Document title

EURONEXT MARKETS – OPTIQ® OEG CONNECTIVITY SPECIFICATIONS

Document type or subject

Optiq® OEG Connectivity Features & Configuration Specifications

Version number
2.2.0

Date
6 Sep 2019

Number of pages
89

Author
EURONEXT

PREFACE

PURPOSE

This document sets out the client connectivity configuration specifications for Optiq® Order Entry Gateways (OEG). It describes the sources of data for connectivity, manner in which clients should attempt to connect to the OEGs. Additionally, this document contains the details of Cancel on Disconnect service, OEG Throttling, and High Availability & Business Continuity functionalities.

This document is a supporting document to the interface technical specifications.

ASSOCIATED DOCUMENTS

The following list identifies the associated documents, which either should be read in conjunction with this document, or which provide other relevant information for the user:

- Euronext Markets – Optiq OEG Client Specifications – SBE Interface
- Euronext Markets – Optiq OEG Client Specifications – FIX 5.0 Interface
- Euronext Cash Markets – Optiq TCS Client Specifications – SBE and FIX 5.0 Interface
- Euronext Cash Markets – Optiq Kinematics Specifications
- Euronext Derivatives Markets – Optiq Kinematics Specifications
- Euronext Markets – Optiq & TCS Error List
- Euronext Markets – Optiq File Specification
- Euronext Markets – Optiq MDG Client Specifications
- Optiq Euronext File Services User Guide

Clients are advised to also refer to the Euronext Rules and Regulations documents for more details.

For the latest version of IT documentation please visit:
https://connect2.euronext.com/en/membership/resources/it-documentation

SUPPORT

Optiq Support Desk
Tel: +33 1 70 48 25 55
Email: optiq@euronext.com

DOCUMENT & REVISION HISTORY

For the details of this and previous updates of this document please refer to the Appendix at the end of this document.

Version	Change Description
2.2.0	Update to combine all connectivity related topics in a single document. Updates for migration of Derivatives markets to Optiq. ▪ Updated list of Associated Documents, Introduction and Glossary to include information related to the added sections and services. ▪ Added section 2.3.1 “Functional Access Role (Derivatives markets)” ▪ Added sections: 5 “OEG Throttling” & 6 “High Availability and Business Continuity: Functional Overview”. This replaces the dedicated documents for these functionalities for Cash and Derivatives markets.

CONTENTS

1. INTRODUCTION

The Euronext Optiq Order Entry Gateway (OEG) provides high-speed and real-time connection to the Euronext markets. This document provides the following information for Cash and Derivatives markets:

- Connectivity information, covering:
  - features of the system that support client's ability to setup connection to Optiq
  - sources of connectivity information
  - segment-wide configuration settings
  - recommended practices for the setup of connectivity
- Details of the Cancel on Disconnect (CoD) services
- Throttling description, including:
  - throttling mechanism supported by the OEG
  - concepts, limits and formulas that support client's ability to manage their message flow in order to:
    - avoid being throttled,
    - be informed of the reason their messages were throttled
  - recommended practices in using the OEG in most optimal way
- Functional overview of Optiq High Availability (HA) and Business Continuity (DR)
  - high availability and business continuity facilities supported by the Optiq trading chain
  - features of the trading chain that support client's ability to:
    - manage their sessions in cases of trading chain recovery,
    - resynchronize with the Exchange if required
  - recommended practices in different cases of failure

⚠ **Important note: During migration to Optiq of the Derivatives markets the platform used for testing purposes is Next External User Acceptance (p-EUA)**

1.1 GLOSSARY

This section provides a list of some terms & abbreviations commonly used in this document. Please note that some of these terms are described in more details in the dedicated sections within this document or in the associated Optiq specifications documents.

- **Optiq**: is Euronext's multi-market full trading chain technology platform.
- **Order Entry Gateway (OEG):** is the software that manages the access for exchanges' clients, and acts as the private interface between the clients and the Optiq matching engine.
- **Market Data Gateway (MDG):** is the software that provides high-speed, real-time market data (public messages) for the Euronext markets.
- **Matching Engine (ME):** is the software that manages the trading services for the Exchange's markets.
- **Optiq Segment:** defines a universe of instruments habitually sharing common trading properties. An Optiq Segment can contain one or several asset classes. An Optiq Segment access is setup through a Logical Access.
- **Partition:** is a technical subdivision of an Optiq Segment. An Optiq Segment may be comprised of at least one or several partitions, physically independent one from another, but connected to each other within the context of the Optiq Segment. Instruments may move from one partition to another within an Optiq segment.

- **Logical Access:** is an OEG (Order Entry Gateway) entry point, setup for clients to connect to a single Optiq Segment, containing the technical configuration for the client's connectivity. Multiple logical accesses can share the same SFTI line.
- **OE Session:** the individual physical connection, to a single Partition. A single Logical access may have as many OE sessions as there are partitions in the Optiq segment.
- **Secure Financial Transaction Infrastructure (SFTI):** The SFTI Network is a wide area network, which provides customers with domestic and international financial markets connectivity from a single SFTI port.
- **Disaster Recovery (DR):** A Euronext Disaster Recovery event occurs when Euronext switches client systems processing from the Euronext production environment to the Euronext DR environment. The DR environment provides redundant standby systems to be used upon the failure of the Euronext production environment.
- **CoD**: Cancel on Disconnect mechanism, subject of this document
- **Financial Information eXchange (FIX):** is an electronic communications and messaging protocol used as one of the solution for private order entry messaging in Optiq. The FIX messaging standard is owned, maintained and developed through the collaborative efforts of FIX Trading Community™ member firms.
- **Simple Binary Encoding (SBE):** is the open source binary protocol used as the solution for market data and order entry messaging in Optiq. SBE was designed within the FIX Protocol Limited organization, with a focus on low-bandwidth utilization and the goal of producing a binary encoding solution for low-latency financial trading.
- **Persisted orders**: an order that is flagged by the client with CoD disabled and is therefore kept in the book once the CoD mechanism is triggered.
- **Original partition**: in cases described in this document, this indicates a partition that is failing over and to which the OE session is connected to. The OE session in question is the one that owns the orders impacted by the examples and explanations described in this document.
- **Meshed or Cross-linked partition**: In case a segment has multiple partitions, OEGs of different partitions will have connectivity to the Matching Engines of other partitions (cross-partition connectivity), allowing Optiq to route orders to the Matching Engine for instruments hosted on other partitions from the OEG of the "original" partition. In cases described in this document, this indicates partitions that are cross-connected to the partition that is failing over. Sending of quotes across-partitions isn't authorized.

2. OEG CONNECTIVITY

2.1 CONNECTIVITY MODEL & ASSOCIATED CONCEPTS

The connectivity model and associated concepts are explained in the beginning of the SBE and FIX message specifications.

⚠ **Important note**: Clients are strongly urged to review the explanations provided in the OEG message specifications in detail before continuing with this document.

2.2 CONNECTIVITY IN A NUTSHELL

To Connect to Optiq clients need to:

- Setup connectivity to the range of IP and Ports specified for each individual environment
- Obtain the partition ID and specific IP of that partition provided in the Cash and Derivatives Standing Data files
- Setup a Logical Access for each segment of interest or for Drop Copy (DC)
- Connect to the IP of the partition using the Logical access ID and the OE partition ID or DC partition ID

This document provides more details associated to these topics.

2.3 LOGICAL ACCESS

Upon creation each Logical Access clients will be provided the associated Logical Access ID and Port, as well as any other operational details (e.g. requirements for Conformance testing).

For more information on provisioning of Logical accesses clients should review the section "Obtaining or Modifying a Logical Access".

2.3.1 Functional Access Role (Derivatives Markets)

For the Derivatives markets each Logical Access is created with one of the following Functional Access roles: Trading, Market Making, or RiskGuard.

Functional Access roles are used to provide the associated Logical Accesses with the best performance for their designated purposes, as such, depending on the role assigned, the Logical Access can submit only a specific sub-set of messages. The purposes for each role are:

- Trading: submit non-Market Making messages for trading on Optiq, provided in SBE and FIX formats
- Market Making: submit Market Making messages for trading and Market Making activities (e.g. Market Maker protection), for Derivatives provided in SBE format only,
- RiskGuard: submit messages associated to Risk Management only (Suspension, Block, Order Size Limit, etc.), provided in FIX format only.

Logical Accesses of functional type Market Making are tuned for best performance in submitting Market Making related messages (i.e. Quotes). Such logical accesses may also submit individual orders, and other non-MM application messages. If used solely for mass submission of non-MM related messages clients will observe that such activity will incur additional latency.

The inbound messages that can be submitted by each Functional Access Role for Derivatives Markets are identified in the table below.

SBE				FIX			
Message Code	**Message Name**	**Trading**	**Market Making**	**Message Code**	**Message Name**	**Trading**	**RiskGuard**
01	New Order	✓	✓	**D**	NewOrderSingle	✓	X
06	Cancel Replace	✓	✓	**G**	OrderCancelReplaceRequest	✓	X
08	Quotes	X	✓				
10	Request For Quote	✓	✓	**R**	QuoteRequest	✓	X
				AG	QuoteRequestReject	✓	X
12	Cancel Request	✓	✓	**F**	OrderCancelRequest	✓	X
13	Mass Cancel	✓	✓	**Q**	OrderMassCancelRequest	✓	X
15	Open Order Request	✓	✓	**AF**	OrderMassStatusRequest	✓	X
18	Ownership Request	✓	✓	**U18**	OwnershipRequest	✓	X
47	MM Sign In	X	✓				
60	Security Definition Request	✓	✓	**C**	SecurityDefinitionRequest	✓	X
62	MM Protection Request	X	✓				
64	New Wholesale Order	✓	✓	**U64**	NewWholesaleOrder	✓	X
66	Request For Implied Execution	✓	✓	**U66**	RequestForImpliedExecution	✓	X
67	Cross Order	✓	✓	**U67**	CrossOrder	✓	X
100	Logon	✓	✓	**A**	Logon	✓	X
103	Logout	✓	✓	**5**	Logout	✓	X
106	Heartbeat	✓	✓	**0**	Heartbeat	✓	X
107	TestRequest	✓	✓	**1**	TestRequest	✓	X
				2	ResendRequest	✓	X
				4	SequenceReset	✓	X
				U68	ERGCommand	X	✓
				U70	GetRiskControls	X	✓

2.4 CONNECTIVITY INFORMATION & INSTRUMENT REFERENTIAL

Connectivity information for all order entry gateways should be retrieved from the

- Cash Standing Data file (9007) for the Cash segments, and
- Derivatives Standing Data file (9013) for the Derivatives segments.

These files are produced for the individual Optiq Segments, and the information for each Optiq Segment is provided in the file for that segment. The Standing Data files are made available on the Euronext File Service (EFS).

The files (for each Optiq Segment), amongst other data, contain the following information required for connectivity to Trading Order Entry (OE) and Drop Copy (DC) gateways:

- *Partition* field with its associated elements provided for each available partition, encapsulating all the connectivity characteristics of that partition, which include the following attributes:
  - *PartitionID* – the unique ID of each partition, and the associated connectivity information is made available for each individual partition hosting at least one tradable instrument within the segment.
  - *IPAddressPrimary* – the IP Address of the Primary OE or DC gateway. The same IP address is used for the Primary and Mirror (secondary, or back-up) instances of the gateways. The connectivity switch between the instances in case of High Availability (HA) event of individual partition is managed via the recovery mechanism by the Exchange. It requires no additional connectivity setup or changes and is transparent to clients. This value is provided for all environments.
  - *IPAddressDR* – the IP address of the Disaster Recovery instance of the OE or DC gateway, and is used in case of an Exchange Business Continuity event, and is only provided in the Production environment.
  - *PartitionType* – used to differentiate the Order Entry (OE) and Drop Copy (DC) connectivity partitions. Use of Order Entry and Drop Copy gateways require separate and individual setup of the Logical access to each of these services.

Section below provides a representative excerpt of Standing Data file structure that represents the connectivity related data and an example of how this data would be represented in the XML file. For complete and accurate details of the file structure and its contents clients should refer to the *Euronext Markets – Optiq File Specification* document.

This OEG connectivity information is associated to the *Partition ID* that is specified in the Standing Data file for each individual instrument. By associating the *Partition ID* specified for the instrument and the connectivity information provided for that *Partition ID* clients should be able to identify to which Partitions they should connect to in order to establish the shortest path for lowest latency in trading.

In segments that contain multiple partitions, to achieve the best possible performance, clients are encouraged to connect to the individual partitions identified as hosting each instrument. For more information about meshed partitions, and benefits of connecting to individual partitions please refer to the SBE or FIX Interface message specifications.

Excerpt of the Connectivity Structures from a Standing Data File:

The information in the excerpt below uses the standards of data identified in the *Euronext Markets – Optiq File Specification* document, and the Length (Len) is expressed in number of characters. In the table below column F/A identifies if the row provides the Field or an Attribute of the field, where Attributes (indicated as A) are listed as indented rows under the field to which they belong.

Each *Partition* field will encapsulate all the connectivity attributes of that partition.

Field / Field Attributes	F/A	Short Description	Format	Len	Values
CashStandingDataFile	**F**				
LogicalAccessConnectivity	**F**				
Partition	**F**				

Field / Field Attributes	F/A	Short Description	Format	Len	Values
PartitionID	A	Identifies uniquely an Optiq OE partition across all the Exchange partitions	Numerical ID	3	From 10 to 999
IPAddressPrimary	A	IP Address of the Primary and Secondary (backup) access to the gateway. Provided for all environments (IP v4)	String	15	Valid IP v4 address
IPAddressDR	A	IP Address of the Disaster Recovery access to the gateway. Populated only for the Disaster Recovery environment, in the file generated for the Production environment. Blank for all other environments (IP v4)	String	15	Valid IP v4 address
PartitionType	A	Indicates the type of Partition, either Order Entry or Drop Copy. Use of Order Entry and Drop Copy gateways require separate and individual setup of the Logical access to each service.	String	2	OE = Order Entry DC = Drop Copy
/Partition	**F**				
/LogicalAccessConnectivity	**F**				
/CashStandingDataFile	**F**				

Examples of Connectivity Structures for Standing Data XML File:

The examples below are provided for illustration purposes only. Clients should refer to the standing data files to obtain the actual connectivity details for each environment, segment and partition. The notation "[…]" indicates the other data present in the file prior to the connectivity structures, which is omitted in this example.

Example of Connectivity Structures for Cash Standing Data XML File:

```
<CashStandingDataFile version="#.#.#">
[…]
  <LogicalAccessConnectivity>
        <Partition PartitionID="10" IPAddresPrimary="212.197.223.23" IPAddressDR="" PartitionType="OE"/>
        <Partition PartitionID="11" IPAddresPrimary="212.197.223.24" IPAddressDR="" PartitionType="OE"/>
         <Partition PartitionID="12" IPAddresPrimary="212.197.223.25" IPAddressDR="" PartitionType="OE"/>
        <Partition PartitionID="13" IPAddresPrimary="212.197.223.26" IPAddressDR="" PartitionType="OE"/>
        <Partition PartitionID="990" IPAddresPrimary="212.197.223.61" IPAddressDR="" PartitionType="DC"/>
        <Partition PartitionID="991" IPAddresPrimary="212.197.223.62" IPAddressDR="" PartitionType="DC"/>
        <Partition PartitionID="992" IPAddresPrimary="212.197.223.63" IPAddressDR="" PartitionType="DC"/>
        <Partition PartitionID="993" IPAddresPrimary="212.197.223.64" IPAddressDR="" PartitionType="DC"/>
  </LogicalAccessConnectivity>
</CashStandingDataFile>
```

Example of Connectivity Structures for a Derivatives Standing Data XML File:

```
<DerivativesStandingDataFile version="#.#.#">
[…]
  <LogicalAccessConnectivity>
        <Partition PartitionID="120" IPAddresPrimary="212.197.194.35" IPAddressDR="" PartitionType="OE"/>
        <Partition PartitionID="121" IPAddresPrimary="212.197.194.37" IPAddressDR="" PartitionType="OE"/>
         <Partition PartitionID="122" IPAddresPrimary="212.197.194.33" IPAddressDR="" PartitionType="OE"/>
```

```
        <Partition PartitionID="980" IPAddresPrimary="212.197.194.61" IPAddressDR="" PartitionType="DC"/>
        <Partition PartitionID="981" IPAddresPrimary="212.197.194.62" IPAddressDR="" PartitionType="DC"/>
        <Partition PartitionID="982" IPAddresPrimary="212.197.194.63" IPAddressDR="" PartitionType="DC"/>
        <Partition PartitionID="983" IPAddresPrimary="212.197.194.64" IPAddressDR="" PartitionType="DC"/>
    </LogicalAccessConnectivity>
</DerivativesStandingDataFile version="#.#.#">
```

2.4.1 Trade Confirmation System (TCS)

Standing Data, Connectivity & EMM

TCS specific messages will be submitted via the Optiq Trader Order Entry Gateways. As for all other instruments in Optiq, submission of TCS message for a specific instrument is possible only via the Optiq Segment by which it is hosted. The instruments that are hosted by a specific segment are identified in the standing data file produced for the individual Optiq Segment. This should allow clients, that submit TCS declarations with order entry gateways, to use the same Logical Access, within an Optiq Segment, to submit messages for the same instrument, but intended for different EMMs that also cover the TCS service.

