

Система контроля рисков в высоконагруженных биржевых и брокерских системах и её тестирование

Алёна Булда
Exactpro Systems
alyona.bulda@exactprosystems.com

Максим Рудовский
Exactpro Systems
maxim.rudovsky@exactpro.com

Алексей Зверев
Exactpro Systems
alexey.zverev@exactprosystems.com

Аннотация. Задачей современных высоконагруженных биржевых и брокерских систем является предоставление клиентам возможности осуществлять финансовые транзакции в условиях высокочастотной и алгоритмической торговли. Финансовая и технологическая устойчивость таких систем напрямую зависит от эффективности и своевременности контроля сопутствующих рисков. В статье представлены технические и архитектурные особенности систем контроля рисков, производящих в режиме реального времени анализ рисков в системах высокочастотной и алгоритмической торговли, производительность систем и используемые алгоритмы в расчетах рисков. Разработана архитектура системы контроля рисков, проанализированы основные аспекты, характеризующие её качество и работоспособность. Созданная архитектура используется для разработки набора методов тестирования и измерения основных функциональных и технических параметров систем контроля рисков. На основе предложенной архитектуры системы контроля рисков может быть построена референтная библиотека тестов.

Ключевые слова: *real-time риск система, управление рисками, контроль рисков, HFT (высокочастотный трейдинг), трейдинговые системы, брокерские системы, DMA (Direct Market Access англ. - прямой доступ к бирже), тестирование.*

1 Введение

По данным Нью-Йоркской фондовой биржи (NYSE - New York Stock Exchange), за четыре года - с 2005 по 2009 - дневной объём торгов на фондовых биржах США вырос в среднем на 164%. Данный рост был обусловлен в том числе и возрастанием объёмов высокочастотного трейдинга [1]. На начало 2009 года общий объём активов под управлением хеджевых фондов, использующих высокочастотный трейдинг, составил \$141 млрд. По данным опроса Aite Group, в США количество фирм,

использующих высокочастотный трейдинг, составляет 2% от приблизительно 20000 действующих сегодня компаний, а на долю высокочастотного трейдинга приходится 73% общего объёма торгов. В 2010 году доля программ для высокочастотного трейдинга в обороте на фондовом рынке составила порядка 11-13 % на бирже ММВБ, что составляет 45% от общего количества заявок [2]. Использование программных приложений для высокочастотного трейдинга становится всё более широким и популярным в мире электронной торговли финансовыми инструментами.

1.1 Особенности высокочастотного алгоритмического трейдинга.

Высокочастотным алгоритмическим трейдингом (High Frequency Trading) называют автоматизированную торговлю финансовыми инструментами, построенную в соответствии с совокупностью правил, объединённых в компьютерный алгоритм. Высокочастотный трейдинг используется для электронной торговли ценными бумагами, и наиболее важной характеристикой для высокочастотного трейдера является скорость, а именно - скорость реагирования высокочастотных трейдеров на те или иные изменения котировок, получаемых с бирж [3]. В высокочастотном трейдинге существует некоторый набор стратегий, например, стратегия по обеспечению ликвидности, стратегия статистического арбитража или стратегия по поиску ликвидности [4]. В стратегии по обеспечению ликвидности высокочастотные трейдеры пытаются заработать на ценовой разнице между спросом и предложением. Высокая волатильность и широкая разница в цене являются источником прибыли для высокочастотного трейдера. В то же время он становится поставщиком ликвидности и уменьшает разницу между спросом и предложением. Трейдеры, пользующиеся арбитражными стратегиями, используют поправку между ценами деривативов и их базовых активов [5]. Стратегии по поиску ликвидности исследуют рынок в поисках крупных заявок. Эффективность работы таких стратегий у высокочастотных алгоритмических трейдеров

практически всегда напрямую зависит от временной задержки между возникшей на рынке возможностью и непосредственным действием трейдера.

Время между отсылкой заявки и реальным событием на бирже является немаловажной как функциональной, так и технической характеристикой для высокочастотных трейдеров. Так же существует ряд внешних событий, которые высокочастотным трейдерам необходимо отслеживать: мониторинг выгодных котировок на разных биржах, своевременный их анализ, запуск алгоритма на вычисление выгоды и так далее. При этом чем быстрее высокочастотный алгоритмический трейдер получает данные и реагирует на них, тем эффективнее и рентабельнее ему обходится его алгоритм. Поэтому чем меньше на пути у высокочастотного трейдера дополнительных проверок, тем больше у него времени на маневрирование в сложившейся на рынке ценовой ситуации.

Поскольку высокочастотные трейдеры заинтересованы в минимальных временных задержках, ведущие международные фондовые биржи стали предоставлять высокочастотным трейдерам прямой доступ на биржевые площадки (Direct Market Access - DMA) [6]. Например, Turquoise MTF, одна из самых быстрых многосторонних торговых площадок в мире, предоставляет высокочастотным трейдерам сервис спонсированного доступа (Sponsored Access) - своего рода вид прямого доступа к бирже с некоторым набором пре-трейдинговых проверок [7].

