

某型自动装弹机故障注入系统研究

邵思杰¹, 熊伟², 曹勇³, 张继红⁴, 高春⁵

- (1. 装甲兵工程学院 兵器工程系, 北京 100072; 2. 解放军驻 617 厂军代室, 内蒙古 包头 014032;
3. 装甲兵工程学院 控制工程系, 北京 100072; 4. 内蒙古科技大学 信息工程学院, 内蒙古 包头 014010
5. 国营 617 厂 科研院所, 内蒙古 包头 014032)

摘要: 针对装甲装备武器系统组成复杂, 故障检测与隔离困难, 维修训练手段落后等问题, 通过对某型自动装弹机典型故障进行统计分析, 兼顾考虑硬件故障注入和软件故障注入技术优缺点, 构建了故障注入模型, 并将成果汇总整理形成故障注入汇编; 采用嵌入式控制技术设计了自动装弹机故障注入系统的故障注入器和故障注入软件, 开展了系统静态测试和实装测试, 试验结果表明, 系统能够按照要求对自动装弹机进行故障注入, 为操作人员维修训练提供技术支持。

关键词: 故障注入; 测试性; 自动装弹机

Study on Fault Injection System for A Special Auto-loader

Shao Sijie¹, Xiong Wei², Cao Yong³, Zhang Jihong⁴, Gao Chun⁵

- (1. Department of Armored Equipment Engineering, Academy of Armored Force Engineering, Beijing 100072, China;
2. Military Representative office of 617 Plants of PLA, Baotou 014032, China;
3. Department of Control Engineering, Academy of Armored Force Engineering, Beijing 100072, China;
4. Information Engineering College, Inner Mongolia University of Science and Technology, Baotou 014010, China;
5. R&D Institute of 617 State-owned Corporation, Baotou 014032, China)

Abstract: Aiming at the problem of armored equipment weapon system, such as complex composition, difficult of fault diagnosis and isolation, backward of maintenance training, through the statistical analysis of typical faults of auto loader, also considering the advantages and disadvantages of hardware and software fault injection technology, the fault injection model was constructed, furthermore, the achievements were summarized to form a fault injection assembly. Using embedded control technology to design software fault injection and fault injector of auto loader fault injection system, to carry out the static test and actual auto loading test on the system, test results show that the system could be in accordance with the requirements for auto loader fault injection, it provides technical support for the operator's maintenance training.

Keywords: fault injection; testability; auto-loader

0 引言

故障注入是一种检验系统容错能力的测试方法。针对装甲装备武器系统组成复杂, 故障检测与隔离困难等问题, 以某型自动装弹机为例开展故障注入系统研究, 为指导操作人员进行故障分析和维修训练, 提供技术支持。

1 自动装弹机典型故障分析

某型自动装弹机是一种机电一体化的综合系统, 主要由旋转输弹机、提升机构、推弹机、火炮闭锁器、抛壳机构、开窗机构等执行机构以及程控箱、弹舱识别器、装弹机 MIC 盒及控制电缆组成^[1]。

1.1 典型故障统计

通过收集近年来总装工厂生产试验以及部队使用维修过程中出现的自动装弹机故障数据, 并对其进行统计分析和优化整理, 共提取常见故障现象 12 个, 如表 1 所示。

表 1 所示故障现象覆盖了自动装弹机各执行机构, 具有典型性和代表性, 可以反映自动装弹机的常见多发故障, 对开展故障注入系统设计, 有着重要的参考价值。

收稿日期:2017-07-13; 修回日期:2017-08-29。

作者简介:邵思杰(1968-),女,北京市人,博士,副教授,主要从事武器测试与故障诊断方向的研究。

表 1 自动装弹机典型故障统计

编号	故障部件	故障现象
GZ1	窗机构	自动工况时,抛壳并关窗后不进行下一步的装弹动作
GZ2		自动工况时,不进行开窗动作
GZ3	升机构	自动工况时,提升到弹丸位时提升机运动不停止,不推弹
GZ4		自动工况时,提升无动作
GZ5	转输弹机	装弹无动作,电磁铁配电显示红色
GZ6		输弹机自动旋转时,只能反向旋转
GZ7	炮	自动工况时,火炮闭锁器闭锁后不抬架
GZ8	闭锁器	自动工况时,火炮闭锁器不闭锁
GZ9	弹机	自动工况时,推弹丸入膛后推弹链不收回
GZ10		推弹机不工作
GZ11	壳机构	开窗到位后,不关窗
GZ12		抛壳机框架不能抬架

