УДК 681.5.09

М.А. Алексеев, Е.И. Сироткина

# ДИАГНОСТИКА И ОТКАЗОУСТОЙЧИВОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРОМЫШЛЕННЫХ SCADA СИСТЕМ ОТВЕТСТВЕННОГО НАЗНАЧЕНИЯ

*Аннотация. Рассматривается математическая модель работы подсистемы самодиагностики и автовосстановления сервера БД в составе сервера промышленной SCADA системы на примере графа состояний ПДВС. Диагностика работы сервера SCADA системы проводится с учетом текущей производительности сервера БД на основе мониторинга его характеристик для ресурсоемких запросов. Предлагается методика автоматического резервирования и автовосстановления сервера SCADA системы после необратимого отказа.*

*Ключевые слова: диагностика, отказоустойчивость, SCADA система, резервирование, автоматическое восстановление, граф состояний.*

**Постановка проблемы.** Надежность работы SCADA системы ответственного назначения как аппаратно-программного комплекса – это свойство сохранения способности выполнять требуемые функции круглосуточно в режиме реального времени на протяжение всего периода эксплуатации.

Оценка надежности работы SCADA системы является интегральной величиной и зависит от многих факторов:

- оптимального выбора оборудования системообразующих узлов SCADA системы, сетевых коммуникаций, приемо-передающей аппаратуры, первичных преобразователей и т.д.;

- оптимального выбора программного обеспечения (ПО) SCADA системы, которое включает в себя базовое ПО для каждой из подсистем SCADA системы, в зависимости от выполняемых ими основных задач. К базовому ПО относятся операционная система, среда проектирования и разработки ПО, включая стандартные библиотеки функций, классов и компонентов данной среды разработки, сетевые службы, серверы баз данных (БД) и т.д.;



 ISSN 1562-9945

- технологии и методов организации работы коллектива системных интеграторов на протяжение всего жизненного цикла ПО и всей системы в целом.

Особого внимания при оценке надежности работы системы требует автоматическая диагностика работы исполняемых модулей ПО в режиме реального времени в процессе эксплуатации SCADA системы.

**Анализ публикаций по теме исследований**

Были рассмотрены методы повышения надежности и отказоустойчивости ПО промышленных SCADA систем на примере выполнения в автоматическом режиме диагностики, резервирования и восстановления БД в составе промышленной SCADA системы ответственного назначения, где одним из важных элементов системного ПО сервера промышленной SCADA системы является система управления базой данных (СУБД).

СУБД в составе сервера промышленной SCADA системы характеризуется интенсивным потоком данных и большими объемами обрабатываемых выборок данных. Системные отказы промышленного сервера могут приводить к значительным для всей SCADA системы последствиям, вплоть до разрушения БД и необратимого отказа [1] всей системы. Таким образом, надежность и отказоустойчивость таких СУБД напрямую зависит от организации сервисов диагностики, резервирования и восстановления баз данных. Обычно функции диагностики, резервирования и восстановления БД выполняются системным администратором БД в интерактивном режиме. При этом, как правило, работа некоторых подсистем промышленной SCADA системы, взаимодействующих с БД, приостанавливается, что в свою очередь ведет к потере актуальных данных и отсутствию полнофункционального диспетчерского мониторинга и управления. Для промышленных SCADA систем ответственного назначения такие служебные остановы сервера могут быть критичны.

**Формулировка цели статьи**

Целью работы является разработка методики автоматической диагностики, авторезервирования и автовосстановления сервера SCADA системы после необратимого отказа, приведшего к разрушению БД.

Параллельно с основной работой СУБД проводится автоматическая диагностика ее работы и автоматическое резервирование БД.

Одним из ранних методов обнаружения отклонений в работе СУБД является диагностика СУБД на основе мониторинга производительности сервера БД.

