International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Scenario Tests on Algorithmic Trading Sanitizers

Bhupinder Paul Singh Sahni

Email: *bhupinder.sahni[at]gmail.com*

Abstract: ***In the Technology era where everything is being digitalized, Trading Systems are also not left behind. In order to get best execution of the Instruments being Traded on the system, different Algorithms and Strategies are put in place that can work better than human in executing the Best Price available. When technology has advanced so much that we are building mathematical algorithms using computer programming, it also comes with a caution. What if the computer program fails or if the Market becomes too volatile or there are human errors. In order to deal with these Risks, various Trading Sanitizers are put in the trading Applications to ensure Traders are stopped if the Risks are too high. These Sanitizers are customized according to the requirements. This paper will cover why Trading Sanitizers are important, different use and forms of Trading Sanitizers, types of Sanitizers and test scenarios that should be checked by Quality Assurance Engineers to make sure they work effectively on trading applications.***

Keywords: Algorithmic Trading; Algorithmic Trading Sanitizers; Quality Assurance; Testing Scenarios; Investment Banking

1. Introduction

There has been a rapid growth in automated trading systems such as algorithmic trading (AT)/ high frequency trading (HFT) and high frequency trading accounts [1]. Algorithmic trading (AT) is defined by CFTC (Commodity Futures Trading Commission) as the use of computer programs for entering trading orders with the computer algorithm initiating orders or placing bids and offers. This means that AT is not fully automated without human intervention but requires input by an operator or trader [2].

These software traders using Algorithmic trading/ high frequency trading have had a strong impact on trading venues, and the debate whether it is positive or negative is ongoing. HFT has also caused incidents on several occasions, the most severe in 2010, known as the "Flash Crash".

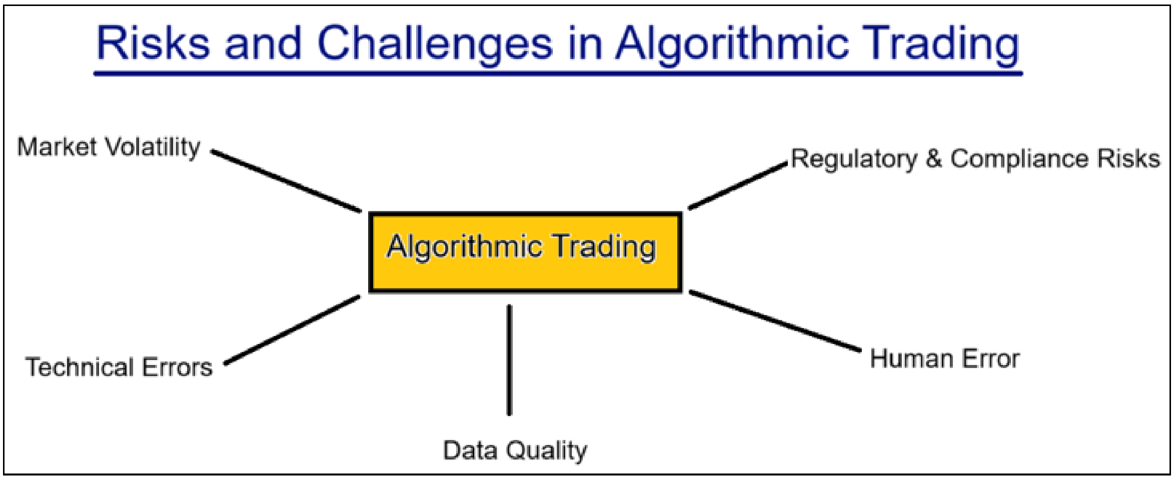
On May 6, 2010, U.S. financial markets experienced a systemic intraday event – "the Flash Crash", where a large, automated selling program was rapidly executed in the E-mini S&P 500 stock index futures market. Using audit trail transaction-level data for the E-mini on May 6 and the previous three days, it was found out that the trading pattern of the most active non designated intraday intermediaries (classified as High-Frequency Traders) did not change even when prices fell during the Flash Crash [3]. In the wake of these events the debate of security and responsibility regarding automated trading has emerged.

So, in order to have these kinds of incidents prevented from happening; Investment Banks, Hedge Fund Companies and other Big Financial Institutions have put checks in place on their trading systems to block Traders to Buy/ Sell Instruments from Market, if the Market is very volatile. These checks in place are also called Sanitizers.

In this paper we would go through various forms where Trading Sanitizers are implemented and useful, some of the different types of Algorithmic Trading and Risk Management based Sanitizers being used on Trading Applications and different test scenarios that Quality Assurance Engineers should consider while testing these Sanitizers.

2. What are Sanitizers

In the trading world, sanitizers based on risk control are mechanisms or tools designed to mitigate various types of risks associated with trading activities. There are checks in place on the trading systems that cause manual intervention when some unusual event happens, like high volume trade, Significant price variation from market price, high frequency trades etc.
Sanitizers in Trading applications can be useful in various forms as explained below:



DOI: https://dx.doi.org/10.21275/SR24522181416

Data Sanitization: In trading, sensitive information such as customer data, trade secrets, and proprietary algorithms are frequently handled. Data sanitization involves removing or masking sensitive information from datasets before sharing it internally or externally. This helps prevent unauthorized access and reduces the risk of data breaches [4].

