



## 适用于自动驾驶 (ADAS) 平台的 ASIL-Ready 智能供电与监控解决方案

Monolithic Power Systems, Inc.

[www.monolithicpower.cn](http://www.monolithicpower.cn)

### 功能安全成为汽车行业关注焦点

近年来汽车行业在追求自动化、互联化、电气化和服务化方面取得了快速进步，而支撑这些领域各种创新的重中之重，则是对功能安全的关注。在最高等级的安全性变得越来越重要的同时，安全标准也越来越严格、具体和新颖。对于此类“安全关键型(Functional Safety)”汽车应用，MPS 推出了 MPSafe™ 汽车级解决方案系列产品，为未来的汽车保驾护航。MPS 开发的智能解决方案，可以提供 ASIL-D 监控器以防止意外情况，并能提供自动驾驶计算行业至关重要的安全检测以及整套高效、快捷的解决方案。

### MPSafe™ 应运而生



图 1: MPSafe™ 为未来汽车保驾护航

### ISO26262 认证的产品开发流程

在汽车自动驾驶应用中，驾驶员或乘客与电气电子设备之间的相互作用正在显著增加，其中自动驾驶汽车的安全关键决策变得尤其重要，它对驾驶员或乘客的安全可能造成的潜在影响不容忽视。随着这些先进安全技术的操作系统从被动转向更加主动，汽车的安全驾驶俨然成为人们关注的焦点和必须解决的问题。同时，自动驾驶平台变得越来越复杂，出现了越来越多的系统性或随机硬件故障的风险。为了帮助确立最高安全性标准，行业发布了最新的符合国际标准化组织 (ISO) 26262 的汽车安全标准。

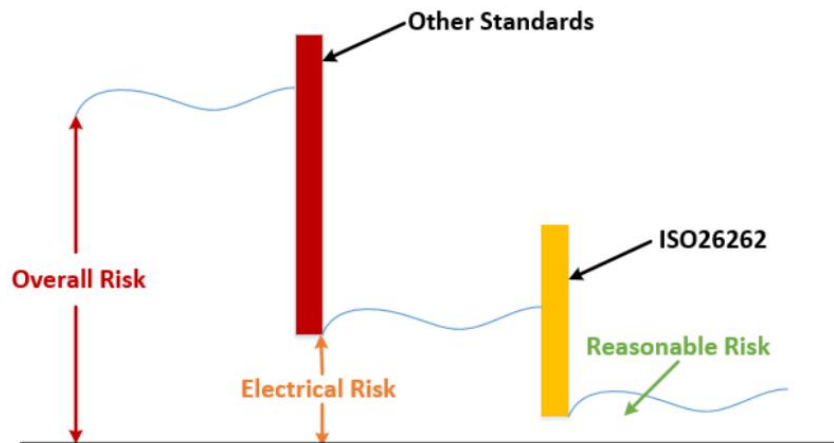


图 2：行业发布最新符合 ISO26262 汽车安全标准

MPS 利用自主开发的 MPSafe™ 开发流程（已被权威认证机构 TUV-SUD 认证），提出并研发了一套完整的解决方案，以应对自动驾驶平台中的安全挑战。该解决方案为自动驾驶平台提供了符合 ISO26262 安规标准的供电与监控系统。

自动驾驶系统供电的安全要求从芯片定义之初，开发人员对系统乃至整车的系统安全需有深刻的理解。根据应用于自动驾驶平台的 MPSafe™ 开发流程的要求，在各个芯片设计正式启动之前，需要从自动驾驶平台在车上的功能安全出发，形成该芯片需要满足的安全要求 (Safety Requirement)。只有站在系统功能安全要求的高度，了解功能安全要求对于芯片规格的制定产生的影响，才能避免最终产品功能和系统安全要求之间存在的偏差。根据芯片需要满足的安全要求，MPSafe™ 开发流程的基本五个步骤包括：