The standing data of the individual Optiq Segments includes the instruments that are eligible to submission of TCS messages, the partition it is hosted on, and the connectivity information for that segment. The connectivity information of the segment / partition is the same, whether client intends to send messages for Central Order Book (COB) or TCS. The symbol Index for instruments that can be traded on COB and receive TCS declarations is the same.

Only Euronext instruments with EMM equal to 5 = Cash On Exchange Off book are eligible for submission of declarations and other TCS messages. As TCS allows for submission of declaration from instruments that are identified by the same Symbol Index and are made available under different EMMs clients need to make sure that for submission of TCS messages the correct EMM is specified.

The market data messages associated to the TCS messages will be sent in the individual partitions indicated for each instrument in standing data file.

Logical Accesses for TCS

To submit and/or to receive TCS specific messages via the Optiq OEGs the associated Logical Accesses has to be set with characteristic that indicates use of TCS service. Only the Logical Access that is setup this way will be able to submit and receive messages to/from TCS. If client has multiple logical accesses on the same Optiq Segment, only the Logical Access that is setup to indicate use of TCS service will receive the unsolicited messages from TCS. Unsolicited messages from TCS will be sent back only to the Optiq Segment on which the instruments are hosted.

TCS messages are not in scope of Cancel on Disconnect service.

TCS messages are included in the messages counted for throttling thresholds set for the Logical Access.

2.4.2 Indices

Indices segment has a standing data file, however it doesn’t have order entry gateways. In this file, section for connectivity data will not be present.

2.5 SEGMENTS

Table below provides the current overview of available Optiq Segments and the indicative number of partitions setup for each segment.

Drop Copy is not a trading segment, and uses different approach to partitions specified separately.

Optiq Segment	Number of Partitions
Equities	4
Funds	1
Fixed Income	1
Warrants and Certificates	1
Equity Derivatives	3
Index Derivatives	1
Financial Derivatives	1
Commodities	1

2.6 DETERMINING THE "SHORTEST PATH" FOR INDIVIDUAL ORDERS

In order to benefit from the best response times for the individual order messages, the clients should send these messages directly to the partition on which the instrument is located. Quotes and other market making messages can't be sent across partitions.

To identify on which partition each instrument is located, clients must use, and update on a daily basis, their referential data by downloading the Standing Data and real-time market data messages, where details of the *Partition ID* assigned to each instrument are provided.

2.7 RANGE OF IPS AND IPS OF INDIVIDUAL PARTITIONS

This section provides the ranges of IP addresses identified for Optiq per environment, and for individual Optiq segments. To facilitate ease of future upgrades (e.g. addition of new partitions) clients are encouraged to setup connectivity from their physical machines to the full range of IP addresses identified. In case new partitions are added to a segment, they'll be added with the IP addresses within the range assigned to that Optiq Segment.

- Each partition as part of an Optiq Segment uses a unique IP address, by environment, from the ranges as specified in the tables below.
- In case of a new partition a new IP address, within the range associated to the Optiq Segment will be used for the new partition.

2.7.1 IP Ranges per Environment

Environment	Range of IPs
Virtual EUA (v-EUA)	212.197.223.0/25
Physical EUA (p-EUA)	212.197.222.0/25
Production	212.197.194.0/24
Disaster Recovery (DR)	212.197.229.0/24

Please note: Table above uses Classless Inter-Domain Routing (CIDR) notation (commonly used in network documentation) to represent the IP ranges. The notations /## indicates the size of the routing prefix used.

2.7.2 Segment & Partition IP Information

The OEG related IP addresses and associated Partition IDs are provided in tables below for each environment.

Important: Tables below indicate IP addresses of individual partitions, however clients are strongly advised to:

- setup connectivity for the full range of IP addresses for each environment, and to
- obtain the IP addresses of each partition provided on a daily basis in the standing data file.

Value of Partition ID column provided in tables below represents the value in the field *PartitionID* provided in the Standing data files and real-time market data messages. This field corresponds to the *OE Partition ID* field used in private order entry messages.

Drop Copy is not a trading segment, and uses different approach to partitions specified separately.

CURRENT (v) EUA Test environment

Optiq Segment Name	Partition ID	IP of Individual Partition
Equities	10	212.197.223.23
	11	212.197.223.24
	12	212.197.223.25
	13	212.197.223.26
Funds (ETFs)	20	212.197.223.27
Fixed Income (Bonds)	30	212.197.223.29
Warrants and Certificates	40	212.197.223.28
Block	140	212.197.223.1
Commodities	80	212.197.223.34
Equity Derivatives	120	212.197.223.32
	121	212.197.223.33
	122	212.197.223.31
Index Derivatives	110	212.197.223.30
Financial Derivatives	130	212.197.223.22

NEXT (p) EUA Test environment

Optiq Segment Name	Partition ID	IP of Individual Partition
Equities	10	212.197.222.2
	11	212.197.222.5
	12	212.197.222.8
	13	212.197.222.11
Funds (ETFs)	20	212.197.222.14
Fixed Income (Bonds)	30	212.197.222.20
Warrants and Certificates	40	212.197.222.18
Block	140	212.197.222.39
Commodities	80	212.197.222.66
Equity Derivatives	120	212.197.222.30
	121	212.197.222.34
	122	212.197.222.24
Index Derivatives	110	212.197.222.22
Financial Derivatives	130	212.197.222.50

Production environment

Optiq Segment Name	Partition ID	IP of Individual Partition
Equities	10	212.197.194.2
	11	212.197.194.5
	12	212.197.194.8
	13	212.197.194.11
Funds (ETFs)	20	212.197.194.13
Fixed Income (Bonds)	30	212.197.194.17
Warrants and Certificates	40	212.197.194.19
Block	140	212.197.194.44
Commodities	80	212.197.194.29
Equity Derivatives	120	212.197.194.35
	121	212.197.194.37
	122	212.197.194.33
Index Derivatives	110	212.197.194.31
Financial Derivatives	130	212.197.194.82

Disaster Recovery (DR) environment

Optiq Segment Name	Partition ID	IP of Individual Partition
Equities	10	212.197.229.2
	11	212.197.229.3
	12	212.197.229.4
	13	212.197.229.5
Funds (ETFs)	20	212.197.229.6
Fixed Income (Bonds)	30	212.197.229.8
Warrants and Certificates	40	212.197.229.9
Block	140	212.197.229.37
Commodities	80	212.197.229.11
Equity Derivatives	120	212.197.229.14
	121	212.197.229.15
	122	212.197.229.13
Index Derivatives	110	212.197.229.12
Financial Derivatives	130	212.197.229.38

2.8 PORTS & PORT RANGES

This document provides a range of ports for each Optiq environment. To facilitate ease of future upgrades clients are encouraged to setup connectivity from their physical machines to the full range of ports identified.

Each Logical Access will be setup with a Port upon its creation. This port will be used by all OE Sessions used by that Logical Access, on all the partitions with the segment to which it belongs. The port assigned to the Logical Access will be unique at minimum within a single Optiq Segment and be specific to the Logical Access, no matter which message protocol is chosen to be used by the client.

The overall range of ports used by the Optiq system is 30000 – 59999. The tables below provide the port ranges used for each Optiq Segment and for each dedicated environment.

Virtual EUA (test) environment

Optiq Segment	Port Range
Equities, Funds (ETFs), Fixed Income (Bonds), Warrants and Certificates, Block	30000 - 39999

Equity Derivatives, Index Derivatives, Financial Derivatives, Commodities	30000 - 39999

Physical EUA (test) environment

Optiq Segment	Port Range
Equities, Funds (ETFs), Fixed Income (Bonds), Warrants and Certificates, Block	30000 - 39999
Equity Derivatives, Index Derivatives, Financial Derivatives, Commodities	30000 - 39999

Production environment

Optiq Segment	Port Range
Equities, Funds (ETFs), Fixed Income (Bonds), Warrants and Certificates, Block	45000 - 59999
Equity Derivatives, Index Derivatives, Financial Derivatives, Commodities	30000 - 39999

Disaster Recovery (DR) environment

Optiq Segment	Port Range
Equities, Funds (ETFs), Fixed Income (Bonds), Warrants and Certificates, Block	45000 - 59999
Equity Derivatives, Index Derivatives, Financial Derivatives, Commodities	30000 - 39999

2.9 DROP COPY

Unlike the “trading segment” OEGs, the Drop Copy (DC) gateways may provide clients with cross-segment data. Standing data file will contain multiple Drop Copy gateway IDs and associated connectivity information.

Clients can **not** connect to multiple Drop Copy gateways using the same Drop Copy Access, and should only use the connectivity information for the DC gateway assigned to their specific Drop Copy Access upon creation.

The associated information, i.e. Drop Copy ID & assigned port, is provided to the firm’s DMA on creation.

As Drop Copy is not a regular trading segment some of the differences associated to it are:

- partitions follow different connectivity and access logic and may not be segment specific
- made available only in FIX protocol
- throttling limits do not apply to the Drop Copy gateway

The range of ports that are used for Drop copy are the same as those used for other trading segment OEGs.

The overall range of ports used by the Optiq system is 30000 – 59999, with the following assignment for the environments as following:

- Virtual & Physical EUA: 30000 – 39999
- Production & DR: 45000 – 59999

For More information about Drop Copy clients should review the Drop Copy specifications document.

2.9.1 IP Addresses for Drop Copy per Environment

For the Cash Markets

Virtual EUA (test) environment

Drop Copy ID	IP Address
990	212.197.223.61
991	212.197.223.62
992	212.197.223.63
993	212.197.223.64

Physical EUA (test) environment

Drop Copy ID	IP Address
990	212.197.222.51
991	212.197.222.52
992	212.197.222.53
993	212.197.222.54

Production environment

Drop Copy ID	IP Address
990	212.197.194.61
991	212.197.194.62
992	212.197.194.63
993	212.197.194.64

Disaster Recovery (DR) environment

Drop Copy ID	IP Address
990	212.197.229.21
991	212.197.229.22
992	212.197.229.23
993	212.197.229.24

For the Derivatives Markets

Virtual EUA (test) environment

Drop Copy ID	IP Address
980	212.197.223.51
981	212.197.223.52
982	212.197.223.53
983	212.197.223.54

Physical EUA (test) environment

Drop Copy ID	IP Address
980	212.197.222.33
981	212.197.222.69
982	212.197.222.70
983	212.197.222.71

Production environment

Drop Copy ID	IP Address
980	212.197.194.83
981	212.197.194.84
982	212.197.194.87
983	212.197.194.88

Disaster Recovery (DR) environment

Drop Copy ID	IP Address
980	212.197.229.40
981	212.197.229.41
982	212.197.229.42
983	212.197.229.43

For More information about Drop Copy clients should review the Drop Copy specifications document.

2.10 LOGIN OVERVIEW

Clients initiate a TCP/IP session to the Order Entry Gateway, and then initiate a logon by sending a **Logon** message. Session Logon is always initiated by the client.

The **Logon** message must be the first message sent by the client otherwise the OEG will drop the connection, and it needs to be sent individually to each partition to which physical connection will be established.

The **Logon** message must contain the following fields:

- ***Logical Access ID***: to be populated with the value obtained from the CAS team upon creation of the Logical Access. The Logical Access ID is provided along with the corresponding **Port** number. Each Logical Access ID is authorized for access to a specific Optiq Segment. Providing a Logical Access ID that is not authorized for access to a Segment will result in the rejection of attempts to connect.
- ***OE Partition ID:***

- For Trading Order Entry Gateways: this field is to be populated with the unique ID of the partition to which client connects to. The ID provided in the Logon for the partition must correspond to the IP address of that partition. To identify the unique ID of the partition clients should use the value provided in the field *PartitionID* in the Standing data files and/or the real-time public messages. The value corresponding to the ID of each Partition should be used to obtain the corresponding **IP address** which is also made available in the Standing data files. The same applies to Logical accesses independently if they are used to submit messages for COB or TCS (for the Cash markets).
- For Drop Copy Gateways: this field is to be populated with the Drop Copy ID to which client is assigned on creation of the Drop Copy access and must connect to. The ID provided in the Logon for Drop Copy must correspond to the IP address of that Drop Copy gateway identified. The ID of the Drop Copy gateway is provided to the client on the creation of the Drop Copy access. The value corresponding to the ID of the Drop Copy gateway should be used to obtain the corresponding **IP address** which is also made available in the Standing data files.

Note

As was done in CCG, and is already in use in OEGs, Firm IDs provided in the private messages are left padded with zeroes to the full length of the field of eight (8) characters.

2.10.1 Cases of Disconnection Initiated by Exchange

In cases of aberrant technical behavior Exchange will automatically disconnect client OE sessions. This section identifies how to recognize the specific cases. As the cases identified are not part of expected behavior, clients are advised to avoid such cases.

Please note: Exchange rules identify other cases of connection suspension and disconnection, not listed above, which would be initiated based on regulatory rules; specific request from regulators or partners (e.g. Clearer); or decision of market operations.

2.10.1.1 Message sequence number inconsistencies

For clients using FIX protocol, if exchange receives messages with the sequence numbers that are inconsistent with what is expected by the OEG the connection will be disconnected. At the moment of disconnection OEG sends to the client a **Logout** (5) message.

These cases include the ones listed below and can be identified by values identified specifically for each case:

- Logon with next sequence number (tag 789) higher than the one expected by the OEG:

  field *SessionStatus* (tag 1409) set to **10** = Received NextExpectedMsgSeqNum (789) is too high

- On first connection or re-connection with the first sequence number (tag 34) equal to zero (0) or lower than the one expected

  field *SessionStatus* (tag 1409) set to **9** = Received MsgSeqNum (34) is too low

2.10.1.2 Unknown messages sent to exchange

- **For SBE**: in case of messages that can't be recognized & processed by the OEG the connection that sent the message will be disconnected from the OEG.

  As in the External User Acceptance environments clients are testing new software, this disconnection will be triggered after client's connection sends more than ten (10) such messages. Messages below this threshold will be rejected using the **Technical Reject** (108) message.

In production environment this is an aberrant and unexpected behaviour – if it occurs, client's connection is immediately disconnected, and as such the number of such messages is equal to zero (0).

At the moment of disconnection OEG sends to the client a **Logout** (103) message. The case can be identified by the following values in the message:

- SBE: field *Log Out Reason Code* set to 2 = Too many unknown messages

- **For FIX**: in case of messages that can't be recognized & processed by the OEG Optiq uses the behaviour prescribed by the FIX protocol.
  - If such messages are received before the client is logged in, the messages are ignored
  - If such messages are received after the client is logged in, OEG uses standard FIX logic to identify if client should be disconnected, or if the message should be rejected.

2.10.1.3 Excessive breaches of the connection rate

Client connections are assigned a maximum message rate, which are enforced by the OEG, in part, by the Exchange's throttling mechanism for inbound messages. Upon breaching the throttling limit messages above the limit are either rejected or queued. In addition, Exchange sets a limit for excessive breaching (either in number of messages or amount of data sent), of the assigned rate / size of connection. Excessive breaching means that client attempted to submit a number of messages, or amount of data in bytes, that is multiple times over their allowed rate.

This case takes into consideration only excessive breaches of limits, as identified below.

In this case, the connection is immediately disconnected, and will be prevented from re-connecting for during of 15 seconds.

This case could occur due to various reasons, including a technical issue in the client's system. To assist clients in identifying the issue and correcting it as quickly as possible, the **Logout** (103) / (FIX 5) message sent on disconnection in such a case provides specific values identified below.

Case	How to identify the case in Logout message	
	SBE *[Log Out Reason Code]*	FIX *[SessionStatus* (tag 1409)]
Excessive number of message	3 = Excessive Number of Messages	106 = Excessive Number of Messages
Excessive amount of data in bytes	4 = Excessive Amount of Data in Bytes	107 = Excessive Amount of Data in Bytes
Excessive number of messages and amount of data in bytes	5 = Excessive Number of Messages & Amount of Data in Bytes	108 = Excessive Number of Messages & Amount of Data in Bytes

2.11 OBTAINING OR MODIFYING A LOGICAL ACCESS

Ordering of the new Optiq Logical Accesses can be done using a form made available in the MCA web portal. The form is shared between the Cash and Derivatives markets.