1.2 故障机理分析

一般情况下,自动装弹机出现故障时,计算机终端上会有简单的故障代码显示,帮助操作人员进行故障的分析和排除。故障代码只是反映目前部件所处的状态是否正确,并不会显示执行部件(电机、电磁体)的工作状态错误,对于判断故障只起辅助作用。为了实现故障注入,需要重点分析典型故障的机

理原因。

例如，对于 GZ1 来说，正常情况下，抛壳机构抛壳后，程控箱输出开窗机构电机关窗驱动信号，开窗机构执行关窗动作，当关窗到位，输出到位信号至程控箱后，程控箱停止输出关窗驱动信号，使开窗机构电机停止工作，之后，开始进行推弹机收回推弹链等一系列后续动作。由此看出，若发生 GZ1 现象，可能原因有以下几个方面：

- 1) 开窗机构微动开关 K1 故障导致关窗到位后没有向程控箱输出到位信号；
- 2) 程控箱本身故障没有接收到到位信号或没有输出下一步进行的推弹机收链驱动信号；
- 3) 推弹机推弹链卡滞或电机故障，无法进行收链动作；
- 4) 电缆故障导致信号无法传递。

GZ1 故障树如图 1 所示。

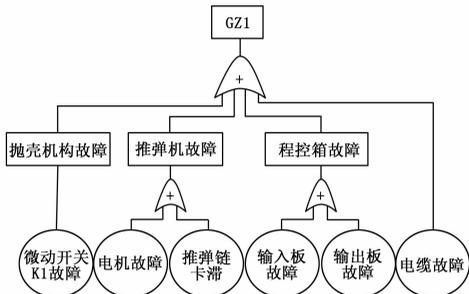


图 1 GZ1 故障树

其他典型故障现象故障机理分析同上，限于篇幅，不再一一赘述，详细内容见后节故障注入汇编表。

2 故障注入实现方案

2.1 故障注入技术

故障注入是指按照选定的故障模型，用人工的方法有意识地产生故障并施加于运行特定工作负载的目标系统中，以加速该系统的错误和失效的发生，同时观测和回收系统对所注故障的反应信息，并对回收信息进行分析，从而向试验者提供有关结果的试验过程^[2]。故障注入技术是对系统性能评价的一个重要手段，通过对注入故障后系统的反应信息进行监测和分析，可获得系统可靠性和容错特性的评测结果。

按所注入的故障注入途径，故障注入总体上可分为硬件故障注入仿真和软件故障注入仿真两大类^[3-4]。硬件故障注入仿真通过附加硬件对目标系统的作用，使目标系统的正常硬件环境受到影响，从而产生故障。软件实现的故障注入无需额外的硬件设备，可以在程序指令能够访问到的硬件或软件上选择故障注入位置。

对于自动装弹机而言，如果采用硬件故障注入技术，一种是在现有装备上人为设置故障，势必要损坏装备；一种是需要消耗大量费用开发相应的半实物仿真平台^[5]，模拟自动装弹机各机构功能，通过在真实环境下人为的进行故障注入来实现有效的故障分析。如果采用软件故障注入技术，则需要改写自动装弹机程序代码，可能会给装备的系统性能带来严重影响，这对于定型装备而言是严格不允许的。