- 1) 芯片定义：包括芯片功能定义以及芯片安全功能定义。MPS 架构团队为该芯片打造所需的功能，同时与 MPS 安全团队紧密合作，了解芯片功能安全对芯片功能的影响。安全团队负责制定、审查并通过该芯片的安全计划，发布属于该芯片的应用假设，建立芯片开发安全档案。
- 2) 芯片设计：根据芯片需要满足的系统安全要求，落实该芯片的规格和功能要求。安全团队对该芯片进行定量安全分析（Quantitative Safety Analysis, FMEDA）以评估风险和确保满足系统安全要求等级。芯片设计团队需提供相关性失效分析(Dependent Failure Analysis)，进行芯片在 IC 功能以及安全机制的失效分析。通过仿真、封装失效分析和质量分析，推演和验证不同失效模式机制，分析芯片的安全机制是否符合要求。芯片设计团队还需与芯片验证团队建立完整的芯片验证方案等等。
- 3) 芯片样品：负责为 MPSafe™ 提供封装的厂商应严格遵循 MPSafe™ 流程及要求生产样品，以满足汽车安规等级。整个芯片样品生产的流程受到安全团队的监管，以保证要求与实际生产不存在偏差。
- 4) 芯片测试：芯片测试包括芯片电气特性测试 (Electrical Characterization)、可靠性测试 (Reliability Test)，IC 表征测试 (IC Characterization)，实验台功能和电气测试 (Road Test Functional and Electrical Verification)，以及



使用自动测试设备进行的大规模测试 (ATE Test)等等。一旦这些测试中出现任何失效或问题，团队立刻对失效和问题进行分析并提出解决方案，重新生产新的芯片样本以确保彻底解决问题和规避风险。

- 5) 成品出货：在以上所有四个步骤都正常进行的过程中，MPS 安全团队始终与第三方权威认证机构紧密合作，以确保 MPSafe™ 开发流程和生产流程所有设计、测试、生产环节均满足安全要求。所有的环节都会通过权威第三方认证，并发行符合认证的安全证书、手册。完成所有安全应用分析以及认证之后，该芯片将在严格的 MPS 标准要求下完成所有出货前测试并出货。

## 广阔的应用场景 — 从 QM 到 ASIL-D

随着电动汽车市场的不断扩张，自动驾驶技术的飞速发展，现阶段，基于 MPSafe™ 开发流程研发的芯片已经覆盖多种自动驾驶应用场景。例如自动驾驶平台的汽车核心计算系统，雷达系统，摄像系统等等。基于 MPSafe™ 开发流程提出的智能供电与监控解决方案和相关芯片，力求帮助客户规避潜在风险，并通过高可靠性和安全性，控制风险及故障，实现了从 QM 到汽车最高安全等级 ASIL-D 级的规定，为自动驾驶平台高效安全供电及监控保驾护航。

		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

图 3：汽车安全完整性等级 (ASIL)

根据应用场景的不同，MPS 在保证产品功能的基础上，提供给用户不同安全等级的灵活选择。如系统安全风险较低，用户可选择具备一定 FIT (Failure in Time) 分析，符合 AEC-Q100 标准的芯片。如需保证系统安全等级较高，MPS 可提供高达 ASIL-D 等级的带有功能安全的系列芯片。功能安全是实现国际 ISO26262 定义的汽车安全完整性等级 (ASIL) 的基础，如有需求，用户可灵活选择不同产品以配备到当前安全等级。与此同时，MPS 积极提供涵盖 QM 到 ASIL 等级芯片的相关安全手册和技术支持，来帮助用户放心选择，灵活配置。



## MPSafe™ — 面向系统的安全设计

### 直面系统级设计痛点，聚力解决安全挑战

随着人们越来越依赖 ADAS 等自动驾驶技术，安全成为整个系统设计和开发过程中面临的巨大挑战和高度关注的问题之一。对于自动驾驶系统中的计算平台，为应对安全挑战，规避潜在风险，自动驾驶计算平台应始终受到监管。稳定的供电电压对于安全正常运行至关重要。电压的任何动态变化或瞬态故障都可能导致计算处理器故障。这意味着对于自动驾驶供电系统来说，需要具备提供稳定的电压的能力，同时也应具备自身与系统故障监测、报告的能力，以保证系统的正常运行。目前，MPSafe™ 开发的系列产品具备的内建自测试 (BIST)、通过冗余的参考电压和时钟进行自我监控等等，力求保证芯片本身的安全状态。