For any information associated to the setup Logical Accesses, clients should contact Customer Access Services at cas@euronext.com.

Obtaining additional Logical Accesses or increased connection size may require members to order extra bandwidth on their SFTI® infrastructure. Members wishing to make such modification should therefore liaise with CCC (Client Coverage Center) at ccc@euronext.com in order to validate that they have sufficient bandwidth.

For Derivatives markets, in addition to other characteristics, when ordering Logical Accesses clients would need to identify whether they are to be used for Market Making activity (to allow use of Quote messages).

Dedicated forms are provided on the portal for ordering Logical accesses for the RiskGuard API and Drop Copy Accesses.

The Order Forms are available online on the Euronext website at the following locations:

- Optiq Order Entry (Trading Logical access)
    - Logical access creation form
    - Logical access modification form
    - Logical access deletion form

- Optiq Order Entry (Market Maker Logical access)
    - Logical access creation Market Maker form
    - Logical access Market Maker temporary deactivation form
    - Logical access Market Maker reactivation

- Optiq Drop Copy
    - Drop copy Access creation form

- RiskGuard (for Derivatives)
    - RiskGuard Logical access creation form
    - RiskGuard Logical access modification form
    - RiskGuard Logical access deletion form

After receiving a request for a Logical Access, Customer Access Services will communicate login information to customer by email.

Customers are required to have passed conformance in EUA before they are enabled for trading in Production environment.

As a reminder:

- Providers cannot order OEG Logical Accesses for Production
- Only trading members can order Production OEG Logical Accesses
- Logical Accesses can only be ordered by a nominated Member Connectivity Administrator (MCA). Any customer without an MCA account should contact the Customer Access Services (CAS) team for more information at cas@euronext.com / Tel: +33 1 85 148 589

3. SEGMENT-WIDE CONFIGURATION SETTINGS

3.1 ADMINISTRATIVE MESSAGE SETTINGS

3.1.1 Delay of Inactivity

The OEG uses the **Heartbeat** and **TestRequest** messages as a mechanism to ensure the connection between the client and the Exchange is up and functioning properly. For more information on administration messages please refer to the SBE or FIX Interface message specifications and kinematics documentation.

The "delay of inactivity" parameter is used to set up the period (in seconds) after which the Heartbeat/TestRequest mechanism is triggered. The parameter is specific for each Optiq Segment and defined as follows (in number of **seconds**):

Optiq Segment	SBE (seconds)	FIX (seconds)
Equities	1	5
Funds	1	5
Fixed Income	1	5
Warrants and Certificates	1	5
Equity Derivatives	1	5
Index Derivatives	1	5
Financial Derivatives	1	5
Commodities	1	5
Drop Copy	N/A	30

3.2 LP QUOTE DRIVEN MARKET SETTINGS

Optiq Segment	AFQ Delay Before Class Auction	AFQ Delay Before Instrument Unhalts
Warrants and Certificates	900 seconds / 15 minutes	2 seconds

For more information about the AFQ Delay and the LP quote driven market model, clients should review *New Warrants & Certificates Market Model – Functional Overview* document.

3.3 EXCHANGE ID IN PRIVATE MESSAGES

The field "Exchange ID" should be populated by the client with value "EURONEXT" in all environments. This value is used as following:

- SBE: In the field *Exchange ID* provided in outgoing messages
- FIX: For fields *TargetCompID* (Tag: 56) and *SenderCompID* (Tag: 49) as needed in incoming and outgoing messages

3.4 INTENTIONAL INCREMENT OF SEQUENCE NUMBER

In some cases when partition Primary instance fails over to the Mirror, or Production fails over to the DR environment the message sequence number may be intentionally increments by a pre-set number. This is being done specifically for cases of HA and Business Continuity to guarantee delivery of full scope of messages for resynchronization and to reduce number of unexpected rejections of client Logon attempts.

Table below provides the configured pre-setup increment number:

Optiq Segment	Intentional Increment of Sequence Numbers
Equities	1000
Funds	
Fixed Income	
Warrants and Certificates	
Equity Derivatives	
Index Derivatives	
Financial Derivatives	
Commodities	
Drop Copy	N/A

4. CANCEL ON DISCONNECT FOR OEG

4.1 FUNCTIONALITY DESCRIPTION

Cancel on Disconnect (CoD) is a mechanism which triggers an automatic cancellation of all non-persisted orders upon disconnection of the client whether voluntary or due to an issue.

CoD functionality applies and behaves in the same manner for all clients, for all their Logical Accesses / OE Sessions and on all Optiq Segments for the Euronext Cash and Derivatives Markets.

In typical day-to-day operations the CoD applies at the level of an OE Session (physical connection), which means that it is triggered per individual OE Session, for orders owned by this session, and it does not affect other OE Sessions that belong to the same Logical Access. Clients should review the details associated to the behavior and scope of CoD in case of failure situations provided in more details in this document.

This functionality is enabled system-wide, and for the orders is managed based on the values populated by clients in individual messages. Optiq only uses the data indicated in the messages to select orders for the scope of CoD and disregards the order characteristics (e.g. order types, order validity, etc.)

Quotes (08) (FIX i) messages do not have a separate field for selection whether to participate in CoD or not as in cases when CoD functionality is triggered all live quotes are mandatorily cancelled.

This means that every single entering order message is checked for the Cancel on Disconnect setting.

The Cancel on Disconnect mechanism is triggered when the connection (physical) between a client and the Order Entry Gateway (OEG) is dropped, either due to client closing the connection or in case of a failure. If the client application is disconnected from the OEG, then all live quotes and orders not flagged to be persisted, belonging to the corresponding OE Session are cancelled for their remaining quantity, regardless of order type and validity type.

Scope of CoD only includes orders sent during the current day. Orders entered during a previous business day are not in scope of CoD and are not impacted.

In cases when CoD kicks in a **Kill** (05) (FIX 8) message is sent to the OE Session for which the mechanism is triggered, for each order and instrument (Symbol Index and EMM) in scope. During the same trading session until the client reconnects the messages will be queued and will be sent to the affected OE Session upon a client's return.

Scope of CoD functionality includes only the orders submitted during the current trading session. I.e. if an order is submitted with validity of one year during the trading session of day 1 with default value for CoD (which means - do not persist order in case of disconnection), during the trading session of day 2 this order will no longer be in scope of CoD.

Orders updated during a trading session after the original day of entry into the system would not re-activate eligibility of the order to CoD.

The next sections in this document list cases when Cancel on Disconnect is triggered and where associated exceptions are applicable.

4.1.1 Rate of Triggering

The CoD mechanism is triggered as soon as the disconnection is submitted by the client or triggered by other detection of disconnection. As soon as the disconnection is identified CoD is triggered.

The detection of client disconnection will depend on the activity on the associated OE session and maximum delay assigned to the Optiq Segment for the TestRequest / Heartbeat mechanism.

The CoD mechanism is checked based on the "*n*" value that is measured in seconds. The minimum possible value for the delay period "*n*" value that could be defined is one second.

The value *n* defined for the processes associated to the TestRequest and HeartBeat messages are made available in section 3 of this document, and are defined per Optiq Segment.

The behavior of check and validation of continued connection is done in two steps (1) TestRequest issued after inactivity that lasts at maximum for the period of delay "*n*", (2) followed by wait for the Heartbeat response, also, at maximum, lasting for the time period "*n*" defined for the delay.

Based on the behavior for the check of connection the maximum period for detection of disconnection is between zero seconds and twice the maximum delay assigned to the Optiq Segment.

4.1.2 Quote Messages & CoD

All **Quotes** (08) (FIX i) messages submitted by the Liquidity Provider (LP) / Market Maker (MM) using a specific OE Session (physical connection) are in scope of CoD if that physical connection is disconnected from Optiq.

LP quote messages do not have validities that allow them to be transferred to another day, and are always treated as "for current trading session" only.

LP quote messages do not have a separate field for selection whether to participate in CoD or not as in cases when CoD functionality is triggered all live quotes of that physical connection are mandatorily cancelled.

The granularity of CoD is always that of an OE session (physical connection). A LP using the same Firm ID may choose to have multiple Logical access, and as such different OE sessions, connecting to a partition on which LP quote driven instruments are traded. If a particular such OE session gets disconnected from the specific partition, only the quotes owned by that OE session are cancelled.

LP Quote messages are restricted to sending quotes for instruments hosted on a single partition only. In case of multiple partitions being setup for the LP quote driven market, any cross partition failure cases described in this document would be treated the same way for quotes as they are for orders.

4.1.3 Controls in Case of Triggering of CoD

In case a client's system loses connection to the OEG, however the disconnection wasn't yet detected by the OEG, the client will be prevented from re-connecting, as multiple physical connections to the same partitions for the same Logical access are not allowed.

If OEG detects clients' disconnection, either upon request (via Logon message) or due to a technical issue, and CoD is triggered, any messages / requests submitted by the client following re-connection will be processed only after all the cancellations triggered by CoD are fully processed. This control is applied only to the OE session(s) impacted by the disconnection and should not impact performance of other OE sessions / clients, if they are not impacted by the disconnection, or do not have CoD enabled.

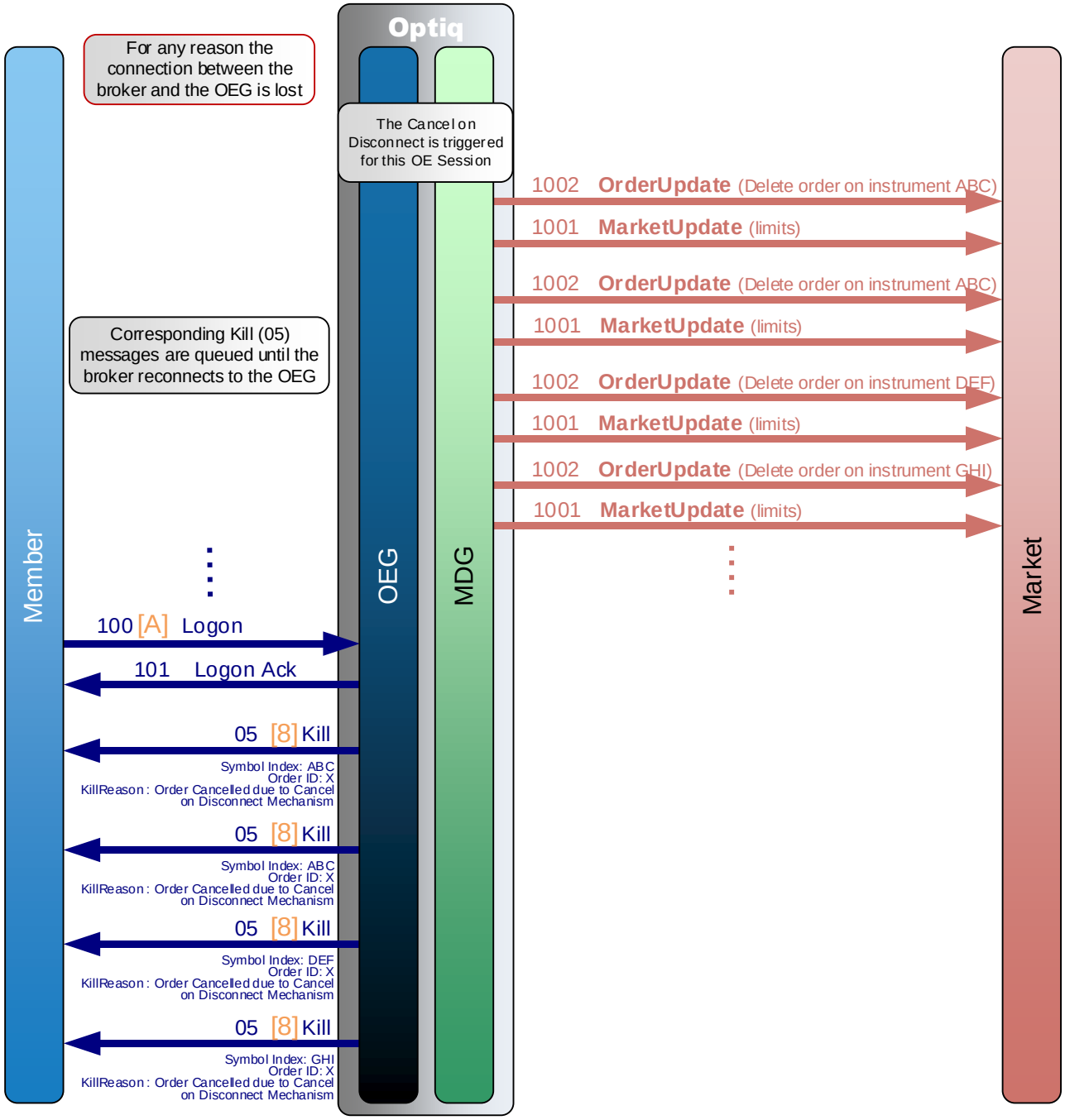
This is done in order to ensure that no new orders submitted upon re-connection are included into the scope of CoD.

4.1.4 Kinematics of Cancel on Disconnect

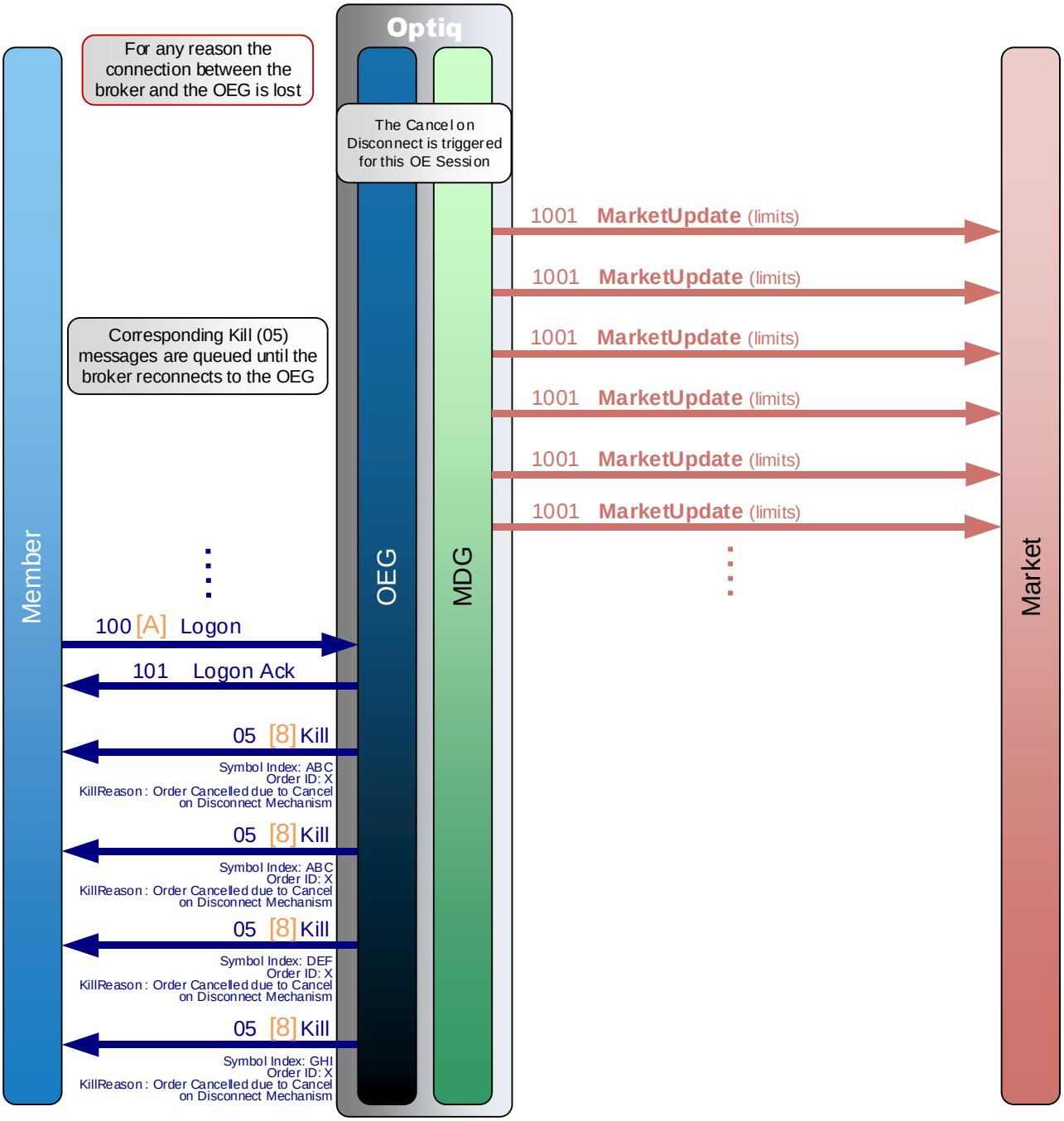
The diagrams below represent generic cases of loss of connection between a member and partition, for Cash and Derivatives markets. Further details on various cases of CoD triggering are identified in this document.

