RECOMMENDED RISK CONTROL GUIDELINES

FPL Americas Risk Management Working Group

FIX PROTOCOL
INDUSTRY-DRIVEN MESSAGING STANDARD℠

TABLE OF CONTENTS

DISCLAIMER

THE INFORMATION CONTAINED HEREIN AND THE FINANCIAL INFORMATION EXCHANGE PROTOCOL (COLLECTIVELY, THE "FIX PROTOCOL") ARE PROVIDED "AS IS" AND NO PERSON OR ENTITY ASSOCIATED WITH THE FIX PROTOCOL MAKES ANY REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, AS TO THE FIX PROTOCOL (OR THE RESULTS TO BE OBTAINED BY THE USE THEREOF) OR ANY OTHER MATTER AND EACH SUCH PERSON AND ENTITY SPECIFICALLY DISCLAIMS ANY WARRANTY OF ORIGINALITY, ACCURACY, COMPLETENESS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SUCH PERSONS AND ENTITIES DO NOT WARRANT THAT THE FIX PROTOCOL WILL CONFORM TO ANY DESCRIPTION THEREOF OR BE FREE OF ERRORS. THE ENTIRE RISK OF ANY USE OF THE FIX PROTOCOL IS ASSUMED BY THE USER.

NO PERSON OR ENTITY ASSOCIATED WITH THE FIX PROTOCOL SHALL HAVE ANY LIABILITY FOR DAMAGES OF ANY KIND ARISING IN ANY MANNER OUT OF OR IN CONNECTION WITH ANY USER'S USE OF (OR ANY INABILITY TO USE) THE FIX PROTOCOL, WHETHER DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL (INCLUDING, WITHOUT LIMITATION, LOSS OF DATA, LOSS OF USE, CLAIMS OF THIRD PARTIES OR LOST PROFITS OR REVENUES OR OTHER ECONOMIC LOSS), WHETHER IN TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), CONTRACT OR OTHERWISE, WHETHER OR NOT ANY SUCH PERSON OR ENTITY HAS BEEN ADVISED OF, OR OTHERWISE MIGHT HAVE ANTICIPATED THE POSSIBILITY OF, SUCH DAMAGES.

DRAFT OR NOT RATIFIED PROPOSALS (REFER TO PROPOSAL STATUS AND/OR SUBMISSION STATUS ON COVER PAGE) ARE PROVIDED "AS IS" TO INTERESTED PARTIES FOR DISCUSSION ONLY. PARTIES THAT CHOOSE TO IMPLEMENT THIS DRAFT PROPOSAL DO SO AT THEIR OWN RISK. IT IS A DRAFT DOCUMENT AND MAY BE UPDATED, REPLACED, OR MADE OBSOLETE BY OTHER DOCUMENTS AT ANY TIME. THE FPL GLOBAL TECHNICAL COMMITTEE WILL NOT ALLOW EARLY IMPLEMENTATION TO CONSTRAIN ITS ABILITY TO MAKE CHANGES TO THIS SPECIFICATION PRIOR TO FINAL RELEASE. IT IS INAPPROPRIATE TO USE FPL WORKING DRAFTS AS REFERENCE MATERIAL OR TO CITE THEM AS OTHER THAN “WORKS IN PROGRESS”. THE FPL GLOBAL TECHNICAL COMMITTEE WILL ISSUE, UPON COMPLETION OF REVIEW AND RATIFICATION, AN OFFICIAL STATUS ("APPROVED") FOR THE PROPOSAL AND A RELEASE NUMBER.

No proprietary or ownership interest of any kind is granted with respect to the FIX Protocol (or any rights therein).

Objective:

This paper provides guidance on risk management best practices in global electronic trading for institutional market participants. The objective is to provide information around risk management and encourage firms to incorporate best practices in support of their electronic trading platforms across a range of asset classes. The automation of complex electronic trading strategies in a volatile marketplace increasingly demands a rational set of pre-trade and intra-day risk controls, such as those recommended through this paper, to protect the interests of the buy side client, the broker[1] and the integrity of the market.

The risk controls recommended in this paper provide the financial services community with a set of guidelines that aim to systemically minimize the inherent risks associated with executing electronic algorithmic and direct to market (DMA) orders. Using the conventions within the existing framework of the FIX Protocol, firms should be able to implement the guidelines detailed in this document with minimal effort.

This document was developed by the Americas Risk Management Working Group of FIX Protocol Ltd (FPL), with input from Asian and EMEA groups. FPL is the non-profit, industry standards association that owns, maintains and continuously develops the Financial Information eXchange (FIX) Protocol in response to market requirements. FIX is a globally recognized messaging standard enabling the electronic communication of pre-trade, trade and post-trade messages, up until pre-settlement, between financial institutions, primarily investment managers, brokers, exchanges and ECNs/MTFs. The FPL organization is focused on improving the global trading process and all initiatives are ultimately focused on supporting the evolving business needs of the trading community to enable firms to optimize efficiencies and reduce costs.

The main purpose of the FPL Americas Risk Management Working Group is to raise awareness regarding the implications of electronic trading on risk management and to encourage the development and adoption of standardized best practices that help mitigate against risk. This document presents proposed best practices for industry consideration.

Overview:

The objective of applying electronic order risk controls is to prevent situations where a client, the broker and/or the market can be adversely impacted by flawed electronic orders. The scope of this particular set of recommended risk controls is for electronic orders delivered directly to an algorithmic trading product, or to a DMA trading destination. Worked orders (for example, cash single stock and/or program trading) typically rely on the sales trader to make a decision regarding whether to accept or decline a given order due to inherent risk. Additional risk controls will be discussed that address the broker's responsibilities when interacting electronically with an exchange.

[1] *The term "broker" is used generically throughout this paper to refer to the Sell Side Broker Dealer or Futures Commission Merchant (FCM) that facilitates client access to an electronic marketplace.*

The typical client order scenarios that brokers are looking to proactively detect, would include:

- An order where the client has mistakenly sent an exceedingly large quantity (i.e. fat finger).
- An order that will adversely impact the market for a given security.
- An order where the client has incorporated incomplete or conflicting order instructions.
- An order where the symbology cannot be resolved to a single security (ambiguous product lookup).
- An order that is potentially duplicative or unintentionally repeating (i.e. runaway).
- An order where adverse or favorable price moves impact the order while it is working.
- An order that may be stale or may have been replayed by the client or a system.
- Large accrued long or short positions that may result in settlement and/or delivery risk if the client cannot settle the trade.