#### 1. 内建自测试 (BIST)

BIST 等集成安全机制，可提供高诊断覆盖率，以确保每个驾驶周期的可靠性。电压监视器中有两种形式的 BIST：

- 1) 模拟电路自检 (ABIST)：ABIST 通过向诊断电路注入电流或电压来执行诊断电路故障。该功能验证诊断电路是否可以在故障和非故障条件之间切换，这表明模拟安全机制运行正常。在此过程中，将检查所有与安全相关的比较器和受监控的参考电压。
- 2) 逻辑电路自检 (LBIST)：LBIST 允许硬件自行测试。LBIST 具有检测内部逻辑电路错误的能力。

#### 2. 参考电压监测

系统的参考电压 (Reference Voltage) 对于芯片的重要性不言而喻，它是芯片中多个电路和模块正常工作的基础。在芯片中，多个模块需要使用参考电压作为精确电压控制的基准，例如模拟数字转换器 (ADC) 等。若参考电压不稳定，会导致芯片工作不稳定、误差增加及性能降低。因此，参考电压的好坏对于芯片能否正常运行至关重要。MPS 为保证芯片的参考电压的精度和稳定性，配有参考电压检测机制，通过引入冗余参考电压，对系统参考电压进行监督。一旦发现系统电压漂移超过预设范围，将拉低并中断该错误。

#### 3. 系统时钟监测

系统的时钟信号是 IC 中各个电路和模块的同步信号，以保证各个电路和模块在正确的时间按照正确的顺序执行相应的操作，例如时钟信号可以同步计数器、状态机、数据采样及数据通信等等。如果时钟信号出现故障，会导致 IC 中的电路和模块无法同步，甚至数据丢失、错误计数、状态机无法成功跳转、甚至系统崩溃等等问题。因此在 IC 设计过程中，时钟信号的监控尤为重要。MPS 通过引入一个参考时钟，与系统时钟互相监测，可以在系统时钟漂移超过预设范围时，拉低中断芯片并报告该错误。





## 用于不同安全等级系统的可扩展、模块化解决方案

MPSafe™ 不仅考虑了设备本身如何处理各种安全案例，安全目标，还可以通过芯片引脚的兼容性以及配套的安全文件，实现解决方案的可扩展和模块化功能，以达到可靠高效快捷的目标。解决方案的可扩展性包括满足不同 ASIL 安全等级、功能需求和应用场景。模块化包括针对系统不同应用模块设计要求具有针对性且灵活性功能的产品。可扩展性和模块化解决方案使得用户能够根据自身的需求，借助不同规格的芯片，实现多样化的安全架构。

现阶段，基于 MPSafe™ 开发流程已发行了多种涵盖不同功能的明星产品。通过集成内建自测试 (BIST) 以及诊断和写保护等复杂的功能安全特性，这些产品已经通过独立认证机构的认证，支持具有高达 ASIL-D 的最高汽车安全完整性级别的应用，符合 ISO26262 标准。为实现不同安全等级系统的可扩展和模块化的解决方案，目前一些基于 MPSafe™ 开发的适用于自动驾驶平台智能供电与监控的产品有：

### 1. 自动驾驶 SoC 核心供电：MPQ2967+Intelli-Phase™ DrMOS

随着自动驾驶功能的不断丰富和完善，系统对于主芯片的算力和信息处理能力的要求不断提高，以满足更丰富的自动驾驶场景的计算需求。主芯片算力的提高也意味着更高的功耗，系统对于核心供电的要求也更高。[MPQ2967](#) 是一款用于汽车高级驾驶辅助系统 (ADAS) 和自动驾驶平台核心供电的功能安全数字化双路多相控制器芯片，它可以与 MPS 的 [Intelli-Phase™](#) 产品配合使用，以更少的外部组件实现多相调压器 (VR) 解决方案。[MPQ2967](#) 基于 MPS 独特的数字多相非线性控制，能以最少的输出电容为负载阶跃提供快速瞬态响应。其集成的多次可编程 (MTP) 存储器能够存储为不同设计和平台定制的个性化配置。

[MPQ2967](#) 支持系统设计达到 ASIL-D 的功能安全等级，其集成了内建自测试、时钟监测、寄存器监测、存储器监测和纠正、ADC 监测、状态机自检、I2C 通信监测和内部电压监测等丰富的功能安全保护，保证芯片的可靠高效运行。它还多相调压器提供了输入电压、输出电压、输出电流和温度的实时监控和报告功能。用户可通过数字化接口灵活设置和监控设备的配置参数和故障参数。

