УДК 621.39.019.3

ПРИМЕНЕНИЕ FMECA - ТЕХНОЛОГИИ ПРИ АНАЛИЗЕ НАДЕЖНОСТИ И БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ ДЛЯ КРИТИЧЕСКИХ ПРИЛОЖЕНИЙ

А.В. Горбенко, д.т.н., проф. В.С. Харченко

Рассматриваются особенности применения метода анализа видов и последствий критических отказов (FMECA) для оценки надежности и безопасности компьютерных сетей. В результате применения FMECA-технологии получена классификация видов, источников, последствий отказов и средств обеспечения отказоустойчивости компьютерных сетей.

Введение. Для обеспечения надежности и безопасности компьютерных сетей комплексов критического применения (КСККП) (энергетических комплексов, диспетчерских систем наземного и воздушного транспорта, банковских систем и систем электронной коммерции и т.д.), выполняющих информационные и управляющие функции, необходимо обнаруживать сбои в сетях и восстанавливать их работоспособность, распределять пропускную способность и уменьшать поток данных при перегрузках, распознавать и парировать задержки и потери пакетов, идентифицировать ошибки в данных и информировать о них прикладное программное обеспечение. Кроме того, они должны обладать средствами для обеспечения отказо- и катастрофоустойчивости.

Применение методов анализа вида и последствий отказов (FMEA) и анализа вида и последствий критических отказов (FMECA) [1, 2] для оценки надежности КСККП позволяет идентифицировать отказы и их последствия, определять необходимость введения резервирования элементов системы и других мер, повышающих вероятность безаварийной работы.

Использование FMECA-технологии может быть важным звеном программы обеспечения безопасности и защиты от критических отказов КСККП. *Целью статьи* является исследование особенностей применения FMECA-технологии для анализа надежности КСККП.

Особенности применения FMECA - технологии для компьютерных систем. Компьютерные сети являются сложными многоуровневыми многоэлементными аппаратно-программными комплексами. Для построения КС используется семиуровневая модель OSI, на каждом уровне которой может быть выполнен анализ надежности с помощью FMECA - технологии. Основными функциональными элементами компьютерных

систем, которые могут быть проанализированы с помощью FMECA - технологии, являются структурированные кабельные системы (СКС), активные (сетевые узлы, коммутаторы и маршрутизаторы) и пассивные (концентраторы) телекоммуникационные устройства, подверженные отказам, обусловленным дефектами аппаратного и программного обеспечения, влиянием внешних факторов (сейсмические воздействия, электромагнитное излучение и др.) и старением электронных компонент.

Особенностью активных телекоммуникационных устройств является то, что в состав входят не только аппаратные, но и программные компоненты, для оценки надежности и безопасности которых может быть использован метод анализа вида и последствий критических отказов программного обеспечения (Software FMECA – SFMECA). Примеры использования FMEA- и FMECA-технологий для программного (ПО) и аппаратного (АО) обеспечения компьютерных систем приведены в [2, 3, 4].

Существующие в настоящее время коммерческие стандарты, фирменные методы и средства, которые решают определённые задачи по обеспечению отказоустойчивости компьютерных сетей, могут быть использованы, реализуя подход COTS [5] для критических приложений.

Среди этих средств можно выделить [6]:

– систему PatchView, обеспечивающую контроль за состоянием коммутационных узлов и схемы физических соединений СКС;

– технологию горячего резервирования сетевых адаптеров – Adapter Fault Tolerance (AFT);

– технологию Adaptive Load Balancing (ALB), распределяющую информационный поток между четырьмя адаптерами сервера и портами коммутатора, а также поддерживающую технологию AFT;

– технологию Fast Ether Channel (FEC), поддерживающую перестраиваемую полосу пропускания и функцию AFT;

– алгоритм динамической реконфигурации Spanning Tree для коммутируемых КС;

– алгоритмы динамической маршрутизации OSPF и CiscoEIGRP для маршрутизируемых сетей.