С другой стороны, в некоторых областях трейдинга существует определённая доля риска возникновения так называемого сбоя высокочастотных роботов, которые могут отправить неконтролируемую, так называемую "плохую", заявку. Следовательно, возникает и потребность в наличии дополнительных систем контроля рисков [8].

1.2 Основные тенденции высокочастотных трейдеров

Финансовые рынки настолько сложны и энтропийны, что зачастую даже программисты, создавшие торговые алгоритмы, не могут до конца точно объяснить, что происходит, когда такие алгоритмы взаимодействуют "в естественных условиях". Например, в 2010 году индекс Dow Jones упал почти на 1000 пунктов, что повлекло за собой падение всего валютного рынка. По оценке компании Wilshire International, за несколько минут рынок потерял более 1 трлн долларов, а индекс S&P 500 - сразу 8,6%. Этот инцидент получил в финансовом мире название "Flash Crash of 2:45" [9]. После события Flash Crash в 2010 году были введены так называемые «прерыватели торгов» («Circuit Breakers» или «trading halts») [10], которые, теоретически, «страхуют» торговлю тем или иным финансовым инструментом.

Дополнительные системы контроля рисков постоянно усложняются, поскольку есть необходимость обеспечить безопасность финансовых рынков без потери в

скоростных возможностях высокочастотных трейдеров. Различные функциональные части системы контроля рисков реализуются как отдельные компоненты одной системы. Каждый компонент такой распределённой системы контроля риска может быть реализован с применением высоких технологий, например таких, как FPGA (field-programmable gate array – «перепрограммируемая матрица логических элементов») или «программируемая логическая интегральная схема» (ПЛИС) - полупроводниковое устройство, которое может быть сконфигурировано или перепрограммировано производителем или разработчиком после изготовления [11], GPU (graphics processing unit - отдельное устройство, выполняющее подготовку фотореалистичных изображений (графический рендеринг) с высокой вычислительной мощностью [12] и другие архитектурные решения.

1.3 Обзор брокерских систем риск-контроля

Большинство ведущих трейдинговых биржевых и брокерских систем подходят к вопросу контроля рисков, ставя их непосредственно прямо "на пути" у высокочастотных трейдеров. Если, например, это брокерская система контроля рисков, то высокочастотные алгоритмические трейдеры могут идти через эту брокерскую систему, которая не может не влиять на временную задержку на размещение заявок от трейдера. [13] [14]

На рисунке 1 представлена схематически брокерская система контроля рисков. В такой ситуации задержка событий от высокочастотного трейдера возрастает [15]. При таком построении связей с брокерской системой и электронным рынком задержки достигают от 90 до 200 миллисекунд [16]. Расшифруем компоненты, представленные на рисунке 1: а) OMS – Order Management System – это компонент для ввода и обработки заявок от клиентов; б) EMS - Execution management systems – это компонент, отвечающий за транзакционную составляющую торговли, содержащий в себе набор алгоритмов для исполнения заявок [24]; в) Market Data – компонент, распространяющий информацию о котировках с рынков; г) Drop Copy – компонент, дублирующий брокеру все транзакционные составляющие заявок; д) Clearing – компонент, отвечающий за пост-транзакционные процессы заявок.

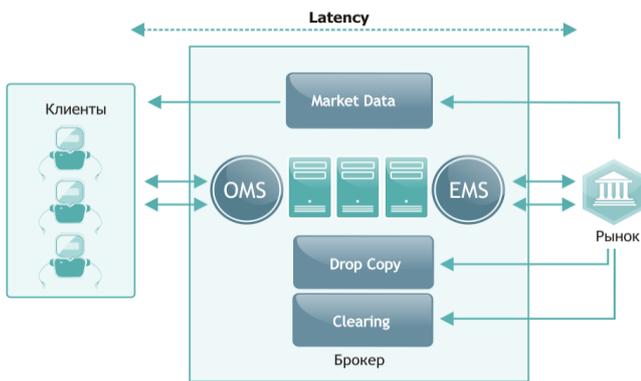


Рис.1. Схема соединений высокочастотного трейдера к бирже через брокерскую систему контроля рисков

При абсолютном же доступе высокочастотных алгоритмических трейдеров к рынку (Naked Sponsored Access или Unfiltered Access) [17] брокер и биржа рискуют тем, что эти алгоритмические трейдеры практически бесконтрольны с точки зрения рисков и их поведения на бирже. Данная модель подразумевает, что действия высокочастотных алгоритмических трейдеров происходят с практически минимальной задержкой. Однако, например, в США уже с 2011 года существует правило “Rule 15c3-5”, согласно которому наличие системы по контролю рисков для высокочастотных трейдеров является обязательным [18].

Отсюда имеем задачу, как оптимизировать задержку, и в тоже время контролировать алгоритмичных трейдеров. Описанная ниже архитектура системы контроля рисков - это своего рода компромисс между торговлей напрямую в бирже и торговлей через брокерскую систему под контролем. Такая нефункциональная характеристика, как низкая латентность (или незначительная задержка во времени), является очень важной характеристикой системы контроля рисков для способности конкурировать с другими системами. Вследствие этого данному техническому требованию при тестировании такой системы уделяется особое внимание, ровно как и алгоритмам, призванным следить за рисками от активностей трейдеров на рынках.