Приведем пример. Как известно [2, 3, 4], сервер БД параллельно с ведением самой БД формирует журнал транзакций. При интенсивном потоке данных, автоматически добавляемых в БД, что характерно для промышленных SCADA систем, быстро увеличивается размер журнала транзакций. При этом возникает обратно-пропорциональная зависимость между размером журнала транзакций и скоростью выполнения этих транзакций сервером БД, что в свою очередь тормозит запись потока данных в режиме реального времени и может приводить к значительному снижению производительности сервера SCADA системы.

**Основная часть**

Рассмотрим математическую модель работы подсистемы самодиагностики и автовосстановления сервера БД (ПДВС) в составе сервера промышленной SCADA системы на примере графа состояний ПДВС.

Определим состояния полного (full backup) и инкрементного (incremental backup) резервирования БД. Известно [2], что при инкрементном резервировании, в отличие от полного резервного копирования, последовательно создаются копии журналов транзакций, в которых прописаны изменения в БД с момента создания последней полной копии БД.

При отказе сервера БД, восстановление происходит путем выполнения команд, запротоколированных в резервируемых файлах журналов транзакций, причем необходимо последовательно, строго по дате и времени обрабатывать все инкрементные резервные копии. При полном резервировании происходит резервирование самого файла БД. Каждый из этих видов резервирования БД имеет свои преимущества и недостатки. Т.к. резервирование БД происходит в фоновом режиме параллельно с транзакциями, то инкрементное резервирование является более ресурсосберегающим процессом, чем полное резервирование. Однако, при необходимости восстановления сервера БД после необратимого отказа, более ресурсосберегающим процессом является восстановление из состояния полного резервирования.

 ISSN 1562-9945

На рисунке 1 приведен граф состояний ПДВС.

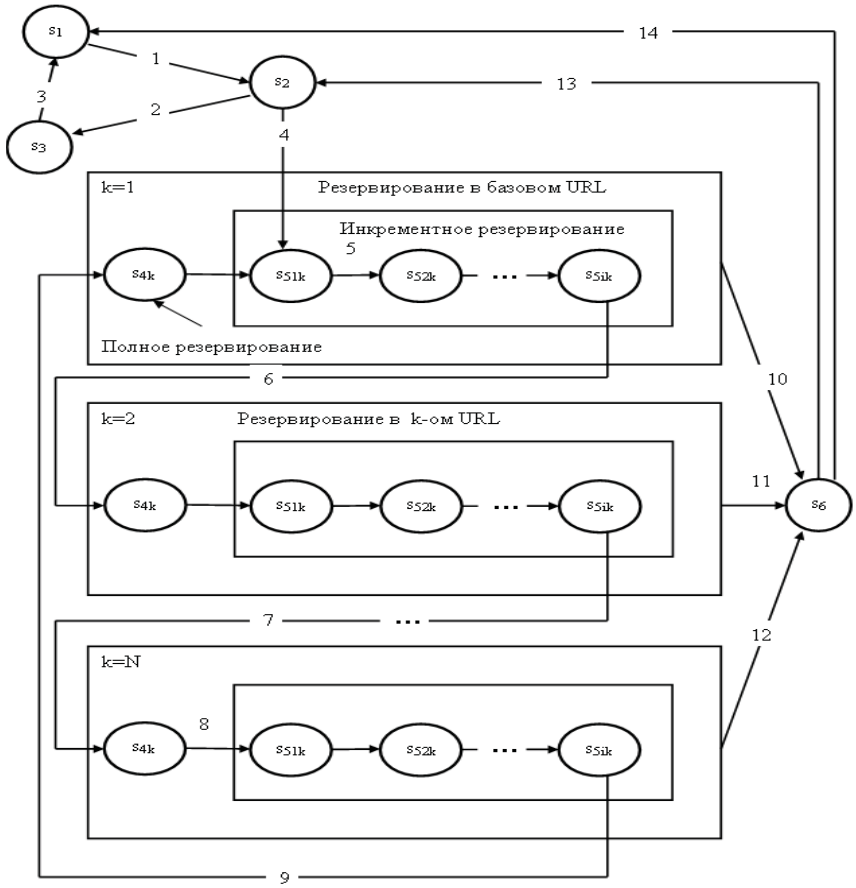


Рисунок 1 - Граф состояний ПДВС

Описание некоторых состояний графа приведено в таблице 1.

