Подобные решения, как правило, проектируются отдельно для каждого случая, тиражироваться могут только какие-то самые общие подходы. Дело в том, что, если предполагается использовать именно КПК, то есть именно носимое устройство, без подключения каких-либо проводных линий (да и куда их подключить? как правило, у КПК предусмотрен всего один разъем, и тот – mini-USB; номенклатура устройств, рассчитанных на подключение к такому разъему, крайне ограничена), то практически единственной возможностью обеспечить связь с другими устройствами является использование беспроводных коммуникаций. А устойчивость связи (по беспроводным каналам), в свою очередь, существенно зависит: на открытой площадке – от рельефа местности и профиля и высоты зданий/сооружений, а в закрытом пространстве (например, заводском цеху) – от конфигурации помещения и наличия и геометрии расположенного там оборудования. В общем случае построение надежно работающей беспроводной сети передачи данных – это очень сложный вопрос (невзирая на множество распространенных заблуждений по этому поводу); и платой за недостаточную аккуратность при его решении будет потеря информации (например, при передаче данных от датчика к компьютеру) со всеми вытекающими из этого последствиями.

Одна из возможных схем построения приложения может быть, например, такой: датчик подключается к АЦП, на выходе RS-232/485 которого устанавливается преобразователь типа Serial-to-Wi-Fi (Lantronix, MOXA и др.). Последний поддерживает связь с точкой доступа, которая, в свою очередь, ретранслирует данные на КПК. При этом радиус зоны покрытия для "обычных" (широко распространенных) точек доступа, если нет препятствий искусственного характера, около 100...110 метров; в пределах именно этой зоны и может перемещаться КПК.

Другая возможная схема – это использовать наряду или помимо встраиваемых (стационарных и мобильных) компьютеров обычный (промышленный или даже офисный) стационарный компьютер, на который возложены задачи сопряжения с внешними устройствами. Этот компьютер подключается к точке доступа, через которую он транслирует данные на мобильные КПК (по Wi-Fi), которые в этом случае играют роль терминалов доступа к данным. Важно, что в целях совместимости по данным и протоколам на стационарном компьютере должна работать Elipse SCADA, а на мобильных – Elipse SCADA CE.

Наконец, если на этом (обычном) компьютере работает SCADA со средствами Web-публикации, то КПК можно использовать просто как "носитель для Internet-браузера". Функционально (с точки зрения АСУТП) такое решение максимально ограничено, поскольку, как правило, позволяет только просматривать выложенные в Internet данные, но зато за счет перехода от среды Wi-Fi в среду GPRS/EDGE оно позволяет снять ограничения на удаленность мобильного компьютера от стационарного.

Официальным эксклюзивным дистрибутором компании Elipse Software в России является ЗАО "НПП "Родник", на сайте которого (www.rodnik.ru) доступны для скачивания демонстрационные версии упомянутых программных продуктов для различных платформ КПК.

Пинаев Александр Львович *– зам. генерального директора по промышленной автоматизации, начальник отдела специальных проектов в промышленной автоматизации ЗАО "НПП "Родник". Контактные телефоны: (499) 613-26-88, 613-70-01. E-mail: maestro@rodnik.ru Http://www.rodnik.ru*

Защищенная от сбоев файловая система

П. Леру (QNX Software Systems)

Представлен новый подход к обеспечению целостности файловой системы во встраиваемых системах критического назначения.

Ключевые слова: файловая система, сбой, восстановление данных, проверка целостности.

Способность хранить большие объемы данных и управлять ими стала критическим требованием для большого числа встраиваемых устройств. Автомобильные информационно-развлекательные системы, системы промышленной автоматизации, медицинские устройства, медиасерверы, портативные музыкальные плееры – во всех этих устройствах используются жесткие диски и другие технологии для хранения больших объемов данных, причем такими способами, которые всего несколько лет тому назад казались еще невозможными.

Во многих случаях требуется, чтобы эти системы были способны непрерывно работать в течение нескольких лет, в том числе с интенсивным выполнением операций чтения и записи. В таких системах не допускаются потери данных или длительные простои из-за необходимости восстановления данных.

Нужно также учитывать, что многие встраиваемые системы эксплуатируются в жестких условиях, например, в автомобилях могут случаться скачки или потери электропитания. Это может вызывать порчу данных, которые хранятся на жестких дисках или других носителях, и приводить к потере критически важной информации. Поэтому файловая система, управляющая данными на устройстве хранения, должна не только обеспечивать высокую производительность чтения и записи, но и предотвращать порчу данных из-за сбоев электропитания. Кроме того, система не должна требовать длительных проверок целостности после таких сбоев, поскольку в боль-

шинстве случаев встраиваемые системы должны быть готовы к работе сразу же после перезапуска.