Использования FMECA-технологии для анализа надежности КС. В формате FMECA-технологии предложена классификация видов, источников, последствий отказов и средств обеспечения отказоустойчивости функциональных элементов компьютерных сетей – СКС, активных и пассивных телекоммуникационных устройств (табл. 1, 2, 3 соответственно). В этих таблицах указаны не только традиционные элементы формата, но и дана оценочная информация – указаны качественные уровни вероятности и критичности отказов. Степень вероятности отказов определяется условиями эксплуатации КС, а уровень критичности отказов – назначением и функ-

циями элемента, тяжестью последствий отказа, и его влиянием на систему в целом.

Классификация видов, источников, последствий отказов и средств

Компонент КС	Вид отказа	Причина отказа	Последствие отказа
Главный кросс	Повреждение коннектора патч-панели	Влияние внешних воздействующих факторов (ВВФ); старение матер.	Нарушение связности КС
	Разрушение патч-панели	«»	«»
	Разрушение кросса	«»	«»
Горизонтальный кросс	Повреждение коннектора патч-панели	«»	«»
	Разрушение патч-панели	«»	«»
	Разрушение кросса	«»	«»
Внешний магистральный кабель	Повреждение (обрыв) кабеля	«»	«»
	Искажение передаваемых сигналов	Влияние электромагнитных помех (ЭМП)	Кратковременное нарушение связности КС; потеря информации; ретрансляция искаженных пакетов
Внутренний и магистральный кабель	Повреждение (обрыв) кабеля	Влияние ВВФ; старение матер.	Нарушение связности КС
	Искажение передаваемых сигналов	Влияние ЭМП	Кратковременное нарушение связности КС; потеря информации; ретрансляция искаженных пакетов
Горизонтальный кабель	Повреждение (обрыв) кабеля	Влияние ВВФ; старение материала	Нарушение связности КС
	Искажение передаваемых сигналов	Влияние ЭМП	Кратковременное нарушение связности КС; потеря информации; ретрансляция искаженных пакетов
Телекоммуникации, розетка\коннектор	Повреждение модульного гнезда коннектора	Влияние ВВФ; старение матер.	Нарушение связности КС
	Разрушение телекоммуникационной розетки	«»	«»
Соединит. корды	Повреждение (обрыв) соединительного корда	«»	Кратковременное нарушение связности КС

Таблица 1

обеспечения отказоустойчивости СКС

Средства восстанов. отказа	**Средства обеспечения отказоустойчивости**	**Вероятность отказа**	**Уровень критичности**
Замена	Резервирование коннекторов патч-панели	Высокая	Низкий
«»	Резервирование патч-панелей; замена	Низкая	Средний
Ремонт и восстановление	Резервирование кросса	Очень низкая	Высокий
Замена	Резервирование коннекторов патч-панели	Высокая	Низкий
«»	Резервирование патч-панелей; замена	Низкая	Средний
Ремонт и восстановление	Резервирование кросса	Очень низкая	Высокий
Замена	Резервирование кабеля; резервирование маршрута прокладки кабеля; резервирование физической среды передачи	Низкая	Высокий
-	Резервирование физической среды передачи; экранирование; прокладка кабеля в стороне от источников ЭМП и силового кабеля электросети	Низкая	Средний
Замена	Резервирование кабеля; резервирование маршрута прокладки кабеля; резервирование физической среды передачи	Низкая	Высокий
-	Резервирование физической среды передачи; экранирование; прокладка кабеля в стороне от источников ЭМП и силового кабеля электросети	Низкая	Средний
Замена	Резервирование кабеля; резервирование маршрута прокладки кабеля; резервирование физической среды передачи	Низкая	Высокий
-	Резервирование физической среды передачи; экранирование; прокладка кабеля в стороне от источников ЭМП и силового кабеля электросети	Низкая	Средний
Замена	Резервирование модульного гнезда коннектора	Высокая	Низкий
Замена	-	Низкая	Средний
Замена	-	Высокая	Очень низкий