These scenarios are equally applicable across different asset classes. Appendix A includes a description of the differences between futures and options versus single stocks.

Benefits of Risk Controls:

The absence of appropriate risk controls can have serious adverse implications to maintaining an orderly market.

Dislocation of a market:
Large orders entered in error, have the potential to artificially move the price of a security. Large orders can quickly sweep through posted quote volume and inadvertently drive down/up the price a stock trades. When the error is detected, the price typically recovers to an equilibrium state which can result in serious financial loss to market participants.

Failure to Settle/Deliver:
Large notional value trades executed in error can exceed the ability of one or more counterparties to finance, settle and deliver the trade, leading to further instability in the market.

Conflict between client's intent and order execution:
In the event that an inbound order message incorporates conflicting or incomplete instructions, the sell side broker's system may execute the order in a manner that conflicts with how the client intended the order to trade. Typical examples include orders being executed by the wrong strategy, orders being displayed in the wrong lit and dark venues, and orders executing too aggressively or too passively. In some cases, the client may refuse to accept the resultant trade, leading to the sell side broker accruing an error position.

Trading the wrong security:
Ambiguous results from a product lookup can lead to situations where a sell side broker inadvertently trades a different security than what the client had intended. The risk implications are that the resultant position from the trade executed in the incorrect security has to be unwound, while a subsequent trade in the correct security has to be executed. This situation can result in both parties incurring significant market risk, and can also have market impact implications in the security which a trade was incorrectly executed.

Algorithmic and DMA Order Definitions:

For the purpose of this paper, the following definitions will be applied to distinguish between algorithmic and DMA orders.

Algorithmic Orders:

- Algorithmic orders are strategy oriented products designed to achieve a client's specific investment benchmark.
- The parent order incorporates FIX message content that indicates which strategy and associated parameters the client wants to trade.
- Brokers apply pre-trade risk checks at the parent order.
- Algorithmic orders typically have longer trade horizons and are less sensitive to latency at the parent order level.
- The parent order size is typically larger than a DMA order.
- Algorithmic orders are typically delivered through a FIX interface from either a 3rd party vendor Order Management System (OMS) / Execution Management System (EMS) or the client's proprietary OMS.
- The client's order is routed to a strategy engine, and does not interact directly with the market.
- The algorithm makes all decisions when to place and execute child order slices.

DMA Orders:

- DMA is defined as direct market access.
- DMA orders interact directly with the market.
- In certain jurisdictions, brokers offering buy side clients DMA products are required to apply pre-trade risk checks against all orders in adherence with local regulations.
- DMA orders typically originate through a client's black box trading strategy or client trading algorithm.
- DMA orders are typically for smaller size (for example, 100 to 1000 shares).
- DMA orders are expected to execute either immediately or over a fairly short trade horizon.
- DMA orders are considered latency sensitive.
- Targeted DMA orders are directed to post at a specific venue per the client's instructions.
- Depending on a client's latency tolerance, there are a number of different types of DMA platforms available.
- For the purpose of this discussion, using a Smart Order Router (SOR) is considered a DMA order type, in terms of having a shorter execution horizon, and a lower tolerance for latency.
- Many brokers may route a client directed DMA order through their SOR, which acts as a pass-through to the market per the client's instructions.

DMA Interface Types:

There are a variety of sell side broker DMA platforms available to buy side clients:

- **Broker Gateway Product at the Broker Data Center**
  - Client FIX Session terminates at the gateway located in broker's data center.
  - The broker applies all relevant regulatory pre-trade risk checks and exchange protocol normalization.
  - Broker SOR products are accessed at the broker data center.

- **Broker Gateway Product Co-Located at the Exchange Data Center**
  - Client's trading strategy resides in the co-location rack within exchange or proximity data center.
  - Client's server cross connects to the broker's co-location rack to access the gateway.
  - Gateways are typically deployed on optimized hardware infrastructure including Field Programmed Gate Array (FPGA) and other accelerated hardware solutions.
- **3rd Party Gateway Products:**
  - There are a number of gateway products offered by 3rd party vendors that facilitate direct access arrangements.[2]
  - The client executes using the sell side broker's trading or membership ID.[3]
  - The gateway adheres to all relevant regulatory pre-trade risk checks.
  - An administrative console is provided to the broker to control risk thresholds.
  - Execution reports are drop copied back to the broker.
- **Exchange Managed Pre-Trade Risk Modules**
  - The exchange provides client gateway that applies all pre-trade risk checks.
  - The client executes trades using the broker's MPID or Futures Commission Merchant (FCM) clearing ID.
  - An administrative console is provided to the broker to control risk thresholds.
  - Execution reports are drop copied back to the broker.

The Client/Broker Relationship:

Brokers that receive electronic orders from a client via FIX assume significant trading and regulatory obligations once an order is accepted and a FIX acknowledgement is delivered. A Broker Dealer or FCM is not obligated to immediately accept all orders and should employ risk controls on inbound orders to identify any client order that exceeds a given client or firm risk threshold.

Neither party should entirely rely on their counterparty to implement comprehensive risk controls. It should be expected that both the buy side and sell side will implement appropriate risk controls on their outbound orders. Brokers typically apply variable risk control thresholds to client orders based on a number of factors, including:

- Pre-negotiated instructions from the client.
- The type of orders and asset classes the client trades.
- The maturity of the trading relationship (new client vs. long term relationship).
- Previous history of settlement and/or delivery issues with the client.
- Client's total level of capitalization as an indicator of settlement risk.
- Client's current account holdings (for prime brokerage accounts).
- Risk tolerances may be adjusted in response to concerns over expected market volatility.
- News and/or volatility in a specific security.

[2] *The European definition of 'sponsored access' includes the use of both 3rd party products and exchange risk module.*
[3] *This would include Market Participant Identifier (MPID) or Futures Commissions Merchants (FCM) clearing ID.*

- Volume profiles and trading patterns of particular securities.

Order validation prior to order acceptance is a key line of defense. A key factor to minimize trading risk is to ensure that the correct security is traded. Resolving client symbology often presents a serious challenge to the sell side broker systems. Clients may employ a variety of approaches, including Ticker, RIC, ISIN, Sedol, BB and other symbologies, depending on how the client's security master is structured.

