Отказоустойчивость производственных систем: практика внедрения платформы «ГиперСфера»

В статье обсуждается проблема отказоустойчивого управления техпроцессами на примере производства молочных и пивобезалкогольных напитков. Рассмотрена платформа «ГиперСфера», позволяющая повысить отказоустойчивость серверов и таким образом обеспечить непрерывность технологических процессов.

ООО «СТР», г. Москва

Для предприятий пищевой промышленности, в частности, молочного или пивобезалкогольного производства, характерны скоротечные технологические процессы. За их выполнение отвечает серверное оборудование, встроенное в АСУ ТП (управление технологическими процессами), MES (общее управление производством) и другие системы. Отказ сервера прерывает процесс передачи данных: в контроллер перестает поступать рецепт (очередной шаг), из-за чего происходит остановка всего техпроцесса. Для скоротечных процессов, не допускающих длительных пауз, даже остановка, превышающая 10 минут, имеет критическое значение (рис. 1).

Специфика пищевой отрасли такова, что незапланированный простой из-за отказа ИТ-системы превращается в технологическую катастрофу. Для расчета стоимости незапланированного простоя на пивоваренном заводе недостаточно просто умножить объем непроизведенной продукции на цену. Например, незапланированный простой автоматизированной системы управления линей розлива часто ведет не только к простою производства, но и каскадным затратам в виде порчи сырья. Помимо упущенного дохода, существуют специфические расходы, связанные с технологическим браком сырья из-за того, что при резкой остановке приложения АСУ ТП процесс пастеризации или фильтрации прерывается. Пиво, находящееся в потоке, подлежит утилизации. Кроме этого, надо учесть расходы на перезапуск линии, которые включают в себя санитарную промывку и затраты на поддержание пивоваренных котлов в режиме ожидания.

И это из-за отказа только одной ИТ-системы! Обычно же на предприятии, производящем напитки, внедрено несколько разных систем: кроме АСУ ТП, SCADA, MES, это могут быть системы, отвечающие за маркировку «Честный знак», за связь с контролирующей государственной системой ЕГАИС, за планирование (1С: ERP), учет и другие бизнес-задачи. Все системы критичны, для каждой из них выделяются отдельные физические или виртуальные машины, и отказ любой из этих машин приводит к простоям. Стандартные методы защиты (резервное копирование данных, холодный резерв оборудования, кластеризация ПО АСУ ТП встроенными средствами) позволяют сохранить информацию, но не обеспечивают непрерывности производственного цикла. Если сервер выходит из строя по любой причине – из-за аппаратного обеспечения, ПО, из-за отключения электроснабжения, – у завода останавливается линия и теряется партия продукта.

Человеческий фактор тоже может привести к остановке технологического процесса на недопустимо долгий срок. На заводе без хорошей технической поддержки операторы, потеряв связь с сервером, делают то, что кажется самым простым решением: перезагружают кластер, на котором находится производственный сервер. Но если

Рис. 1. Для пивоваренного завода характерны скоротечные технологические процессы, не допускающие долгих простоев. Изображение сгенерировано ИИ

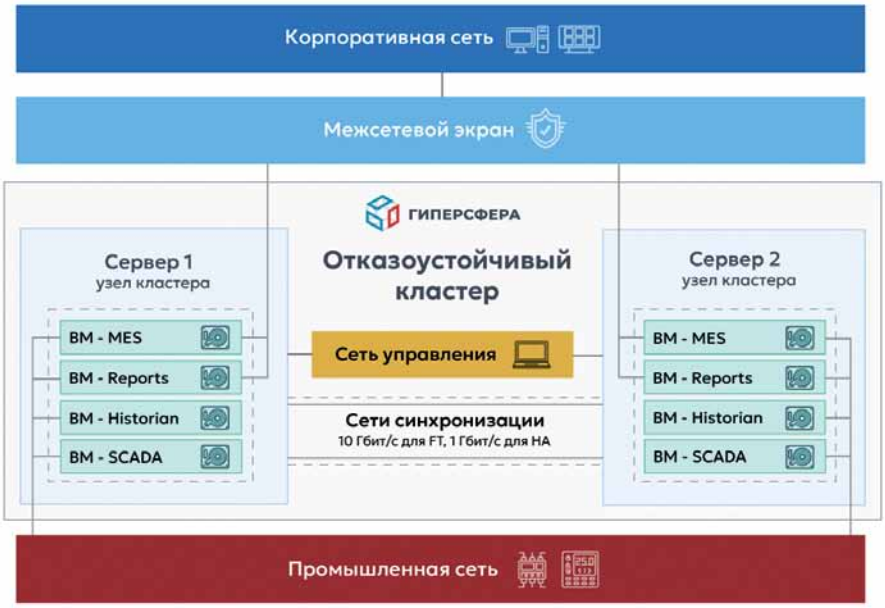

Рис. 2. Архитектура отказоустойчивой системы управления техпроцессом на базе ПО «ГиперСфера»

проблема была, например, в коммутационном оборудовании, то ни первая, ни вторая, ни третья перезагрузка не принесут результата, но будет потеряно время, потерян продукт и рассинхронизирован кластер, который необходимо будет восстанавливать, оплачивая услуги технических служб из операционных затрат (OPEX).