К сожалению, обычные файловые системы блочной архитектуры, применяемые в жестких или твердотельных дисках, никогда не предназначались для обеспечения целостности файлов в случае отказов электропитания или других неожиданных сбоев. Некоторые файловые системы, например ZFS, предназначенные для корпоративных серверов высокой готовности, обеспечивают такую защиту, но они потребляют слишком много системных ресурсов, необходимых для работы встраиваемого устройства. Файловая система QNX с защитой от сбоев электропитания позволяет преодолевать эти проблемы с помощью эффективного встраиваемого решения на основе сложных серверных механизмов. Таким образом, в системе обеспечивается целостность данных, необходимая для современных встраиваемых приложений с большими объемами хранимых данных.

Отказоустойчивое оборудование решает не все

Во многих случаях во встраиваемых системах применяют твердотельную флеш-память типа NAND или NOR. Однако во многих других случаях приходится применять жесткие диски, так как они обеспечивают большие объемы хранения и низкую стоимость хранения на каждый бит. К сожалению, не во всех встраиваемых системах возможно применить те методы хранения данных на жестких дисках, которые используются в мире корпоративных систем, например, репликацию данных в нескольких хранилищах, высокую частоту резервного копирования, применение источников бесперебойного питания (ИБП) и др. Поэтому очень важно, чтобы встраиваемые файловые системы обеспечивали специальные средства для защиты от потери или порчи данных.

Надежность хранения данных не сводится только к применению отказоустойчивого оборудования для хранения. Она в существенной мере зависит от целостности файловой системы. А самой главной проблемой для сохранения целостности файловой системы является предотвращение порчи данных из-за отказов электропитания. Такие сбои могут быть вызваны ударами молний, неисправностью систем электроснабжения, дефектами аккумуляторов, неисправностями электропроводки и целым рядом других причин.

Хотя многие существующие файловые системы можно считать надежными, они все же не защищены от отказов электропитания. Например, могут случиться следующие сценарии:

• сбой электропитания происходит во время записи в блок файловой системы. Когда жесткий диск теряет электропитание, он автоматически перемещает головки в безопасную зону парковки или перемещает их таким образом, чтобы защитить от столкновения с поверхностью диска. Если драйвер файловой системы записывает блок данных во время такого перемещения головки, операция записи будет не завершена. При этом код ECC для данного сектора записи станет ошибочным и приведет к потере всех хранимых в нем данных;

• сбой электропитания происходит во время записи в несколько блоков файловой системы. В процессе записи файла файловая система, как правило, должна произвести запись в несколько блоков на диске. Если сбой электропитания случается после того, как файловая система не успела записать данные во все блоки (а только в несколько из них), данные теряются. Для минимизации этого риска файловые системы могут синхронно записывать обновления в каталоги, индексные дескрипторы, блоки экстентов, битовую карту и другие структуры в строго определенном порядке. Тем не менее, все эти средства не устраняют полностью риск потери данных.

Обычные решения для восстановления данных

Для восстановления испорченных файлов и каталогов обычно применяют специальную утилиту для проверки и восстановления целостности файловой системы (например, chkdsk для Windows или fsck для Unix и Linux). Однако эти утилиты имеют два серьезных недостатка: 1) они проверяют только структуру файловой системы и метаданные; 2) для их выполнения требуется много времени, а также монопольный доступ к файловой системе (как правило, сразу после загрузки системы).

Если испорчен файл корневого каталога, битовой карты или индексного дескриптора, некоторая возможность восстановить файловую систему остается. Однако делается это только вручную с помощью длительных процессов восстановления, требующих больших знаний структуры файловой системы. Если испорченным становится корневой блок или корневой каталог, пользователь не сможет смонтировать файловую систему и все данные могут быть потеряны.

Такие сценарии восстановления файлов не подходят для встраиваемых систем, которые во многих случаях должны непрерывно работать месяцы или годы без вмешательства человека. Поэтому для встраиваемой файловой системы критическое значение имеет, прежде всего, предотвращение таких сбоев. Если же порча данных произошла, то зачастую делать что-либо уже поздно.

Для решения такого рода проблем компания QNX Software Systems предложила новую, защищенную от сбоев электропитания файловую систему. Используя технологии, изначально разработанные для корпоративных информационных систем, и оптимизировав их для встраиваемых систем с ограниченными ресурсами, компания QNX создала инновационную файловую систему на основе технологии копирования при записи (copy-on-write), которая позволяет обеспечить целостность данных. При таком подходе файловая система никогда не перезаписывает оперативные данные. Вместо этого она создает новый образ файловой системы в свободных блоках диска. Новый образ становится оперативным только после того, как все необходимые обновления надежно записаны на диск.