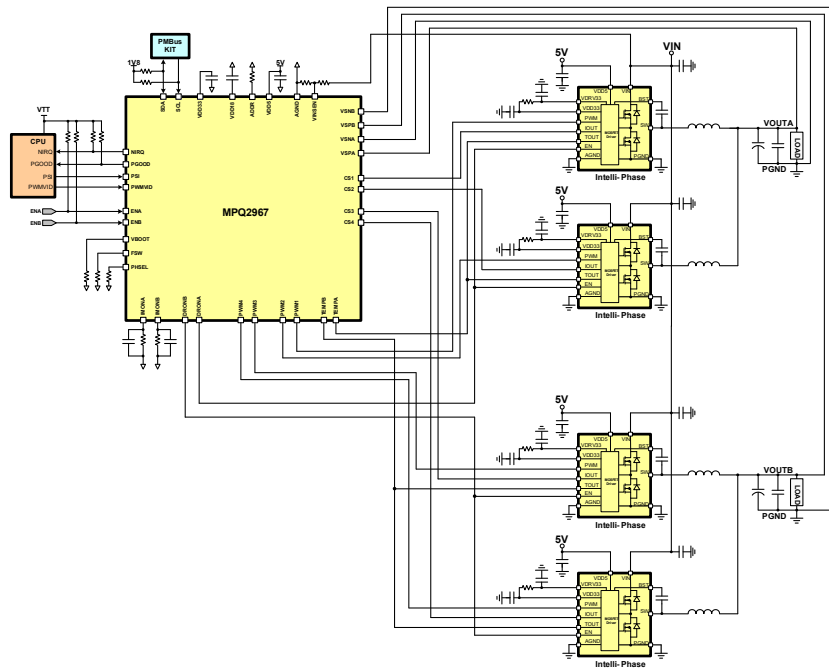


图 4: MPQ2967+Intelli-Phase™ DrMOS 方案框图

## 2. 电源时序芯片: MPQ79700FS-AEC1

一些高性能 ADAS 上的 SoC 往往需要电源轨道为内部电路供电, 如内核、内存和 I/O 等等。这些电源轨道常常需要特定的上下电时序来实现安全的通电和断电, 如上下电顺序发生错乱, 可能会导致意外电压尖峰、系统无法正常开启和关断甚至烧毁等危险。因此, 电源轨道正确有序的上下电对于保证系统的可靠开启、运行和关断有着极为重要的作用。

[MPQ79700FS](#) 是一款专为汽车高级驾驶辅助系统 (ADAS) 和自动驾驶平台设计的 12 通道功能安全电源时序芯片, 可为需要多个电源轨道供电的 SoC 提供必要的上下电时序控制。该设备的可配置性和灵活性支持跨不同的设计应用。用户可通过 I2C 对 12 个通道进行独立配置每个通道的拉高拉低时序序列。同时, 12 个通道中的四个还可以被设置为 GPIO, 以满足用户的额外需求。[MPQ79700FS](#) 电源时序芯片包含一个振荡器, 通过驱动芯片外部晶体震荡以发出 32.768 kHz 的时钟信号, 以及一个具有报警功能的实时时钟 (RTC)。该芯片还包含可通过 I2C 接口访问的可配置看门狗, 低电平有效的系统复位以及中断输出来保证故障监测和报告。