Для решения указанной проблемы надо сместить акцент с сохранности данных на отказоустойчивость инфраструктуры. Платформа виртуализации «ГиперСфера» (рис. 2) производства ООО «СТР» предназначена для того, чтобы повысить отказоустойчивость серверов. Архитектурно решение строится на двух физических серверах x86-64, на которых поддерживаются синхронные копии виртуальных машин, содержащих SCADA, базу данных, MES и шлюзовые компоненты. Принципиальным отличием от классических кластеров является отсутствие потребности в выделенной системе хранения данных: синхронизация памяти и состояния ввода/вывода происходит по выделенному каналу 10 Гбит/с напрямую между узлами. В случае аппаратного отказа одного из серверов (выход из строя блока питания, диска, потеря сети) второй узел подхватывает выполнение критической нагрузки без потери состояния, то есть остановки техпроцесса не происходит.

После внедрения «ГиперСферы» продолжают фиксироваться стандартные события: отказы жестких дисков, выход из строя блоков питания серверов или источников бесперебойного питания. Однако эти инциденты не приводят к производственным авариям. В рассматриваемом случае (производство молочной и пивобезалкогольной продукции) с помощью синхронизации реализуется высокая доступность (high availability, HA) виртуальных машин, то есть восстановление связи с сервером приложений происходит автоматически в течение 5–10 минут. Операторы технологических линий могут зафиксировать кратковременную потерю сигнала на мнемосхеме, но она не приведет к отклонению в технологическом регламенте или срабатыванию защитных блокировок. Благодаря быстрому автоматическому восстановлению не требуется пытаться вручную перезагружать кластер и потом восстанавливать данные, достаточно провести в дальнейшем плановую диагностику сбоя.

С помощью платформы «ГиперСфера» можно реализовать и более защищенный вариант – виртуальные машины с непрерывной доступностью (fault tolerance, FT). Режим непрерывной доступности практически исключает переходные процессы и, в случае отказа одного из физических серверов, обеспечивает продолжение выполнения виртуальных машин на другом сервере без перерыва и, естественно, без потери данных. Но такое решение востребовано реже, оно применяется в процессах, критически чувствительных к любым задержкам, например, в энергетике или атомной промышленности. Для пивного и молочного производства, где допустимы паузы в 3–5 минут, вполне достаточно высокой доступности с автоматическим перезапуском виртуальной машины на резервном узле.

Практика внедрения подтверждает, что отказоустойчивость на уровне гипервизоров эффективна только при резервировании физических серверов и в целом физической инфраструктуры. Обязательным условием является применение RAID-массивов, дублированных блоков питания в серверах, резервирование сетевых подключений. Комплексный подход дает максимальный результат. Внедрение системы отказоустойчивости на объекте занимает порядка месяца от планирования до реализации. Если же реализуется комплексное решение с новым оборудованием и системой АСУ ТП, то от 3 до 6 месяцев.

По мере накопления опыта меняется и подход к архитектуре вычислительных мощностей. Раньше наблюдалась тенденция к выделению одного кластера под один проект – участок производства. На этом кластере, как правило, работали одна-две виртуальные машины. Сейчас тренд меняется в сторону укрупнения: предприятия постепенно переходят к увеличению мощности кластеров и размещению на них множества виртуальных машин по всем участкам производства. Это сокращает количество физических единиц оборудования и упрощает администрирование.

Таким образом, внедрение ПО «ГиперСфера» переводит отказоустойчивость из категории программных «костылей» в разряд базовых свойств архитектуры производственной ИТ-системы. Отказоустойчивость требуется для всех критически важных процессов, главное – реализовать ее своевременно и качественно, а не по факту «рухнувшего» сервера.

ООО «СТР», г. Москва,
тел.: +7 (495) 646-8511,
эл. почта: info@str-technologies.com,
сайты: str-technologies.com,
отказоустойчивость.рф

Иллюстрации предоставлены ООО «СТР»