КАК ОБЕСПЕЧИТЬ ВЫСОКУЮ ДОСТУПНОСТЬ ИНДУСТРИАЛЬНЫХ КОМПЬЮТЕРОВ

ТИМ МАНРО (TIM MUNRO)
ПЕРЕВОД: ВЛАДИМИР РЕНТЮК

По мере того, как критически важные приложения становятся все более обыденными, растет потребность в надежных компьютерных системах с высокой степенью доступности.

За последние 30 лет возможности по применению индустриальных компьютеров и технические характеристики данных устройств претерпели значительные изменения и сильно эволюционировали. Первые промышленные компьютеры обеспечивали на заводах поддержку человеко-машинного интерфейса (human-machine interface, HMI) для автоматизированного оборудования, а также диспетчерское управление и сбор данных, известные как SCADA (supervisory control and data acquisition). Сегодня приложения межмашинного взаимодействия (Machine-to-Machine, M2M) и аналитики, построенные на основе так называемых больших данных, создали потребность в надежных компьютерах, которые могли бы безотказно работать в жестких условиях окружающей среды, в том числе вне помещений. В настоящее время сфера применения таких компьютерных систем чрезвычайно широка, от мониторинга солнечной фермы до терминала оплаты парковки на автостоянке.

Первые индустриальные компьютеры были более надежными, чем их коммерческие собратья, но не были предназначены специально для критически важных приложений. Сегодня такие показатели, как класс защиты от внешних воздействий, результаты испытаний на механическую устойчивость (удары и вибрацию) и на работу при определенных климатических условиях (температура и влажность), позволяют квалифицировать компьютер как промышленный. Однако мы по-прежнему сталкиваемся с недостаточной отраслевой стандартизацией в отношении того, как измерять и отображать данные о надежности, доступности (долговременной работоспособности) и эксплуатационной надежности (в том числе оценке удобства обслуживания) компьютера. В англоязычной терминологии эти характеристики обозначаются как reliability, availability и serviceability.

Первый персональный компьютер (ПК), продаваемый для промышленных приложений, был выпущен в 1984 г. компанией IBM. Компьютер IBM 5534 был изготовлен в виде темно-коричневой версии традиционного светло-бежевого компьютера IBM XT. Такие функции, как охлаждение с помощью двойного вентилятора, прочный металлический корпус, высокопроизводительный источник питания, термодатчик и блокируемая крышка отсека накопителя для хранения данных, сделали IBM 5534 подходящим для применения на производственных предприятиях. К 1990-м гг. индустриальные компьютеры уже широко использовались, работая в основном с программными приложениями SCADA и HMI. Также развитие шло в сторону замены систем управления с переходом от программируемых логических контроллеров (ПЛК) на ПК с соответствующим управляющим программным обеспечением.

Однако уже к 2000 г. в большинстве отраслей промышленности из-за нестабильности работы операционных систем (ОС) и постоянного изменения их версий предприятия отказались от концепции управления на базе ПК. Сегодня ПЛК и аппаратное обеспечение распределенной системы управления остаются наиболее частым выбором в части управляющей платформы, в то время как индустриальный компьютер является предпочтительной платформой для приложений SCADA и HMI. Варианты использования промышленных компьютеров также включают системы безопасности и удаленные серверы аутентификации. Но сегодня пока еще существует неопределенность в отношении того, является ли индустриальный ПК подходящим выбором для критически важных приложений производственного и технологического процессов.

Дистрибутивы ОС Linux, такие как Red Hat, CentOS и Ubuntu, были направлены на решение проблем стабильности ОС и жизненного цикла. Однако для Linux-систем доступно меньше коммерческих, готовых и индустриально ориентированных приложений, чем для операционных систем под управлением Microsoft Windows. Гипервизоры виртуализации, такие как VMWare vSphere, Microsoft Hyper-V и Stratus Technologies everRun, обеспечивают отказоустойчивость между приложением и оборудованием. Однако разработка отказоустойчивой системы исключительно с применением программного обеспечения, операционных систем или гипервизоров добавляет сложности. Поэтому получается палка о двух концах: хотя эти дополнительные элементы предназначены для повышения надежности, из-за усложнения системы они в результате могут привести к большему количеству сбоев.

Упрощенный подход к разработке высоконадежной индустриальной компьютерной вычислительной системы начинается с аппаратного обеспечения. Это напрямую связано с тем, что большинство сбоев в работе компьютеров, особенно при функционировании в условиях воздействия чрезмерного тепла, пыли и электростатического разряда (рис. 1), вызывают источники питания, вентиляторы, память и дисковые накопители. Чтобы смягчить последствия отказов такого оборудования, разработчикам критически важных систем необходимо учитывать, как уже было сказано в начале статьи, три ключевых показателя: надежность, доступность и эксплуатаци-

онную надежность. Далее они будут рассмотрены подробнее.