Классификация видов, источников, последствий отказов и средств обес-

Элемент КС	Компонент КС	Вид отказа	Причина отказа	Последствие отказа
1	2	3	4	5
Рабочая станция	Сетевой интерфейс	Отключение напряжение питания		Нарушение связности КС
		Повреждение порта связи	Влияние ВВФ; старение материала	«»
		Неисправность АО	«»	«»
		Сбой АО	Влияние ЭМП	Кратковременное нарушение связности КС
	Драйвер сетевого интерфейса	Отказ ПО	Проявление ошибки ПО	«»
	Стек сетевых проток. ОС	«»	«»	«»
	Прикладное сетевое ПО	«»	«»	«»
Сервер	Сетевой интерфейс	Отключение напряжение питания		Нарушение связности КС
		Повреждение порта связи	Влияние ВВФ; старение материала	«»
		Неисправность АО	«»	«»
		Сбой АО	Влияние ЭМП	Кратковременное нарушение связности КС
	Драйвер сетевого интерфейса	Дефект ПО	Проявление ошибки ПО	«»
	Стек сетевых проток. ОС	Дефект ПО	«»	«»

	Прикладное сетевое ПО	Дефект ПО	«»	«»

Таблица 2

печения отказоустойчивости активных телекоммуникационных устройств

Средства восстановления отказа	**Средства обеспечения отказоустойчивости**	**Вероятность отказа**	**Уровень критичности**
6	7	8	9
-	Применение ИБП	Высокая	Средний
Замена	Резервирование порта связи; резервирование сетевого интерфейса	Высокая	Средний
«»	Резервирование сетевого интерфейса	Очень низкая	Средний
-	Установка рабочей станции в стороне от источников ЭМП и силового кабеля электросети	Низкая	Низкий
Использование сертифицированного ПО	Использование дефектоустойчивого ПО	Очень низкая	Средний
«»	«»	Низкая	Средний
«»	«»	Средняя	Средний
-	Применение ИБП	Высокая	Высокий
Замена	Резервирование порта связи; резервирование сетевого интерфейса	Высокая	Высокий
«»	Резервирование сетевого интерфейса	Низкая	Высокий
-	Установка сервера в стороне от источников ЭМП и силового кабеля электросети	Низкая	Средний
Использование сертифицированного ПО	Использование дефектоустойчивого ПО	Низкая	Высокий
«»	«»	Низкая	Высокий

«»	«»	Средняя	Высокий

1	2	3	4	5
Коммутатор	-	Отключение напряжения питания		Нарушение связности КС
		Повреждение порта связи	Влияние ВВФ; старение материала	«»
		Сбой АО	Влияние ЭМП	Кратковременное нарушение связности КС
		Перегрузка	Увеличение сетевой нагрузки	«»
		Неисправность АО	Влияние ВВФ; старение материала	Нарушение связности КС
		Дефект ПО	Проявление ошибки ПО	Кратковременное нарушение связности КС
Маршрутизатор	-	Отключение напряжения питания		Нарушение связности КС
		Повреждение порта связи	Влияние ВВФ; старение материала	«»
		Сбой АО	Влияние ЭМП	Кратковременное нарушение связности КС
		Перегрузка	Увеличение сетевой нагрузки	«»
		Неисправность АО	Влияние ВВФ; старение материала	Нарушение связности КС

		Дефект ПО	Проявление ошибки ПО	Кратковременное нарушение связности КС

Продолжение таблицы 2

6	7	8	9
-	Применение ИБП	Средняя	Высокий
Замена коммутатора; замена модульных портов связи	Резервирование портов связи, резервирование связей	Средняя	Высокий
-	Установка коммутатора в стороне от источников ЭМП и силового кабеля электросети	Низкая	Средний
Снижение сетевой нагрузки	Применение алгоритмов управления перегрузками	Высокая	Средний
Замена	Резервирование коммутатора	Низкая	Высокий
Использование сертифицированных коммутаторов	Использование дефектоустойчивого ПО	Низкая	Высокий
-	Применение ИБП	Средняя	Высокий
Замена маршрутизатора; замена модульных портов связи	Резервирование портов связи; резервирование связей	Средняя	Высокий
-	Установка маршрутизатора в стороне от источников ЭМП и силового кабеля эл/с	Низкая	Средний
Снижение сетевой нагрузки	Применение алгоритмов управления перегрузками	Высокая	Средний
Замена маршрутизатора	Резервирование маршрутизатора	Низкая	Высокий