因此，需要针对自动装弹机特点以及典型故障机理分析，充分借鉴各种技术优缺点，设计一种合理可行的故障注入方案。

2.2 故障注入模型

自动装弹机各执行机构主要是在程控箱输出的驱动信号作用下响应执行各动作程序，而程控箱是在采集各执行机构有关状态信息后按照一定的程序输出相应的驱动信号，可以看出程控箱中核心控制单元的程序软件的主要功能就是按照一定的逻辑和时序，控制各类信号的传递。若采用软件故障注入仿真的方法，修改程控箱核心控制单元软件源代码，使程序变异进而导致系统产生故障，实际上仍是依靠破坏信号的正常传递流程来实现故障注入。为此，可以借鉴软件故障注入仿真方法的思想，通过在自动装弹机各执行机构与程控箱之间加入一个采用硬件结构的故障注入器，按照一定的故障注入逻辑和控制程序对自动装弹机系统的有关信号进行控制，进而实现故障仿真及注入。

例如：对于 GZ1 而言，由故障机理分析可以看出，开窗机构微动开关 K1 故障，程控箱输入板、输出板故障，推弹机电机故障，以及电缆故障均能导致 GZ1 故障现象的发生，而微动开关 K1 故障和程控箱输入板故障实际上就是中断了关窗到位信号的正常传递，而程控箱输出板故障和推弹机电机故障实际上就是中断了推弹机收链驱动信号的正常传递，电缆故障同样是中断了这些信号的正常传递。因此，通过控制这些信号通断即可实现 GZ1 的故障注入，故障注入模型如图 2 所示。

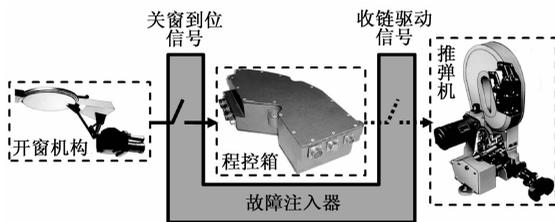


图 2 GZ1 故障注入模型

2.3 故障注入汇编

其他典型故障现象故障注入模型原理同上。这里，将自动装弹机各典型故障机理分析以及故障注入模型原理分析成果进行汇总整理，形成故障注入汇编，如表 2 所示。通过故障注入汇编将故障现象、故障机理与部件接口、故障注入方案一一对应，同时进行故障编号，形成应用于故障注入实现的故障模型，为故障注入系统设计提供依据。

3 故障注入系统设计

根据故障注入实现方案，自动装弹机故障注入系统主要由故障注入器和故障注入管理软件组成，系统通过中继电缆，采用高可靠的隔离技术，与自动装弹机实现无缝接入。系统总体组成如图 3 所示。

系统工作原理为：首先，故障注入器采集自动装弹机各执行机构输出的状态信号，即故障注入器的输入信号；其次，故障注入器能够模拟这些状态信号，根据相应的控制命令，输入至自动装弹机程控箱，同时，也可以模拟程控箱输出的驱动信号，根据相应的控制命令，输入至自动装弹机各执行机构，故障注入器模拟的信号即其输出信号。故障注入软件安装在 PC 终端，能够实时监测并显示故障注入器采集的状态信号，同时根据故障注入策略，通过通信总线将相应的控制命令发送到故障注入器，进而通过控制故障注入器输出不同的信号给自动装弹机各执行机构或程控箱，实现故障注入。当注入某一故障