It is the responsibility of the buy side and sell side to reach an agreement in advance, with each party to define and then certify the agreed upon symbology format.

The Broker/Exchange Relationship:

Modern electronic markets provide facilities for registered broker firms to interact directly with the order book and matching engine through electronic connectivity. Each direct exchange line for equities trading is assigned an identifier[4] used to identify the member broker firm executing the trade.

For futures, each direct exchange line will use the exchange assigned execution and clearing IDs of the FCM. It is possible for members of futures exchanges to act in different capacities on behalf of clients requiring direct access. For example, one FCM may execute client trades on a particular exchange but another FCM clears the trades on their behalf. In such a case, the exchange will ask for both IDs of the executing FCM and the clearing FCM to be identified on the exchange line. Many futures exchanges also offer incentives for participants to become non-clearing members (NCMs) that do not have the same capital requirements that an FCM is subject to. In such cases, the NCM must specify the FCM that clears on its behalf on all direct connections to the exchange.

In most jurisdictions, brokers dealers and FCMs directly accessing markets have significant regulatory, clearing, settlement, capital and risk management obligations designed to protect the integrity of the exchange and ensure an orderly market.

In certain markets, broker exchange lines can be used both by the broker to execute orders on their own behalf, or arrangements can be made to allow for external clients executing through an identifier. Under certain cases, a broker will allow clients to establish an exchange connection, whereby the institutional client interacts directly with the market through the broker MPID or FCM clearing ID. This arrangement is known as sponsored access.

Broker interaction with electronic markets:

Broker Executions: Exchange lines terminating between the Broker Data Center and Exchange:

- Used by a broker to execute their own electronic trades (i.e. child orders from algos and/or smart order routers, etc.)

[4] *Identifiers include Market Participant Identifier (MPID), Futures Commissions Merchants (FCM) clearing ID, etc.*

- Used by a broker to execute their own electronic trades through an internal EMS with direct market access destinations.
- Used by a broker to electronically post, hit and take bids/offers in the capacity of a market maker.

Exchange Co-located DMA Products:

- For many DMA arrangements, the client co-locates their trading engine at an exchange, and accesses the market through a broker trading system (also co-located at the exchange) that runs pre-trade risk checks and manages exchange protocol normalization.
- Clients may co-locate their trading engine at an exchange, and access the market through a 3rd party vendor trading system that runs pre-trade risk checks and manages exchange protocol normalization.
- Another approach is sponsored access, where the client can access the exchange directly using pre-trade risk checks provided by the exchange itself. The exchange will typically provide the member firm with an admin console to manage risk limits.
- The parameters used for all of the risk checks for the DMA products listed above are defined, and administered by the member broker, not the client.

For futures and options, the same principles generally apply as equities, and participants that are not FCMs can connect directly to a futures exchange under a sponsored access arrangement. Exchange rules regarding sponsored access vary. Some exchanges allow for direct access by non-members and provide risk management tools that allow the client to be individually identified under the FCM's membership, whereas other exchanges only allow members (non-clearing or general clearing) to connect directly.

Broker Dealer / FCM risk controls applied to orders prior to delivery to the exchange:

Broker Exchange Lines Terminating Between the Broker Data Center and Exchange:

There are a wide range of pre-trade risk checks that a broker will apply at the exchange facing FIX layer, in advance of delivering an order to the exchange:

- Basic pre-trade checks are applied on each individual order leaving the house (order Qty, ADV, notional value, etc.).
- Price checks that calculate +- % difference between order limit price and market price (last traded price, NBBO or previous close, in order of availability or where applicable per asset classes).
- Symbology validation checks are implemented to ensure that the client order matches with a single security. Orders that map to multiple securities must be paused or rejected.
- Duplicative orders check which is based on a duplicate Order ID (FIX Tag 11).
- Validation for specific order types supported by the exchange.
- Leveraging specific order types (limit order vs. market order) to ensure best execution.
- Upstream system monitoring for adverse price moves to prevent market dislocation. Price moves vs. arrival, limit price, and would price (paused back if too far from current market price).

- Short sell regulatory checks (i.e. uptick rule, locates, easy-to-borrow/dynamic locate code check etc.) where applicable per asset class.
- Restricted security trading checks (reject principal orders for security broker if restricted from trading) where applicable per asset class.
- Child orders cannot be larger than the absolute size of the parent order, matching ticket/order instructions.
- Adherence to specific exchange/market structure constraints (market on close, limit on close, market imbalance orders, etc.).
- Venue latency monitoring can indicate possible configuration issues around primary and backup connections.
- Pattern controls can also be implemented to ensure that an upstream trading engine (algo) is in control of their order flow. Runaway checks can monitor the behavior of algorithms to ensure it is working correctly by monitoring cancel/replace rates on a black box trading engine.

Exchange Mandated Risk Checks:

Many exchanges apply risk checks on inbound orders that serve as the "last line of defense", applied after upstream risk checks are applied by the broker or FCM. Depending on the securities traded, and corresponding market structure, the exchanges apply a variety of pre-trade risk checks which may include the following:

- Most exchanges apply order size limits that set a maximum size order that can be placed in the market. Depending on the exchange, order size limits may be set by product class, product, customer/clearing member, outrights, spreads, etc.
- Exchanges typically apply some types of limits that restrict the number of messages that can be sent to the matching engine within a specified period of time. Some exchanges allow trading firms to purchase additional message capacity.
- A number of exchanges have a price banding mechanism that only accepts orders within a specific price range. Price banding is a common feature of futures exchanges. It is intended to avoid dislocation of a market due to erroneously priced orders that are outside a pre-defined tolerance of the current bid/ask and/or last traded price. A few exchanges do not reject orders that are outside the price band if they are from market makers.
- Some exchanges incorporate stop logic functionality that can prevent orders from creating a domino effect in the market.
- A limited number of exchanges support intraday position limits, which set maximum positions a firm can take at any time within the day, but these limits are optional and not mandatory.
- Exchanges also implement circuit breakers, limits on close, limits on open, and market imbalance checks.
- Several futures exchanges convert market and triggered stop orders to limit orders based on a pre-defined price band so as to prevent accidental disruption by trading too far through the order book or accidentally leaving an open market order that may obscure true price discovery. If an exchange does not offer such functionality it is recommended that the broker implement this logic for all clients who trade electronically.

