文章编号：1005-8451（2013）11-0040-03

基于故障注入的ATP系统测试设计

唐　艳，王长林
（西南交通大学　信息科学与技术学院，成都　610031）

摘　要：本文研究了基于故障注入的ATP系统测试方法。通过对ATP系统进行安全性分析寻找系统的故障来源；结合抽象描述的方式对故障进行建模，并提取测试案例；在特定事件触发点将案例注入到ATP系统中，实现测试的自动执行，从而达到对运行环境中故障状态的系统反馈实现监测、分析、及定位的目的。

关键词：ATP；故障注入；故障模型；故障案例
中图分类号：U284：TP39　**文献标识码：**A

Design of ATP System testing based on fault injection

TANG Yan, WANG Changlin
(School of Information and Technology, Southwest Jiaotong University, Chengdu　610031, China)

Abstract: This paper studied on the ATP System testing method based on the fault injection method, By analyzing the security of ATP System, the source of system failure could be found. Combined with the way of the abstract description to modeling the fault events and extracting the test cases, it was injected into the ATP System in the case of specific events trigger point, which could implement automatic testing, and achieve the design goal of monitoring, analysis, and fault location for the system feedback of the failure status in the operating environment.

Key words: ATP; fault injection; fault model; fault case

在基于通信的列车控制系统（CBTC）中，车载ATP系统是保障列车运行安全的重要组成部分。车载ATP系统与地面系统保持不间断通信，接收移动授权（MA）以及临时限速信息等，并将通过测量计算而产生的精确位置信息，结合列车运行方向反馈给地面控制系统。保障列车在无故障状态下的安全行驶。因此，对ATP系统进行全面测试验证试验至关重要。

故障注入技术是通过特定的程序对系统中关键软件、硬件或故障数据进行仿真，借助系统反馈结果检测系统的安全性，评价系统的功能设计水平。本文根据ATP系统的特点和软件故障注入的优势，采用将软件故障注入方法应用于ATP系统测试中，提高ATP系统的可靠性和容错性。

1　故障注入技术

基于故障注入的系统测试是一种非传统的测试技术，通过将有效故障模式样本注入到系统中，观察及分析测试系统在被引入故障情况下的表现，获取定性或定量的测试结果。采用故障注入的目的是为了加速失效，在较短时间内获得足够多的失效数据，以此评价系统的功能设计水平。

1.1　故障注入原理

故障注入过程主要包括以下4个步骤：选择故障模型；执行故障注入；监视系统行为；分析试验结果[1]。如图1所示，选择故障模型以及分析试验结果这2个步骤是试验者与系统直接进行交互的，是离线行为；而执行故障注入以及监视系统行为则是和目标系统的直接接口，是在线完成的。

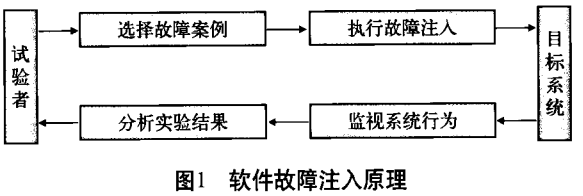

图1　软件故障注入原理

1.2　故障模型建立

真实故障具有多样性、复杂性等特征，所以建模时需要将故障情形进行抽象提取真实故障中的共性。建模的过程即解决“需要什么信息，如

收稿日期：2013-03-05
作者简介：唐　艳，在读硕士研究生；王长林，教授。

何进行描述”的问题。因此在建模前需要分析被测系统中的故障点，并对软件的故障特征进行抽象描述，生成故障模型。采用故障注入时间、故障位置、持续时间、重要度、故障率等对故障进行抽象描述。故障建模框架如图 2 所示。