表 2 自动装弹机故障注入汇编

编号	故障分析 机理	故障注入信号	
		可选信号	类型
GZ1	①开窗机构微动开关 K1 故障导致关窗到位后没有向程控箱输出到位信号;②程控箱本身故障没有接收到关窗到位信号或没有输出收链驱动信号;③推弹机推弹链卡滞或电机故障,无法收链;④电缆故障导致信号无法传递。	关窗到位	低电平/悬空
		收链驱动	低/高电平
GZ2	①推弹机微动开关 K1 故障导致推送弹丸到位后没有向程控箱输出推弹丸到位信号;②程控箱本身故障没有接收到推弹丸到位信号或没有输出开窗驱动信号;③开窗机构电机故障或开窗口卡滞,无法开窗;④电缆故障导致信号无法传递。	推弹丸到位	低电平/悬空
		开窗驱动	低/高电平
GZ3	①提升机构微动开关 K1 故障导致提升弹丸到位后没有向程控箱输出提升弹丸到位信号;②提升机构电磁铁故障导致没有闭锁;③提升机构开关盒内的仿形轮错位、损坏或分度盘松动、错位导致的故障;④程控箱本身故障没有接收到提升弹丸到位信号或没有输出提升驱动信号;⑤电缆故障导致信号无法传递。	提升弹丸到位	低电平/悬空
		提升驱动	低/高电平
GZ4	①旋转输弹机电磁铁故障导致没有向程控箱输出大电磁铁闭锁闭锁信号;②程控箱本身故障没有接收到相关信号或没有输出电磁铁吸合、提升驱动信号;③提升机构电机故障或电磁铁故障,无法进行提升动作;④电缆故障导致信号无法传递。	大电磁铁闭锁	低电平/悬空
		提升驱动	低/高电平
		电磁铁吸合	
GZ5	①旋转输弹机电磁铁微动开关 K1 故障导致电磁铁配电显示红色;②程控箱本身故障没有接收到小电磁铁闭锁信号;③电缆故障导致信号无法传递。	小电磁铁闭锁	低电平/悬空
GZ6	①旋转输弹机电机故障导致无法反转;②程控箱没有输出反向旋转驱动信号反向旋转驱动或接触器故障没有执行驱动;③电缆故障导致信号无法传递。	反向旋转驱动	低/高电平
GZ7	①火炮闭锁器微动开关 K1 故障导致闭锁到位后没有向程控箱输出闭锁到位信号;②程控箱本身故障没有接收到闭锁到位信号或没有输出抬架驱动信号;③抛壳机构框架卡滞或电机故障,无法进行抬架动作;④电缆故障导致信号无法传递。	闭锁到位	低电平/悬空
		抬架驱动	低/高电平
GZ8	①火炮闭锁器电机故障导致无法闭锁;②程控箱没有输出伸出闭锁销驱动信号伸出闭锁销驱动;③电缆故障导致信号无法传递。	伸出闭锁销驱动	低/高电平
GZ9	①推弹机微动开关 K1 故障导致推送弹丸到位后没有向程控箱输出推弹丸到位信号;②推弹机电机故障或开关盒内的仿形轮错位、损坏导致弹链无法收回;③程控箱本身故障没有接收到推弹丸到位信号或没有输出收链驱动信号;④电缆故障导致信号无法传递。	推弹丸到位	低电平/悬空
		收链驱动	低/高电平
GZ10	①推弹机电机故障或推弹链卡滞导致无法工作;②程控箱本身故障没有收到相关输入信号,或输出相关信号;③电缆故障导致信号无法传递。	提升弹丸到位	低电平/ 悬空到位
		提升药筒	
		推弹链原位	低/高电平
推弹驱动			
GZ11	①抛壳机构电磁铁故障导致没有向程控箱输出抛壳信号;②程控箱本身故障没有接收到抛壳信号或没有输出关窗驱动信号;③开窗机构电机故障或窗口卡滞,无法进行关窗动作;④电缆故障导致信号无法传递。	抛壳	低电平/悬空
		关窗驱动	低/高电平
GZ12	①抛壳机构电机故障或框架卡滞导致无法抬架;②程控箱没有输出抛壳电磁铁吸合信号或接触器故障没有执行驱动;③电缆故障导致信号无法传递。	抛壳电磁铁吸合	低/高电平