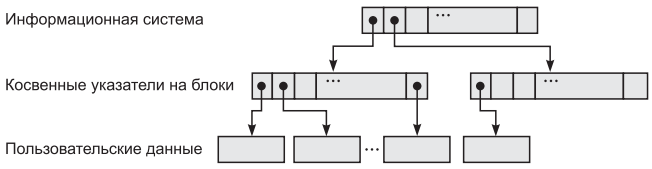

Рис. 1. Файловая система до изменения данных

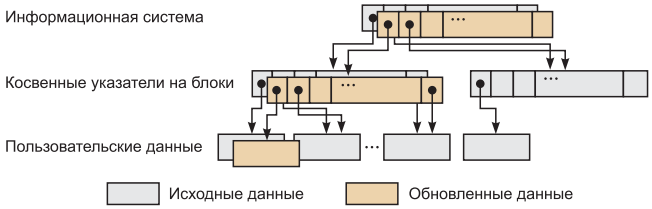

Рис. 2. Файловая система после изменения данных

Новейшая файловая система QNX работает на основе технологии копирования при записи, которая позволяет защитить все данные, в том числе метаданные и пользовательские данные. Как только происходит какое-либо изменение данных, отказоустойчивая файловая система QNX выполняет следующие действия:

• записывает новые пользовательские данные в один или несколько свободных блоков, оставляя первоначальные данные неизменными;

• копирует существующий список непрямых указателей на блоки, затем изменяет эту копию, чтобы добавить ссылки на ранее заполненные блоки;

• копирует индексный дескриптор, хранящий основную информацию о файлах и каталогах, и затем обновляет копию, чтобы добавить ссылки на новые непрямые указатели на блоки.

После завершения операции первоначальные данные и указатели на эти данные остаются прежними, однако теперь появляется новый индексный дескриптор, состав блоков и непрямых указателей, относящихся к модифицированным данным. На рис. 1 показана файловая система до операции записи, а на рис. 2 – файловая система после завершения операции (обновленные данные обозначены коричневым.

Для обеспечения высокой производительности файловая система может группировать несколько операций до их совершения, что избавляет от необходимости выполнять вышеописанную процедуру при каждом изменении какого-либо файла. В этом случае файловая система производит запись одновременно множества изменений на диск после запуска соответствующей операции (commit to disk). При этом разработчик может настроить частоту выполнения этой операции.

Сверхбыстрое восстановление

В отказоустойчивой файловой системе QNX используется концепция "суперблока" – глобального корневого блока, содержащего индексные дескрипторы для системной битовой карты и файлов индексных дескрипторов. Более того, в системе используется два суперблока: один отражает первоначальную версию всех блоков, другой – модифицированные данные. В случае сбоя электропитания система сможет восстановить последнее стабильное состояние файловой системы посредством простого считывания суперблоков с диска, проверки подписей и кодов CRC и определения суперблока с наибольшим порядковым номером.

Этот подход избавляет от необходимости длительных проверок целостности, которые обычные файловые системы должны выполнять после отказов электропитания или других неожиданных сбоев. Таким образом достигается огромная экономия времени, особенно в системах с множеством мегабайт или гигабайт данных, в том числе мультимедийного контента и метаданных (например, в автомобильных информационно-развлекательных системах). Благодаря отказоустойчивой файловой системе время, необходимое для монтирования файловой системы при загрузке, постоянно остается предсказуемо небольшим.

В итоге новая отказоустойчивая файловая система QNX предоставляет встраиваемым системам следующие преимущества:

• использование больших хранилищ и жестких дисков с низкой стоимостью хранения данных из расчета на 1 бит;

• использование жестких дисков и твердотельных дисков на основе флеш-модулей (SSD) в системах с высоким риском сбоя электроснабжения;

• использование эффективного и низкозатратного решения для защиты от порчи или потери данных;

• реализация значительно более высокой степени готовности системы.

***Леру Поль** – аналитик по технологиям компании QNX Software Systems.*
Контактный телефон (812) 702-08-33. Http://www.swd.ru

QNX Software и Real-Time Systems объединяют ОС РВ QNX Neutrino и технологию Hypervisor

Последняя версия продукта RTS Hypervisor 2.2 дает возможность клиентам запускать ОС РВ QNX Neutrino на том же оборудовании, что Windows, Linux и другие ОС. Такая консолидация оборудования не только снижает энергопотребление, но и уменьшает стоимость системы за счет отказа от использования дополнительных процессоров.

Данное решение особенно полезно для рынка промышленного и медицинского оборудования, где многие клиенты доверяют ОС РВ QNX Neutrino при решении критически важных задач и задач РВ, например, управления движением. При этом другая ОС может использоваться для других функций, например, обслуживать традиционный ЧМИ. Поскольку решение не зависит от ОС, установленной на хост-машине, ОС могут перезагружаться независимо, не прерывая работу друг друга.

В пределах среды RTS Hypervisor за счет использования виртуальной сети на базе TCP/IP упрощаются внутрисистемные связи. Технология компании Real-Time Systems поддерживает также прерывания, инициируемые сообщениями (message-signaled interrupts, MSI), для ОС РВ QNX Neutrino и других ОС, исключая конфликты при прерываниях и упрощая системную конфигурацию.

Http://www.swd.ru