The sending of messages due to cancellation of orders via public and private message is available at the same time, however the diagram represents delayed sending of private message to the broker, as this sending also depends on the broker's reconnection to the OE session.

4.1.4.1 CoD for the Cash Markets



4.1.4.2 CoD for the Derivatives Markets



4.2 HOW TO ACTIVATE OR DISABLE CANCEL ON DISCONNECT

The CoD functionality is managed directly within the order message (please note that CoD behavior for LP **Quotes** (08) (FIX i) messages is described elsewhere in this document). No subscription or forms are required to use it, however checks that clients can correctly process CoD functionality are part of the regular conformance tests.

Clients can indicate within each order message if they want the order to be persistent, i.e. not included in the scope of the Cancel on Disconnect mechanism. If the field associated to disabling / activation of Cancel on Disconnect feature is set to "CoD disabled" for an order, this order will not be cancelled even if the CoD is triggered for the OE Session it belongs to.

The CoD values may be updated by the client using **Cancel Replace** (06) (FIX G). As indicated above, the modification of the indicator will be taken into consideration by the CoD functionality only during the trading session during which the order is entered into the system.

IMPORTANT NOTE:

It is important to note that the notification for individual order, after an **Ownership Request** (15) (FIX U18) message submitted in an OEG, results in sending of **ExecutionReport** (FIX 8) message to Drop Copy, which will contain the values set when the order was originally submitted, or last modified.

The value received may still indicate eligibility of the order to CoD, however if the order was persisted over at least one day, or longer, it will no longer be in scope of the cancellation.

4.2.1 SBE Field & Values for Cancel on Disconnect

In SBE protocol the data for the CoD in the order messages is to be specified as one of the values of a bitmap. The details of the messages, fields and values are described in the table below.

Quotes (08) (FIX i) messages do not have a separate field for selection whether to participate in CoD or not, as in cases when CoD functionality is triggered all live quotes are mandatorily cancelled.

In Incoming Messages:

Message Code	Message Name	Field	Value	Notes
01 / 06	New Order / Cancel Replace	Execution Instruction (bitmap) Position 3 - Disabled Cancel On Disconnect Indicator	0: Cancel on Disconnect enabled	Default Value Order included in the scope of cancellations when CoD mechanism is triggered
			1: Cancel on Disconnect disabled	If selected, order is persisted, and it **not** included in the scope of cancellations when CoD mechanism is triggered

4.2.2 FIX Fields & Values for Cancel on Disconnect

In FIX protocol the details of the order messages, fields and values are described in the table below.

Quotes (08) (FIX i) messages do not have a separate field for selection on whether to participate in CoD or not, in cases where the CoD functionality is triggered, all live quotes are mandatorily cancelled.

In Incoming Messages:

Message Code	Message Name	Field	Value	Notes
D / G	NewOrderSingle / OrderCancelReplaceRequest	CancelOnDisconnectionIndicator Tag: 21018	0 = Per Default Configuration	Default Value Order included in the scope of cancellations when CoD mechanism is triggered
			1 = Order not in the scope of Cancel On Disconnect	If selected, order is persisted, and it **not** included in the scope of cancellations when CoD mechanism is triggered

In Outdoing Messages:

Message Code	Message Name	Field	Value	Notes
8	ExecutionReport	CancelOnDisconnectionIndicator Tag: 21018	0 = Per Default Configuration	Provided only as a response to the Ownership Request [message OwnershipRequest (U18)] via Drop Copy
			1 = Order not in the scope of Cancel On Disconnect	

4.3 CLIENT DISCONNECTS FROM OEG

4.3.1 Normal disconnection at the End of session / Logout Message from Client

In Optiq, clients are encouraged to send a Logout message per OE Session (physical connection) in order to close their connection with the Exchange. The **Logout** (103) (FIX 5) message should be used for these purposes.

Sending of this message will trigger the Cancel on Disconnect mechanism, and will issue a cancellation of any orders submitted during the trading session that are flagged not to be persisted.

When the system shuts-down in a scheduled manner (i.e. not due to a failure; system reaches the Inaccessible phase) Cancel on Disconnect mechanism will no longer apply. For clients connected to the system when system reaches this phase any orders that haven't been cancelled due to their normal expiration or client triggered cancellation, will be transferred to the next trading session and will no longer be in scope of CoD.

Please note – order transferred to the next trading session may still be subject to cancellation by mechanisms other than CoD; i.e. at the start of the session in cases of a corporate event or expiration of GTD orders during start of day processing.

4.3.2 Client application does not reply to the Test request

After a predefined time of inactivity (delay value set per Optiq segment) from the client's OE Session (physical connection), the OEG sends a **TestRequest** (107) (FIX 1) message to that OE Session. In case client does not reply to this message within a pre-set amount of time with either a **Heartbeat** (106) (FIX 0), or any other application message, OEG will close the connection for the impacted OE Session.

Closure of connection by the OEG will trigger the Cancel on Disconnect mechanism for the impacted OE Session, and will issue cancellation of any orders submitted and owned by the impacted physical connection during the trading session and flagged not to be persisted.

While Optiq is detecting the failover, orders that belong to the impacted connection could be matched. As a consequence, members could receive trade Fill messages when reconnecting.

4.3.3 Disconnection due to technical issues between client application & OEG

In case client's OE session loses connectivity to an OEG, and depending on the activity of the OE session (physical connection) in question, Optiq may detect a client's disconnection sooner than the maximum time identified as the delay for the TestRequest / Heartbeat mechanism. As such the maximum period for detection of disconnection is between zero seconds and twice the maximum delay assigned to the Optiq Segment. In all cases, the CoD mechanism is triggered as soon as the disconnection is detected.

While Optiq is detecting the failover, orders that belong to the impacted connection could be matched. As consequence members could receive trade Fill messages when reconnecting.

4.4 EXCHANGE BUSINESS CONTINUITY CASES

4.4.1 Simple Partition failover (Single Partition in Segment, Non-Meshed Case)

Simple partition failover triggers cancelation of orders and quotes that have been sent during the current day, and were flagged as not to be persisted, from the impacted OEG. Simple partition failover covers the following cases:

- when the failover occurs on a single non-meshed partition, or
- when the connection on the partition that failed over does not own any orders on other partitions of the same Optiq segment, while the node B of an OEG is taking over

While Optiq is detecting the failover, orders that belong to the impacted connection could be matched. As a consequence, members could receive trade Fill messages when reconnecting.

4.4.2 Multiple Meshed (cross-linked) partitions & associated cases

Clients have the ability to send orders from one partition to another meshed (or cross-linked) partition residing within the same Optiq Segment. Instruments identified by Symbol Index and EMM allow one OEG to route the required messages to the ME of the partition where the instrument is hosted. Orders on the different (meshed) partition(s) are owned by the OE Session (physical connection) which submitted them, i.e. the session physically connected to the "original" sending partition. Such connections and orders are

subject to the cases of failure described below (e.g. disconnect between partitions within a single Optiq Segment, failover of one of the partitions).

4.4.2.1 Failover on the Partition to Which OE Session is Connected To

In case of failover, the scope of CoD is defined by the partition and any orders submitted from it to other partitions. CoD scope spans all instruments and orders for these instruments (that are flagged as CoD), that are hosted by the partition failing over. This includes any orders in scope, whether they are owned by the OE sessions connected to the partition failing over (original partition), or by the OE sessions connected to a meshed partition(s).

This section describes the case of failure on the partition to which the owner of the orders is connected to.

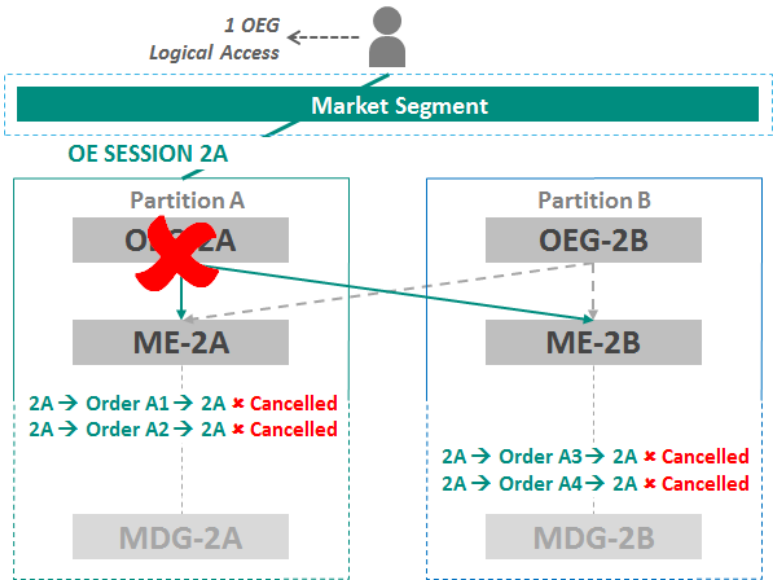
For any existing orders, owned by the OE Sessions connected to the original partition, that were submitted to the instruments hosted on the original partition, the OE session will receive **Kill** (05) (FIX 8) messages once the partition becomes once again available. When the start-up of the partition commences, any orders in scope of CoD are cancelled and **Kill** (05) (FIX 8) messages will be sent once clients reconnect to the partition.

For any existing orders, owned by the OE Sessions connected to the original partition, that were submitted to instruments hosted on the other meshed (cross-linked) partition(s), the orders will be cancelled as soon as the disconnection between the partition is detected, however the client's OE Session will receive the associated **Kill** (05) (FIX 8) messages only when the original partition becomes available.

Please note: The timestamp fields provided in the **Kill** (05) (FIX 8) messages will be set to the time when partition becomes available again.

For any messages submitted by the client, during the failover of the original partition, to the original or meshed partition, a client's connection will receive a "Technical Error" (5001) error message for those messages.

Messages for instruments hosted on the partitions unaffected by the failover, and submitted by the OE Sessions connected to those unaffected partitions, will be processed normally and won't be subject to CoD.



While Optiq is detecting the failover, orders that belong to the impacted connection could be matched. As a consequence, members could receive trade Fill messages when reconnecting.

4.4.2.2 Failover on the Partition to Which OE Session is NOT Connected To

In case of failover, the scope of CoD is defined by the partition, and not individual OE sessions. CoD scope spans all instruments and orders for these instruments (that are flagged as CoD), that are hosted by the partition failing over. This includes any orders in scope, whether they are owned by the OE sessions connected to the partition failing over (original partition), or by the OE sessions connected to a meshed partition(s).

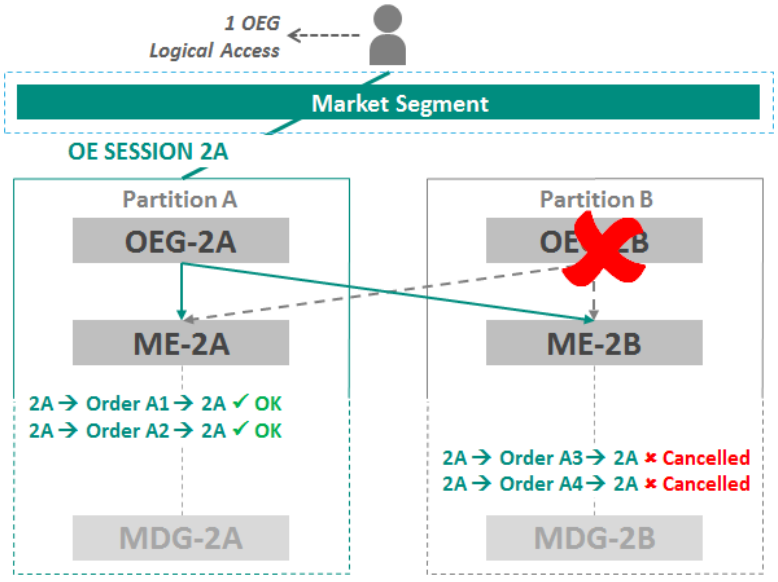
This is the case of failure of the partition to which the owner of the orders is NOT connected to, but has submitted orders via other partitions.

For any existing orders, owned by the OE Sessions connected to the original partition, that were submitted to the instruments hosted on the original partition, there will be no impact, and they will not be in scope of CoD triggered in this case.

For any existing orders, owned by the OE Sessions connected to the original partition, that were submitted to instruments hosted on the other meshed (cross-linked) partition(s), the OE session will receive **Kill** (05) (FIX 8) messages when the partition becomes available again. When the start-up of the partition commences, any orders in scope of CoD are cancelled and **Kill** (05) (FIX 8) messages will be sent once clients reconnect to the partition.

For any messages submitted by the client to the original or meshed partition, after failure has been detected and before a partition is available again, a client's connection will receive a "Technical Error" (5001) error message for those messages.

Messages for instruments hosted on the original partition, or any other partitions within the Optiq Segment unaffected by the failover, and submitted by the OE Sessions connected to those unaffected partitions, will be processed normally and won't be subject to CoD.



While Optiq is detecting the failover, orders that belong to the impacted connection could be matched. As a consequence, a member could receive trade Fill messages when reconnecting.

4.4.2.3 Network Disconnection Between Partitions within a Single Optiq Segment

Any orders that belong to the meshed partitions (crossed-linked between partitions) will be subject to CoD if the connectivity between the partitions is lost between them. Orders existing on both partitions, even if the partitions themselves remain active, will be considered as being in scope of CoD and will be cancelled.

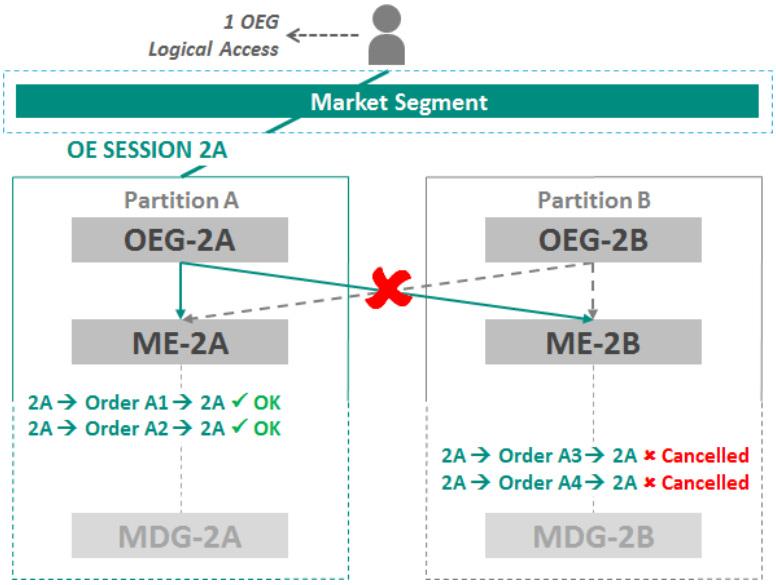
Partitions within the same segment monitor their connectivity to each other, and if connection is lost, and CoD is triggered, OE sessions on each partition will receive the associated Kill messages when the two partitions reconnect to each other.

If client attempts to submit new messages to the instruments hosted on the meshed partition(s) clients will receive a “Technical Error” (5001) error message for those messages.

Examples below provide more details on how the associated mechanisms will function. These examples in all cases assume that orders were submitted during that day’s trading session and are flagged with default setting of CoD set to Yes (orders not persisted).

Example 1: Single connection to one partition, with orders submitted to multiple meshed partitions

OE Session (physical connection) 2A on partition A submits orders A1 and A2 on instruments hosted on partition A, and orders A3 and A4 on instruments hosted on partition B. When connection is lost between the two partitions, orders A3 and A4 are in scope of CoD and are cancelled.

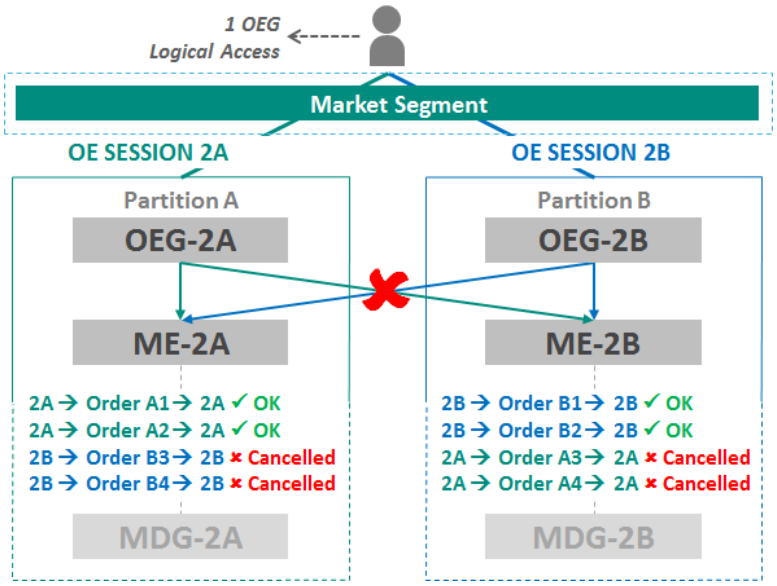


Example 2: Connections to multiple partitions, with orders submitted to multiple meshed partitions

OE Session (physical connection) 2A on partition A submits orders A1 and A2 on instruments hosted on partition A, and orders A3 and A4 on instruments hosted on partition B.

