# Regulatory Oversight and Automated Trading Design: Elements of Consideration

Andrea M. Corcoran
John C. Lawton

## INTRODUCTION

One of the major challenges currently facing regulatory authorities around the world is the need to adapt existing programs and to develop new programs for the oversight of automated trading systems. New screen-based trading systems continue to be introduced and the volume of trading on existing systems continues to grow.[1] It is too early to tell if the movement of substantial trading activity to automated venues will or should fundamentally alter the concerns of regulators and/or the persons subject to regulatory intervention.

Traditionally, financial regulation has centered on customer protection and market integrity (including financial integrity). In the United States, customer protection regulation has focused primarily on the fiduciary duties of regulated intermediaries who undertake transactions as agents of customers. Financial integrity regulation has focused primarily on the protection of customer funds and protection against systemic risk. Regulators seek to ensure, for example, that market participants receive adequate disclosure of relevant information; that market prices are free from manipulation; and that funds are not lost due to the failure of a financial intermediary, the default of a counterparty, or the peculations of a custodian. The advent of automated trading should not change these fundamental objectives of regulation. It may, however, shift the focus of regulatory attention and the mechanisms by which these goals are achieved.

[1] The following exchanges used automated systems to trade futures and/or futures options as of January 1992. Average daily volume is in parentheses (Source: ***Futures Magazine,*** January 1992, Vol. XXI, No. 2, pp. 51–52): Deutsche Terminborse (V: 76,573); Irish Futures and Options Exchange (V: 300); London Futures and Options Exchange (V: 2,600); London International Financial Futures Exchange (V: 7,334); Mercado de Futuros Financieros (V: 4,512); New Zealand Futures and Options Exchange (V: 3,157); Swiss Options and Financial Futures Exchange (V: 43,400); Sydney Futures Exchange (V: 2,012); Tokyo Grain Exchange (V: 40,400); Tokyo International Financial Futures Exchange (V: 81,301); Tokyo Commodity Exchange (V: 3,402); Tokyo Stock Exchange (V: 56,068). In 1992, the Chicago Mercantile Exchange (CME) and the Chicago Board of Trade (CBOT) launched the Globex system (V: 2,000) and CBOT also began trading through the Project A system. The New York Mercantile Exchange expects to launch its NYMEX ACCESS system in 1993. The views expressed herein are solely those of the authors and do not necessarily reflect those of the Commodity Futures Trading Commission or the Division of Trading and Markets.

---

*Andrea M. Corcoran is Director of the Division of Trading and Markets at the Commodity Futures Trading Commission.*

*John C. Lawton is Associate Director of the Division of Trading and Markets at the Commodity Futures Trading Commission.*

The Journal of Futures Markets, Vol. 13, No. 2, 213–222 (1993)

CCC 0270-7314/93/020213-10

In 1990, the International Organization of Securities Commissions (IOSCO) adopted ten Principles for the Oversight of Screen-Based Trading Systems for Derivative Products.[2] The Principles and the accompanying Report discuss the following matters relevant to such systems: the need to define potentially applicable regulatory standards; market transparency; order execution algorithms; operational issues including capacity and response time; system vulnerability issues such as security procedures and backup facilities; system access; financial integrity; surveillance; relevant disclosure including disclosure of liability for malfunctions; the role of system providers including designers and communications suppliers not traditionally subject to regulatory programs; and the allocation among regulators of responsibility for terminals located in different jurisdictions. The Report was prepared by Working Party 7, chaired by the commodity Futures Trading Commission (CFTC), and was the result of a cooperative effort by the representatives of a number of jurisdictions.[3] It set forth broad guidelines and a framework for analysis while recognizing that regulatory approaches may vary among jurisdictions.

This article examines the regulatory implications resulting from some of the elements of the design of screen based systems. The article focuses on three broad categories of design features: access, order execution algorithms, and relationships to other systems, and suggests that how these features function will affect determinations as to the optimal level or degree of oversight of the system..

**Access**

Following is a listing of some system features in the area of access that impact oversight.