As discussed earlier, it is becoming increasingly common for futures and equities exchanges to provide sophisticated risk management tools that feature some or all of the above and allow an FCM the granularity to set checks for each client that accesses the exchange directly. Such tools allow FCMs to facilitate direct access without having to impose their own or 3rd party risk management tools between the client and the exchange, should they choose to take this approach.

Typical Electronic Order Workflow:

Algorithmic and DMA orders are considered to be low touch order flow. The order is delivered and routed directly to a given destination without human intervention. Automated risk controls can be applied in several points along the order routing path. The intent is to identify faulty orders before they are delivered to a point where they will execute in the market. For DMA orders with short trade horizons and low latency expectations, orders are either immediately accepted or rejected.

Algorithmic orders typically incorporate trading horizons across a relatively long interval. For an algorithmic order, the market impact from pausing an order to verify the instructions with the client would be negligible. For ultra low latency/high frequency trading products, where the typical order size is small and would be expected to execute immediately, the guidelines are that any order that exceeds a given risk tolerance threshold should be rejected outright.

For algorithmic orders where it has been determined to have been entered as the result of a fat fingered error, and/or exceed a client's agreed upon settlement risk, this should be rejected back to the client OMS. For the scenarios where both sides agree that the order is legitimate, the order can be accepted by the sales coverage, and forwarded back into the system. The three primary scenarios are accept, pause and reject as defined below:

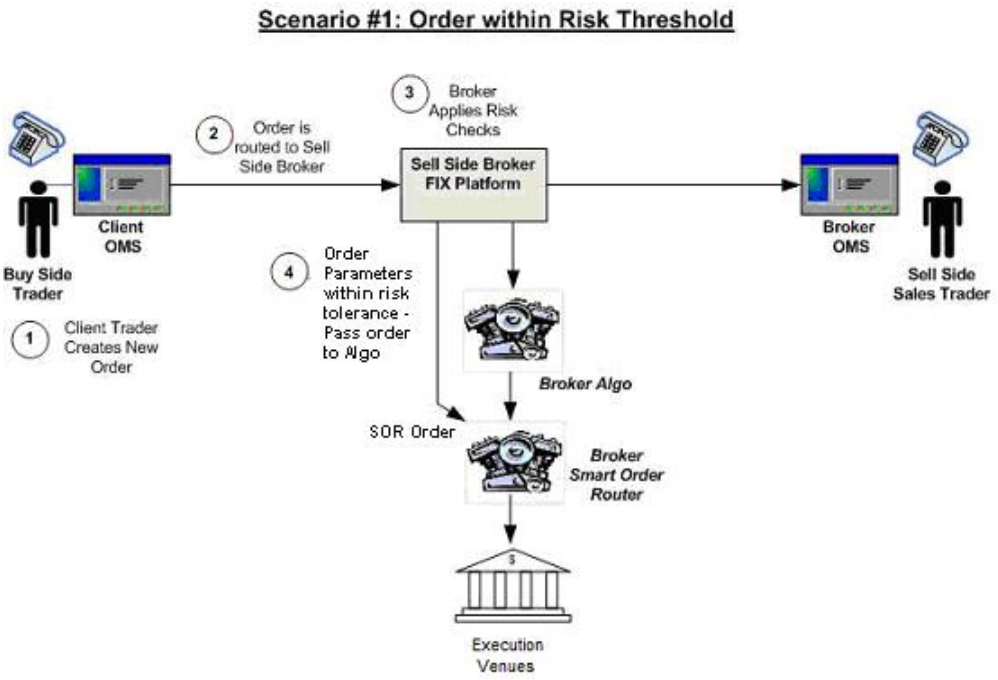
Accept: Orders that fall within prescribed risk parameters are passed directly to their destination.

Pause: The concept of pausing an order is only relevant to algorithmic orders submitted to a broker. Orders that exceed prescribed risk parameters are converted from automatic to manual state and sent to a sales/trader's OMS blotter where a subsequent decision to accept or reject the order will be made. A" pending new" message will be delivered back to the client OMS to indicate that the order is in a paused state, pending some action to be taken by the sell side broker. In the event that the order is ultimately accepted, a corresponding acknowledgement message will be delivered from the broker system to the buy side client OMS. It should be noted that at this time, not all proprietary client and 3rd party OMS products can support a 'pending new' message so the generation of this message by brokers will be subject to bilateral agreement between the brokers and their clients.

Reject: Orders for which the client acknowledges are in error, or for which the broker does not wish to accept, are rejected back to the client's OMS or EMS.

The next few pages illustrate workflows for each of the scenarios described above.

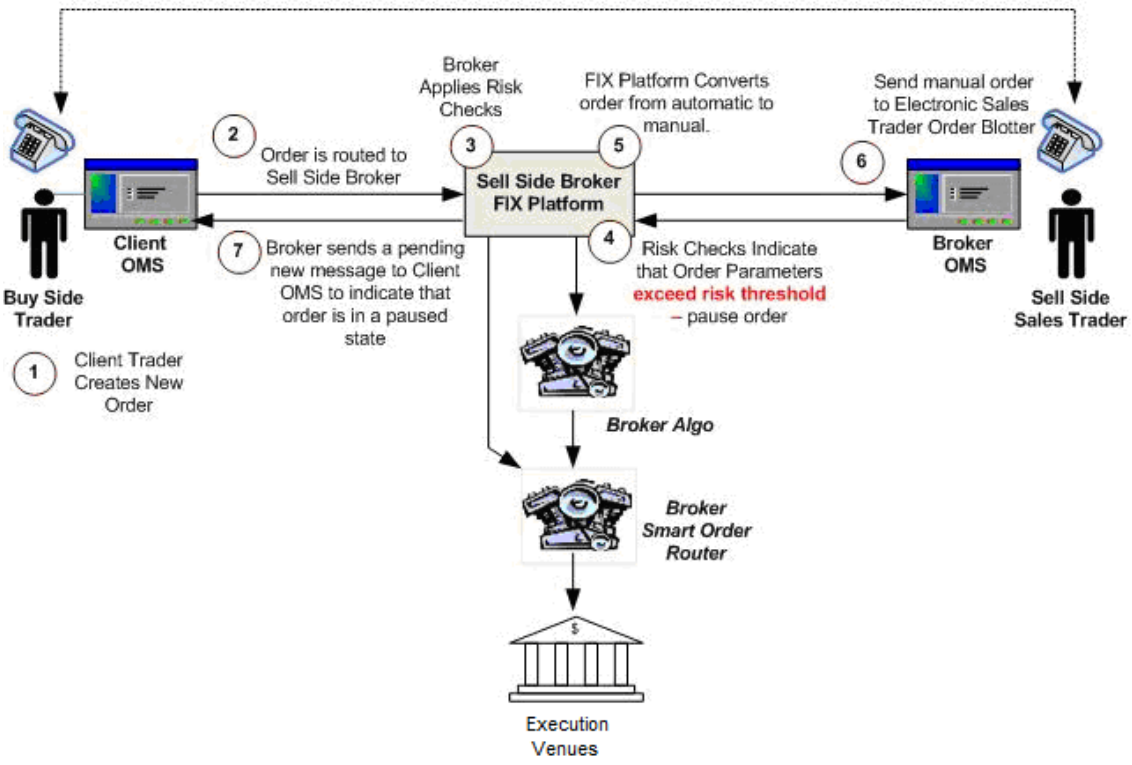
The following diagram illustrates the workflow for the first scenario where an algorithmic order passes the internal risk check and is accepted.