Таблица 1

Состояния графа ПДВС

| № п/п | Состояние | Описание |
|---|---|---|
| 1 | s1 | СУБД отсутствует |
| 2 | s2 | работоспособное состояние сервера БД, резервирования нет |
| 3 | s3 | отказ сервера БД, резервирования нет |
| 4 | s4k | работоспособное состояние сервера БД после полного резервирования БД для k-го URL |
| 5 | s5ik | работоспособное состояние сервера БД после i-го инкрементного резервирования для k-го URL |
| 6 | s6 | отказ сервера БД, резервирование есть |

Переходы графа ПДВС характеризуют соответственно создание БД, отказ сервера БД. инкрементное и полное резервирование в базо-

вом и k-ом URL, успешное и неудачное автоматическое восстановление сервера БД после отказа. Резервирование происходит по методу заполнения кольцевого буфера.

К основным параметрам математической модели ПДВС относятся:

- размер БД на момент времени $t$ – $Sd(t)$, байт;

- размер журнала транзакций на момент времени $t$ – $Sl(t)$, байт;

- изменение размера БД за период времени $\Delta t$ – $\Delta Sd(\Delta t)$,байт;

- изменение журнала транзакций за период времени $\Delta t$ – $\Delta Sl(\Delta t)$, байт;

- размер полной резервной копии на момент времени $t$ – $Sbf(t)$, байт;

- размер единичной инкрементной резервной копии на момент времени $t$ – $Sbi(t)$, байт;

- длительность полного резервирования для $k$-ого URL – $Tbf_k$, сек;

- длительность i-го единичного инкрементного резервирования для k-ого URL – $Tbi_{ki}$, сек;

- количество инкрементных резервных копий в $k$-ом URL – $m_k$;

- количество URL для резервирования и восстановления БД – $N$;

- период времени между созданием двух соседних резервных копий в $k$-ом URL – $\tau b_k$, сек;

- период времени на восстановление СУБД после отказа в k-ом URL – $\tau r$, сек;

- период времени на восстановление СУБД после отказа с использованием полного резервирования в k-ом URL – $\tau rf_k$, сек;

- период времени на восстановление СУБД после отказа с использованием инкрементного резервирования в k-ом URL – $\tau ri_k$, сек;

- дата и время обнаружения отказа сервера БД – $Tfl$ (fault location time);

- время реакции сервера на запись блока данных в БД – $trsw$ (server response time on write);

- время реакции сервера на выборку данных из БД – $trsr$ (server response time on read).

 ISSN 1562-9945

Временная диаграмма резервирования и восстановления БД приведена на рисунке 2.

