写 | 2 |
| | 安全监测 | 3 |
| 应用安全 | 安全启动 | 3 |
| | 操作系统安全 | 6 |
| | 系统代码安全 | 3 |
| | 系统安全漏洞 | 2 |
| | 系统安全刷写 | 2 |
| | 安全监测 | 3 |
| 安全通信 | CAN通信安全 | 2 |
| | 以太网通信安全 | 2 |
| | Ethernet Switch | 4 |
| | 远程通信身份认证 | 3 |
| | 远程通信数据加密 | 2 |
| | GNSS安全 | 1 |
| 数据安全 | 安全存储 | 3 |
| | 动态脱敏 | 1 |
| | 车内数据安全 | 4 |
| | 车外数据安全 | 1 |



# 路特斯机器人产品安全基线介绍
## CYBERSECURITY BASELINE

通过对法律法规、标准规范、安全实践的分析总结，路特斯机器人建立了覆盖车载关键终端（ADC、IVI等）和智能驾驶云端的信息安全基线。如左表所示，路特斯机器人共建立覆盖终端硬件、系统、应用（服务）、通信、数据处理5个不同维度，共71条安全基线。为进一步确保车端信息安全基线的有效实施，制定了企业零部件信息安全需求规范，明确不同安全等级的信息资产与安全基线的对应关系，指导各项要求落地。

### 硬件安全
### HARDWARE SECURITY

主要包含芯片和PCB板相关硬件安全要求，芯片关注自身的安全防护能力和基于芯片的安全服务。构建物理安全和信任底座形成第一维度的信息安全保护，主要涉及密钥的安全存储、可靠的密码算法、安全调试等。第二维度是基于芯片的安全服务，如使用trust zone、真随机数生成等。除此之外，在硬件层应尽可能地减少攻击面和可用信息的留存，例如调试接口保护、最少可读丝印等。

### 系统安全
### HARDWARE SECURITY

安全启动作为系统程序完整性和真实性的基础保障，在系统层通常是必须实现的一个安全要求。系统的开发需符合公司安全编码规范，减少由于编码不规范、接口调用不当导致的安全漏洞。后续通过安全配置、漏洞修复、删除或禁用不必要的服务等方式，进一步进行加固。为满足后续的安全运营需求，对系统安全日志进行采集，通过车辆安全运营中心VSOC统一监测。

### 应用安全
### APPLICATION SECURITY

应用（服务）层级的安全维度与操作系统类似，在保证应用代码安全的前提下，通过安全配置，使得应用&服务最小化，使用密码技术对重要数据加密，再确保漏洞的修复达标等手段提升安全性。在进行刷写时，必须按照安全诊断及安全更新的标准进行。通过应用加固，对应用程序提供二进制级的深度混淆、固件防逆向、程序逻辑防破解、代码防篡改、运行防调试、防止恶意代码植入、防止核心算法/逻辑/信息破解分析等多重保护手段，也是充分保护应用程序安全的有效手段。

# 路特斯机器人产品安全基线介绍
## CYBERSECURITY BASELINE

### 通信安全
### COMMUNICATION SECURITY

车内外通讯安全是车联网安全关注的重点之一。SecOC和IPsec可以确保车内CAN和以太网通讯数据的完整性和真实性。通过访问控制降低对以太网通讯的攻击面，保证接入访问安全。车外通讯则常用身份认证和加密算法实现安全保障。

### 数据安全
### DATA SECURITY

在充分分析欧盟GDPR、中国数据安全法和汽车数据若干管理规定等法律、标准后，路特斯机器人建立数据分类分级标准，对需存储的敏感数据、重要数据等进行安全存储，对无存储需求的敏感数据进行动态脱敏，确保依照“合法、正当、透明”、“目的限制”、“最小化”、“准确性”、“完整性与保密性”、“可归责”等数据保护基本原则进行开发和设计。



# 云端安全基线
## CYBERSECURITY BASELINE

| 安全维度 | 安全项 | 基线数 |
|---|---|---|
| 网络架构安全 | 架构设计 | 6 |
| | 策略管控 | 8 |
| 账号管理安全 | 账号管理 | 6 |
| | 账号认证 | 3 |
| 数据安全 | 数据保护策略 | 2 |
| | 静态数据保护 | 7 |
| | 数据传输安全 | 3 |
| 日志安全 | 日志记录 | 2 |
| | 监控告警 | 2 |
| 基础配置安全 | 云服务器 | 4 |
| | 云数据库 | 2 |
| | 对象存储 | 2 |
| | SSL证书 | 4 |
| 上云应用安全 | 应用开发 | 5 |
| | 应用发布 | 5 |