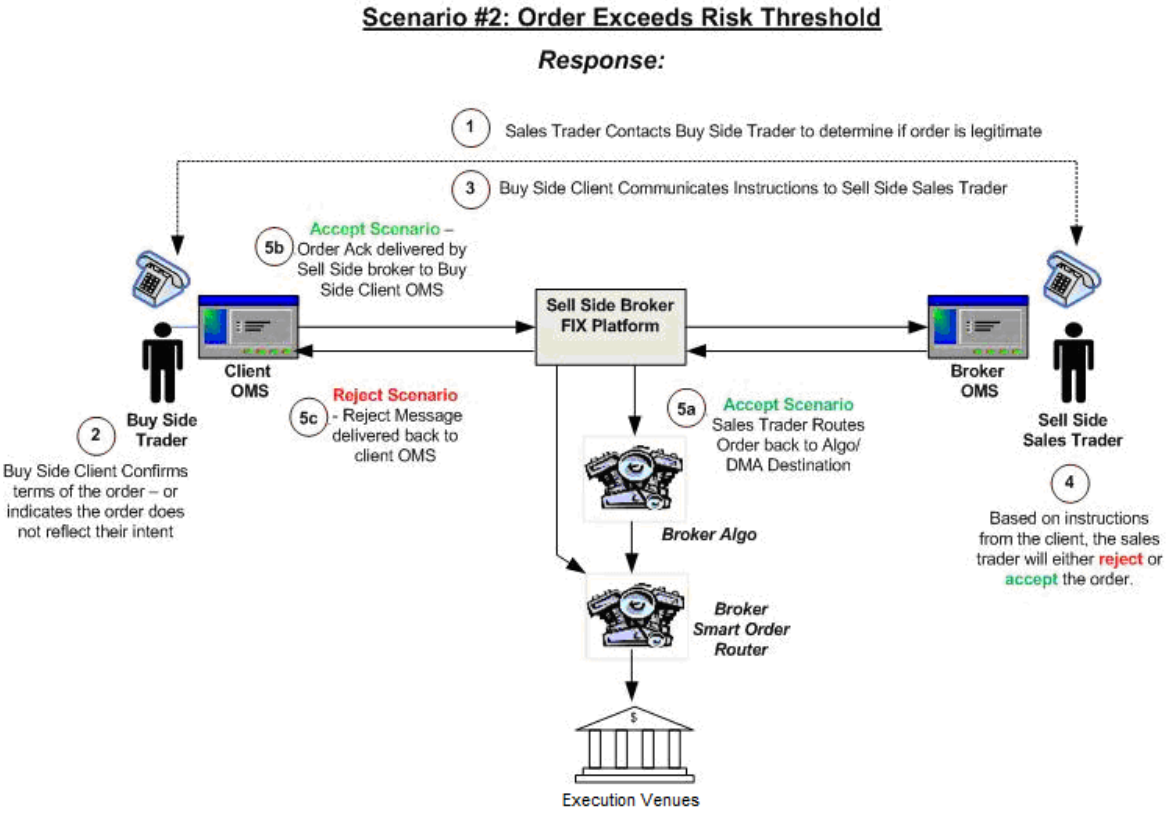
The next two diagrams illustrate the scenario where an order exceeds the prescribed risk threshold and is paused. The first diagram illustrates the workflow around detection.

Scenario #2: Order Exceeds Risk Threshold

Detection:

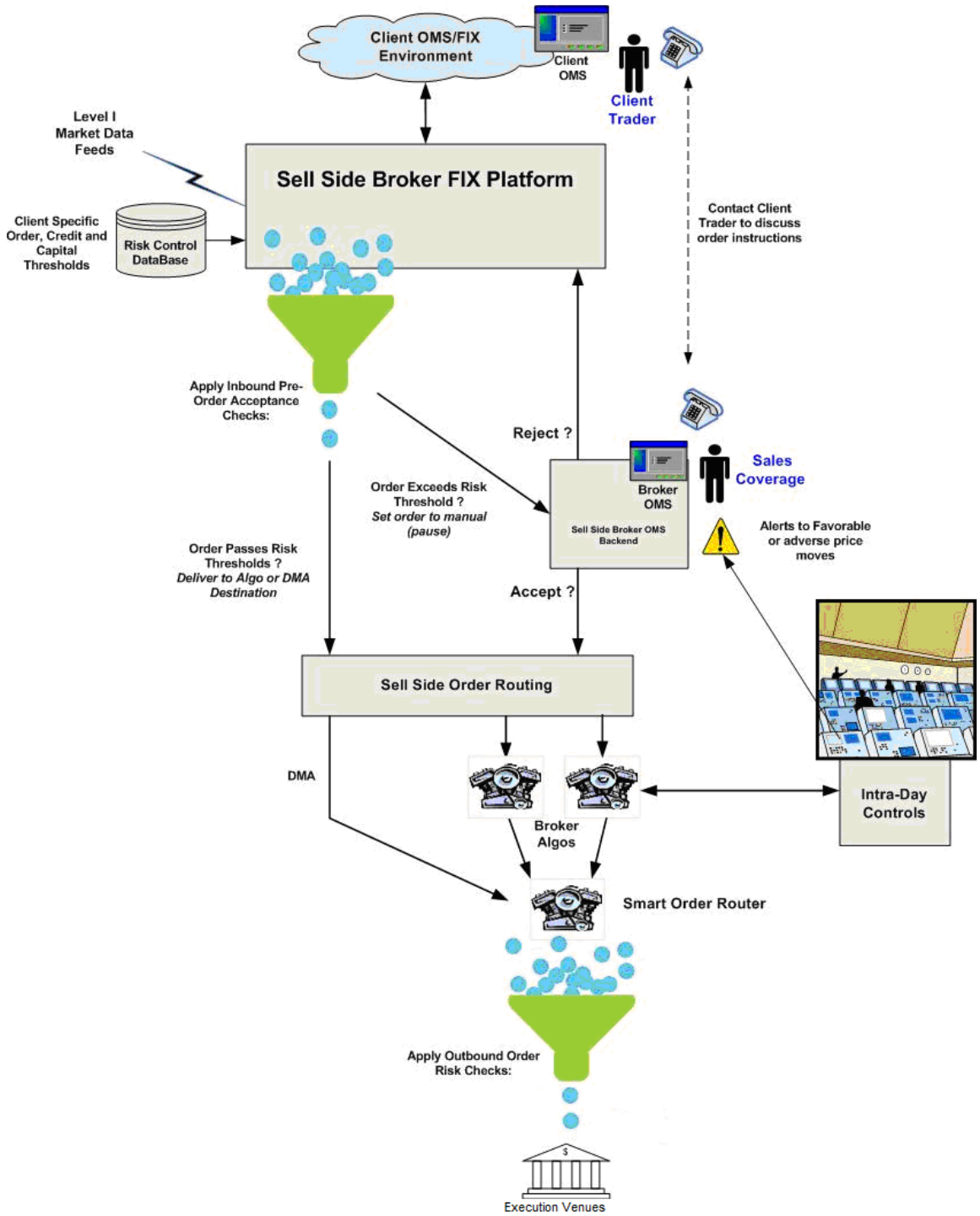


This second diagram explains the response. The key component of the workflow is that when an order is paused, the sales trader should evaluate the order, confer with the client as well as internal parties in compliance and supervision to determine whether to accept or reject the order.



The diagram below reflects the collective electronic trading interface between the client and broker with corresponding pre-trade and intra-day risk controls.

High Level Electronic Order Risk Controls



Order Pausing: Interaction between the Broker and Client OMS:

As sell side broker risk management systems become more comprehensive, particularly around broker provided execution algorithms, it is important to convey more information regarding algorithm generated risk management events. These algorithm-generated events are a separate category of risk management compared to the basic "Order Exceeds Limit" type of fat finger rejection already enumerated in OrdRejReason (103). To clearly denote such events, our approach is to leverage OrdRejReason(103) with a new defined value for "algorithm risk threshold breached".

The FIX Protocol clearly defines that for operations such as a new order, cancel and or cancel/replace, there is a requirement for the message recipient to immediately generate a corresponding response message. In the event that the broker has determined that an order will be paused within their systems, it is important to generate a response message to indicate, to the buy side client OMS. that the order has been paused allowing the client OMS to be in sync regarding the state of the order.

For any new orders (35=D) where the client order has breached a broker's pre-determined limits and has been paused within the broker's internal systems, the FPL Americas Risk Management Working Group proposes the generation of a pending new message (35=8, 39=A) with the addition of OrdRejReason on the message (103=21, Algorithm risk threshold breached) to denote that the order has been paused as opposed to accepted or rejected.

It is recommended that the broker incorporate additional information in the Text (58) field on the pending new message including the algorithmic risk check that failed and the parameters, eg. "Aggregate Limit Breach", "exceeds x% ADV", or other details indicating the reason why the order has been paused. The format of the data delivered in the Text (58) field will be structured so as to incorporate the necessary information across a pre-defined character space.

It is suggested that the sell side brokers will work with the 3rd Party OMS/EMS vendors and buy side clients running proprietary OMS/EMS systems to correctly handle the pending new message and additional OrderRejReason value.

The client OMS should have the ability to cancel an order in a pending new state. The sell side broker platform must accept and act accordingly in response to a client attempting to cancel an order that is in a paused state. This is not only true for orders that exceed a risk threshold, but equally relevant for orders that may be received, but not yet accepted by a system (i.e. an algo order for the U.S. market delivered by a European client at 4:00am EST). The expectation is that the client side OMS will respond to the pause message and provide the buy side trader with an indication that the order has been paused, along with the relevant information as to what threshold has been exceeded.

It is understood that at this time, the number of buy side/sell side systems currently supporting the implementation of the "Pending New" message type, and associated workflow is relatively small. The majority of buy sides are not currently running order management systems that supports the "Pending New" message. It should be highlighted that whilst the implementation of "Pending New" is recommended, the broker dealer will not be responsible for executing the order until an acknowledgement message is delivered back to the client.

Following the standard workflow of "New Order Single" followed by "Accept" or "Reject", the buy side client must be aware that an order is not be considered to be "working in the market" until an acceptance message is sent by the broker.

The "Pending New" message workflow is pre order acceptance. For buy side clients who do not currently support the "Pending New" message type the broker will need to feedback indication of any pre-trade limit check failure by another means. The most likely alternative would be through a phone conversation.

Implementation of Risk Controls:

To monitor and manage risk, market participants generally have risk controls incorporated into their trading platforms. Implementations include controls to monitor trading on a pre-trade (i.e. order by order limits) and intra-day basis (i.e. trading style, capital requirements).

FPL recommends the implementation of pre and post-trade risk controls to limit financial exposure and ensure compliance with the rules of the marketplace.

Pre Order Acceptance Risk Controls:

“Pre Order Acceptance” risk controls are typically applied on receipt of the order, prior to an acknowledgement being generated. In the event that an order passes these initial risk checks, the order will be accepted and delivered to a downstream algorithmic or DMA system. Orders that fail a given risk criteria may be rejected outright, or set to manual and passed to a sales trader who may choose to accept the order, after conferring with the client. Unless stated otherwise, it can be assumed that these controls are applicable for all asset classes covered in this paper.