2 Архитектура системы контроля рисков

2.1 Схематичное представление архитектуры системы контроля рисков

На рисунке 2 схематически представлена разработанная нами архитектура системы контроля рисков с основными зависимостями от тех или иных внешних условий, а также показана основная её функция - своевременное управление рисками и отключение трейдера от шлюзов торговли [19]. Данная архитектура системы рисков призвана вовремя отследить “плохую”

заявку высокочастотного трейдера, приняв необходимые меры по устранению роковой ошибки, и в то же время уменьшить временные задержки на пути у трейдера. Немного поясним, что значит “плохая” заявка – это, например, когда цена заявки существенно отличается от рыночной, или когда трейдер отправляет заявку, на которую не имеет одобренных у брокера средств, и тому подобное. Определений “плохая” заявка, ровно как и алгоритмов по контролю за рисками в системе, может быть огромное количество.

Разработанная нами архитектура позволяет высокочастотному трейдеру размещать заявки без больших задержек, при этом существует элемент в системе - *управление трейдерской активностью*, который согласно заложенным в него проверкам (алгоритмам расчета рисков), своевременно разорвёт TCP/IP соединение между трейдером и биржей.

Риск брокера тут, конечно, присутствует, потому что та самая “плохая” заявка уже окажется на рынке, но своевременное вмешательство предотвратит большие последующие потери, сравнимые с теми, что произошли во время “Flash Crash of 2:45”.

Нашей системы контроля рисков, а также и самому высокочастотному алгоритмическому трейдеру необходимо отслеживать как саму активность этого трейдера, так и рыночную стоимость тех или иных акций или деривативных инструментов, которыми этот трейдер торгует. При этом, чем сложнее деривативный инструмент, тем больше смежной информации о нём необходимо отслеживать и обрабатывать.

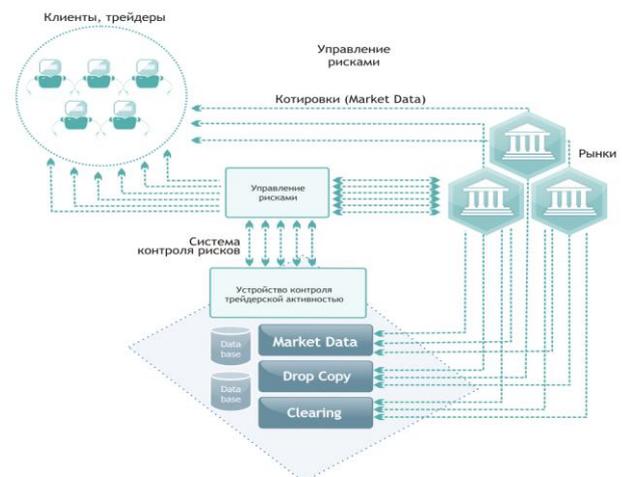


Рис. 2. Схематичное представление архитектуры системы контроля рисков брокера.

Считывание и анализ котировок с различных бирж, хранение и обработка информации, поступающей брокеру с электронных трейдинговых площадок по Drop Copy (информационный сервис, предназначенный для получения всех отчетов о заявках [20]) или Clearing-соединениям (взаимозачет между участниками торгов), хранение, обработка и анализ электронной активности

высокочастотных алгоритмических трейдеров - весь этот огромный поток информации должен поступать различным компонентам нашей системы контроля рисков, призванным его обрабатывать и анализировать. Компоненты системы контроля рисков отвечают за определённые функциональные блоки системы в зависимости от сложности существующих в ней связей и параметров.

2.2 Основные компоненты предложенной системы контроля рисков.

Вследствие огромного потока информации и из-за необходимости её обработки представляется вполне логичным и разумным, что система контроля рисков должна быть распределённой. Другими словами, наша система разделяется на функциональные блоки, которые, в свою очередь, также могут быть реализованы при помощи различных технологических и инженерных подходов, призванных улучшить скорость работы с данными и отказоустойчивость самой системы.

На рисунке 3 представлена разработанная нами архитектура идеализированной распределённой системы контроля рисков. Мы выделили её основные функциональные блоки.



Рис. 3. Архитектура распределённой системы контроля рисков.

Управление соединениями клиентов - блок в нашей архитектуре системы контроля рисков, отвечающий за своевременный разрыв соединения высокочастотного трейдера с биржей. Существует способность управлять этой частью системы и самим брокером в случае непредвиденных обстоятельств. В данный блок должны поступать и управляющие команды с модулей расчёта и анализа рисков и текущих позиций трейдеров. При обнаружении того или иного риска специальные алгоритмы, вычисляющие риски и запускающие стандартные проверки рисков, а также дополнительные проверки, зависящие от ряда поступающих извне условий, подают сигналы на компонент управления соединениями, который, в свою очередь, останавливает при необходимости соответствующего высокочастотного трейдера. Реализация процесса остановки

высокочастотного трейдера может быть осуществлена несколькими путями: от "грубого" разрыва TCP/IP соединения, до перекрытия сети (Network) между трейдером и биржей.