Regulatory Compliance Sanitization: Regulatory compliance is the process of complying with applicable laws, regulations, policies and procedures, standards, and the other rules issued by governments and regulatory bodies [5].

Regulatory compliance is a significant concern in the trading world due to the strict rules and regulations governing financial markets. Rules and Regulations have been enforced by Regulatory systems like Securities and Exchange Commission (SEC) regulations, the Financial Industry Regulatory Authority (FINRA) rules, Markets in Financial Instruments Directive II (MiFID II) and other relevant guidelines to ensure there are no fraudulent transactions, transactions are transparent and financial institutions have enough funds to execute those transactions, amongst many other objectives. Regulatory Compliance Sanitization processes are established by Financial Institutions to ensure that trading activities comply with these laws and other relevant guidelines. There are heavy fines on the Financial Institutions if they do not comply with these rules and guidelines. This may involve scrubbing trading data to remove any potentially non-compliant activities or ensuring that trades meet specific reporting requirements.

Risk Management Sanitization: Trading in the financial markets can be an exciting and potentially lucrative venture, but it also comes with inherent risks. Risk management is essential in trading to mitigate potential losses and protect investors' interests. Risk Management Sanitizers are used to identify and mitigate risks associated with trading activities, such as market volatility, liquidity risks, and operational risks. By sanitizing trading processes and data, firms can better assess and manage their exposure to various risks.

Algorithmic Trading Sanitization: Algorithmic trading relies on complex mathematical models and algorithms to execute trades automatically. Trading Sanitizers play a crucial role in ensuring the integrity and security of these algorithms by identifying and addressing potential vulnerabilities, such as data leakage or manipulation.

3. Types of Sanitizers

There are different types of Sanitizers implemented within the algorithmic trading systems to ensure that trading decisions align with predefined risk parameters and to protect against potential losses. Some of the Risk Management and Algorithmic Trading based Sanitizers used in Trading Applications are explained below:

Fast Market Check Sanitizer: A Fast market is a market condition that is officially declared by a stock market exchange when the financial markets are experiencing unusually high levels of volatility combined with unusually heavy trading [6]. Fast Market Check Sanitizer does not allow quotes to be put in Market and gives Fast Market Error, if Prices move by more than x basis points in y seconds. This secures trader against volatile market conditions.

Futures Check Sanitizer: If the futures price and the market futures price differ by more than ‘x’ basis points, then it does not allow quote to be put in market and gives Future Off Market Error.

Limit Down is one such behavior where future Prices are very volatile. Limit down is a decline in the price of a futures contract or a stock large enough to trigger trading restrictions under exchange rules. Limits on the speed of market price movements, up or down, aim to dampen unusual volatility. Trading curbs triggered by extreme price movements are sometimes also called circuit breakers [7].

Limit down measures the decline from a reference price, usually but not always the prior session's closing price. Limit down is typically expressed as a percentage of the reference price, but occasionally in absolute terms as a dollar value [8].

As most of the Bond prices are derived from future prices, if Future Prices are incorrect or very volatile, then the Bond Prices will also be incorrect. So, the incorrect Bond prices are stopped from being quoted on the Market.

Future Check Sanitizer will be triggered, if
Quoted Future Buy Price > (Best Sell Future Price - tolerance)
or quoted Future Sell Price < (Best Buy Future Price + tolerance)

Market Price Check Sanitizer: If Price varies with market price by more than the tolerance specified, then Market Price Sanitizer kicks in and does not allow the quote into Market.

Market Price Check Sanitizer will be triggered, if
quoted Buy Price > (Best Sell Price - tolerance)
or quoted Sell Price < (Best Buy Price + tolerance)

Market Yield Check Sanitizer: Similar to Market Price Check Sanitizer, Market Yield Check Sanitizer is on Yield variations. If Yield varies with market yield by more than the tolerance specified then Market Yield Check sanitiser kicks in and does not allow the quote into market.

Market Yield Check Sanitizer will be triggered, if
quoted Buy Yield < (Best Sell Yield + tolerance)

or quoted Sell Yield > (Best Buy Yield - tolerance)

Market Spread Check Sanitizer: If Bid and Ask Price varies more than the market spread tolerance specified, then Market Spread Check Sanitizer kicks in and does not allow the quote into the Market.

Market Spread Check Sanitizer will be triggered, if
(Best Buy Price - Best Sell Price) > tolerance

Size Check Sanitizer: Size Check Sanitizer keeps a check on the size Trader is quoting in the Market. If quoting size falls outside the limits specified by the Trader, then Trader gets Sanitizer error and does not allow quote into the Market.

Size > Max Bid/ Ask Size;

Sanitize System: Trading Applications can have Master flag in place which controls All the Sanitizers listed above. This is to ensure that no Instruments can be Bought or Sold into the Market if this Sanitizer is set to "Off" for the Application.

