引信全电子安全系统安全性研究

黄　东　史潇飞　闵玮亮
江西国科军工集团股份有限公司　江西南昌　330000

摘　要：引信作为弹药系统中的关键组件，直接关系到武器的作战可靠性与安全性。随着现代军事技术的进步，引信逐渐向全电子化方向发展，采用了电子元件和数字化控制技术，提升了引信的精度、灵活性和响应速度。然而，电子系统的复杂性也带来了新的安全性挑战。引信全电子安全系统安全性研究具有重要的军事战略意义，不仅能确保弹药的使用安全，减少事故风险，还能提升武器装备的整体作战效能。通过深入研究电子引信的安全性，能够有效防止外部干扰和系统故障，优化多重安全保护机制，提高系统的抗干扰能力和冗余设计，从而满足日益严格的军事安全标准，并为未来技术创新奠定基础。因此，这一领域的研究不仅对武器系统本身具有重要意义，也对提升国家安全和战略威慑力具有深远的影响。

关键词：全电子安全系统；环境信号；安全失效率；时序逻辑设计

引信全电子安全系统是一种基于现代电子技术的高效、安全的解决方案。通过集成先进的传感器、控制单元和冗余机制，电子引信能够提供更高的安全性、可靠性和智能化控制。在理论分析中，我们可以看到其多重安全机制和智能响应方式，以及在弹药使用中的关键作用。然而，随着技术的不断进步，如何应对电子元件的可靠性、抗干扰能力和系统复杂性等挑战，仍是未来电子引信研究的重点方向。

一、引信全电子安全系统分析

引信全电子安全系统是现代弹药设计中的一种重要技术创新，采用电子元件和数字化控制手段来保证弹药在特定条件下的安全性，避免提前或误爆。在引信系统中，安全性是最为关键的指标之一，尤其是在军事应用中，如何确保武器在发射和使用过程中的安全性，避免意外引爆、提前爆炸或者故障爆炸是设计的核心目标之一。全电子安全系统利用电子技术对引信的安全性能进行控制和监测，并根据外部条件和内部状态做出响应。

1.引信全电子安全系统的组成

电子安全锁定机制通过电子电路或控制器实现的电子锁定，防止在弹药未达到发射条件时启动引信。常见的电子安全锁定方式包括加速度传感器、温度传感器和时间延迟机制等。内置加速度传感器、旋转传感器、倾斜传感器等，用于实时监测弹药的飞行状态或接触情况，确保在特定条件下才允许引信启动。微处理器与控制单元用于接收各类传感器数据，判断当前状态是否满足引信启动条件。如果满足条件，微处理器会发送信号激活引信，否则维持安全状态。现代引信系统还可以通过无线通讯模块与外部系统（例如发射平台或战场指挥中心）进行数据交换，实时更新其状态和安全信息。为了提升安全性，系统通常具有冗余设计，如双通道或多通道传感器和控制单元。如果一个传感器或通道失效，另一个可以替代，从而保证系统的持续可靠性。

2.引信全电子安全系统的工作原理

（1）初始状态：电子锁定

在弹药发射前，电子安全系统会将引信保持在锁定状态，防止任何外部干扰或误操作引发爆炸。这一阶段，电子安全系统通过加速度传感器、温度传感器等多种监测装置检测环境变化。只有当弹药进入发射过程，且其外部和内部条件达到预定标准时，安全锁定机制才会解除。

（2）飞行阶段：状态监测与验证

在弹药飞行阶段，系统持续监测其状态。加速度传感器实时检测飞行中的加速度变化，确保弹药没有因为外部冲击或撞击而提前引爆。如果系统检测到异常的冲击或温度超限，安全系统会立即采取措施，禁用引信触发。

（3）接近目标阶段：引信启动

当弹药接近目标时，传感器会检测到适当的飞行状态，例如预设的加速度、旋转速率等，满足启动条件后，控制单元解锁引信，并触发爆炸机制。此时，引信的安全机制解除，弹药会根据设定的时间延迟或距离触发爆炸。

（4）失败保护机制：故障检测与容错

如果在任何一个环节中，电子安全系统检测到异常或故障（如传感器失效、电源中断等），冗余和容错设计会立即生效，确保系统不受单点故障的影响。这种冗余设计可以显著提升整个系统的可靠性。

3.引信全电子安全系统的安全机制

全电子安全系统具有多种安全机制，用于确保弹药在各种环境下的可靠性和安全性。在弹药发射时，利用加速度传感器判断是否已进入发射状态。当加速度超过预设阈值时，系统解锁引信并准备触发爆炸。通过温度传感器监控引信内部和外部的温度，避免因过热或温度剧烈变化引发不安全情况。温度异常时，系统会阻止引信启动。系统设计中包含时间延迟模块，确保弹药在达到一定飞行距离或时间后才会启动引信，避免在发射初期就触发爆炸。