1. **Symbology Validation:** A fundamental risk check is to ensure that the symbology information incorporated on the inbound client order resolves to a single security. In the event that an ambiguous product lookup result occurs, the order must be either rejected, or paused, to allow the sales trader to speak with the client to ensure that the appropriate security is selected.

   For clients trading dually listed securities that trade in multiple markets, pre-defined default conditions must be established to designate the primary market where the client wishes to trade. As an example, unless the client includes specific tags such as FIX Tag 100 (ExDestination), or FIX Tag 15 (Currency), the sell side broker should apply default conditions to resolve to the agreed upon primary market.

   Other techniques used to identify the correct security and venue, include the use of:

   - Exchange identifiers (including US ticker symbols)
   - Bloomberg symbols
   - Reuters codes

   These parameters may be used on their own, to identify a specific listing of an instrument. It should be noted ISINs and SEDOLs are not always listing-specific and so

should be accompanied by ExDestination or SecurityExchange. To apply further distinction, SecurityExchange (Tag 207) should be used to help identify a specific listing of an instrument, and ExDestination (Tag 100) should be used to identify the target trading venue.

2. **Order Quantity:** An extremely large order quantity is often a strong indicator of a fat finger error. Large orders that are determined to be legitimate should be carefully checked since the broker may want to advise the client on the optimum way to execute a large order. Additionally, unusually small orders should be flagged as well as they can also be the result of a fat finger error. More generally, an 'unusual' order quantity should be flagged where 'unusual' means both for the product being traded, and the client trading it.

3. **Notional Value:** For many products, such as equities securities, notional value is defined as (price * order quantity). An order with an extremely high notional order value may also be an indicator of a client "fat finger" error. Brokers executing client orders with excessive notional values may be exposed to settlement risk. For futures trading, notional value is not typically used for pre order acceptance risk management of futures due to additional static data required for the multiplier of the futures contract. An exception may occur where futures are used specifically to provide a hedge for an equity portfolio.

4. **ADV:** Defined as Average Daily Volume, ADV is an important factor that indicates the extent that a client order may influence the market price of the security. Client orders that represent a very high percentage of ADV, may consume a significant amount of available liquidity in the market resulting in an unfavorable average execution price and/or temporary or lasting impact to the market. For futures and options, any ADV checks should reference the volume in the specific contract since it varies across individual maturities or strikes.

5. **Price Limit:** A bad limit price on an order can have an extremely adverse impact on execution quality or result in the order not being "marketable". A limit price that is significantly far from the prevailing market is often an indicator of a fat finger client error.

6. **Validation of Order Instructions:** A client order may contain conflicting or illogical combinations of order instructions and or algo parameters that create a level of ambiguity for how an algo should trade that order. The broker FIX platform should typically incorporate order validation checks to detect this type of scenario.

7. **Stale Order Checks:** Disparity between order sending time and order receipt time indicates a potential system problem between the client system sending the order and the broker system receiving an order. A stale order represents risk since the market may have moved or changed during the interval when the order delivery was delayed.

8. **Duplicate Order Checks:** A client OMS/EMS or black box trading system may inadvertently send a duplicate order. Two orders delivered on the same day with the same ClientOrderId would typically indicate an error at the client OMS or strategy. The second order should always be rejected. Regardless of whether the order details are the same on both orders, this is an invalid situation in FIX and so the broker's FIX engine should detect this and reject the second order.

Intra-Day Risk Controls:

Intra-Day Risk Controls are typically applied to working orders that have passed the initial pre order acceptance control checks. The broker has the option to "pause" the order and/or stop the order from executing further. The primary function of intra-day risk checks is to protect the client and/or broker from executing an order where their aggregate position may result in settlement or delivery risk, or when market conditions have significantly changed since the time that the order was accepted. Additional considerations include the resultant change to a client's aggregate long/short position in the event that an order executes. There are direct implications to settlement and delivery risk in the event that a client's aggregate position grows long or short past a given threshold. The thresholds applied for intra-day position and credit checks would be specific to each individual client. Factors that would be considered include capitalization, and the maturity of the electronic trading relationship.

Unless stated otherwise it can be assumed that these controls are applicable for all asset classes covered in this paper.

1. **Favorable/Adverse Price Moves:** The broker tracks the trading price for a given security against arrival price. A significant move in either direction may indicate that the conditions under which the client created the original order should be reconsidered.

2. **Position Limit:** These include dynamic position checks executed to evaluate the instantaneous position a client has accrued. It is common for futures and options to use a position limit as a proxy for credit checks due to the additional margin information required to correctly assess the client's exposure (see point 3).

3. **Credit / Capital Checks:** These checks are related to position checks in that they are applied to evaluate the potential settlement obligation that a client would incur should the order execute. Credit check thresholds are specific to a given client. The required financial risk management controls and supervisory procedures must include those reasonably designed to prevent the entry of orders that exceed appropriate pre-set credit or capital thresholds. Credit / capital checks for futures and options are typically performed on a post trade basis due to the use of initial margin and / or SPAN methodology required to calculate the actual capital required for the position. Please see footnote 1 in the Appendix on page 23 for further information on SPAN technology.

Price-Limit Controls:

A buy side trader may choose to direct either a Limit or a Market order to a broker's algorithm or a DMA pipe. While client-specified price limits, when determined diligently, provide an effective level of control against market displacement, specifying them on every order is not logistically easy for all types of clients and trading situations. It is, however, within the powers of a broker to make sure that each outbound order to a market center is protected by a price limit. When a buy side trader sends an order with a MKT instruction on it, a trading algorithm may protect each "child" order with a limit that is reasonable within prevailing market conditions at the time of its generation and meets the objectives and constraints of the strategy. A MKT DMA order may be protected by a synthetic aggressively priced "market-able" limit price, calculated based on the price at the time of the order's arrival. One possible consequence of such an approach would be a MKT order that doesn't

get fully filled due to a protection price being reached. A broker should make sure that such situations generate an alert to the trading desk and are subsequently resolved with a client. Care should also be taken not to post such an order at the protection price, unless this is a behavior preferred by a client. Note that many futures exchanges offer price protection in the form of (a) converting market and stop orders to a limit order at the last trade price, and (b) through the setting of price banding. Such protections prevent accidental disruption of the market by trading outside of a closely defined range around the last traded price. Where an exchange does not offer such functionality, it is good practice for the broker to provide such controls for both client DMA and the output from broker algorithms.[5] Such controls are applicable to all asset classes covered in this paper.