1. Placement of terminals
   a. with exchange officials
   b. with exchange members
   c. with nonmembers
2. Location of terminals
   a. on the exchange premises
   b. at remote locations in a single jurisdiction
   c. in multiple jurisdictions
3. Terminal operators
   a. exchange members
   b. employees of exchange members
   c. nonmember users
4. Activities permitted terminal operators
   a. proprietary trading only
   b. customer trading only
   c. both proprietary and customer trading ("dual trading")
   d. trading in all instruments on the system
   e. trading in certain instruments only
   f. trading only on one system
   g. contemporaneous trading on more than one system
   h. accepting orders directly from customers
   i. accepting orders from order-taking intermediaries
   j. communicating directly with other terminal operators

[2] IOSCO Technical Committee, *Screen-Based Trading Systems for Derivative Products* (June 1990). These principles are attached as Appendix 1.

[3] Jurisdictions represented on the Working Party included Australia, France, Italy, Japan, Switzerland, the United Kingdom, the United States, and West Germany. Ms. Corcoran chaired the working party for the CFTC.

The potential differences in design features that affect access are reflected in two systems already approved by the CFTC—the Chicago Mercantile Exchange's and Chicago Board of Trade's Globex system and the Amex Commodities Corporation's Electronic Limit Order System (ELOS).[4] A brief outline of some of the differences in the area of access between the two systems follows.

1. Globex terminals are available to all CME and CBOT members and certain member affiliates and arrangements can be made to receive multiple terminals. The ELOS will make terminals available to only the Board Broker (a member firm appointed by the exchange to enter orders into the system).
2. Globex terminals are located at sites around the world. ELOS terminals will be located only at exchange-controlled facilities in New York City.
3. Globex allows orders to be entered by individual members and by employees of member firms. ELOS will allow orders to be entered by employees of the Board Broker only.
4. Globex permits some terminal operators to dual trade; other terminal operators are limited to proprietary trading only; while still others are limited to customer trading only. Terminal operators are permitted to speak directly to customers. ELOS terminal operators will execute customer business only. They will be permitted, however, to handle both cash market and derivative market orders from customers at the same time. At least initially, they will not speak directly to customers but receive instructions from separate order-takers.
5. Each member firm in the Globex system is responsible for regulatory compliance by its terminal operators. On ELOS, the Board Broker will be the only member firm having responsibility for compliance by terminal operators.
6. Globex operates after hours; ELOS will operate during regular trading hours.

Of course, the differences between these two systems do not cover the entire range of different design possibilities. For example, a system could provide terminals directly to non-member customers or place no limitation on who can act as a terminal operator.

*Regulatory Implications of Access Features*

Certain access features make supervision easier. These features can be outside or inside the system. On ELOS, for example, there will be external controls. All terminals will be operated by the personnel of a single entity at an exchange-controlled location. Thus, fewer steps will be necessary to prevent unauthorized access than on a system with remote terminals connected by an international network.

Other systems may have internal controls. That is, special features may be programmed into a system to control access. For instance, system developers have investigated the use of identification devices based on unique individual characteristics such as fingerprints to assure that only the assigned individual can log-on at a particular terminal. Such features could reduce the need for routine visual oversight. Similarly, restrictions on what an individual can do once logged-on, such as limiting trading by particular terminal operators or through particular terminals to certain contracts or certain aggregate exposure levels,

[4] Rules for the implementation of CME trading on Globex were approved by the CFTC on February 2, 1989. For a description of the system see the "Chicago Mercantile Exchange's Proposed Globex Trading System" prepared by the CFTC Division of Trading and Markets (T&M) dated February 2, 1989. Rules governing trading on ELOS were approved by the CFTC on September 26, 1989. For a description of the system see "Application of the Amex Commodities Corporation for Designation as a Contract Market in Ten-Year Treasury Note Futures contracts" prepared by T&M dated September 19, 1989. Rules for the implementation of CBOT trading on Globex were approved by the CFTC on June 8, 1992.

could be programmed into a system and thereby reduce the need for certain types of supervisory controls. Provision also could be made for automatic log-outs under certain circumstances.