OE Session (physical connection) 2B on partition B submits orders B1 and B2 on instruments hosted on partition B, and orders B3 and B4 on instruments hosted on partition A.

When connection is lost between the two partitions, orders B3 and B4 owned by connection 2A, AND orders A3 and A4 owned by connection 2B, are all in scope of CoD and are cancelled.



Any orders on the partition that is not meshed, and which itself didn't lose connection from the client, will be maintained and will not be in scope of CoD.

While Optiq is detecting the failover, orders that belong to the impacted connection could be matched. As a consequence, member could receive trade Fill messages when reconnecting.

4.4.3 Cancel on Disconnection for Cases of Disaster Recovery (DR)

4.4.3.1 Pre-scheduled Disaster Recovery Testing

During pre-scheduled, agreed Disaster Recovery (DR) tests, the Exchange has the ability to disable CoD functionality to facilitate testing. Whether this option is taken for individual DR tests will be communicated by the exchange for the individual instances of tests.

4.4.3.2 Business Continuity Event with Failover to the Secondary Data Center

In case of an event which triggers failover to the secondary data center (Disaster Recovery infrastructure) CoD functionality will be triggered by the DR environment, according to the policy, rules and cases defined for Disaster Recovery policy.

5. OEG THROTTLING

Objectives of OEG throttling are similar to those found in any system that has to manage high amount of message exchange with multiple participants, to:

- Regulate message / data traffic by evening out the concentration flow of messages, and distributing the use of available system processing ability and bandwidth across all users of the system
- Help minimize or limit message exchange and processing congestion, which assists in ensuring latency of the trading system remains stable and predicable
- Reduce the risk of disruptive events

Furthermore, for a trading venue OEG throttling mechanism allows to:

- Prevent disorderly trading conditions and detect potential threats to the orderly functioning of the market
- Ensure compliance with the articles in MIFID II supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organizational requirements of trading venues *(a.k.a. RTS7)*

The Optiq throttling solution is built to provide flexibility and predictability.

- Flexibility: clients can choose:
  - how many messages they can send (vs. how often) to avoid being throttled
  - how their throttled messages should be handled (Rejected or Queued)
- Predictability: in most cases clients can use the concepts and formulas provided to calculate the number of messages and time required, without having to wait for Optiq to send them specific messages

Optiq OEG Throttling applies in the same manner to the Euronext Cash and Derivatives markets.

⚠ **Important note**: Clients are strongly encouraged to review the explanations provided in the various OEG and MDG specification, Connectivity specifications and kinematic documents in detail before continuing with this document

5.1 MAIN CONCEPTS & LIMITS FOR OEG THROTTLING

The section below provides details on the concepts and limits used for OEG throttling. Please note that some of the concepts listed below have further explanations in dedicated sections within this document.

- Overall throughput limit / Per second rate: the max number of messages setup as the rate for the Logical Access, and used by its physical connections
  Example: 100 messages per second
  - Client connections cannot go over this limit defined as their rate within a second. This is accomplished mechanically, as the more granular size / time management of throttling limit will keep the overall throughput within the rate limit
- Max burst (or bucket) size: the max number of messages that a client may send at once before being throttled, in a single "burst" of messages (measured in number of messages).
  - represents a constant figure, calculated as a fraction of the overall throughput limit
- Time to replenish a single message: time needed for a single token to be added into the bucket
  - This time equals to: 1 divided by the client's rate (1/throughput)

Example: if client's rate is 100 messages per second, then Time to replenish will be 1/100 = 0.01 second

- Token: Represents the system's ability to process 1 message. 1 token gives the right to send 1 message
- Bucket: is a measuring mechanism used to calculate how many messages can still be sent and when, in order not to be throttled. The bucket doesn't store any messages. All messages are stored in the queues
  - Size of the bucket: Bucket is currently 100% of the client rate per second, and is measured in tokens
  - The bucket size is the maximum number of messages that can be sent at once (or a burst)
  - Messages in the bucket start being used upon client sending a single application message to the OEG, as such the bucket use employs the concept of the sliding window
- Scope of Messages for Throttling:
  - All **application** messages are in scope of throttling (no exclusion list), including those rejected by the OEG for non-throttling reasons. Each application message uses up an available token. This is the main level of throttling in the mechanism.
  - All **administrative** messages and **technically invalid** messages are out of scope of main throttling mechanism, but do contribute to the anti-flooding mechanism
  - All messages are in scope of the anti-flooding mechanism

5.1.1 Summary of Formulas

Concept / Limit	Formula
Throttling queue – Ts (messages)	For Queuing – 2 x Rate (size) of connection For Rejection - Zero
Size of the Bucket – Sb (messages) This is the allowed burst size, i.e. max number of messages a session can send in a row before the throttling kicks in.	100 % of the rate
Replenish Time (to replenish single token [Tr] (seconds))	1/throughput **
Maximum # of "burst" messages to send at once (messages)	Equal to Sb
Wait time to send 1 (more) message (seconds)	1/throughput
Wait time to send "X" messages	(1/throughput) * X (messages)
Max messages before rejection (messages)	Ts + Sb

*** Rounding is clarified in the section below*

5.1.2 Notes on rounding

1) Figures expressed as rate (msgs / sec) are rounded down to the lower nanosecond.

   Example: The replenish time is 1/Throughput. If Throughput is equal to 375 messages/second, the calculated time when token will be put back into the bucket is every 0.00266666666666666666666666666667 seconds. The figure used is rounded down to the lower nanosecond, that is 2666666 nanoseconds (2,666666 milliseconds).

2) Currently not in use - *Figures expressed in number of messages are rounded up to the closest whole number.*

5.1.3 Private Messages Used by the OEG Throttling Mechanism

Optiq supports the following sub-set of private OEG messages that participate in the process of (i) throttling, (ii) settings of throttling configuration, and (iii) communicating the reasons for throttling event or disconnection.

Message Name	SBE Message Code	FIX Message Code	Details
Logon	100	A	Used to select queue vs. reject behavior for throttling
Technical Reject	108	3	Used to indicate rejection of messages due to throttling, and the reason throttling event occurred This message is not sent to Drop Copy
Logout	103	5	Used to indicate reason for disconnection in case of anti-flooding

For more details about these messages clients are advised to review the OEG client specifications for SBE and FIX protocols.

5.1.4 Use of the Bucket Concept

- Each message sent to the OEG uses up a token
- The maximum size of the bucket is always constant. The size of bucket never goes above the maximum size, even if client does not send any messages for a long period of time
  - Any tokens above the size of the bucket disappear, i.e. fall out of the bucket and are not counted
- On every logon bucket is full, allowing them to immediately start sending messages.
  - i.e. client can send a burst of the full bucket size following logon
- When choosing bursts, clients are free to choose the size of their bursts as long as the bursts don't exceed the bucket size, and wait for replenishment before sending the next burst. Both policies can also be combined, taking into account the same two constraints.
- If the bucket is empty, client messages are either rejected or stored in a throttling queue
- 1 token is put back into the bucket (replenished) after a single period of time equal to "Time to Replenish" has passed
- The number of messages in the bucket is replenished continuously up to the maximum size of the bucket, independently of whether client submitted new messages or has been inactive for a long period of time

5.2 OEG THROTTLING INTERACTION WITH OTHER MECHANISMS & COMPONENTS OF OPTIQ

- **High Availability (HA):** OEG throttling mechanism works in the same manner on the Mirror instance of the OEG, in any HA scenario, as it does on the Primary instance, with identical settings and limits.

  In the case of an HA event, any messages that were in a throttling queue are dropped, without further notification to the client.

- **Business Continuity (DR):** OEG throttling mechanism works in the same manner in the Disaster Recovery environment as it does in Production, with identical settings and limits.

  In the case of a Business Continuity event, any messages that were in a throttling queue in Production environment are dropped, without further notification to the client.

- **MDG**: OEG throttling and associated messages are not reflected in any public messages.
- **Drop Copy:** OEG throttling does not apply to Drop Copy gateways.

5.3 DETAILS OF OEG THROTTLING

The sections below provide the details associated to the OEG Throttling mechanism, associated concepts and limits.

5.3.1 Queue vs. Reject

At log on, clients choose whether to queue or to reject messages once the throttling limit is reached.

In the **Logon** (100) / (FIX A) message, the field used is

- SBE: *Queueing Indicator*
- FIX: *QueueingIndicator* (tag: 21020)

Where values used are:

- **0** – False, which indicates clients wish to Reject over the limit messages
- **1** – True, which indicates clients wish to Queue over the limit messages

If client chooses to Reject – any limit breached will result in a rejection message.

If client chooses to Queue – over the limit messages are stored in a limited size Throttling queue.

Please note – any messages rejected due to throttling are not read by the OEG. **The sequence number of rejected messages is not taken into consideration by the OEG**. If clients do not take this into account on the FIX protocol, a gap in the sequence number will occur. When sending messages after being rejected, the OEG will initiate the standard FIX protocol mechanism for reset of sequence / gap fill.

5.3.2 Communication of Throttling Events

In case of any rejection due to OEG throttling, Optiq sends the following rejection messages & codes:

- In SBE, clients receive **TechnicalReject** (108) message, where the field *Error Code* is set with the value indicating the reason throttling event has occurred.
- In FIX, clients receive **Reject** (3) messages, where the field *SessionRejectReason* (tag: 373) is set with the value indicating the reason throttling event has occurred.

Three types of rejection are possible in OEG throttling. The table below provides the correspondence of values used for these three types of rejection in SBE and FIX:

SBE Error Code	FIX SessionRejectReason (373)	Description of the OEG Throttling Rejection
2085 = Rate exceeded	26 = Throttling Rate exceeded	Individual message sent is over the limit allocated to the Logical Access. This rejection occurs when client chose to Reject over the limit messages
2087 = Throttling queue full	25 = Throttling queue full	This rejection occurs when client choses to Queue over the limit messages, and after the initial throttling queue limit based on the rate is breached, and the throttled messages are stored in the throttling queue, the limit of the queue has also been breached.
2086 = System busy	27 = System busy	This rejection may occur when client chose to Reject over the limit messages, and the system is overloaded by processing of previously

SBE Error Code	FIX SessionRejectReason (373)	Description of the OEG Throttling Rejection
		sent messages and can't accept more messages until the processing has finished.

5.3.3 Behavior in Case of Queueing

After a client's OEG throttling limit is breached, and the client chose to queue their messages, over the limit messages are stored (or queued) in a buffer called throttling queue.

From the throttling queue:

- messages are processed one at a time at a pre-defined period of time (replenish time)
- messages being processed from the queue are
  - considered as activity, and during 1 second do not strictly require client sending a heartbeat
  - consume 1 token for each messages processed from the queue

While messages in the throttling queue are processed:

- the client may submit additional messages which will also be stored in the throttling queue, until the queue limits have been reached
- as throttling queue is limited in size to the maximum of the throughput,
  - **any messages over the queue size are rejected**, even if the client chooses to queue their messages
  - as soon as a single message is processed from the throttling queue, and a replenish time has passed, the client's next submitted messages will be added to the throttling queue
  - clients do not receive a specific notification message for messages that were queued, however the acknowledgement messages have a field that indicates that the message in question was queued due to throttling
    - SBE: **Ack** (03) message contains a field *Ack Qualifiers*, one of the positions of which is used for the Queue Indicator. For messages that were queued due to OEG throttling this position is set to one (1)
    - FIX: **ExecutionReport** (8) message contains a field *AckQualifiers* (tag: 21014), one of the positions of which is used for the Queue Indicator. For the acknowledgement of new order messages that were queued due to OEG throttling this position is set to one (1)
- even if clients choose to Queue their over the limit messages, if their connections breach their rate, either with a large number of messages, or data, within the allocated time, such messages are not processed.

⚠ **Important note**: In such cases, and especially if the client is disconnected for any reason,

- client messages may not be acknowledged or rejected, and
- the queue is dropped

Clients are strongly urged to send at maximum their rate per second to guarantee no rejections.

5.3.4 Behavior in Case of Rejection

After a client's OEG throttling limit is breached, and the client chose to reject their messages, over the limit messages are rejected.

A rejection message will be sent to identify messages processed by the OEG that are over the throughput limit.

Note that throttling is applied at the individual message level. One message can be throttled at one given time, even though a previous or subsequent message can be accepted.

To provide an indication of which message is rejected due to OEG throttling, the following fields are provided in the rejection messages:

- SBE**: TechnicalReject** (108) message contains the following fields for this purpose:

Field	Short Description
Rejected Client Message Sequence Number	Indicates the Client Message Sequence Number of the rejected message
Rejected Message	Provides the Type of message rejected, by indicating its Template ID
Error Code	Indicates the type of OEG throttling rejection that occurred

- FIX: **Reject (3)** message contains the following fields for this purpose:

Tag	Field	Short Description
45	RefSeqNum	Indicates the reference sequence number of the rejected message
372	RefMsgType	Provides the Type of message rejected, by indicating its MsgType (35)
373	SessionRejectReason	Indicates the type of OEG throttling rejection that occurred

The rejection messages do not contain any of the following identified fields: Client Order ID, Order ID, Quote Request ID or Mass Status Request ID

5.3.5 Behavior for Excessive Breach of Rate

In addition to the queue and rejection in place when the throttling limit is reached, the Exchange sets a limit for excessive breaching (either in number of messages or amount of data sent), of the assigned rate / size of connection.

Excessive breaching means that the client attempted to submit a number of messages, or amount of data in bytes, that is multiple times over their allowed rate.

In case a client's connection breaches their rate limit, either in number of messages or in the amount of data, such connections will be immediately disconnected, and won't be allowed to reconnect for 3 seconds. If a client's connections are breaching limits in this manner multiple times and are continuously disconnected, Market Operations will contact the client and may choose to suspend the client's access.

This case could occur due to various reasons, including a technical issue in the client's system. To assist clients in identifying the issue and correcting it as quickly as possible, the **Logout** (103) / (FIX 5) message sent on disconnection in such a case provides specific values identified below.

Case	How to Identify the Case in Logout message	
	SBE [Log Out Reason Code]	FIX [SessionStatus (tag: 1409)]
Excessive number of message	3 = Excessive Number of Messages	106 = Excessive Number of Messages
Excessive amount of data in bytes	4 = Excessive Amount of Data in Bytes	107 = Excessive Amount of Data in Bytes
Excessive number of messages and amount of data in bytes	5 = Excessive Number of Messages & Amount of Data in Bytes	108 = Excessive Number of Messages & Amount of Data in Bytes

5.3.6 Behavior on Intra-session Disconnection

The OEG throttling behavior in case of intra-session disconnection is independent of (i) whether the disconnection occurred in the Exchange or Client systems, (ii) whether it occurred on the same instance of the OEG continuously available, or (iii) whether a disruptive incident triggered a HA or a Business Continuity event.

- Any messages at the moment of disconnection present in the throttling queue are dropped, as if never received by the Exchange. Such messages do not receive acknowledgement or rejection from the OEG
- On Reconnection, during the usual sequence number processes and resynchronization mechanism, clients could receive throttling rejection messages that serve as an indication of messages that were throttled and as such were never processed prior to the disconnection.

5.4 GUIDELINES FOR CLIENTS

5.4.1 What To Do After OEG Throttles Messages

Various cases of OEG throttling may occur and are identified by the fields provided in rejection and logout messages. The section below provides the guidelines on measures clients should adopt following an OEG throttling event.

5.4.1.1 Over the OEG Throttling Limit (Queueing)

For clients that choose to queue throttled messages over the OEG throttling limit, queued messages are indicated by a flag in the Ack message. Such messages are processed by the Exchange with a delay associated to queuing.

As the maximum size of the OEG throttling queue is equal to the rate of the client's connection for the duration of 2 seconds, the processing of the queued messages, in normal conditions, is expected to last between 0 and 2 second, depending on the number of messages being queued.

To avoid being queued clients should:

- assess the speed and/or number of messages being sent by their system and either
  - reduce the frequency of sending to be in line with their replenish time, or
  - reduce the number of messages sent to be in line with the rate and associated throttling limits set for their logical access

5.4.1.2 Over the Throttling Queue Size (Queueing)

A customer can be rejected when they choose to queue messages and they send more messages than the number available in the queue.