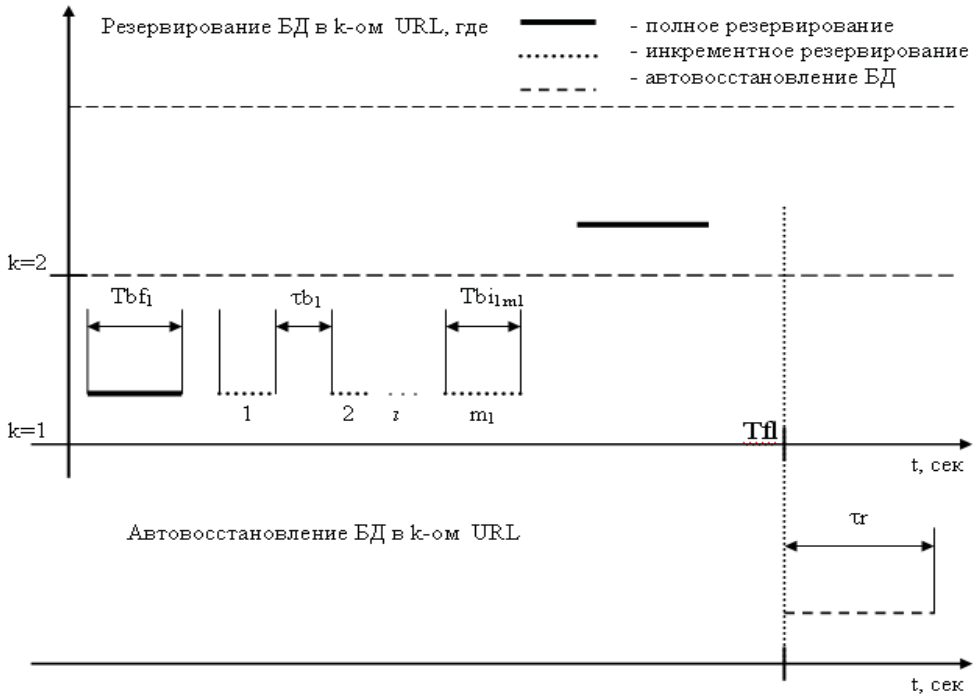


Рисунок 2 - Временная диаграмма резервирования и автовосстановления БД

По интенсивности потока записываемых данных для промышленной SCADA системы ответственного назначения и принятому регламенту сохранения актуальных данных в БД рассчитывается и экспериментально проверяется скорость изменения размера БД

$$vd(t) = \frac{\partial Sd}{\partial t} \qquad (1)$$

и скорость изменения размера журнала транзакций

$$vl(t) = \frac{\partial Sl}{\partial t} \qquad (2)$$

Определяем время реакции сервера БД на запись и выборку наборов данных различной длины $L$, в зависимости от начальных размеров БД и журнала транзакций, а также скорости их изменения.

$$t_{rsw} = f(L, Sd_0, Sl_0, vd, vl) \qquad (3)$$

Определяем максимальные значения $Sd_{max}$, $Sl_{max}$, $vd_{max}$, $vl_{max}$ для выборки длины $L$, не приводящие к значительному отклонению времени реакции сервера БД

$$\Delta t_{rsw} \le \xi \qquad (4)$$

Определяем зависимость времени автоматического восстановления БД после отказа, как

$$\tau_{rf} = \phi_1(Sbf_k) \quad (5)$$

$$\tau_{ri} = \varphi_2(\sum_{i=1}^{m_k} Sbi_{ki}, \tau b_1) \quad (6)$$

Для задаваемых пределов значений $Sd$, $Sl$, $vd$, $vl$, $L$, $t_{rsw}$, $\tau_{rf}$, $t_{ri}$ необходимо найти такие $\tau b_1$, $m_k$, которые позволили бы максимально экономить время и машинные ресурсы сервера SCADA системы как на резервирование, так и на восстановление БД при минимальных потерях данных во время отказа системы и заданном объеме свободного дискового пространства для резервирования и восстановления СУБД в $k$-ом URL.

На сегодняшний день существует много различных инструментальных средств мониторинга производительности SQL серверов. В качестве примера приведем результат использования MS SQL Server Activity Monitor. Данное ПО выводит информацию о ресурсах, находящихся в состоянии ожидания (см. рисунок 3), время отклика и исполнения файловых операций ввода/вывода данных (см. рисунок 4), характеристики по производительности машинных ресурсов при исполнении последних ресурсоемких запросов (см. рисунок 5).