Pattern Controls:

There are patterns and behaviors that indicate a client's system may be in distress and that orders should be paused and or rejected. There are also pattern indicators that can be used to detect system anomalies, including order timing, repeated orders and cancel/replace ratios. Unless stated otherwise, it can be assumed that these controls are applicable for all asset classes covered in this paper.

1. **Runaway Checks:** The purpose of this type of check is to identify the scenario where a client's trading algorithm has stopped working correctly and/or is no longer under control of the client. One fundamental check is for trading systems to evaluate historical client trading patterns and order, cancel/replace rates for a given client. Significant differentials from historical trading patterns often are a good indicator of a potentially serious fault on the client side OMS or black box trading engine. Specific examples of metrics to compare are:
   - The ratio of order cancels or cancel/replaces to new orders is unusually high relative to the client's historical trading patterns.
   - The ratio of orders to executions is unusually high.
   - Multiple orders being created over a short period of time with the same details.
   - Trading patterns indicating the algorithm may have gone into a loop (e.g. repeatedly sending an order and then canceling it).

Assessing Current Risk Management Practices:

It is recommended that firms perform an assessment of their current electronic trading platforms and their ability to manage risk. This analysis should include reviews of firm's current implementation against the recommended set of controls detailed in this document as well as an assessment of current internal policies, procedures and the governance model around risk.

Key areas of focus:

1. Understanding the effectiveness of risk controls in the current platform.
2. Reviewing current risk control settings in the platform.
3. Evaluating the current process around limit change approvals

[5] *In Europe, ESMA goes further than this and states that brokers must have such controls to ensure orderly behavior on the market.*

Risk Management Process and Procedures:

Buy side

It is recommended that buy side firms discuss their risk parameter settings with all of their broker counterparties. Brokers tend to have default risk parameter settings for their platforms but generally these parameters can be overridden on a per client basis.

Key areas of focus:

1. Understand how your broker counterparties have set your firm's various risk control limits.
2. Review broker counterparties' ability to manage risk in terms of technology, process and procedures.

Sell side

Sell Side broker dealers/FCMs should use the **Risk Control Matrix (see next page)** to document their risk parameters settings with all of their clients. Sell side broker dealers and FCMs should implement the appropriate roles, services tools and approval processes to effectively manage risk controls in their trading platform.

Key areas of focus:

1. Regularly review client and default risk control settings to ensure they are current with market conditions.
2. Implement new and existing client limit approval change process.
   a. Ensure that requests to Approvers include basic know your client information and are sent in a format that can be stored for future review.

Risk Control Matrix:

The grid included below reflects a recommended matrix of risk control factors that should be applied. It is expected that the specific values will vary on a per client basis. Please note that any limits that are triggered by the matrix below will result in subsequent actions – Accept, Pause or Reject – which are further described on pages 11-15 of this document.

Flow Types	Pre Order Acceptance Controls					Intra Day Controls			Pattern Controls	
	Max Shares / Contracts	Notional Value Checks	ADV Checks	Price Limit Checks	Stale Order Checks	Favorable and Adverse Price Moves	Position Limit Checks	Credit / Capital Checks	Runaway Checks	Duplicate Order Checks
DMA	SS VOL FUT	SS VOL	SS	SS VOL FUT	SS VOL FUT	N/A	SS FUT	SS VOL FUT	SS VOL FUT	SS VOL FUT
Algorithmic	SS VOL FUT	SS VOL	SS FUT	SS VOL	SS VOL FUT	SS VOL FUT	SS FUT	SS VOL FUT	SS VOL FUT	SS VOL FUT
Low Latency	SS VOL FUT	SS VOL	SS	SS VOL FUT	SS VOL FUT	N/A	SS FUT	SS VOL FUT	SS VOL FUT	SS VOL FUT

SS = Single Stock
VOL = Options
FUT = Futures

We welcome your feedback on this document so please send any comments / questions to fpl@fixprotocol.org.

APPENDIX A:

Futures and Options vs. Single Stocks:

This paper covers the pre-trade risk controls for stocks, options and futures. There are a number of specific product and market structure features specific to futures and options trading that should be considered.

Futures and options trade in numbers of contracts, rather than shares. Each contract is defined by the exchange where it trades and has a multiplier, which is typically expressed in one of the following ways:

- a dollar value for financial futures and options.
- a defined quantity of an underlying commodity.
- a number of underlying shares for single stock options.

For example, the contract size for the Emini S&P 500 future is $50 per index point. If the future is trading at 1200, the notional value of the contract is $60,000 (50 x 1200). Other futures trades have more complicated notional calculations. For example, fixed income futures and options typically use a price calculated based on yield, as well as a percentage of par of the underlying asset.

Pre-trade risk checks for futures are often based on margin requirements since the settlement of a futures trade is not based on its notional value. Each participant settles an initial margin value defined by the exchange on which the contract trades, making futures instruments inherently leveraged. The margin requirements for options are typically calculated using SPAN[6] methodology. Margin checks are not typically used in pre-trade risk management for future and options due to the complexity of the calculation and the static data required.

Since the trading and clearing of a futures contract is typically tied to a specific exchange and their clearing house, there is currently no concept of smart order routing for futures. Where alternative versions of a particular futures instrument are offered on different exchanges they are not currently fungible. For U.S. single stock options, the Options Clearing Corporate facilitates central clearing across multiple execution venues, and smart order routing techniques can be applied.

Due to the complexity of notional calculations across various futures and options contracts, it is typical to set pre-trade risk management limits using the number of contracts rather than notional value.

Similar to the FPL recommended guidelines for stocks, futures limits can be implemented for single order and aggregate or cumulative quantities. Additionally, limit alerts can be triggered by both soft and hard limits. Although futures and options contracts have individual maturities, it is typical to treat the underlying product as a single security and apply the same limits across all maturities as though they were the same instrument.

---

[6] *Standard Portfolio Analysis of Risk, or SPAN, is the leading margining system adopted by futures and options exchanges globally. Originally developed by the Chicago Mercantile Exchange, it is based on a sophisticated set of algorithms that determine margin based on a total portfolio assessment of the one-day risk for a trader's account.*