НАДЕЖНОСТЬ

Под надежностью подразумевается вероятность того, что устройство выполнит требуемую от него функцию в установленных условиях в течение определенного периода времени. В количественном выражении это среднее время между отказами (mean time between failures, MTBF). Производители обычно определяют эту характеристику путем испытания продукта — через модель прогнозирования надежности (например, по методикам стандарта MILHDBK-217 или компании Telcordia) — или посредством анализа статистики по отказам продукта с мест эксплуатации. Хотя испытания и моделирование надежности до запуска продукта в серию и дают полезные оценки, эти приблизительные значения плохо коррелируют с данными, полученными от пользователей, когда продукт уже оказывается в условиях эксплуатации на том или ином объекте. Данные об отказах в условиях реальной эксплуатации обеспечивают бóльшую точность определения MTBF — естественно, при условии, что производитель ведет их статистический учет.

Общий подход для вычисления среднего времени между отказами по данным из мест эксплуатации таков:

MTBF = Количество продуктов, находящихся в эксплуатации в течение года / Количество обнаруженных сбоев в течение года.

Например, MTBF, равное 100 годам, подразумевает, что на каждые 100 продуктов в течение одного года произойдет один отказ. Чем больше размер выборки, тем точнее определение MTBF.

Устранение основных причин сбоев оборудования значительно увеличивает MTBF. Так или иначе влияют на число таких отказов вентиляторы, физические носители информации, память с исправлением ошибок (error-correcting code, ECC) и конформное покрытие.

Вентиляторы

Чтобы обеспечить возможность работы на более высокой тактовой частоте и использования широких шинных архитектур, разработчики микропроцессоров обычно полагаются на принудительное охлаждение с применением вентиляторов. Однако вентиляторы изнашиваются, часто выходят из строя и вместе с воздухом затягивают в корпус компьютера из окружающей среды пыль и различный мусор. Все это оседает на печатных платах и создает своеобразное теплоизолирующее покрытие, что приводит к ухудшению теплообмена — которое, в свою очередь, влечет за собой преждевременные отказы компонентов индустриального компьютера. При этом необходимо учитывать, что такие компьютеры, как правило, подвергаются воздействию более высоких температур окружающей среды, чем их коммерческие аналоги, поэтому та или иная технология охлаждения является необходимой. Технологии пассивного охлаждения, такие как радиаторы или теплоотводы с развитой поверхностью (обычно за счет специально спроектированных ребер) и теплопроводящие трубы, заменяют собой вентиляторы, а следовательно, устраняют связанные с ними отказы (рис. 2).

Физические носители данных

В целом MTBF твердотельных накопителей (solid-state drive, SSD) в три раза выше, чем у магнитных, вращающихся жестких дисков (hard-disk driver, HDD). В первую очередь это связано с тем, что SSD не содержат движущихся частей, а раз их нет, то и нет каких-либо шансов на механический сбой. Также SSD лучше, чем жесткие диски, подходят для использования в местах с сильной вибрацией и повышенной в разумных пределах температурой. Однако при выборе твердотельного накопителя важно учитывать различия между

РИС. 1. ▲ Электростатический разряд является одним из факторов, угрожающих компьютерным системам

технологиями SLC (single-level cell) и MLC (multilevel cell), т. е. ячейкой с одним уровнем (хранение 1 бита в ячейке) и многоуровневой ячейкой (хранение 2 битов в ячейке). SLC является самой старой технологией, но по сравнению с более дешевыми и современными SSD технология MLC обеспечивает в 30 раз больше операций записи/стирания и более долговременное хранение данных.

Память с исправлением ошибок

Наличие электромагнитных помех внутри компьютера может привести к тому, что один бит динамической памяти произвольного доступа перейдет в противоположное состояние. Это явление может повлечь за собой незаметное изменение пикселя на экране или разрушительный сбой системы. В памяти с исправлением ошибок (ECC) для проверки и избавления от этих ошибок используется алгоритм на основе четности контрольной суммы.

Конформное покрытие

Защитное покрытие, или полимерная пленка, которая соответствует топологии печатной платы,

РИС. 2. ◄ Использование теплоотводов и тепловых трубок в системе охлаждения исключает ненадежные и часто отказывающие вентиляторы

ТАБЛИЦА. ДОСТУПНОСТЬ ПРОТИВ ВРЕМЕНИ ПРОСТОЯ

Доступность	Время простоя
90% (одна девятка)	36,5 дня/год
99% (две девятки)	3,65 дня/год
99,9% (три девятки)	8,76 ч/год
99,99% (четыре девятки)	52 мин/год
99,999% (пять девяток)	5 мин/год
99,9999% (шесть девяток)	31 с/год
99,99999% (семь девяток)	3,1 с/год

называется конформным покрытием. Оно защищает электронные схемы от воздействия условий окружающей среды на предприятии, которая может содержать влагу или химические загрязнения, вызывающие коррозию.