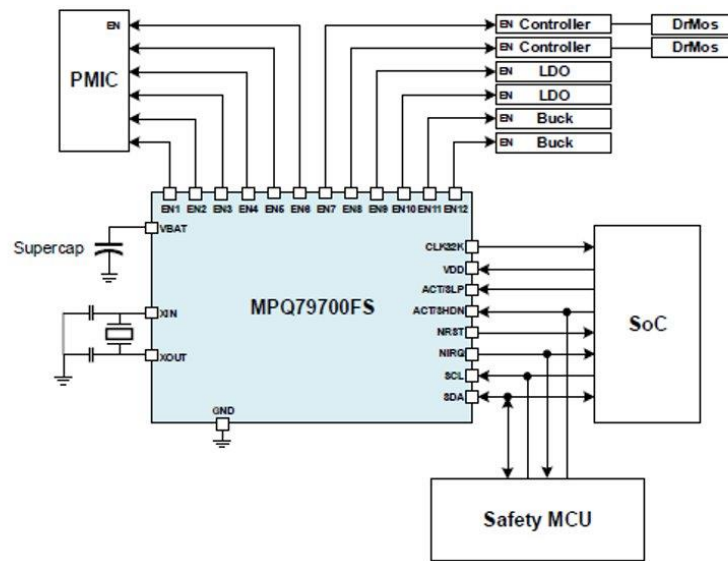


图 5: MPQ79700FS-AEC1 原理框图

### 3. 电压监控芯片 MPQ79500FS-AEC1

[MPQ79500FS-AEC1](#) 六通道电压监控芯片是一款专为监控汽车安全应用系统级芯片 (SoC) 的产品。对于 SoC 来说，超出范围的电源电压可能会导致系统运行性能不佳甚至系统故障，因此电压监控芯片在确保受监控的电源电压方面发挥着关键作用。

[MPQ79500FS-AEC1](#) 电压监控芯片会在被监控电压超过阈值时检测过压 (OV)，或在电压降至阈值以下时检测欠压 (UV)。一旦发生过压或者欠压，电压监控芯片会向安全微控制器单元 (Safety MCU) 报告故障，使 MCU 在故障发生后能够及时做出判断，保证系统的正常运行。[MPS79500FS](#) 电压监控芯片可以更智能高精度地监控六个通道的低频 (LF) 电压漂移和高频 (HF) 电压噪声。

- 1) 低频电压漂移：由高精度模数转换器 (ADC) 转换为数字信号。
- 2) 高频电压噪声：通过高精度比较器，监测电压噪声或尖峰。

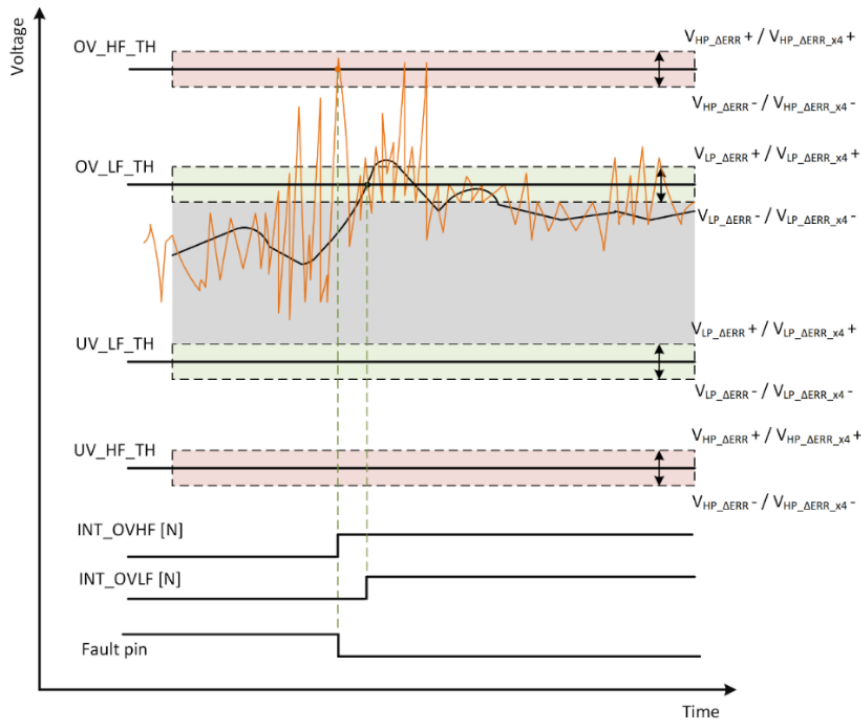


图 6：发生 OVHF 和 OVLF 故障事件时的故障检测

用户可以通过 I2C 来访问并配置 OV 和 UV 监控阈值和受监控范围。图 6 显示了 [MPQ79500FS](#) 在发生 OVHF 和 OVLF 故障事件时的 OVHF、OVLF、UVHF 和 UVLF 监控以及故障报告和记录。

[MPQ79500FS](#) 具有多个嵌入式通道，为监控大量通道的应用提供了理想的解决方案。这增加了用户使用一个集成电压监控芯片监控多轨电压的灵活性，在保证被监控设备的安全运行的同时，为用户节约了系统空间和降低成本。用户还可通过同步多个电压监控芯片到同一时序中来监控多个电压监控芯片的所有电压轨。对于 [MPQ79500FS](#)，此序列监控同步功能由 /SYNC 引脚启用，所有电压轨共享一个同步域。