If a client receives a rejection indicating that their messages were throttled because their throttling queue is full (flagged as follows):

SBE			FIX		
Message	**Feld**	**Value**	**Message**	**Feld**	**Value**
Technical Reject (108)	Error Code	2087 = Throttling queue full	Reject (3)	SessionRejectReason (373)	25 = Throttling queue full

The message rejected is not processed by the Exchange. Clients should:

- take this rejection into consideration in their system, and if required resend an instruction to the exchange,
- wait for, at minimum, 1 replenish time period before sending any further messages,
- assess the speed and/or number of messages being sent by their system and either
  - reduce the frequency of sending to be in line with their replenish time, or
  - reduce the number of messages sent to be in line with the rate and associated throttling limits set for their logical access

5.4.1.3 Over the OEG Throttling Limit (Rejection)

For clients who choose to reject messages over the throttling limit. If a client receives a rejection indicating that their messages were throttled because they have exceeded their rate (flagged as follows):

SBE			FIX		
Message	Feld	Value	Message	Feld	Value
Technical Reject (108)	Error Code	2085 = Rate exceeded	Reject (3)	SessionRejectReason (373)	26 = Throttling Rate exceeded

The message rejected is not processed by the Exchange and clients should:

- take this rejection into consideration in their system, and if required resend an instruction to the exchange,
- wait for, at minimum, 1 replenish time cycle before sending any further messages,
- assess the speed and/or number of messages being sent by their system and either
  - reduce the frequency of sending to be in line with their replenish time, or
  - reduce the number of messages sent to be in line with the rate and associated throttling limits set for their Logical Access

5.4.1.4 System Busy (Rejection)

If a client receives a rejection indicating that their messages were throttled because System is Busy (flagged as follows):

SBE			FIX		
Message	Feld	Value	Message	Feld	Value
Technical Reject (108)	Error Code	2086 = System busy	Reject (3)	SessionRejectReason (373)	27 = System busy

This rejection may occur when the client chooses to reject messages over the throttling limit, but the system is overloaded by processing of previously sent messages and cannot accept more messages until the processing has finished.

The message rejected is not processed by the Exchange and clients should:

- take this rejection into consideration in their system, and if required resend an instruction to the exchange
- wait for, at minimum, 1 second before sending any further messages,
- review the Market Status page for information on a possible disruptive incident,
- assess the speed and/or number of messages being sent by their system and either

- reduce the frequency of sending to be in line with their replenish time, or
- reduce the number of messages sent to be in line with the rate and associated throttling limits set for their logical access

5.4.1.5 Excessive Breaches of Rate

In case a client is disconnected with one of the excessive breaches of message or data reasons, the reason for such disconnection is identified in the **Logout** (103) / (FIX 5) message in the fields identified in the table below for each protocol.

Case	How to Identify the Case in Logout message	
	SBE [Log Out Reason Code]	FIX [SessionStatus (tag 1409)]
Excessive number of message	3 = Excessive Number of Messages	106 = Excessive Number of Messages
Excessive amount of data in bytes	4 = Excessive Amount of Data in Bytes	107 = Excessive Amount of Data in Bytes
Excessive number of messages and amount of data in bytes	5 = Excessive Number of Messages & Amount of Data in Bytes	108 = Excessive Number of Messages & Amount of Data in Bytes

In case of such a disconnection clients are urged to review the rate at which they are sending messages to the OEG vs the allowed rate for the logical access, or assess if there is a technical issue in the client's system. For further assistance clients should contact one of the Exchange's support teams.

5.4.2 How to Avoid being Throttled & Examples

If the message throughput is linear, clients need to ensure the maximum number of messages sent to the OEG are below the throttling limit.

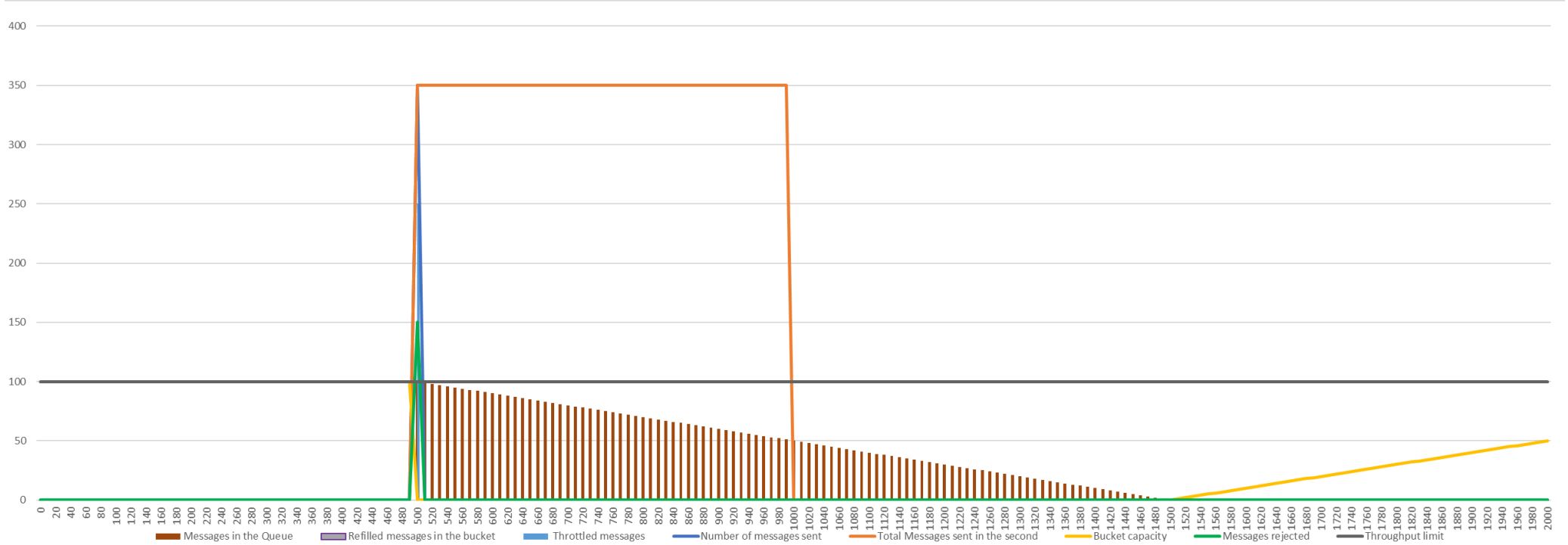
If the message throughput is split into bursts, clients need to respect the buckets available and monitor their tokens available.

Examples in the section below provide indicative information for different behaviors and chosen methods for management of throttling.

⚠ **Important note**: The values and distribution of messages will be different depending on the throughput of individual connections, client's rate of message injection and examples below should not be used to calculate the actual rates and limits of throttling.

5.4.2.1 Flooding, in Queueing Case

Assumptions: Logical access for 1 session with 1 partition, throughput is 100 msg / second.
Client sends a burst of 350 messages. 50 messages get rejected for excessive breach, 200 are queued, and 100 are immediately processed by the system.
For the next 2s, the queue is processed and the bucket is used by the queue.



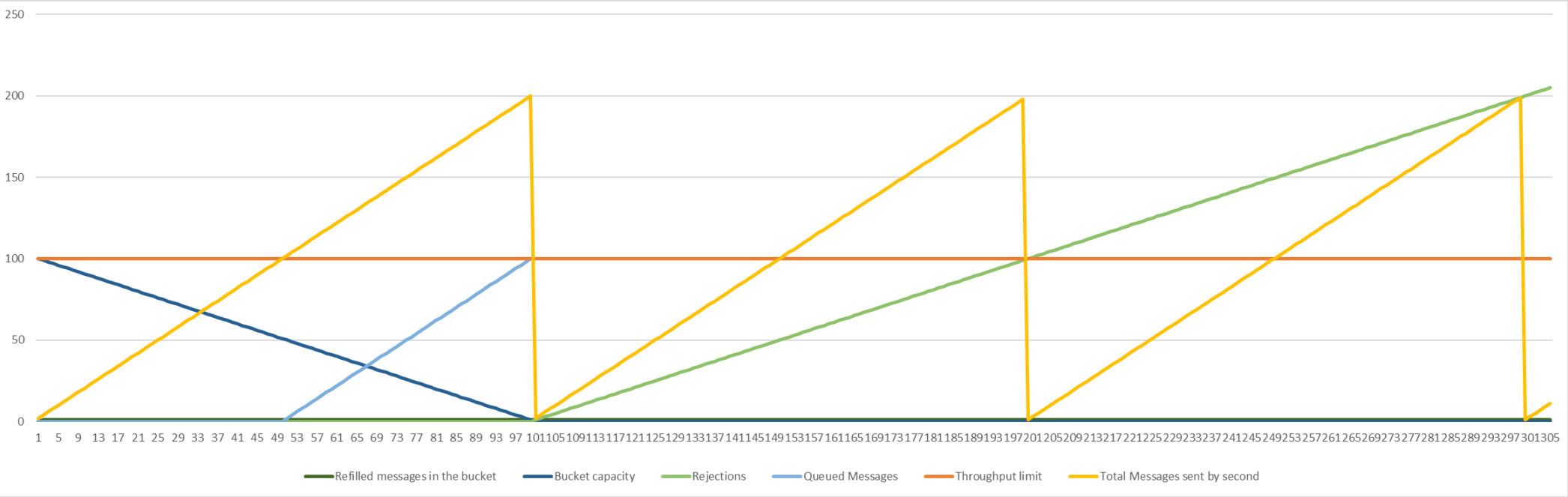
Reason for Throttling: The client sends multiple times their rate. Flooding increases the risk of disruptive incidents and may give rise to disorderly trading conditions, which the Exchange is obligated to avoid.

Recommendation: Distribute messages within the throughput and time allocated to the logical access

5.4.2.2 Queuing Cases

Linear injection, with messages above throttling queue

Assumptions: Logical access for 1 session with 1 partition, throughput is 100 msgs/s.



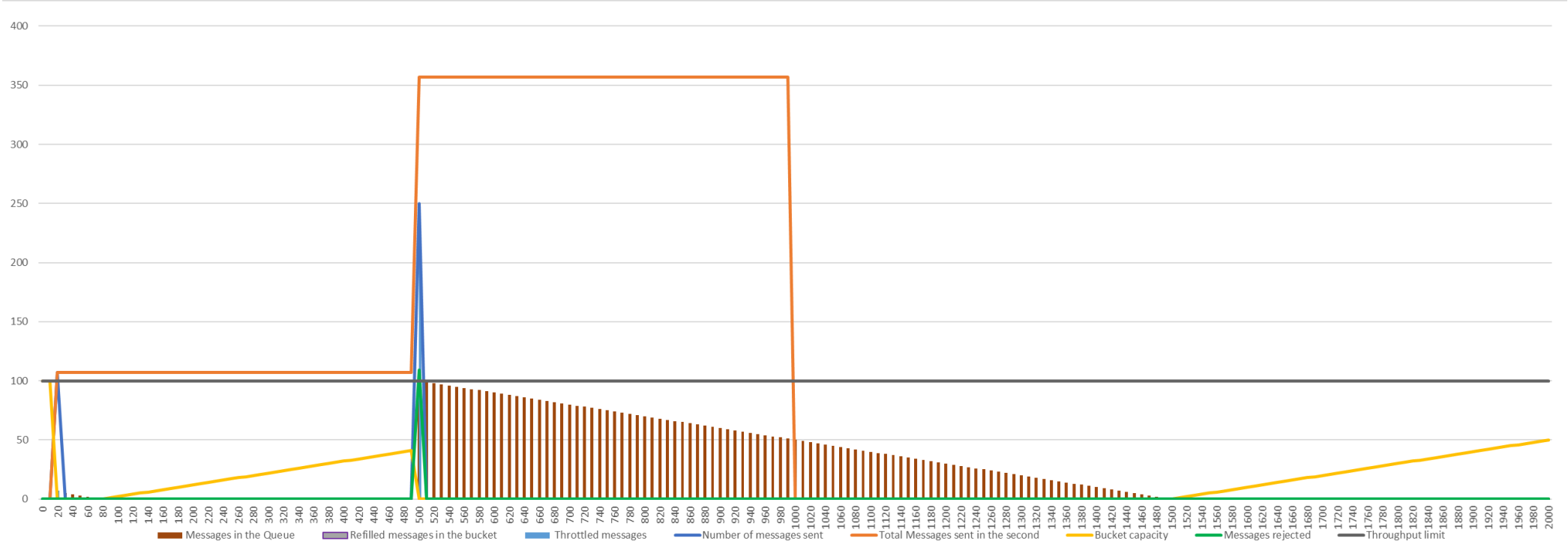
Reason for Throttling: While sent in small number of messages on the continuous basis, the overall sum of messages sent within 1 second is more than the throughput.

Recommendation:

- send fewer messages than the 1 bucket + throttling queue size, within 1 second, to avoid message being rejected over the size of the throttling queue
- split the sending of bursts into fewer messages, which allows for shorter amount of time before the next sending is possible

Injection in Bursts, with messages above the limit of the throttling queue

Assumptions: Logical access for 1 session with 1 partition, throughput is 100 msgs/s.



Reason for Throttling: While not sent in one burst, the overall sum of messages sent within 1 second is more than twice the throughput.

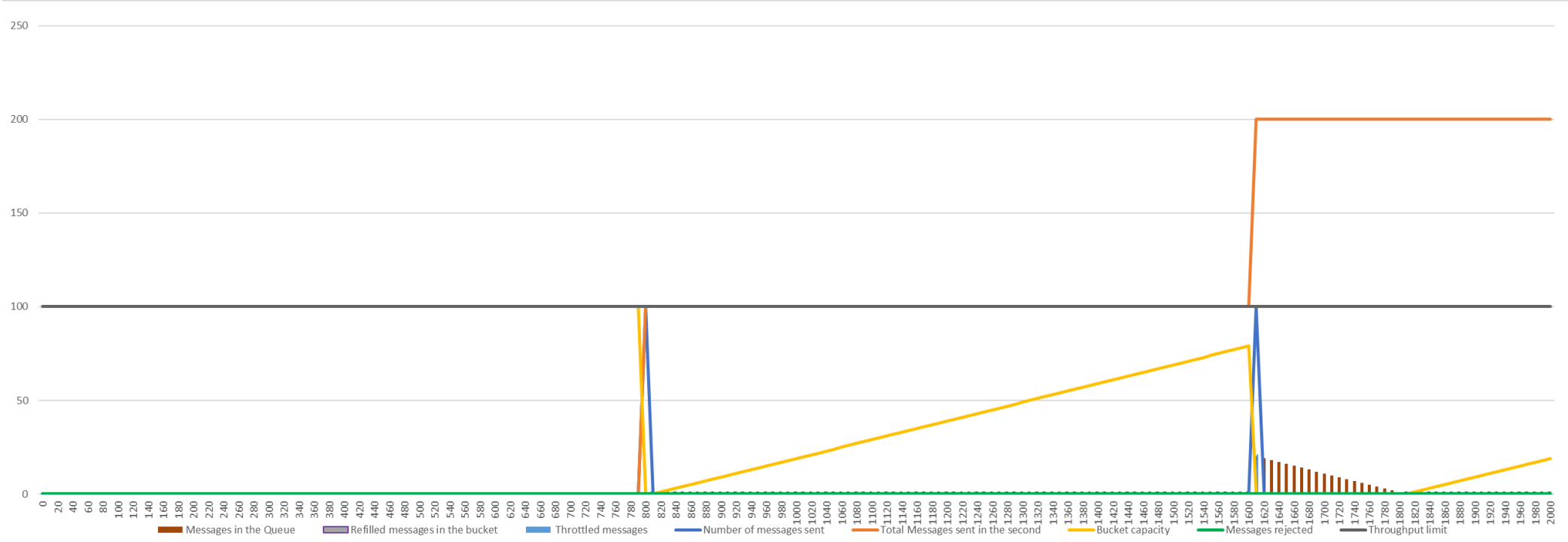
Recommendation:

- send fewer messages than the 1 bucket + throttling queue size, within 1 second, to avoid message being rejected over the size of the throttling queue
- split the sending of bursts into fewer messages, which allows for shorter amount of time before the next sending is possible

The kinematics of this case (Queueing - Injection in Bursts, with messages above the limit of the throttling queue) are as follows.

Injection in Bursts, with queuing of messages above the throttling limit

Assumptions: Logical access for 1 session with 1 partition, throughput is 100 msgs/s.