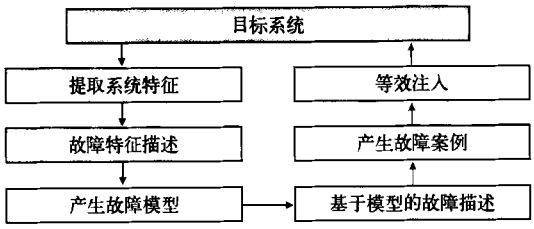

图2　故障建模框架

（1）故障编号：区分不同故障的分类，使待注入故障具有可辨识性和唯一性；

（2）故障注入设备：描述在系统中直接发生故障的设备；

（3）故障注入类型：描述故障内容；

（4）持续时间：按照故障持续时间，故障可以分为永久故障、间歇故障和偶然故障等；

（5）危险等级：风险优先数可以综合反映产品的危险等级；

（6）故障率：工作到某时刻尚未发生故障的产品，在该时刻后单位时间内发生故障的概率。

故障模型如下：

```
structFA_modle
{
    CString number;
    CStringFA_Equipment;
    CStringFA_Type;
    doubleFA_Time;
    intFA_Level;
    doubleFA_Rate
}FA_Modle [500];
```

1.3 故障注入触发方式

软件故障注入后，需要一定的触发方式激活，从而达到将故障案例注入到 ATP 系统中加速其失效的目的。即应研究故障的特定触发方式，以保证故障注入时机的合理性。触发方法可分为：

1.3.1 定时触发

利用定时器预先设定时间从而触发故障，但不能重现故障注入，而且还可能对故障注入结果产生不可预料的影响。

1.3.2 路径/事件触发

利用某个事件或条件发生触发故障。与定时触发不同，这种方法可以在某个事件或条件发生的任何时间进行故障注入。

1.3.3 负载触发

利用目标系统的负载来触发故障，该方法需要特殊负载，因此用得比较少。

综合以上 3 种触发方式及 ATP 系统的特点，事件触发更适合常规车载设备故障注入测试验证。

2 故障注入在ATP系统测试中的应用

2.1 软件故障注入系统功能

车载 ATP 作为一个安全相关系统，为了保证列车运行的安全，使系统符合安全技术要求，需要对系统进行安全分析。软件故障注入系统要求能够实现以下功能。

2.1.1 故障设置

根据系统安全性分析获取影响 ATP 系统功能的危险源，并能够根据用户要求灵活设置各类故障。

2.1.2 实时数据传输

能采集系统状态，并将故障信息实时送入 ATP 系统中，确保不影响原系统运行的实时性。

2.1.3 故障注入

按照事件触发方式在特定的时间向特定的故障位置注入规定数量的故障。用户可以控制故障注入的起始时间，并在故障注入过程中随时监视故障注入情况。

2.1.4 试验结果保存分析

将测试结果以文件形式保存，并提供数据分析，以评测列车运行控制系统的各项性能指标。

此外，故障注入系统应具有较好的可扩展性要求，以便系统功能升级。

2.2 故障案例库设计

由于 ATP 系统庞杂且所涉及的危险源多，本文只讨论与 ATP 系统存在交互的外围设备出现系统故障、操作失误、部分数据错误的情况下，ATP 能否完成预期功能的测试工作。

将车载 ATP 系统功能需求规范（FRS）作为顶级设计的基础，采用了故障树方法对系统中可能存在的危险源进行分析，寻找可能存在的安全隐患和危险源。如图 3 所示，与 ATP 交互的外围

设备故障可分为3大类：接口子系统故障、司机操作失误、不完整信息。具体包括ATO系统故障、MMI系统故障、无线通信系统故障、测速测距系统故障、I/O控制器故障、应答器天线故障、司机误操作I/O量输入，司机输入错误信息，车门错误开启等方面。

为了使所建立的故障模型具有准确性、可处理性，需要对软件的功能模块进行划分，并针对各个功能模块的测试需求建立故障模型，例如车门故障模型是针对ATP软件的车门防护功能模块的测试而建立的。