4. Testing Scenarios on Sanitizers

Having understood different use and forms and some of the types of Trading Sanitizers, it becomes imperative to test them in QA (Quality Assurance) Environments before they can be deployed in Production to ensure they work as designed. Testing trading sanitizers involves verifying that trading sanitizers effectively protect sensitive data, ensure regulatory compliance, and mitigate risks in trading activities. Below are some test scenarios that can be considered for testing trading sanitizers:

Risk Management Testing: Test the effectiveness of risk mitigation strategies implemented by sanitizers, such as limiting exposure to high-risk assets or preventing unauthorized trading activities. Simulate various risk scenarios (e.g., market crashes, liquidity shortages) to evaluate the sanitizer's ability to detect and respond to potential threats. Verify that sanitized data accurately reflects risk exposure and helps traders make informed decisions to manage their portfolios effectively.

Algorithmic Trading Verification Testing: If QAs are testing Application involving Algorithmic Trading, then they should consider test scenarios on Trading Sanitizers implemented on different Trading algorithms. Test the integrity and security of algorithms by injecting test cases designed to trigger potential vulnerabilities, such as edge cases around algorithms. Evaluate the sanitizer's performance under different market conditions and trading strategies to ensure robustness and reliability.

Compliance and Regulatory Testing: Test for compliance with regulatory requirements such as SEC regulations, FINRA rules, and GDPR (General Data Protection Regulation) standards. Ensure that trading activities are appropriately flagged and reported for regulatory review, including trades that exceed specified thresholds or involve restricted securities. Verify that sanitized data includes necessary audit trails and metadata to demonstrate compliance with regulatory mandates.

Trade Surveillance Testing: Trading involves a lot of money, so there are high chances that there could also be suspicious trading patterns or anomalies indicative of market abuse or insider trading. Test the Trading sanitizer's ability to identify and flag suspicious trading patterns. Validate the effectiveness of trading algorithms in detecting potential misconduct while minimizing false positives.

Integration Testing: Trading Applications are complex, interacting with a number of other Applications like Downstream systems, trading APIs, Market Data Applications, etc. Integration Testing should be performed to test trading sanitizer's integration with trading platforms, risk management systems, and regulatory reporting tools to ensure seamless data flow and interoperability. There should also be test scenarios to validate compatibility with third-party applications and data sources, including market data feeds and trading APIs, to support end-to-end trading workflows.

Performance and Scalability Testing: Trading volumes vary every day; we need to ensure the Trading Strategies in place can handle different workload conditions. Verify the performance of Trading sanitizers under different workload conditions, including peak trading hours and high-volume trading days. Test scalability by simulating increased data volumes and user activity to ensure that sanitizers can handle growing trading demands without compromising performance or reliability.

Data Security Testing: Verify that sensitive information such as customer names, addresses, and financial details are properly masked or removed from trading data. Validate that sanitized data remains usable for analysis and reporting purposes without compromising privacy or security.

5. Conclusion

Overall, Trading Sanitizers are essential components of algorithmic trading systems, providing critical functions such as data validation, risk management, regulatory and compliance, system stability, performance optimization, and error prevention. Trading Sanitizers help traders achieve better outcomes and navigate the complexities of financial markets more effectively. By running appropriate Test Scenarios on Trading Scenarios in QA Environments, we can ensure the integrity and reliability of trading operations and ensuring mitigating risks in trading activities.

References

[1] Andrei Kirilenko, Andrew Lo. "Moore's law vs. murphy's law: Algorithmic trading and its discontents". 2013.

[2] A. Lehmann, "Quality and governance in high frequency trading systems", Network and System Administration Oslo University College, pp.1-67 May 22' 2013.

[3] A. Kirilenko, A. Kyle, M. Samadi, T. Tuzun, "The Flash Crash: High-Frequency Trading in an Electronic Market", The Journal of Finance, vol. 72, issue. 3, pp. 967-998, June 2017. https://doi.org/10.1111/jofi.12498

[4] A. Amiri, "Dare to share: Protecting sensitive knowledge with data sanitization", Decision Support

Systems, vol. 43, issue. 1, pp. 181-191, Feb 2007. https://doi.org/10.1016/j.dss.2006.08.007

[5] “What is Regulatory Compliance?” metricstream.com. Available at: https://www.metricstream.com/learn/comprehensive-guide-to-regulatory-compliance.htm#:~:text=Regulatory%20compliance%20is%20the%20process,Authority%20(FCA)%2C%20etc

[6] W. Kenton. “Fast Market: What It Means, How It Works” Investopedia.com. Available at: https://www.investopedia.com/terms/f/fastmarket.asp#:~:text=Key%20Takeaways,with%20the%20pace%20of%20trading

[7] J. Chen. “Limit Down: Definition and How It Works for Stocks and Futures” Investopedia.com. Available at: https://www.investopedia.com/terms/l/limitdown.asp

[8] CME Group. “Product Examples for Daily Price (Trading) Limits”. Available at: https://www.cmegroup.com/confluence/display/EPICSANDBOX/Product+Examples+for+Daily+Price+%28Trading%29+Limits