**Resource Waits**

| Wait Category | Wait Time [ms/sec] | Recent Wait Time | Average Waiter Count | Cumulative Wait Time [sec] |
|---|---|---|---|---|
| Buffer I/O | 1267 | 2307 | 1.9 | 35480 |
| Latch | 185 | 144 | 0.4 | 154 |
| Logging | 28 | 35 | 0.0 | 789 |
| Network I/O | 11 | 9 | 0.0 | 3658 |
| Other | 0 | 0 | 0.0 | 6 |
| Memory | 0 | 0 | 0.0 | 0 |
| Lock | 0 | 0 | 0.0 | 297 |
| Buffer Latch | 0 | 0 | 0.0 | 8 |
| Compilation | 0 | 0 | 0.0 | 0 |
| Backup | 0 | 0 | 0.0 | 38451 |

Рисунок 3 - Панель ресурсов ожидания

**Data File I/O**

| Database | File Name | MB/sec Read | MB/sec Writen | Response Time [ms] |
|---|---|---|---|---|
| msdb | C:\ProgramFiles\Microsoft SQL ... | 0.0 | 0.0 | 154 |
| tempdb | C:\ProgramFiles\Microsoft SQL ... | 73.9 | 0.0 | 122 |
| energydb | C:\ProgramFiles\Microsoft SQL ... | 0.0 | 18.4 | 106 |

Рисунок 4 - Панель файловых операций ввода/вывода данных

**Recent Expensive Queries**

| Query | Executions/min | CPU (ms/sec) | Physical Reads/sec | Logical Writes/sec | Logical Reads/sec | Average Duration (ms) |
|---|---|---|---|---|---|---|
| SELECT ... | 12 044 | 15 | 0 | 3 | 1260 | 1 |
| SELECT ... | 5680 | 13 | 0 | 0 | 479 | 0 |
| SELECT ... | 1496 | 5 | 0 | 0 | 255 | 0 |

Рисунок 5 - Панель последнего ресурсоемкого запроса

 ISSN 1562-9945

**Выводы и перспективы дальнейших исследований**

Использование аналитических, численных и экспериментальных методов моделирования работы промышленного сервера SCADA системы, диагностика его работоспособности и производительности во время и после резервирования БД показали, что автоматическое восстановление БД после необратимого отказа, приводящего к разрушению БД, возможно не менее чем в 80% случаев таких отказов. При этом, применение автовосстановления после отказа в сотни раз сокращает время восстановления работоспособности системы без влияния человеческого фактора. В качестве перспективных исследований может быть рекомендована разработка методики полного автоматического восстановления работоспособности системообразующего узла SCADA системы ответственного назначения.

## ЛИТЕРАТУРА

1. Военный энциклопедический словарь ракетных войск стратегического назначения / [Военная академия РВСН имени Петра Великого]. — М.: Научн. изд-во «Большая Российская энциклопедия», 1999. — 634 с., ISBN 5-85270-315-X
2. Sybase SQL Anywhere. A System 11 Server Product. User's Guide. Sybase Inc., 1995. — 1165p., ISBN 1-55094-110-0
3. Брайан Хичкок. Sybase. Настольная книга администратора./ Хичкок Б. — М. : Издательство «Лори», 2000. — 420с.
4. К. Дейт. Введение в системы баз данных, 6-е издание:Пер.с. англ./Дейт К.К.,М.,СПб.:Издательский дом «Вильямс»,2000. -848с.
5. Канер Сэм. Тестирование программного обеспечения. Пер. с англ./ Канер С., Фолк Д., Нгуен Е. — К.: Издательство «ДиаСофт», 2000. — 544с.
6. SCADA – системы: взгляд изнутри / Андреев Е.Б., Куцевич Н.А., Синенко О.В. — М.: Издательство «РТСофт», 2004. — 176с.
7. Ricky W. Butler. A Primer on Architectural Level Fault Tolerance. / Butler R. — National Aeronautics and Space Administration. — Langley Research Center, Hampton, Virginia. — 23681-2199. — 2008. — 53p.
8. Гнеденко Б.В. Математические методы в теории надежности. (Серия: «Физико-математическая библиотека инженера»). / Гнеденко Б. В., Беляев Ю. К., Соловьев А. Д. — М.: Наука, Главная редакция физико-математической литературы, 1965. — 524 с.