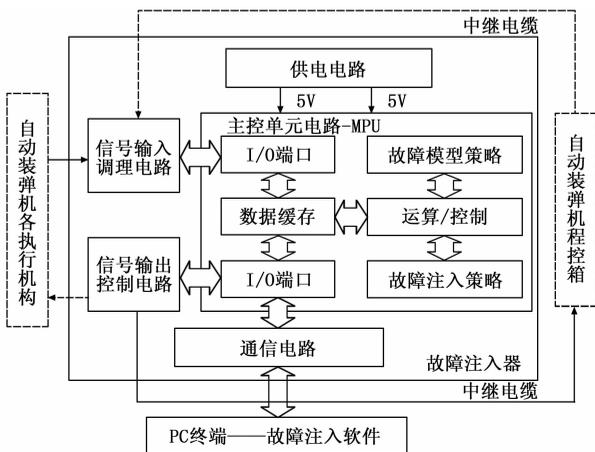


图 3 自动装弹机故障注入系统组成

后,软件能够自动调出故障原因分析数据库,用于指导操作人员。

3.1 故障注入器设计

故障注入器主要由主控单元电路、信号输入调理电路、信号输出控制电路、通信电路、供电电路等部分组成。

主控单元电路的 MPU 选用 ST 公司 32 位高性能嵌入式产品 STM32F407ZE。为了避免自动装弹机系统对故障注入器的干扰,同时降低 MPU 功耗,信号输入调理电路主要采用光电隔离技术实现故障注入器对自动装弹机各执行机构输出状态信号的实时采集。信号输入调理电路如图 4 所示。

自动装弹机各执行机构输出的状态信号,经过信号输入调理电路实现光电隔离处理后,送入 MPU 的 I/O 端口,MPU 经过数据缓存及运算后实时监测这些状态信号,进而判断各执行机构工作状态,并通过通信电路上传至 PC 终端的软件中。信号输出控制电路如图 5 所示。

操作人员通过操作 PC 终端的故障软件向故障注入器发送

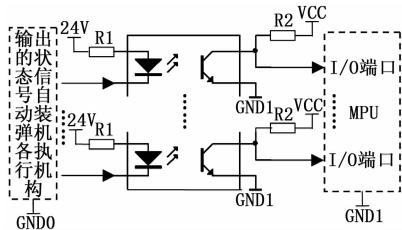


图 4 信号输入调理电路

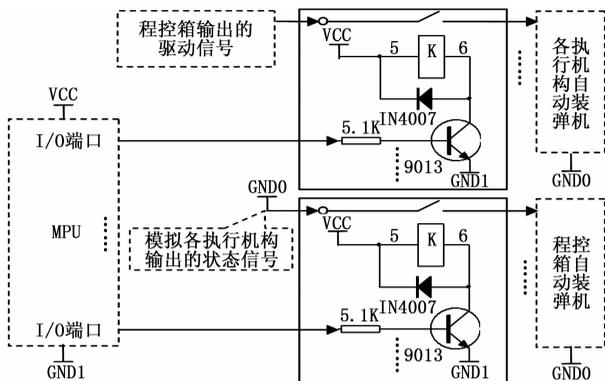


图 5 信号输出控制电路

故障注入指令，MPU 按照故障注入策略控制 I/O 端口输出不同状态信号至信号输出控制电路，经过继电器隔离处理后发送至自动装弹机相应的部件，进而实现故障注入。

3.2 故障注入软件设计

软件采用 LabWindows/CVI 集成环境开发，主要作用是驱动系统硬件、与故障注入器进行通信、提供交互式操作界面并完成故障设置、故障原因分析等。

软件设计流程为：程序开始运行后，第一步，配置通信。第二步，进行硬件初始化，主要是监测自动装弹机各执行机构输出的状态信号，控制故障注入器输出匹配的信号至程控箱，确保故障注入器与自动装弹机相互兼容。第三步，进入系统主界面，等待用户选择。第四步，根据用户的选择，或进入相应功能界面。

系统对故障注入器硬件进行初始化，实时监测自动装弹机各执行机构输出的状态信号，并根据信号状态，通过输出信号控制电路一一对应送至程控箱。此时，若要进行故障注入，按照表 2 故障注入汇编选择相应的故障注入信号，通过软件界面的开关按钮进行状态切换即可实现故障注入。