The types of access permitted to a system and the means by which access controls are enforced can affect the degree and manner of regulatory oversight necessary. For example, restrictions as to whom access is available may affect: fitness and competency requirements of terminal operators; supervision requirements for firms which receive terminals; and operational requirements for the system.

A regulatory authority might impose one set of requirements on a system where terminal operators deal directly with customers and another set of regulations where terminal operators are under the direct supervision of the exchange, are not permitted to enter proprietary orders, do not deal directly with customers, and have no discretion in the handling of orders. (This is consistent with current practice in the United States where persons performing only clerical functions on the floor of an exchange or upstairs at a firm are not subject to CFTC registration requirements.) Determining the particular combination of terminal operator functions and system features which might or might not trigger licensing requirements for operators could result in the lines of regulatory oversight being drawn somewhat differently than is currently done for upstairs operations related to floor-based markets.

Limitations on the type of access permitted could affect the type of supervision needed to be exercised by firms and their regulators. For instance, suppose the system could be programmed to assign all orders from a particular terminal to a predesignated account or accounts. If the accounts for a particular terminal are proprietary only, the optimal supervisory arrangements might differ from those that would be advisable if customer orders are allowed at that terminal.

The nature of a system also could make the regulation of certain operational aspects unnecessary. For example, performance standards regarding response time differentials from different locations may be necessary for a system that allows terminals in remote locations. However, such standards would not be necessary if all terminals are located in the same building. Similarly, if more sophisticated access control features are programmed into a system, fewer human supervisory elements may be needed, but more technical operational concerns may become regulatory issues.

The following summarizes the potential regulatory implications of certain access features:

| Access Feature | Supervisory Effect |
|---|---|
| 1. Distribution of terminals | The more individuals and entities that receive terminals, the greater the potential demand on supervisory resources. |
| 2. Location of terminals | The more dispersed the location of terminals, the greater the potential demand on supervisory resources. |
| 3. Authorization to operate terminals | The more individuals authorized to operate terminals, the greater the potential demand on supervisory resources. |
| 4. Activities of terminal operators | |

| | |
|---|---|
| a. Principal/Agency Trading | Dual trading may create greater demand on supervisory resources than does trading on behalf of customers which in turn may create greater demand than proprietary trading only. |
| b. Single/Multiple Instruments | The ability to trade many instruments may create greater demand on supervisory resources than the ability to trade only one. |
| c. Direct contact with customers | Terminal operators who deal directly with customers may create greater demand on supervisory resources than those who deal through order-taking intermediaries. |
| d. Direct contact with other terminal operators | Terminal operators who can communicate with one another may create greater demand on supervisory resources than those who cannot. |

As access to a system increases, the need for supervisory safeguards from a customer protection standpoint also increases, up to the point that customers receive direct access. At that point, the need for customer protection safeguards may diminish or disappear but other concerns from a market integrity standpoint may increase. Since the end user in an open access system may not be a regulated intermediary and may not be identified to other users, counterparties using such a system may wish for their own protection to have all users subject to net worth requirements or financial controls. This would be a profound expansion of current regulatory practice which presently addresses the financial integrity of intermediaries but not that of end users. As traders, end users currently *are* subject to antimanipulation requirements.

**Order Execution Algorithm**

The term *order execution algorithm* refers to the set of rules governing the processing and execution or orders entered into a screen-based system. It determines the degree of transparency of bids and offers and includes procedures for determining for each trade: the identity of the parties, the price, the quantity, and the time of execution.

A wide variety of execution formulas is possible. The algorithm may disclose the identity of the parties entering an order to other users or such parties may remain anonymous. Orders may be matched by the system in accordance with certain rules of priority or participants may be able to select the counterparty. The model may expose the entire quantity (as in ELOS) or it may permit portions of an order to be hidden (as in Globex). The same system may use a different algorithm at the open and during the rest of the trading session.