Хранилище настроек трейдеров - это база данных с настройками, которые брокер определяет каждому трейдеру, получившему доверительный прямой доступ к бирже. Данный блок несёт в себе большое количество входных условий и параметров алгоритмов, контролирующих риски. Например, это могут быть определённые проверки, в запуске которых для данного активного трейдера может возникнуть необходимость, или ликвидность (или так называемый лимит на количество активных заявок, которым может располагать трейдер в условиях электронного трейдинга) или что-то другое.

Плагины для сбора и агрегации биржевых котировок (или Market Data плагины) - эта часть системы контроля рисков отвечает за сбор и агрегацию котировок с разных электронных бирж, перевод этой информации о котировках в вид, который наша система контроля рисков воспринимает. Здесь подразумевается использование протокольного интерфейса, разработанного с целью передачи сообщений между компонентами. Протокол содержит минимальную необходимую информацию и призван уменьшить временные задержки, которые могут возникнуть при обмене информацией между компонентами самой системы. В электронном трейдинге существует большое количество различных бирж, и каждая биржа имеет возможность предоставлять котировки не только через стандартные финансовые протоколы [21], но и через протоколы с фиксированной длиной сообщений, разработанные самой биржей с теми или иными улучшениями и особенностями. Получается, что данный плагин выступает в роли market data-клиента биржи. Сбор и анализ котировок с различных бирж может быть необходим для определения рыночной стоимости тех или иных акций или финансовых инструментов. Эта информация так же необходима при оценке рисков.

Drop Copy и Clearing плагины - эта часть системы контроля рисков так же, как и плагин для сбора и агрегации котировок, приводит к унифицированному виду информацию, поступающую брокеру с трейдинговой платформы. Основная информация - это отчёты о состоянии заявок высокочастотных трейдеров на биржах и о сделках, которые они совершили.

Данные Market Data, Drop Copy и Clearing - компонент, представляющий собой оперативную базу данных, в которую по внутреннему протоколу вносится информация с плагинов. Этот поток данных также является входящим набором для запуска брокерских алгоритмов для расчёта рисков.

Модуль расчёта позиций трейдеров - каждый трейдер отправляет на биржу заявки на те или иные финансовые инструменты, такие как акции и деривативы, поэтому расчёт всех видов открытых позиций является немаловажным для брокера, так как представляет собой

ликвидный лимит высокочастотного трейдера, который тот не должен превышать.

Модуль анализа и расчёта рисков - это компонент с набором алгоритмов брокера для расчёта рисков. Брокерские алгоритмы расчёта рисков могут запускаться как в режиме реального времени (real-time), так и “пост-транзакционно” в зависимости от приоритетности и необходимости в принятии немедленного решения в связи событиями на бирже, возникающими как реакция на действия высокочастотного трейдера.

GUI-интерфейс для брокера - интерфейс для выставления настроек как высокочастотным трейдерам, так и алгоритмам расчёта рисков брокера. Это необходимо для определения приоритетов проверок. Брокер при помощи графического интерфейса может осуществлять мониторинг действий высокочастотных алгоритмических трейдеров в режиме реального времени и контролировать их, а также разрабатывать новые алгоритмы по расчёту и определению рисков на основе анализа потоков данных в системе.

При разработке больших распределённых систем электронного трейдинга всё чаще и чаще используют методику, заключающуюся в представлении компонентов в виде двух частей - основного и резервного. Эта методика применяется для улучшения отказоустойчивости таких систем. Основной компонент независим от резервного. Он функционирует с остальными частями системы и выполняет свою функцию по обработке входящего потока информации. Резервный компонент всегда работает в фоновом режиме и в определённые промежутки времени сверяется (синхронизирует данные) с основным узлом. Чаще эти промежутки периодичны с фиксированной длиной отрезка времени. В случае отказа основного узла происходит перехват управления - процесс передачи функций управления дублирующему узлу. Так система преодолевает отказы своих компонентов, которые могут произойти вследствие возникновения различных функциональных или технических условий.

Таким образом, мы имеем идеализированную архитектуру системы контроля рисков. В некоторых областях, наша система контроля рисков упрощена, но её уже можно рассматривать в контексте тестирования основных функций. Она также позволяет выделить наиболее приоритетные компоненты и планировать процесс тестирования.

3 Основные области тестирования систем контроля рисков

Проанализировав представленную систему контроля рисков, мы выделили приоритетные технические и функциональные параметры для тестирования. Для удобства представим области тестирования в виде таблицы ниже. Хотелось бы заметить, что те области тестирования, которые не рассмотрены ниже в таблице, или на Ваш строгий взгляд рассмотрены не полно, вовсе

не являются незначительными. Мы их не рассматриваем потому, что они либо присутствуют в любой другой системе и имеют вполне стандартный набор проверок для успешного тестирования, либо не являются архитектурной особенностью этой системы.