因故障注入系统应具有良好的扩展性，为此设计了自定义案例添加模块，使用户能够按照要求设置各类故障，不断扩展丰富案例库。

图3　故障模型库

2.3 故障注入控制器设计

故障注入控制器通过监控ATP系统运行状态，收集系统数据，读取包含测试用例的数据库文件；并根据故障触发条件，控制测试用例的执行，通过调用相应的接口函数，执行故障注入操作。故障注入控制器包括接口软件和注入方法。接口软件包括与故障模式库的接口、与ATP系统的接口以及与评测模块的接口。同时，故障注入控制器也起着协调故障注入过程和测试结果收集过程，获取并记录测试结果的作用。软件故障注入控制器实现流程如图4所示。

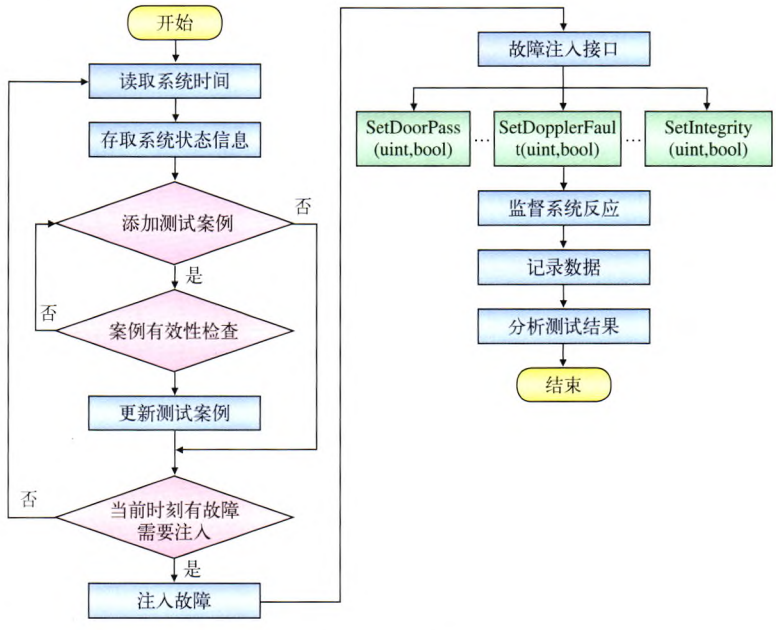

图4　软件故障注入控制器实现流程图

3 结束语

本文采用故障注入方法实现了ATP系统的测试验证，对列车自动防护系统故障模型的构建、案例的生成进行了描述，并以与ATP系统存在交互的外围设备故障为例，说明了论文方法的有效性。但还有改进的空间，如果能对故障集中的测试案例进行某种逻辑排列，促成测试序列地自动运行，将极大提高ATP系统测试的效率，这也是今后需要完善的工作。

本文还分析了故障注入控制器的总体结构和各部分的详细功能结构，以及故障注入控制器的设计过程，通过采集系统状态并根据故障触发条件，控制测试用例的执行，记录并分析测试结果。控制器的设计实现是现阶段正在完成的工作，后期将应用到ATP系统测试中。

参考文献：

[1] 上官伟，苟晨曦，蔡伯根，王　剑，王海龙．基于故障注入的CTCS-3型列控系统可靠性评估技术研究[J]．铁道通信信号，2010，46（7）．

[2] 李　亮，陈宁宁．CBTC软件仿真辅助开发系统的研究与实现[J]．铁道通信信号，2010，46（Z1）．

[3] 谭　玲，曲　峰，董　剑，杨孝宗．基于软件故障注入的容错性能评测技术[J]．计算机工程与科学，2005（2）．

[4] 王胜文．基于软件的故障注入方法研究[D]．哈尔滨：哈尔滨工业大学，2005.

[5] 孙　鑫，余安萍．VC++深入详解[M]．北京：电子工业出版社，2006.

责任编辑　方　圆