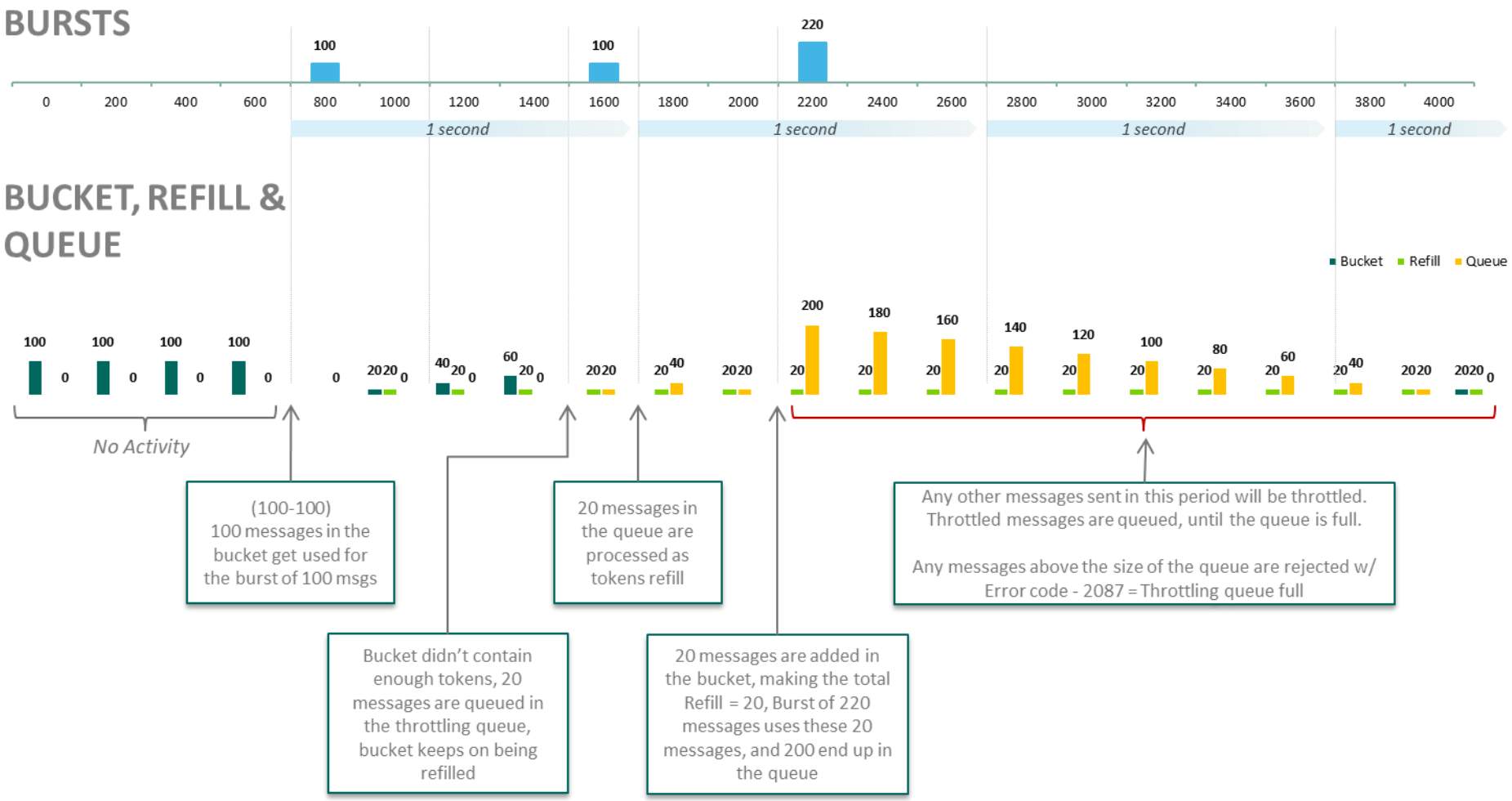


Reason for Throttling: Bursts are larger than the bucket size, or are sent too quickly.

Recommendation:

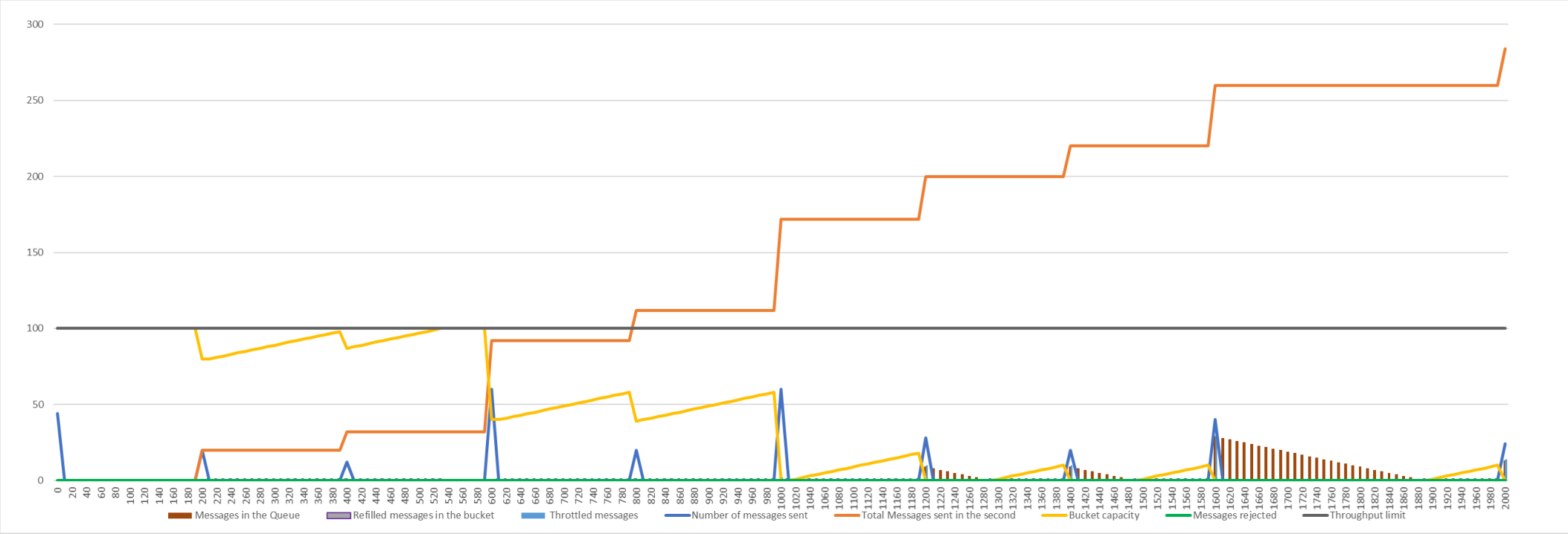
- send at maximum the number of messages equal to the allocated throughput to ensure no rejection over the throttling queue limit. Any messages over the bucket size will be queued until fully processed
- split messages into smaller bursts. This will reduce amount of queued messages
- wait for the period of time required to fully replenish the bucket before sending their full bucket size again

The kinematics of this case (Queueing - Injection in Bursts, with queuing of messages above the throttling limit) are as follows:



Linear Injection

Assumptions: Logical access for 1 session with 1 partition, throughput is 100 msgs/s.

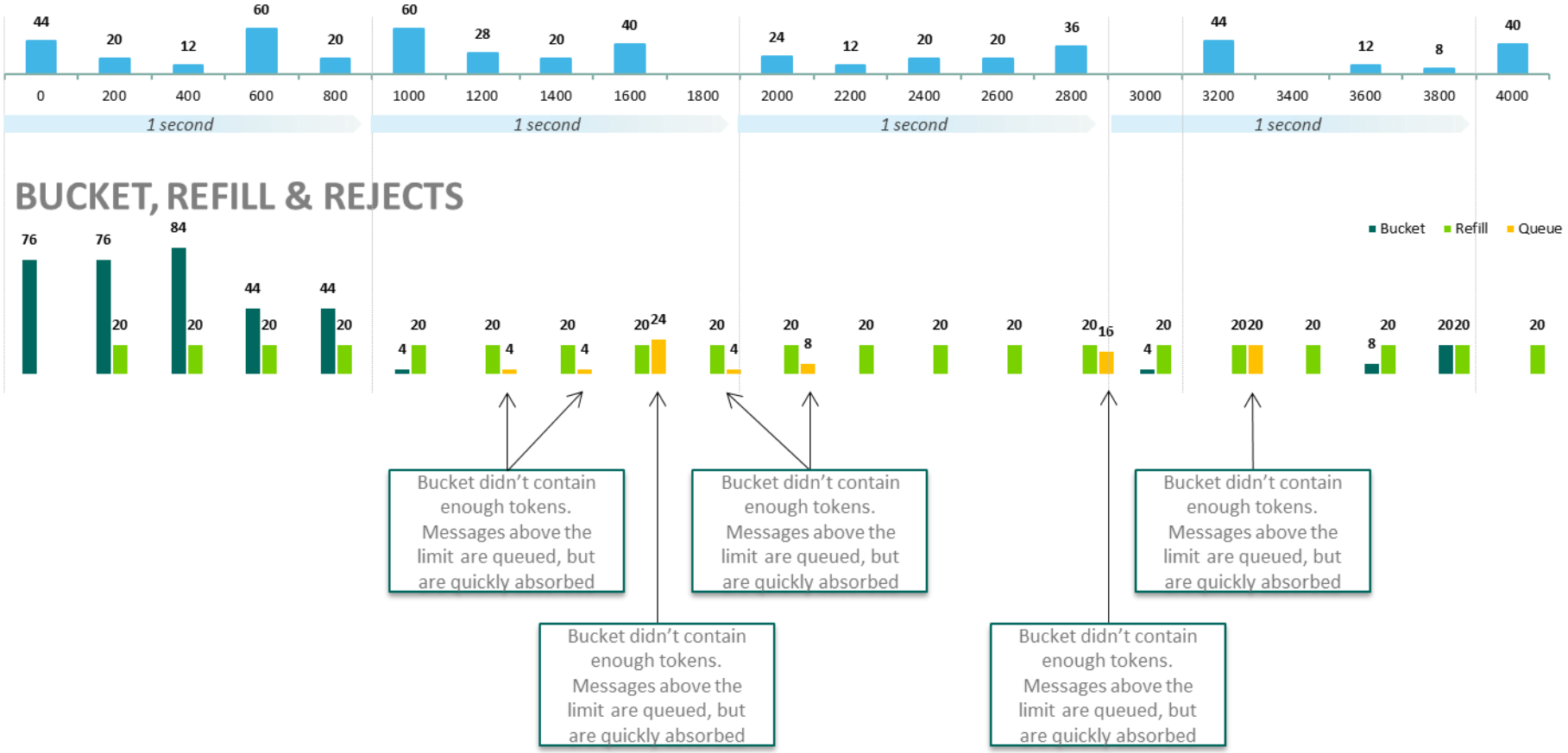


Reason for Throttling: The client sent more messages than the allocated throughput, and some messages are queued

Recommendation:

- send fewer messages than the bucket size, no more frequently than the associated replenish time. This avoids queueing of messages

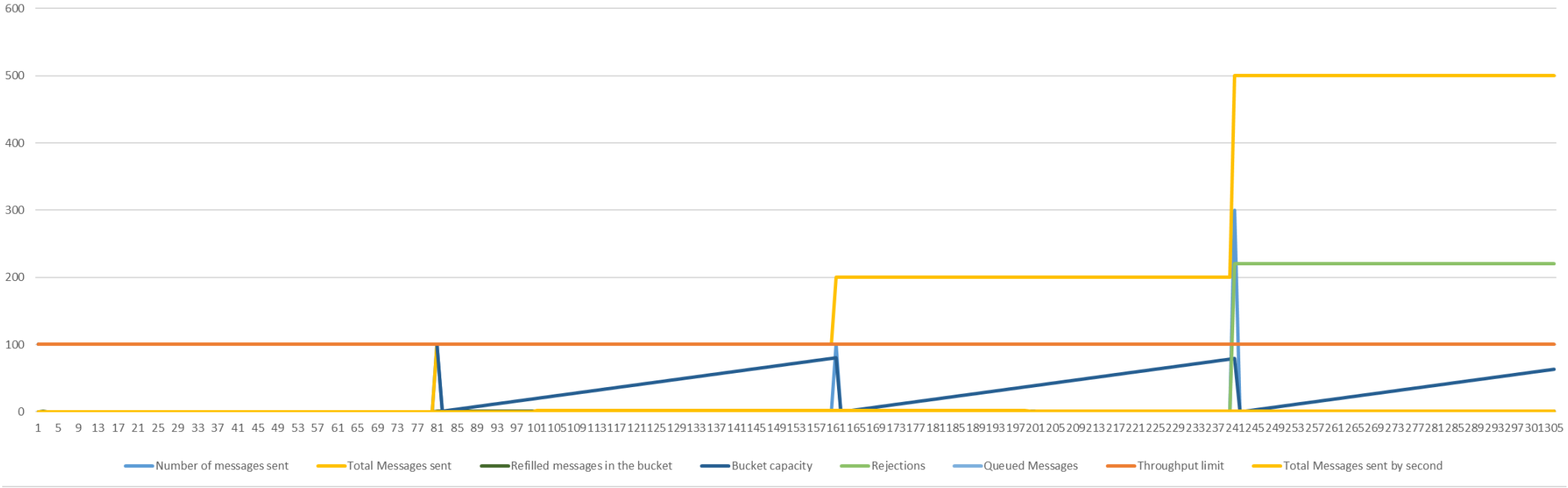
The kinematics of this case (Queuing - Linear Injection) are as follows:



5.4.2.3 Rejection Cases

Injection in Bursts

Assumptions: Logical access for 1 session with 1 partition, throughput is 100 msgs/s.

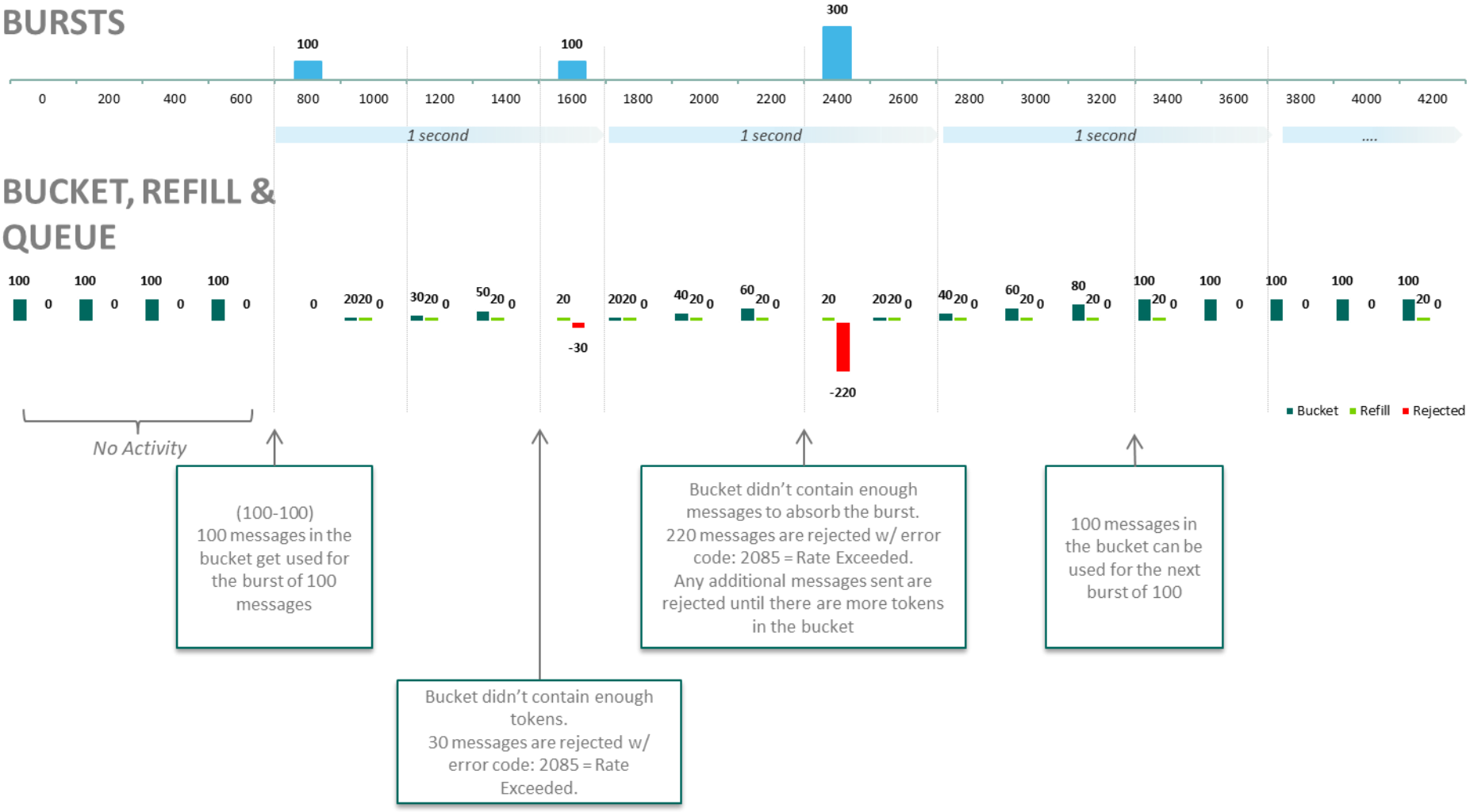


Reason for Throttling: The client sent more messages than the allocated throughput or too quickly (more frequently than 1 second)