Табл. 1. Области тестирования системы контроля рисков.

Область тестирования	Примечание
1. Управление соединениями клиентов	Тесты для данного компонента покрывают реагирование системы на те или иные команды от управляющего компонента, при обнаружении ею риска. Правильность отсылки сообщения перед разрывом соединения и дальнейшее блокирование соединения, клиентского аккаунта и т.п.
2. Хранилище настроек трейдеров	В первую очередь, проверяются так называемые рабочие сценарии (use cases), затем создаётся набор трейдеров с различными (в том числе и негативными) настройками и с ними проводится тестирование системы на стабильность и корректность работы на границах функциональности.
3. Плагины для сбора и агрегации биржевых котировок (Market Data плагины)	Важно проверить и покрыть тестами обработку информации поступающей с площадок и скорость её поступления и обработки самим плагином. Большая часть тестов описана в статье про тестирование Market Data систем, таких как Ticker Plant. [25]
4. Drop Copy и Clearing плагины	Так же как и область №3, проверяется на те же аспекты. Отличия заключаются в специфике поступающей информации и правилах её обработки и сортировки для системы контроля рисков.
5. Данные Market Data, Drop Copy и Clearing	Большая часть проверок этой области уже описана в пунктах №3 и №4, но всё же вынесена как отдельная для тестирования нормализации межкомпонентного протокола, протокола, по которому осуществляется передача данных между основными компонентами системы контроля рисков представленной архитектуры.

	Поскольку информация и правила обработки полей содержащих эту информацию могут быть одни и те же.
6.Модуль расчёта позиций трейдеров	Область, содержащая алгоритмы и правила расчёта позиций каждого трейдера. В зависимости от особенности и обширности алгоритма, библиотека тестов так же варьируется. Библиотека тестов опирается на каждый блок алгоритма и на каждое правило расчёта.
7.Модуль анализа расчёта рисков	Как и в пункте №6, тесты направлены на проверку правильности расчёта рисков на основе потока информации из соседних компонентов системы, а также проверку управляющих команд и действий, которые вызываются модулем на основе расчёта.
8.GUI-интерфейс для брокера	Стандартный набор GUI тестов, направленных на удобство пользователей-брокеров отслеживать, проверять, настраивать те или иные данные.
9.Нефункциональное тестирование - латентность	В условиях большой конкуренции и защиты трейдеров от несанкционированного поведения, такой параметр, как латентность (latency) является одним из важных аспектов функционирования. Подробнее о целях тестирования этой области будет рассмотрено ниже в статье.
10.Нефункциональное тестирование – отказоустойчивость (системы и её компонентов по отдельности)	Тестирование поведения системы контроля рисков при отказе компонентов биржи и при отказе компонентов самой системы (Failover сценарии при потоке данных с биржи и при потоке управляющих команд из системы): - восстановление данных после отказа основного и/или запасного каналов поступающих данных; - возможность перепоключения к внешним источникам информации и системам; - правильная последовательность сообщений и их обработка; - возможность дальнейшей обработки данных после восстановления. [25]

11.Нефункциональное тестирование - нагрузочное	Каждая система должна иметь краевые характеристики (подтверждённые опытным путём через тестирование), при которых система способна функционировать без задержек и неисправностей достаточно долгий промежуток времени. Тесты этой области направлены на нахождение такой зависимости.
--	---

Это, конечно, не полный набор областей тестирования, но мы и не ставили перед собой задачу предоставить полное покрытие тестирования системы. Поэтому выше, в таблице, представлена лишь их часть. А именно функциональное тестирование выделенных компонентов архитектуры и нефункциональное тестирование. В дополнение к описанному тестированию в таблице, мы представим подробные подходы тестирования системы контроля рисков для следующих основных областей представленной архитектуры: а) алгоритмы расчета рисков; б) реагирование системы на краевые моменты; в) латентность. Эти области выделяются как наиболее значимые. В условиях конкуренции на рынке подобного рода систем, представленной в данной статье системе контроля рисков необходимо доказать своё преимущество в областях а, б и в.

3.1 Оценка точности алгоритмов расчёта рисков

Как уже упоминалось выше, система контроля рисков содержит в себе огромное количество проверок, распределённых по приоритетам как в режиме реального времени, так и с некоторыми задержками по времени. Чтобы протестировать все сочетания условий, необходимо большое количество как ресурсов, так и времени. Первая ступень - рассмотреть простую математику и рассчитать, как ведёт себя алгоритм. Например, отправляем 2000 заявок по определённой цене и количеству, затем отправляем ещё 2000 заявок с ценой намного меньше первой и наблюдаем, как реагирует на это событие алгоритм анализа рисков в нашей системе.

Разрабатываемая библиотека содержит сценарии тестирования, при которых срабатывают сразу несколько алгоритмов контроля рисков. Это делается для того, чтобы отследить проблемы, возникающие при параллельной обработке данных ("Concurrency Issues"). Весь набор тщательно обрабатывается и представляется в читаемой форме, которую можно анализировать и на основе полученных данных оценивать процесс тестирования. Значительная часть тестов отводится на проверку расчёта открытых позиций трейдера, имеющего лимиты на ликвидное количество открытых заявок.