To illustrate, Globex uses an opening procedure whereby the maximum number of contracts possible will be executed at a single market-clearing price. For the rest of the session, it uses a price/time priority anonymous order matching system. That is, bids are assigned priority from the highest price to the lowest; offers are assigned priority from the lowest price to the highest; among orders at the same price, priority is assigned according to time of entry. The identity of the party placing the order is not revealed. The London International Financial Futures Exchange's Automated Pit Trading System

(APT) uses an algorithm under which the identity of the parties is revealed to the market but executions are allocated among all orders at the same price regardless of entry time. Orders expire automatically on APT every 10 seconds unless refreshed.

The nature of the algorithm is a key factor in determining the potential for trading abuses. An order execution algorithm in a screen-based trading system, in effect, acts as a substitute for certain external floor trading rules by automating certain requirements relative to the type of auction, the degree of competition among orders, and the amount of transparency. Assuming that the algorithm cannot be altered or tampered with, certain trading abuses are impossible where certain algorithms are used. In such cases, the concern of regulators for enforcing the trading rules would become, at least in part, a pure mechanical concern that the approved algorithm is, in fact, the algorithm actually in use by the system. Other abuses, however, may be facilitated unless additional features are added.

To illustrate, trading outside regular hours (kerb trading) should be impossible under automated systems. Prearranged trading may be more or less difficult under automated systems. For example, prearranged trading would be very difficult under a single-price algorithm. It might be relatively easy in a counterparty selection system with terminals at remote locations, especially if the terminal operators are allowed to communicate directly with one another. Similarly, abuses involving the disclosure of or withholding of a customer order might be easier under such circumstances.

An order execution algorithm may contain ancillary features specifically designed to combat abuses. For example, automated systems should be capable of producing a superior audit trail. Such an audit trail should contain a precisely timed and sequenced record of every entry, modification, cancellation, and execution which can be used to generate exception reports for study by supervisory authorities. Preprogrammed account limitations also could address potential abuses. Trading against a customer order would not be possible if a system is preprogrammed with the terminal operator's proprietary account number(s) along with preprogrammed prohibitions against matching such proprietary orders with customers orders. Similarly, misallocation of executions would not be a problem if account numbers are required at the time of order entry.

### *Regulatory Implications of Order Execution Algorithm*

The algorithm governing order execution may affect the manner in which regulatory authorities carry out their obligations. In particular, the algorithm may affect the need for or applicability of certain restrictions on trading practices and on the types of surveillance procedures used by exchanges and regulatory authorities.

Dual trading restrictions, if a feature of local regulation, might be more appropriate in the case of certain algorithms than others. A system which uses a periodic single price auction as its exclusive method of trading would seem to be less susceptible to dual trading abuses than a system that permits counterparty selection. In the former case, where all orders are brought together at preestablished times, abuses such as prearranged trading or trading ahead of a customer would be very difficult. In the latter case, where the terminal operator has more control over the timing of trades and can identify the other party, abuses might be easier. Regulatory authorities will need the technical capacity to analyze system software for susceptibility to particular abuses. This includes the ability to determine if it is possible to subvert the algorithm. Regulators and system designers must weigh the advantages of an improved audit trail against the costs of designing systems which preclude certain abuses by screening out certain orders from the execution process.

Although an improved audit trail would enhance the ability to detect some abuses, on-site surveillance or supervision may still be necessary. There is no completely foolproof

way within a trading algorithm to preclude all potential abuses, particularly those which involve collusion among multiple terminal operators or tampering with the system. Regulatory oversight programs, therefore, will need to be sure that the algorithm actually operates mechanically in the manner specified and to be aware of any circumstances which could alter that fact.

