устранения неисправностей. Благодаря ей электромеханик, зайдя на сайт нашего предприятия, в любое время суток получит помощь в решении проблем эксплуатации. Такой подход дополнительно улучшает параметры RAMS/LCC. План внедрения IRIS в НПЦ «Промэлектроника» находится в завершающей стадии и предусматривает сертификацию в январе 2014 г.

УДК 621.3.019.3

ВЕРОЯТНОСТЬ ПОСЛЕДОВАТЕЛЬНОГО НАКОПЛЕНИЯ ОТКАЗОВ ПРИ РЕГУЛЯРНОМ ТЕСТИРОВАНИИ СИСТЕМЫ

Д. Н. ШЕВЧЕНКО

Белорусский государственный университет транспорта, г. Гомель

Концепция безопасности современных систем железнодорожной автоматики и телемеханики (СЖАТ) предусматривает то, что все одиночные отказы элементов не должны переводить систему в опасное состояние и должны обнаруживаться на рабочих или тестовых воздействиях не позднее, чем в системе возникнет следующий отказ.

Поскольку предотвратить появление кратных отказов в системах невозможно, их анализу (в том числе, с учетом периодического тестирования систем) посвящено множество публикаций последних лет. При этом считается, что любой кратный отказ – опасный. Подобное допущение существенно упрощает модель надежности, но значительно занижает значения показателей безопасности функционирования по сравнению с (неизвестными) истинными значениями. В особенности такое допущение неадекватно для систем, в которых наступление двух отказов, произошедших в одной последовательности, переводит систему в защитное состояние, а в иной последовательности – в состояние опасное.

Для некоторых классов систем управления концепция безопасности может быть менее жесткой, чем для СЖАТ, и допускать кратные отказы. В связи с этим представляет большой научный и практический интерес определение вероятности безопасного функционирования систем, подверженных накапливающимся в определенной последовательности отказам с учетом тестирования, которое в компьютерных системах выполняется (обычно) через равные интервалы времени.

Таким образом, рассматривается абстрактная техническая система, подверженная двум отказам: A и B. В случае, когда данные отказы происходят в последовательности (A, B), система переходит в опасное состояние; в противном случае (B, A) – в защитное состояние. Наряду с отказами в системе предусмотрено тестирование. Интервал времени между тестированиями – есть константа T, которая много меньше средней наработки системы между отказами. Предполагается, что в процессе тестирования все отказы обнаруживаются наверняка. После обнаружения отказов система полностью восстанавливается.

В указанных условиях время τ до обнаружения первого отказа (из двух) практически подчиняется равномерному распределению на интервале $(0, T)$. А время наработки до опасного отказа представляет собой несобственную случайную величину η, которая равна времени до наступления отказа B, если перед ним уже произошел отказ A и он не успел обнаружиться в процессе тестирования.

В данной работе определяется функция распределения времени η до накопления двух отказов в последовательности (A, B, т. е. до опасного отказа) с учетом периодического тестирования системы, а также вероятность безопасного функционирования системы в течение заданной наработки и средняя наработка до опасного отказа. В качестве исходных данных используются функции распределения времени до наступления каждого из двух рассматриваемых отказов.

Предлагаемая модель применима для количественного анализа безопасности функционирования широкого класса технических систем (в том числе, современных СЖАТ) на основе деревьев отказов с использованием причинно-следственных связей «приоритетное И», которые учитывают последовательность отказов и других воздействий на объект. В случае, когда реальная система подвержена нескольким кратным опасным отказам, необходимо отдельно рассматривать каждый из них с последующим применением теоремы сложения вероятностей.