В целом, проверка таких алгоритмов - это объёмная работа. В большинстве случаев у каждого из участников электронного трейдинга своё представление о том, как именно должен работать тот или иной алгоритм.

3.2 Проверка корректности реагирования системы контроля рисков на события

Сценарии и основные шаги по тестированию нашей системы контроля рисков дополняются следующими частями: проверками на то, как система реагирует на события, как и когда алгоритмы оценки рисков срабатывают, и что система контроля рисков делает после разрыва соединения высокочастотного трейдера.

Например, если в нашей архитектуре системы контроля рисков компонент, отвечающий за управление соединениями трейдеров, запрограммирован разрывать TCP/IP соединение высокочастотного трейдера при обнаружении неблагоприятного события, в нашем случае также будет необходимо проверить, что система контроля рисков контролирует и предупреждает дальнейшие попытки трейдера восстановить соединение, а также, что система корректно выполнила инструкцию «заблокировать» трейдера. Например, это может быть запрос на блокирование трейдера, отсылаемый дополнительно на биржу или запрос на подтверждение, что трейдер действительно сейчас неактивен.

При детальном рассмотрении таких событий, как "Flash Crash of 2:45", возникает вопрос, насколько эффективным и быстрым является предложенное решение устройства контроля соединениями трейдеров, и насколько при этом рискует брокер. Поэтому в системах контроля рисков большое внимание уделяется и её латентности.

3.3 Латентность, задержки (latency). Подход измерения латентности.

В условиях высокой загруженности брокерских и биржевых систем особое внимание всегда уделяется *временным задержкам (латентность, latency)*. Задержки влияют как на самих высокочастотных алгоритмических трейдеров, так и на способность системы контроля рисков вовремя среагировать на событие на бирже.

Итак, как же нам измерить, насколько наша модель системы контроля рисков влияет на сообщения между высокочастотным трейдером и биржей с точки зрения временных задержек? Рассмотрим представленную на рисунке 2 выше архитектуру системы контроля рисков. Предположим, что у нас есть идеальные условия для тестирования: есть электронная платформа, способная генерировать большой, сравнимый с реальными условиями на рынках, поток данных – нагрузку; есть возможность имитировать активность большого числа высокочастотных алгоритмических трейдеров, торговля которых контролируется рассматриваемой системы контроля рисков. Определяем матрицу, то есть набор

настроек трейдеров и алгоритмов контроля рисков для них в системе. В этой матрице перебираем, в зависимости от определённых приоритетов, все эти настройки и их сочетания. Так мы обеспечиваем всевозможные условия, в которых наши высокочастотные трейдеры будут работать в режиме большого количества потока данных и реагировать на возникшие в нашей электронной платформе ситуации. Конечно, исходя из требований в спецификации системы, относящихся к способности выдерживать указанный поток данных, мы определяем начальную ступень для создания входящей нагрузки. Так, когда у нас готовы все параметры трейдеров, рынка, торговых сессий, инструментов (reference data), когда готовы так называемые образцы (templates) для создания нагрузки, и есть инструменты тестирования для анализа (инструмент для тестирования "Shsha" [22]) и создания большого потока данных (инструмент для тестирования "Loadinjector" [23]), мы начинаем наше измерение. В связи с тем, что система контроля рисков является распределённой, необходимо убедиться, что серверы, на которых установлены компоненты системы, синхронизированы между собой.

Латентность - это время отклика системы на то или иное событие. Поэтому очень важно, что поток данных, который мы собираемся использовать для измерения этого параметра, должен быть собран ("захвачен") на одном сервере. Так мы с большой точностью можем измерить задержки. Допустим, что первую итерацию теста мы выполнили, получили большое количество данных, которые теперь необходимо проанализировать. Находя то или иное событие (или определённую ситуацию) и отклик самой системы контроля рисков на это событие, мы замеряем время задержки, с которой этот отклик был получен. После первого прогона теста на латентность всегда становится понятно, что именно упущено в начальных условиях или что необходимо ещё для определения тех или иных событий. Исходя из этого проводятся следующие прогоны. После этого данные анализа собирают вместе и представляют в виде сводных таблиц, графиков задержек, в зависимости от условий нагрузок.

Чтобы оценивать риски финансовых инструментов, и, в частности, деривативов, брокеру необходимо анализировать рыночную информацию по ним, включая котировки. И тут дополнительные задержки по времени, поскольку системе контроля рисков, а именно её компоненту, который собирает и агрегирует котировки, нужно обрабатывать 50-80 тысяч сообщений в секунду для того, чтобы иметь представление о BBO (Best Bid Offer, то есть лучшую цену спроса (Bid) и лучшую цену предложения (Offer) из цен, предоставляемых мировыми поставщиками ликвидности на момент исполнения заявки), и цены сделок на финансовых инструментах. Это связующее звено в модели системы контроля рисков подвержено возникновению больших задержек по времени. Отсюда задача - измерить суммарную задержку, а также задержки на каждом отдельном участке связей

системы контроля рисков, чтобы определить значения задержек её компонентов и в случае проблем с латентностью иметь возможность локализовать проблемный компонент. На рисунке 4 схематично представлена процедура описанного выше теста на латентность.