Использование сертифицированных маршрутизаторов	Использование дефектоустойчивого ПО	Низкая	Высокий

Классификация видов, источников, последствий отказов и средств обеспечения

Элемент КС	**Комп. КС**	**Вид отказа**	**Причина отказа**	**Последствие отказа**
Концентратор	-	Отключение напряжения питания		Нарушение связности КС
		Повреждение порта связи	Влияние ВВФ; старение материала	«»
		Сбой АО	Влияние ЭМП	Кратковременное нарушение связности КС
		Неисправность АО	Влияние ВВФ; старение материала	Нарушение связности КС

Заключение. В результате применения FMECA-технологии для анализа надежности компьютерных сетей определены виды, причины и последствия отказов различных элементов КС, проведена классификация отказов по степени критичности и вероятности возникновения, определен состав необходимых средств и мер, направленных на восстановление отказов и обеспечение отказоустойчивости КС. На основе предложенной классификации может быть выполнен анализ надежности конкретных реализаций КСККП, и проведена оценка критичности отказов с помощью построения матрицы критичности (с координатами «вероятность-тяжесть отказов»), что позволит определить состав наиболее критичных отказов и первоочередных мер, необходимых для их предупреждения.

Дальнейшие исследования могут направляться по пути детализации предложенной классификации по уровням модели OSI, а также разграничения программных и аппаратных компонентов КС для их раздельного анализа с помощью FMECA-технологии. Для сетей, допускающих деградацию структурных и функциональных характеристик, этот анализ может быть детализирован с использованием Д-матриц [7]. Разрабатывае-

мые модели и методики – это основа для создания моделирующих и оценочных утилит, необходимых для выбора вариантов реализации сети, информационной и аналитической поддержки экспертизы КСККП.

Таблица 3

отказоустойчивости пассивных телекоммуникационных устройств

Средства восстановления отказа	**Средства обеспечения отказоустойчивости**	**Вероятность отказа**	**Уровень критичности**
-	Применение ИБП	Средняя	Высокий
Замена концентратора	Резервирование портов связи; использование резервных портов связи	Средняя	Высокий
-	Установка концентраторов в стороне от источников ЭМП и силового кабеля эл/с	Средняя	Средний
Замена концентратора	Резервирование концентраторов	Низкая	Высокий

ЛИТЕРАТУРА

1. IEC 812 Std. Analysis Techniques for System Reliability – Procedure for Failure Modes and Effects Analysis (FMEA)- Geneve, 1985. – 41 p.

2. ANSI/IEEE Std 352. IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems, 1987.

3. Newi H., Kiefer J., Wolberg J., Mihm H.. Availability and Train Delays – The CADM Approach // Safety and Reliability.- Rotterdam: Balkema, 1999. – P. 159 - 163.

4. Bowles J. B., Chi Wan. Software Failure Modes and Effects Analysis for a Small Embedded Control System //Proceedings Annual Reliability and Maintainability Symposium, 2001, 6 p.

5. Scott J.A., Preckshot G.G.,Gallagher J.M. Using Commercial-Off-The-Shelf(COTS) Software in High-Consequence Safety Systems //Lawrence Livermore National Laboratory, UCRL -122246, 1995.

6.Кульгин М. Технологии корпоративных сетей. Энциклопедия. – СПб.: Питер, 1999. – 704 с.

7. Kharchenko V.S., Cherepakhin D.A. Risk Analysis of Control Systems by Use of QD-diagrams and FMECA-approach // Proceedings of 12th European Conference on Safety and Reliability, Turin, Italy, September, 16-20, 2001.

Поступила в редколлегию 15.10.2001