# 路特斯机器人产品安全基线介绍
## CYBERSECURITY BASELINE

如云端安全基线表所示，云端共制定包括网络架构、账号管理、数据、日志、基础配置、云上应用6个维度，共57项基线要求。配合云上安全开发和安全管理相关规范、流程，实现基线落地。同时定期开展云端安全能力测评，持续优化。

### 网络架构安全
### NETWORK ARCHITECTURE SECURITY

云端本身给安全架构的搭建赋予了一定的基础能力。在边界部署必要的安全防护产品、设置有效的防护策略，另外通过VPC、安全组、ACL的灵活使用，对不同的网络环境之间实现有效隔离和防护，保护不同业务的安全性。

### 账号管理安全
### ACCOUNT MANAGEMENT SECURITY

云端账号必须严格受控，权限必须按需开放。在云端账号体系建设的基础上，做好用户身份管理和资源访问控制是关键。根据账号类别和重要程度，配合采用多因素认证、密码策略、密钥等安全限制，加强账号认证管理，也是进一步提高账号安全性的常用有效手段。

### 数据安全
### DATA SECURITY

云端数据安全在分类分级的基础上，通过加密、备份等措施，保证云上静态数据的存储安全和动态数据的传输安全，保护重要数据免受网络威胁的干扰和破坏、未经授权的访问等。



### 日志安全
### LOG SECURITY

确保日志收集覆盖安全所需日志，如网络日志、安全日志、操作系统日志、流量日志、应用程序等，并满足法规及业务需求的留存时间。通过日志的分析，联动告警支持安全监测、安全审计、安全事件响应等工作。

### 基础配置安全
### BASIC CONFIGURATION SECURITY

云上服务器、数据库、对象存储必须进行安全配置。云服务器需使用标准的安全镜像，并进行终端安全管理。云数据库关注数据加密、访问控制等。对象存储确保不同等级资源的隔离，同样需关注数据加密，以及读写权限的管控等。

### 上云应用安全
### CLOUD APPLICATION SECURITY

为确保上云应用安全生命周期的安全，依照路特斯机器人安全开发技术要求，需实现登录、注册、登出、密码安全、输入校验等安全设计。在严格按照安全编码规范进行安全开发的同时，结合静态扫描、渗透测试等工作进一步确保应用的安全性。对公应用的发布需满足域名发布、最小化端口开放、WAF策略配置等基线要求，并作为重要资产跟进后续管控和运营。

# 专家总结

## EXPERT SUMMARY

## 发展智能网联汽车是我国汽车产业的重要战略机遇

### IMPORTANT STRATEGY

发展智能网联汽车是我国汽车产业的重要战略机遇，政府监管部门、整车企业、关键零部件供应商、互联网企业、通信企业等需协同地、标准化、系统化构筑产业安全体系，切实推动智能网联汽车行业安全发展。

面对空前复杂的汽车信息安全形势，统筹安全与发展是全行业共同的挑战，各方应进一步推动信息安全监管体系建设，明确自身的信息安全主体责任，推动信息安全管理体系建设及技术研究，同时加强各主体安全责任意识，加强安全防护设计，遵循安全开发规范，落实安全测试与验证，逐步探索形成业务及产品安全治理体系及最佳实践。

路特斯机器人也将在后续的安全实践中，以上层法规标准为指引，积极响应国家、监管的号召，持续优化信息安全管理体系，提高信息安全技术实力，提升车、云安全防护水平，旨在为用户带来高安全级别的智能驾驶产品，打造全球化的信息安全合规企业。

世界新一轮科技革命和产业变革方兴未艾，汽车产业整体的变革发展之路需要行业伙伴的共同奔赴。路特斯机器人也希望在这发展之路上与行业伙伴加强沟通协作，合力推动行业信息安全能力建设，携手为智能网联汽车产业的安全可持续发展保驾护航。