ЭКСПЛУАТАЦИОННАЯ НАДЕЖНОСТЬ

С помощью такого показателя, как эксплуатационная надежность, оценивается то, как быстро компьютер может вернуться к нормальному функционированию после сбоя в работе системы. Измеряется она как среднее время восстановления работоспособности (mean time to repair, MTTR). Это более сложное значение для расчета, чем MTBF, поскольку MTTR зависит от времени, необходимого для получения запчастей, того, как техническая служба укомплектована персоналом, его квалификаций и конфигурации самого компьютера. В зависимости от условий конкретного пользователя, MTTR может варьироваться от секунд до нескольких недель. Стратегии, направленные на сокращение MTTR, включают использование резервных источников питания и дисков, а также управление через локальный порт или по внешнему каналу связи (технология out-of-band management, OOBM).

Резервные источники питания

Некоторые индустриальные компьютеры содержат очень надежные источники питания, а другие нет, поэтому требуют резервирования питания. Надежность питания зависит не только от резервирования собственных блоков питания компьютера, но и от разнообразия источников, от которых осуществляется их запитка. Дело в том, что отказ питания может произойти как непосредственно во внутренней системе питания индустриального компьютера, так и во внешней. Поэтому включение каждого основного или резервного блока питания от разных внешних источников (например, розетки промышленной сети напряжения переменного тока и аккумуляторной батареи в системе источника бесперебойного питания) гарантирует, что компьютер никогда не останется без питания, даже если один из источников неисправен или имела место авария на питающей его сети. Кроме того, обслуживающий персонал может полностью исключить MTTR, используя возможности горячей замены блоков питания, которая осуществляется без выключения и сбоев в работе системы.

Резервные дисковые накопители

Избыточный массив независимых дисков (Redundant Array of Disk, RAID) — это технология виртуализации хранилищ данных, которая позволяет нескольким дискам копировать данные друг друга. В общем представлении это массив из нескольких дисков, управляемых контроллером, взаимосвязанных скоростными каналами и воспринимаемых внешней системой как один логический диск. Технология RAID может значительно снизить MTTR, поскольку в случае отказа одного из дисков система может продолжать функционировать.

OOBM

Стратегия, основанная на управлении через локальный порт или по внешнему каналу (OOBM), включает группу технологий, которая позволяет владельцу удаленных компьютерных активов выполнять множество задач по их техническому обслуживанию и восстановлению. Например, восстанавливать ОС или производить перезагрузку системы по сети. Без возможности удаленного доступа специалистам системы приходится ездить к каждому компьютеру. Исключая необходимость таких поездок в места размещения оборудования, технология OOBM значительно снижает MTTR.

ДОСТУПНОСТЬ

Доступность — это показатель надежности и удобства обслуживания, который определяет процент времени работоспособности системы. Данная функция выражается уравнением:

$$\text{средняя доступность} = MTBF / (MTBF + MTTR) \times 100\ \%,$$

где MTBF — среднее время между отказами, MTTR — среднее время до восстановления работоспособности.

Максимизация доступности требует увеличения MTBF и уменьшения MTTR. Обычный способ выразить уровень доступности компьютера — через «девятки», или время простоя. Уровень доступности в 99,999% («пять девяток») может показаться хорошей целью для проекта, однако на самом деле даже пять минут простоя могут быть катастрофическими для технологического процесса или самого предприятия (табл.).

В то же время при добавлении компонентов, которые обеспечивают избыточность, направленную на увеличение надежности, — таких как, например, резервные источники питания и накопители — возникает парадокс. Это приводит к уменьшению MTBF из-за возможности возникновения дополнительных сбоев в таких компонентах. Отсюда следует, что крайне важно, чтобы компоненты для резервирования были простыми (т. е. не оказывали заметного влияния на значение MTBF), но при этом достаточными для полной реализации своих функций.

Хотя определение компьютера как индустриального по-прежнему весьма субъективно, существуют объективные показатели, которые следует учитывать при выборе уровня доступности, требуемого для конкретного применения. Поскольку критически важных приложений становится все больше, вместе с тем возрастает потребность в надежных компьютерных системах с высокой степенью доступности. Если оптимизировать такие показатели, как среднее время между отказами и среднее время до восстановления работоспособности, компьютерные системы могут не только соответствовать требованиям по доступности, но и превышать их. ●