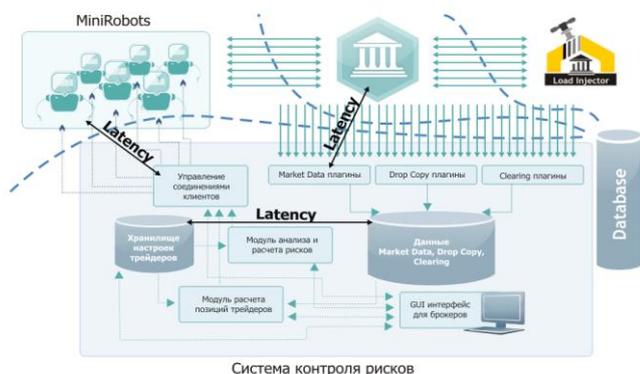


Рис. 4. Процедура тестирования системы контроля рисков на латентность.

Тестовый подход на рисунке 4 рассмотрен с учётом 3-х инструментов для тестирования: «Loadinjector» (создает большой поток данных), «Minirobots» (программируемые трейдеры, написанные на Java, которые эмулируют поведение высокочастотных алгоритмических трейдеров), и «Shsha» (база данных для анализа данных) [22].

Латентность, существующая в архитектуре системы контроля рисков, то есть задержка по времени между срабатыванием алгоритма контроля рисков и фактическим отсоединением высокочастотного трейдера от торгов, зачастую является важнейшим параметром. Любой сбой или увеличение такого временного интервала приводит к различным инцидентам на финансовых рынках.

В связи с этим, немаловажно оценить, в каком временном интервале сработает алгоритм нашей архитектуре системы контроля рисков, и в каком временном интервале фактически будет разорвано соединение высокочастотного трейдера к бирже, поскольку это может оказать большое влияние на рыночную ситуацию. Для наглядности на рисунке 5 представлена шкала зависимости задержки по времени нашей модели системы контроля рисков от падения цен на финансовый инструмент по примеру «Flash Crash of 2:45». Горизонтальная ось - это секунды. На примере получается, что за промежуток равный около 4 секундам, стоимость резко упала и владельцы понесли большой ущерб.

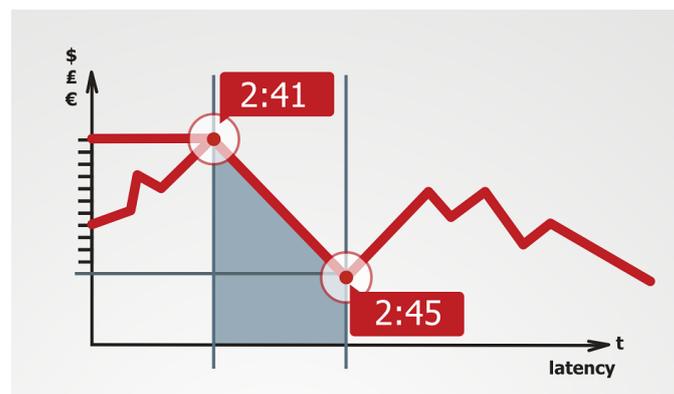


Рис. 5. Шкала зависимости задержки по времени и падения цен на финансовый инструмент.

Примерно такую же характеристику и показатели по латентности нам необходимо предоставить при тестировании системы контроля рисков, т.е. как быстро система контроля рисков «понимает», что поведение трейдеров не корректное.

4 Заключение

Данная архитектура системы рисков может быть использована при планировании процесса тестирования систем контроля рисков. Также она может быть задействована в качестве инструмента для тестирования высокочастотных алгоритмических трейдеров. Разработанная референтная библиотека по наиболее приоритетным областям тестирования системы контроля рисков может быть применима в качестве пособия для тестирования других систем контроля рисков.

В данной статье был проведён обзор систем контроля рисков, дан общий обзор приоритетов, характерных для этих систем, проанализированы основные приоритеты клиентов таких систем. Была разработана идеализированная архитектура системы контроля рисков и выделены основные области в тестировании, которые являются приоритетными для систем контроля рисков в условиях конкуренции на рынке.