4.引信全电子安全系统的优势

相比传统机械引信，电子引信能够更加精确地控制引信的启用条件，减少由于机械部件磨损、松动等引发的故障。通过多重安全机制的设计，电子引信能够防止由于外部震动、碰撞等因素引发的误爆，显著提高了作战过程中的安全性。电子引信具有较强的适应性，能够根据弹药的飞行环境、外部状态、时间等多维度因素作出智能判断，从而增强其安全性和准确性。现代电子引信可根据需要进行编程，支持不同类型弹药的定制化设计，能够根据任务需求调整启动条件。

5.引信全电子安全系统面临的挑战

尽管全电子安全系统在很多方面展现了显著的优势，但在实际应用中电子元件的性能可能受环境变化（如温度、湿度、电磁干扰等）影响，如何确保在极端环境下的稳定性和可靠性，仍是电子引信设计中的一个挑战。全电子引信系统的设计和调试需要高水平的电子技术支持，系统可能因为复杂的电路、软件算法等出现故障，导致系统可靠性受到影响。电子引信的研发和制造成本相较于传统机械引信较高，需要高精度的元件和严格的质量控制，同时其生产工艺也较为复杂。

二、安全失效率计算原理和方法

1.全电子安全系统框图与引用声明

全电子引信安全系统设计的主要目标是确保引信的安全性和可靠性，防止误爆、延误爆等安全问题的发生。本系统采用了三种环境激励信号作为三级解保环境信号，从而增强了安全性。系统框图如图1所示，包含了多个关键组件，每个组件的功能和交互关系都在设计中得到了详细说明。为确保系统的安全性和可靠性，设计采用了静态开关和动态开关。

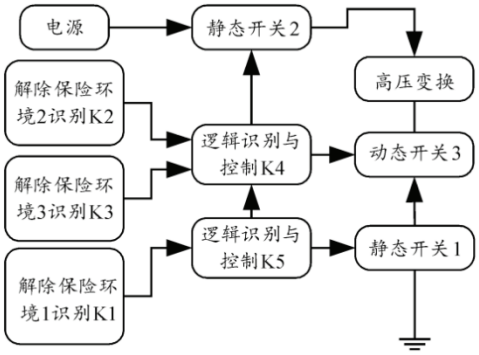

图1　全电子安全系统原理框图

概率定义如表1所示。

表1　概率定义

概率符号	定义声明
p11、p21、p31 p1d1、p2d1、p3d1 p1d2、p2d2、p3d2 pK1d、pK2d、pK3d pK1K、pK2K、pK3K pK1S、pK2S、pK3S pK5S1、pK4S2、pK4S3	静态开关1、2和动态开关3分别在非工作状态下出现正常工作的概率静态开关1、2和动态开关3分别在非工作状态下发生短路的概率 静态开关1、2和动态开关3分别在工作状态下发生短路故障的概率环境识别K1、K2、K3分别错误输出概率 环境识别K1、K2、K3分别使器件发生故障导致误输出的概率 环境识别K1、K2、K3分别出现识别错误导致误输出的概率

假设PK21是某种电气系统或电力电子电路中，启动升压的成功概率，它可能与系统的启动条件和稳定性相关。为了确定PK21，升压电路通常要求输入电压达到一定阈值才能启动。如果输入电压过低，则升压电路可能无法正常工作。电力电子电路中的开关元件（如MOSFET或IGBT）通常由控制信号驱动，启动升压过程可能依赖于开关控制信号的质量和时序。系统负载变化也可能影响升压的启动概率。负载过重或变化过大时，可能影响升压过程的稳定性。在某些情况下，系统中的噪声或外部干扰可能会影响电路的启动行为，导致升压过程的启动失败。

三、引信全电子安全系统安全性提升策略

1.增强冗余设计

冗余设计是提升安全性的核心策略之一，尤其是在关键模块的设计中。通过冗余设计，可以确保系统即使在某些组件出现故障时仍能保持安全性和正常工作。在系统中引入双重或多重处理单元，确保当一个模块发生故障时，其他模块能够接管工作并保证系统的安全性。在关键传感器（如加速度传感器、温度传感器、压力传感器等）上设计冗余通道。如果某个传感器发生故障，