Algorithms can be designed to enforce speculative position limits, credit limits, price limits, circuit breakers, or other trading halts. Such algorithms may be relatively complex and must be designed carefully so that they do not increase risk and cannot be manipulated for ulterior reasons.[5]

The following summarizes the potential regulatory implications of some algorithm features:

| **Algorithm Feature** | **Supervisory Effect** |
|---|---|
| 1. Discretion as to counterparty | A system which permits counterparty selection may create greater demand on supervisory resources than one which provides for anonymous matching of orders. |
| 2. Discretion as to price | A system which has no price limits or rules for the permissible range of bids and offers may create greater demand on supervisory resources than one which has limits programmed-in. |
| 3. Discretion as to quantity | A system which has no position limits may create greater demand on supervisory resources than one which has programmed-in limits. |
| 4. Discretion as to time | A continuous matching system where the momentary withholding of an order could have a significant effect may create a greater demand on supervisory resources than a system which periodically runs a single price algorithm. |
| 5. Contingent orders | A system that allows terminal operators to handle contingent orders such as market orders and stop orders may create a greater demand on supervisory resources than an algorithm which accepts such orders directly. |

The need for external supervisory safeguards over terminal operators increases with the amount of discretion a terminal operator has over order execution. On the other hand, technical and operational concerns may increase as programming complexity increases as a result of price limits or limits on the discretionary activity of operators.

[5] For example, in 1987 the National Association of Securities Dealers system was programed to shut down when the market was crossed, i.e., the price of the best bid is higher than the price of the lowest offer. It has been alleged that in times of market stress, traders have deliberately created a crossed market in order to halt trading. See *The October 1987 Market Break*, SEC Staff Report (February 11, 1988).

**Relationship to Other Systems**

Screen based trading systems can be designed to interface with other related automated systems such as the clearing system, order routing systems, or special surveillance systems. The trading system may provide for on-line transmission to clearing. This could prevent certain trading abuses such as misallocation of executions. Similarly, abuses that arise in connection with the creation and resolution of outtrades under a floor trading system may be impossible under a screen-based system which locks-in the terms of a trade at the time of execution and clears it on a real-time basis. For example, a trader could no longer create an outtrade after execution in an effort to postpone having to post margin on a position.

Direct connection between systems, however, could increase operational and technical concerns especially about system security and capacity. It could create additional concerns about adequate protection against systemic risk because of the immediacy of the impact of the trade on the actual movement of funds which, in turn, may result in additional financial requirements for system access.

The trading system could be connected to an order-routing system thereby separating the functions of order acceptance and order entry. Customers would not deal directly with terminal operators and additional audit trail information dating from time of receipt of an order could be created. In that case, concerns about the ability of terminal operators to commit abuses, such as the withholding or disclosure of customer orders, might be alleviated as would many concerns about the need for a pre-input audit trail.

Other types of complementary features could be created outside the actual trading system. For example, all telephone calls to a firm's terminal locations could be recorded. Provision could be made for video surveillance of terminal locations. Terminal operators could be physically isolated from order takers and not provided with telephones to prevent communication with other terminal operators. These sorts of measures might improve supervisory controls, and, therefore, reduce the need for other regulatory requirements concerning retention of hard-copy inputs, such as requirements for order ticket preparation and concerning on-site surveillance.

The following summarizes the potential regulatory implications of some design interfaces:

| Feature | Supervisory Effect |
|---|---|
| 1. On-line transmission to clearing | By making certain abuses such as misallocation of executions more difficult to commit, this could alleviate certain concerns arising from dispersion of terminals and discretion vested in terminal operators. |
| 2. Order-routing systems | By making certain abuses such as the withholding of a customer order more difficult to commit, this could alleviate concerns arising from dispersion of terminals and discretion vested in terminal operators. |

| | |
|---|---|
| 3. Audio and/or video surveillance | By making certain abuses such as trading ahead of a customer order easier to detect this could alleviate concerns arising from dispersion of terminals and discretion vested in terminal operators as well as decrease the need for on-site surveillance or order ticket preparation. |

Interfacing systems may limit the potential for abuse arising from any given trading system or may reduce the need for supervision external to the system. However, additional technical complexity resulting from the juxtaposition or connection of systems may create operational concerns.

## CONCLUSION

This article is not intended to suggest any particular set of regulatory solutions. Rather, it seeks to illustrate the complexity of issues to be considered in designing oversight regulations to accommodate the new screen-based trading systems. The traditional objectives of oversight are customer protection and market integrity. The manner in which these goals are achieved will depend on the design of the system and on the potential need for supervision and technical assessment of the system mechanism (that is, internal supervision) as well as the potential need to supervise direct users in addition to or in place of the customary external supervision of intermediaries which exists in other markets.