**编写成员**

李博、潘坚伟、宋超、赵兴臣、迟宝群、毛倩花、王奇源、毋超、崔岩

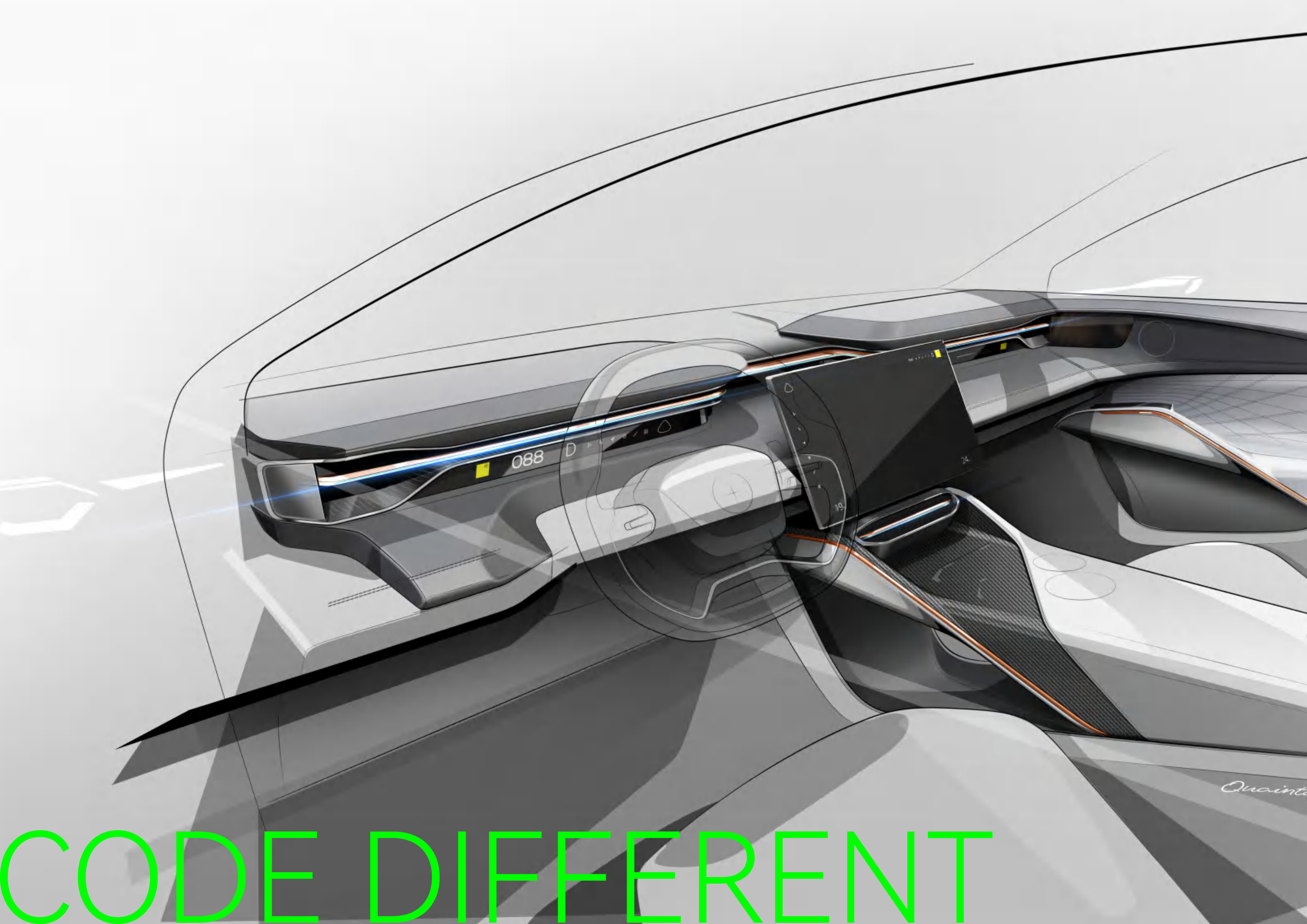


**版权说明**

本白皮书版权归属于宁波路特斯机器人有限公司。非经路特斯机器人书面同意，任何单位和个人不得擅自引用本白皮书内容。本白皮书仅反映白皮书发布之时的观点和实践信息，信息仅供参考，不构成任何承诺。路特斯机器人保留一切权利。




ROBO


088
D
CODE DIFFERENT