## 高效、快捷、成本可控的安全解决方案

高级驾驶辅助系统（ADAS）以其良好的驾驶体验和安全保障赢得了大量消费者的青睐，除了基本的驾驶需求，消费者对更安全更智能的驾驶有了更高的期待。在新型电动汽车厂商大力推进、传统汽车厂商积极转型的过程中，整个 ADAS 市场增长迅猛。原有的为高端市场服务的 ADAS 技术的厂商，为更好的迎合市场需求，都在积极寻求向中端甚至低端市场布局。对于汽车厂商而言，只有尽快实现量产跟进旺盛的需求才有可能在激烈市场竞争中赢得一席之地。同时，市场需求也大大加速了 ADAS 技术的系统迭代。如何利用每一次技术迭代，高效、快捷、成本可控地跟进市场需求，是每一个汽车厂商在这硝烟弥漫的市场竞争中取得成功的重中之重。

针对现如今电动汽车及自动驾驶激烈的飞速发展和激烈竞争，MPS 力求为客户提供一整套完整的系统供电及监控解决方案的同时，从客户角度出发，与客户一同高瞻远瞩，帮





助客户加速开发进程，快速反应市场，更好适应现阶段乃至未来若干代自动驾驶技术的革新。

图 7 展示了一个位自动驾驶平台计算中心供电的顶层架构。该架构为符合 ASIL-D 标准的智能自动驾驶平台供电与监控平台。整个架构大体分为 SoC 供电模块，摄像供电模块两部分。MPS 提出的解决方案通过采用 MPSafe™ 开发流程，在保证功能安全的基础上，同时能帮助用户实现高效、快捷和成本可控。

图 8 展示了由 MPS 开发的具有智能电压监控功能的 MPSafe™ 电源子系统参考设计板。

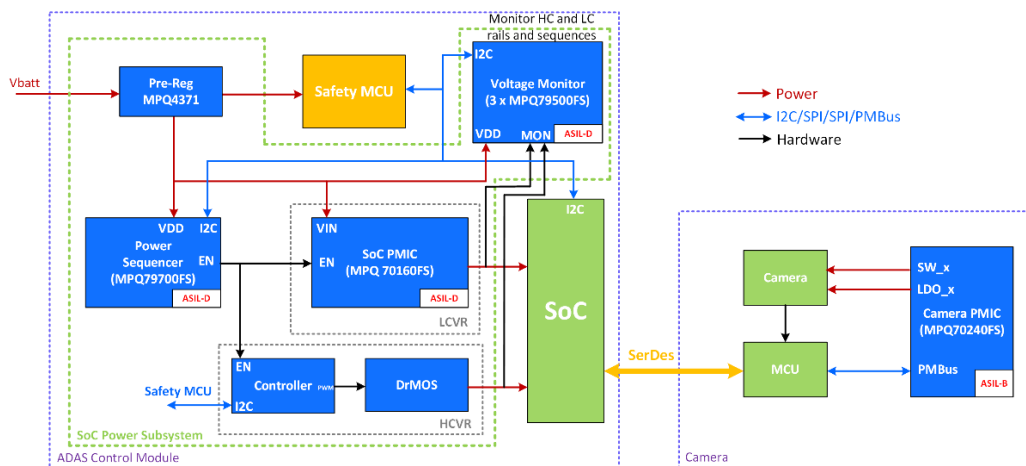


图 7：智能电压供电与监控应用于自动驾驶平台的顶层架构



图 8：具有智能电压监控功能的 MPSafe™ 电源子系统参考设计板

(注：有关参考设计的更多信息，请联系 MPS)



## 总结

随着自动驾驶技术的不断发展，安全是重中之重，绝不能妥协。为了自动驾驶的安全和正常运行，MPS 提出的智能电源供电系统集成了功能安全、电压监控和安全供电等功能，可以实现高精度、高可靠性和可配置性持续安全供电与系统监测。

## 参考资料

[1] For more details on MPSafe™ Solutions:

[MPSafe™解决方案 - 汽车（车规级） - 产品 \(monolithicpower.cn\)](#)

[2] A Brief Primer on MPSafe™, MPS' s Process to Functional Safety Automotive Development. [A Brief Primer on MPSafe™, MPS' s](#)

MPS 市场部