4 系统测试

4.1 静态测试

在 PC 终端故障注入软件中对有关信号进行开关操作，用万用表测量故障注入器相应输出接口管脚的电压变化情况。测试数据记录表如表 3 所示。

由表 3 可知，通过在软件中操作被测信号开启或关闭，相应输出管脚的电压状态均对应切换低电平或高电平（悬空），说明故障注入系统信号控制功能正常。

4.2 实装测试

根据故障注入汇编表，在软件中选择故障注入信号，对照界面故障信息栏，观察装备故障现象是否与控制界面设置一致，观察车长指挥终端是否显示故障提示，测试结果示例如图 6

所示。

表 3 系统静态测试数据记录表

测试信号	被测管脚	电压变化/V	结论
关窗到位	20B41-6	0.16→悬空	正常
收链驱动	20B90-10	0→4.98	正常
推弹丸到位	20B41-11	0.18→悬空	正常
开窗驱动	20B90-5	0→4.98	正常
提升弹丸到位	20B41-1	0.18→悬空	正常
提升驱动	20B90-1	0→4.96	正常
大电磁铁闭锁	18B32-2	0.22→悬空	正常
电磁铁闭合	20B90-4	0→4.97	正常
小电磁铁闭锁	18B32-1	0.12→悬空	正常
反向旋转驱动	18B8-6	0→4.96	正常
闭锁到位	20B41-8	0.12→悬空	正常
抬架驱动	18B8-6	0→4.98	正常
伸出闭锁驱动	20B90-7	0→4.98	正常
提升药筒到位	20B41-2	0.24→悬空	正常
推弹链原位	20B41-12	0.12→悬空	正常
推弹驱动	20B90-9	0→4.94	正常
抛壳	18B32-5	0.18→悬空	正常
关窗驱动	20B90-11	0→4.98	正常
抛壳电磁铁吸合	18B8-8	0→4.96	正常

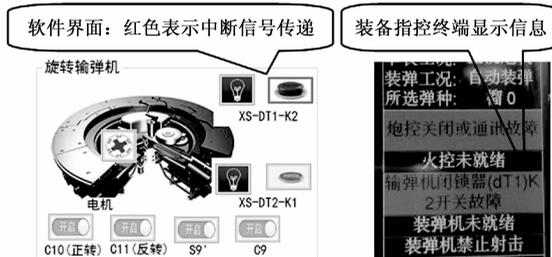


图 6 实装测试结果示例

由图 6 可知，输弹机正常工作时，XS-DT1-K2 信号导通，通过故障注入软件强行关闭该信号后，装备指控终端报警显示装弹机未就绪，输弹机闭锁器 (DT1) K2 开关故障，说明故障注入系统成功对装备注入故障。

5 结论

通过系统静态测试和实装测试，结果表明：故障注入模型正确，故障注入系统能够按照预先设定对自动装弹机进行故障注入，为指导操作人员进行故障分析排查和维修训练提供了可靠的技术支撑和方便有效的手段。

参考文献：

- [1] 冯益柏. 坦克装甲车辆设计—武器系统卷 [M]. 北京: 北京化学工业出版社, 2015.
- [2] 徐晓露. 基于故障注入的嵌入式系统测试研究 [D]. 杭州: 浙江大学, 2008
- [3] 李志宇, 黄考利, 连光耀. 基于测试性设计的软件故障注入研究综述 [J]. 计算机测量与控制, 2013, 21 (5): 1112-1114.
- [4] 朱鹏, 张平. 基于单片机的故障注入系统 [J]. 计算机测量与控制, 2004, 12 (10): 996-998.
- [5] 李志宇, 黄考利, 连光耀. 基于半实物仿真的故障注入系统设计 [J]. 计算机测量与控制, 2013, 21 (3): 570-572.