The challenge to regulatory authorities is to avoid impeding innovation while avoiding regulatory gaps so as to safely foster a diversity of system designs, worldwide access, and effective linkages. As automated trading system use increases, more information will become available to test various regulatory approaches. The end result should be systems designed to provide optimally fair and efficient markets.

# Appendix 1

## PRINCIPLES FOR THE OVERSIGHT OF SCREEN-BASED TRADING SYSTEMS FOR DERIVATIVE PRODUCTS

The regulatory authorities responsible for oversight of screen-based trading systems for derivative products,[1] whether governmental, quasi-governmental, or private ("relevant regulatory authorities"), should articulate the jurisdictional interest and supervisory principles applicable to the organizations responsible for the system such as an exchange ("system sponsor"), the organization or organizations which provides or provide the hardware, software, and/or the communications network and related services ("system providers"), the persons authorized to execute transactions on the system such as a broker-dealer ("system user"), and persons with financial exposure to the system ("system

[1] For purposes of these Principles, the term *derivative products* refers to those products in which the exchange or market ("market") itself is the issuer, which are subject to the rules of the issuing market, and for which a clearing organization is used to settle profits and losses, make deliveries, and guarantee cleared trades.

customers"). These principles should reflect the shared objectives of ensuring that, among jurisdictions, the levels of investor protection and regulation are adequate.[2]

To that end, it is suggested that jurisdictions adopt the following ten non-exclusive, general principles for the oversight of screen-based trading systems for derivative products which identify areas of common regulatory concern. It is understood that individual jurisdictions will take account of differences in national legal standards, regulatory policies, and market custom or practice in addressing these concerns.

1. The system sponsor should be able to demonstrate to the relevant regulatory authorities that the system meets and continues to meet applicable legal standards, regulatory policies, and/or market custom or practice where relevant.
2. The system should be designed to ensure the equitable availability of accurate and timely trade and quotation information to all system participants and the system sponsor should be able to describe to the relevant regulatory authorities the processing, prioritization, and display of quotations within the system.
3. The system sponsor should be able to describe to the relevant regulatory authorities the order execution algorithm used by the system, i.e., the set of rules governing the processing, including prioritization, and execution of orders.
4. From a technical perspective, the system should be designed to operate in a manner which is equitable to all market participants and any differences in treatment among classes of participants should be identified.
5. Before implementation, and on a periodic basis thereafter, the system and system interfaces should be subject to an objective risk assessment to identify vulnerabilities (e.g., the risk of unauthorized access, internal failures, human errors, attacks, and natural catastrophes) which may exist in the system design, development, or implementation.
6. Procedures should be established to ensure the competence, integrity, and authority of system users, to ensure that system users are adequately supervised, and that access to the system is not arbitrarily or discriminatorily denied.
7. The relevant regulatory authorities and the system sponsor should consider any additional risk management exposures pertinent to the system, including those arising from interaction with related financial systems.
8. Mechanisms should be in place to ensure that the information necessary to conduct adequate surveillance of the system for supervisory and enforcement purposes is available to the system sponsor and the relevant regulatory authorities on a timely basis.
9. The relevant regulatory authorities and/or the system sponsor should ensure that system users and system customers are adequately informed of the significant risks particular to trading through the system. The liability of the system sponsor, and/or the system providers to system users and system customers should be described, especially any agreements that seek to vary the allocation of losses that otherwise would result by operation of law.
10. Procedures should be developed to ensure that the system sponsor, system providers, and system users are aware of and will be responsive to the directives and concerns of relevant regulatory authorities.

[2] The Principles set out in broad terms regulatory considerations arising from cross-order screen-based trading, and not the specific concerns of some members in respect of the particular laws applying to their jurisdiction (e.g., those dealing with anticompetitive rules and practices, margin levels, or capital requirements).