其他冗余传感器可以提供有效数据，保证系统仍能判断是否处于安全状态。通过冗余电源系统确保系统在主电源发生故障时，能够切换到备用电源，避免因电源问题导致系统失效。

2.加强故障检测与诊断能力

故障检测和诊断能力对于提升系统安全性至关重要，能够实时监测系统状态，及时发现潜在故障，并采取措施避免引信误爆或未爆的危险。在系统设计中加入自检机制，定期或实时对系统进行健康检查，检测关键部件是否正常工作。通过自检功能，系统可以主动监测传感器、控制电路和执行器等部件的状态。在发生故障时，系统应能够准确判断故障类型，并采取适当的措施，如切换到备用模块或进入安全模式，以防止故障扩展和引发事故。系统应设计为能够在某些组件发生故障时仍能继续安全运行。比如，通过增加冗余路径、采用故障切换等技术保证系统在发生部分故障时不会立即失效。

3.提升抗干扰与防护能力

全电子引信安全系统的设计需要具备较强的抗干扰能力，以避免外部干扰导致引信误动作或失效。系统内部电路需具备抗电磁干扰的设计，采用屏蔽措施、滤波器以及差分信号传输技术，确保系统不会受到外界电磁波的干扰。可以使用低噪声放大器（LNA）、屏蔽和地线设计等技术来降低系统对电磁波的敏感性。由于EMP可能会破坏电子设备，因此需要设计防EMP能力，例如通过使用抗EMP的元件、外壳屏蔽设计、增加地面保护等。设计时需要考虑到引信系统在极端震动条件下的稳定性，采用抗震和抗冲击设计，如使用阻尼材料、加强内部支撑和电路布局等措施，以确保系统在受到剧烈碰撞或振动时不会发生误动作。

4.增强物理安全性

引信全电子安全系统的物理安全性是避免系统在受到外部物理攻击或意外影响下引爆的基础。强化物理安全性可有效减少误触发的风险。设计时需要考虑到敌方破坏和攻击的可能，确保电子系统能抵御物理攻击，避免系统受到损坏导致误爆。采用密封外壳，防止外界环境对电子系统的影响，从而保持系统的长期可靠性。系统外壳应具备足够的强度，避免外界物理力量对电路和元件造成损害。

5.多层次安全激活机制

为了确保引信在仅满足严格条件时才激活，可以设计多层次的安全激活机制。通过综合判断多个参数来决定是否激活引信，从而提高安全性。利用多种传感器来共同判断是否符合引信激活条件。例如，只有当加速度传感器检测到一定的加速度，并且温度、湿度等其他传感器也显示系统处于工作环境时，才会解除保险并激活引信。引信系统可以采用分阶段的激活机制，避免一旦系统处于危险状态时立即触发引信。通过先解除一部分保险，然后进行后续检查，确保系统条件稳定，最后才允许完全解锁。

6.完善软件与算法安全性

全电子安全系统的核心不仅仅是硬件，还包括系统的控制软件和算法。软件部分的可靠性和安全性也对整个系统的安全性至关重要。引信系统的软件应具备加密措施，防止外部干扰或恶意操作。通过加密通信、加密存储等手段保护系统的关键数据和指令，确保系统不被未经授权的人员篡改。所有控制逻辑和判断算法必须经过严格的验证和测试，以确保在各种极端情况下依然能够准确判断并执行安全操作。通过形式化验证、仿真验证等方式来提高算法的可靠性。系统应具备远程诊断和更新的能力，能够及时发现和修复软件中的漏洞，提升系统的安全性。

7.强化系统测试与认证

在系统设计完成后，需要进行严格的测试和认证，确保其在各种条件下都能正常工作，并具备足够的安全性。通过模拟极端环境条件来测试系统的可靠性和安全性，确保在恶劣环境下不会发生失效。模拟系统可能遇到的故障情况以及外部攻击，验证系统是否能够有效应对。确保系统符合国际标准或国家标准的安全认证要求，如ISO/IEC15408（信息安全技术，通用准则）等，以增加系统的可信度和合法性。

总结

提升引信全电子安全系统的安全性需要从多个方面着手，包括冗余设计、故障检测、抗干扰能力、物理安全性、多层次激活机制、软件安全性和系统测试等。这些策略相互结合、相辅相成，能够有效提高系统的安全性，降低误爆、误操作和故障的风险，确保武器系统的可靠性和战术执行的安全性。在实际应用中，这些策略需要根据具体的战场需求、环境条件和技术水平进行优化和实施。

参考文献

[1]中央军委装备发展部.引信安全性设计准则：GJB373B—2019[S].北京：国家军用标准出版发行部，2019：2-5.

[2]汪仪林，马秋华.全电子安全系统失效率计算[J].探测与控制学报，2023，45（1）：1-10.

[3]王雨时，纪永祥.引信安全性现状分析与试验考核建议[J].探测与控制学报，2021，43（4）：1-8，26.