Литература

1. http://www.nytimes.com/2009/07/24/business/24trading.html?_r=0
http://www.nytimes.com/2009/07/24/business/24trading.html?_r=0
2. Смородская П.: ММББ взялась за роботов. Газета «Коммерсантъ» № 129 (4429) от 20.07.2010
<http://www.kommersant.ru/doc/1455743>
<http://www.kommersant.ru/doc/1455743>
3. Michael Durbin: All about High-Frequency Trading. Mc Graw Hill, New York, 2009
4. M. Chlissalla: High-frequency trading Better than its reputation? Deutsche Bank research report, 2011.
5. J. Chiu, D of On-chip Local Memories (Nikola Vujic, Lluc Alvarez, Marc Gonzalez, Xavier Martorell, Eduard Ayguade)
[http://www.lseg.com/sites/default/files/content/documents/Sponsored Access factsheet.pdf](http://www.lseg.com/sites/default/files/content/documents/Sponsored%20Access%20factsheet.pdf)
<http://www.lseg.com/sites/default/files/content/documents/Sponsored Access factsheet.pdf>
6. Glasserman P., Heidelberger P., Shahabuddin P.: Variance Reduction Techniques for Estimating Value-at-Risk, Management Science 46(10), pp. 1349–1364, October 2000.
7. <http://online.wsj.com/article/SB10001424052748704029304575526390131916792.html>
<http://online.wsj.com/article/SB10001424052748704029304575526390131916792.html>
8. <http://www.sec.gov/investor/alerts/circuitbreakersbulletin.htm>
<http://www.sec.gov/investor/alerts/circuitbreakersbulletin.htm>
9. A Low-Latency Library in FPGA Hardware for High-Frequency Trading (HFT) Lockwood, J.W. Algo-Logic Syst. Inc., Santa Clara, CA, USA
10. Gupte, A. ; Mehta, N. ; Blott, M. ; English, T. ; Vissers, K.
11. O'Rourke, J.: CUDA-Enabled Optimisation of Technical Analysis Parameters O'Rourke, J. Sch. of Sci. & Comput., Inst. of Technol., Dublin, Ireland Burns, J.
12. Статья Computer trading and systemic risk: a nuclear perspective, <http://www.bis.gov.uk/assets/foresight/docs/computer-trading/12-1059-dr26-computer-trading-and-systemic-risk-nuclear-perspective.pdf>
<http://www.bis.gov.uk/assets/foresight/docs/computer-trading/12-1059-dr26-computer-trading-and-systemic-risk-nuclear-perspective.pdf>
13. Статья Systemic risk arising from computer based trading and connections to the empirical literature on systemic risk, <http://www.bis.gov.uk/assets/foresight/docs/computer-trading/12-1062-dr29-systemic-risk-from-computer-based-trading.pdf>
<http://www.bis.gov.uk/assets/foresight/docs/computer-trading/12-1062-dr29-systemic-risk-from-computer-based-trading.pdf>
14. Equity Risk Controls FPL Risk Management Committee, http://www.fixprotocol.org/documents/5537/FPLEquityRiskControls_final.pdf
http://www.fixprotocol.org/documents/5537/FPLEquityRiskControls_final.pdf
15. <http://helpdesk.commercialnetworkservices.net/index.php?m=knowledgebase&a=viewarticle&kbarticleid=174>
<http://helpdesk.commercialnetworkservices.net/index.php?m=knowledgebase&a=viewarticle&kbarticleid=174>
16. <https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=25&ved=0CE0QFjAEOBQ&url=http%3A%2F%2Fwww.afme.eu%2FWorkArea%2FDownloadAsset.aspx%3Fid%3D6055&ei=hYj3UdyeG->
17. <http://www.automatedtrader.net/headlines/81377/sec-grants-limited-extension-to-naked-access-ban>
<http://www.automatedtrader.net/headlines/81377/sec-grants-limited-extension-to-naked-access-ban>
18. Anna Zvereva, Senior QA Analyst; Boris Rabinovich, Lead of Complex Derivatives Projects; Alexey Yermolayev, Hardware Implementation Analyst; Iosif Itkin, Managing Director: The Future of Risk Controls, Exactpro Systems, http://extentconf.com/images/stories/Share/extent3_exactpro_the_future_of_risk_controls.pdf
http://extentconf.com/images/stories/Share/extent3_exactpro_the_future_of_risk_controls.pdf
19. <http://fs.moex.com/files/2285>
<http://fs.moex.com/files/2285>
20. <http://www.fixprotocol.org/http://www.fixprotocol.org/>
21. Alexey Zverev, Managing Director, Exactpro Systems, Head of CFT QA
22. Alyona Bulda, QA Lead for Borsa Italiana, Innovative Trading Systems
23. Marina Kudryavtseva, QA Manager, Innovative Trading Systems, Olga Moskaleva, QA Analyst, Innovative Trading Systems: Four Houses Fight to Control Test Automation, http://extentconf.com/images/stories/Share/extent3_exactpro_four_houses_test_tools_2012.pdf
http://extentconf.com/images/stories/Share/extent3_exactpro_four_houses_test_tools_2012.pdf
24. Maxim Rudovsky: Exactpro Testing Tools
<http://www.slideshare.net/IosifItkin/exactpro-test-tools-extent-feb-2011>
25. http://en.wikipedia.org/wiki/Execution_management_system
26. Булда А., Буянова О., Зверев А. - Статья Применение симуляторов рынка ценных бумаг для тестирования систем агрегации и распределения информации о котировках (Ticker Plant), <https://yadi.sk/d/eKKxTtEGCCeF6>