Recommendation:

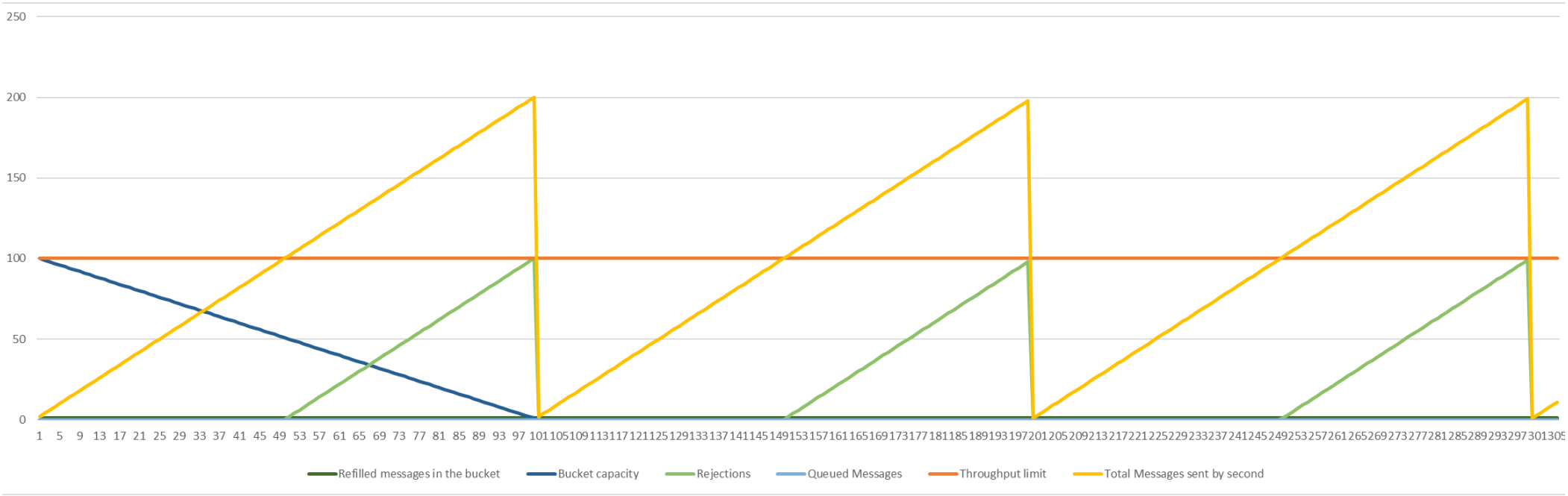
- send at once at maximum the number of messages equal to their bucket size, and wait for the period of time required to fully replenish it, before sending their full bucket size again to avoid being rejected

The kinematics of this case (Rejection - Injection in Bursts) are as follows:



Linear Injection

Assumptions: Logical access for 1 session with 1 partition, throughput is 100 msgs/s.



Reason for Throttling: The client sent more messages than the allocated throughput

Recommendation:

- As in case of queueing, client should send fewer messages than the bucket size, no more frequently than the associated replenish time. This allows to avoid queueing of messages

The kinematics of this case (Rejection - Linear Injection) are as follows:

6. HIGH AVAILABILITY & BUSINESS CONTINUITY: FUNCTIONAL OVERVIEW

6.1 MAIN CONCEPTS OF TRADING CHAIN RECOVERY IN OPTIQ

Section below provides high level description of the high availability and business continuity concepts and features in Optiq.

In Optiq High Availability (HA) and Business Continuity (DR) functionalities function in the same manner for the Euronext Cash and Derivatives markets.

⚠ **Important note**: Clients are strongly urged to review the explanations provided in the various OEG and MDG specification and kinematic documents in detail before continuing with this document.

6.1.1 High Availability (HA)

In the event of disruptive incident resulting in failure of a partition Optiq trading chain application will switch client system processing from Primary instance of this partition (or node) to its Mirror instance within the same environment. This is a case of a High Availability (HA) event / failover.

HA event occurring on the Exchange's trading system will at minimum encompass all components, OEG, ME and MDG, of a partition. In a segment containing multiple partitions, a single partition may go through an HA event independently from all of the other partitions within the segment.

The same IP address is used for the Primary and Mirror instances of the partition and the Exchange manages the switch between the instances via the recovery mechanism. This means no additional connectivity setup is required for the Primary and Mirror instances making the connectivity aspects of the switch transparent to the clients.

For the Production environment to facilitate the standard Exchange High Availability mechanism Primary and Mirror instances are hosted in a cluster.

As identified elsewhere in this document, in case of disconnection due to HA, messages in throttling queue are dropped as if never received.

Intentional Increment of Sequence Number:

- In some cases when partition Primary instance fails over to the Mirror the message sequence number may be intentionally increments by a pre-defined number. This is being done specifically for cases of disruptive incidents (either HA or Business continuity) to guarantee delivery of full scope of messages for resynchronization and to reduce number of unexpected rejections of client Logon attempts.
- The values of this increment are provided in the section "Segment-Wide Configuration Settings" in this document.
  Currently on Optiq this value is set to 1000 for all trading segments. If any changes are done to this increment clients will be informed ahead of time.
  To simplify explanation throughout this section the increment used is 1000, however clients should review values provided in the section "Segment-Wide Configuration Settings" to have the most up to date setup information.

The partition ID, as well as the Logical Access ID and assigned port remains unchanged between the Primary and Mirror. For MDG multicast groups and ports will not change either.

For MDG: When a market data source restarts and is not able to keep its sequential behaviour, the Market Data Gateway initiates a new start sequence for this source. The Market Data Gateway then sends an order book retransmission sequence, and a list of corrected trades asynchronously inside the real-time channel used for trades. These messages are flagged as a retransmission (rebroadcast Indicator set to "1").

In case of an HA event trade retransmission should be used to update the status of each trade that is resent, to complete trades not already taken into account, and even in certain cases, to indicate that some trades should be removed.

Please refer to the section "Book and Trades Retransmission" in the "*Euronext Markets – Optiq MDG Client Specifications*" document for details retransmission of book and trade information.

6.1.2 Business Continuity (DR Environment)

A Business Continuity event occurs when Exchange switches client systems processing from the production environment to its Back-up, or secondary site (DR environment). The DR environment provides redundant standby systems to be used upon the failure of the Exchange Production environment.

A business continuity event occurring on the Exchange's trading system will encompass a whole market, including all the segments and partitions belonging to that market. That means for Euronext markets that both Cash and Derivatives would be in scope of failover to the DR environment.

For the Business continuity mechanism data between Production and DR environments is continuously replicated, and the DR environment is online in standby mode.

While the partition ID, Logical Access ID and assigned port remains unchanged between the Production and DR environments, to ensure business continuity the IP addresses between the environments for each partition are different and defined with the rest of the connectivity details.

- Interaction with the throttling mechanism: In case of disconnection, messages in throttling queue are dropped as if never received.
- As mentioned above, in some cases of HA and Business continuity the message sequence number may be intentionally increments by a pre-defined number.

6.1.3 Obtaining Connectivity Details

For Private Messages (OEG):

For private messages the connectivity details made available include information for the trading Order Entry gateways, as well as the Drop Copy gateways.

- High Availability: In case a disruptive incident, which results in an HA event, the same IP address is used for Primary and Mirror instances of the partition within the same environment. The IP address is set in the field *IPAddressPrimary* of the Standing Data files[1] and is provided in all environments.
- Exchange Business Continuity: For the case of Exchange Business Continuity event and switch of activity to the DR environment every partition has a specified & dedicated IP address. The DR IP address is set in the field *IPAddressDR* of the Standing Data file[1] and the values of such IP addresses are provided only in the file produced for the Production environment.

[1] For Cash Standing data file - CashStandingDataFile (9007); For Derivatives Standing data file - DerivativesStandingDataFile (9013)

In both cases, the port assigned to the Logical Access created for the client on the Optiq segment in question remains the same.

Clients must ensure that their connectivity to the DR environment is setup to the IP addresses provided in this document, as well as indicated in the Standing Data files[2].

For Public Messages (MDG):

For public messages, standing data contains the IP addresses dedicated to the DR environment. Clients should ensure that all configurations for the DR environment are setup as described in the *Euronext Optiq Market Data Gateway Production or External User Acceptance Environment* document, and ready to use in case of a business continuity event.

The channels for market data are the same for both Production and DR environments, which allows to keep their configuration, and just change the source IP for the switch between the Production and DR environments.

6.1.4 Messages Used for High Availability or Business Continuity

Optiq supports various messages that enable clients to manage their order book, and provide notification via public and private messages of events on the trading engine that impact it. The section below lists a sub-set of the messages that furthermore assist clients to run a smooth and safe recovery.

Private messages:

Message Name	SBE Message Code	FIX Message Code	Details
Instrument Synchronization List	50	U50	This message is not sent to Drop Copy
Synchronization Time	51	U51	This message is not sent to Drop Copy
Open Order Request	15	AF	This message is not sent to Drop Copy
Ownership Request	18	U18	While this message is not sent to the Drop Copy, the order acknowledgement messages sent to an OEG in response to this messages are sent to Drop Copy
Ownership Request Ack	17	U29	This message is not sent to Drop Copy

Notes below on the recovery message provide details that are referenced in this document. For full information about structure and behavior of messages clients should rearview the message specifications and kinematics documents.

Timestamps to Enable Synchronization

The timestamp that enables synchronization of clients with the OEG is provided in the **Synchronization Time** (51) / (FIX U51) message. The time stamp within the messages is provided with nanosecond granularity, and is the last known valid and stored state of the trading chain events for the *Resynchronization ID* assigned by the exchange to group instruments.

A single partition is setup with multiple different Resynchronization IDs. Synchronization Time messages are issued for each individual Resynchronization ID setup on the partition. Resynchronization ID used in message **Synchronization Time** (51) / (FIX U51) is unique across all partitions of an Optiq segment.

[2] For Cash Standing data file - CashStandingDataFile (9007); For Derivatives Standing data file - DerivativesStandingDataFile (9013)

In case of a disrupting incident, using the timestamp provided in this message clients can identify messages sent to and from the OEG that should be discarded as they are not stored by the exchange, and will not be valid.

Identifying Instruments Assigned to the Resynchronization ID

The first message provided upon client's connection to the OEG at the start of the session, and in case of a re-connection if client sends a Logon with the message sequence number of zero (0) for SBE [one (1) for FIX] is **Instrument Synchronization List** (50) / (FIX U50).

This message contains the mapping between the Resynchronization ID and the instruments to which it is assigned.

A single Resynchronization ID is assigned to multiple instrument + EMM combinations (representing an Order Book) of the partition. A single instrument + EMM combination (an Order book) is always assigned one, and only one, Resynchronization ID.

The Resynchronization ID is assigned to the instruments before the start-up of the system, and may be different from one trading day to another. The mapping between a Resynchronization ID and the instruments assigned to it remain the same for the duration of the trading session, either in case of HA or Business Continuity events.

In case of multiple partitions, in order to determine which partition is sending the **Synchronization Time** (51) / (FIX U51) messages clients may use one of the two following options:

- Option 1: Link the instrument details (symbol index, partition) provided in the Standing Data file with symbol Index provided in the **Instrument Synchronization List** (50) / (FIX U50) message;
- Option 2: Identify the partition ID that is stored within the Resynchronization ID field, based on the structure of the data, as described below
  - Resynchronization ID is constructed with the unique identifier of the partition included into the value. Partition ID, includes the Optiq Segment id, is up to 3 characters in length, and can be retrieved from the Resynchronization ID field by discarding the last two characters.

    Example 1:

    For Cash segment "Equities" (1), Partition ID (0), the Resynchronization ID sent: 1001

    After the last two characters are discarded, the remaining value of 10 provides the unique partition ID.

    Example 2:

    For Derivatives segment "Equity Derivatives" (12), Partition ID (0), the Resynchronization ID sent: 12009

    After the last two characters are discarded, the remaining value of 120 provides the unique partition ID.

Public messages:

MDG uses the following dedicated mechanisms to manage cases of disruptive incidents (HA or DR):

- Book retransmission,
- Trade retransmission, and
- Package flag & counters used in case of disruptive incidents (HA or DR)

Please refer to the dedicated sections for these topics, as well as Gap Detection and System Failures, in the *Euronext Markets – Optiq MDG Client Specifications* document for details of messages and mechanisms used.

6.2 DETECTING EXCHANGE TRADING CHAIN HA EVENT & MITIGATION

Different indicators may identify to clients that an HA event has affected the exchange trading chain partition, and its different states:

Detecting Failover for Order Entry Gateways (OEG):

- One possible indication is unexpected drop of connection by the OEG.
  - Please note – an unexpected drop in connection may be caused by different events
  - If following this client is not able to reconnect to the OEG and / or no longer receives MDG messages, they should review standard cases of network and connectivity failure, as well as consult the Exchange Market Status page
- Another possible indication is reception of **Reject** (07) / (FIX 8) message from the OEG with status "System Unavailable" (*Error code: 5002*) from the partition.
  - Please note that such a message may be caused by different events, and should be investigated for root cause.
- Reception of the **Synchronization Time** (51) / (FIX U51) messages serves as confirmation of the switch to the Mirror instance.
- In case of a multi-partition segment, reception of the **Synchronization Time** (51) / (FIX U51) messages on one of the partitions may occur without client being disconnected, as it would indicate that an HA even has occurred on one of the other partitions

Detecting Failover for Market Data Gateways (MDG):

The High Availability (HA) functionality failover to a Mirror for MDG can be identified by

- Period of silence in the real-time and snapshot channels, including lack of heartbeats until the failover to Mirror is completed
- Followed by the change of sequence in the Packet headers (the Packet Sequence Number restarts to "1" and bits between 1 and 3 in the "Packet Flags" field increase by "1". Keep in mind that these 3 bits can overflow and it will result with a "0" again). In this case the rebroadcast indicator is also set to one (1).

For more details on this topic for MDG please refer to the *Euronext Markets – Optiq MDG Client Specifications* document.

Risk Mitigation:

To mitigate the risk of an HA event, upon reception of the Synchronization Time messages client may use one of the following options for resynchronization:

- Follow the automated book resynchronization scenarios described in this document for the OEG;
- Obtain status of individual orders using the **Open Order Request** (15) / (FIX AF) messages;
- Use MDG automatic snapshot & retransmission mechanisms to reconcile data in their system;
  - To ensure full resynchronization of the order book, in conjunction with MDG resynchronization mechanisms, clients must use the recovery mechanisms provided for / by the OEG
- Cancel orders entered during the current trading session in the affected partition;

- Review Market Status page & contact market surveillance for further information

6.3 RECOVERY & BUSINESS CONTINUITY CASES

This section provides description of the methods of handling of Exchange's trading chain and drop copy infrastructure for cases of:

- High Availability (HA) event, with switch of activity between Primary and Mirror instances of a partition
- Business Continuity event, with switch of activity for the whole market from Production to DR environment

6.3.1 High Availability (HA) for the Trading Chain

Cases below provide information on which messages are sent out by Optiq and the guidelines for clients on handling the event and associated mechanisms. The goals of the HA process in Optiq are to:

- Ensure the time of the disruptive incident to a minimum via streamlining and automation of the process
- Reduce loss of data to a minimum
- Provide clients with the means to recover in a smooth and automated manner

6.3.1.1 General Methodology (Single Partition)

If Exchange experience a disruptive incident resulting in failure of a partition, the scope of the failover to the Mirror instance encompasses all components of that partition, including the OEG, ME and MDG.

The segregation of Exchanges instruments into segments and partitions reduces the risk of unavailability to the subset of instruments hosted on the partition.

For management of disruptive incidents Exchange systems may be handled with two possible scenarios: Standard and Non-Standard.

Standard HA Scenario (Trading Chain)

In case of a standard HA scenario switch between Primary and Mirror instance of a trading chain partition will occur automatically.

In case of Standard HA event the impacted Instruments / Contracts are in state Halted, and order entry is not allowed.

In the unlikely event of a disruptive incident on the trading chain partition that follows a standard HA scenario Exchange expects the Mirror instance to become available for client reconnection within 30 seconds following occurrence of the incident on the Primary instance.

Clients are always informed of any disruptive incidents via the Market Status page.

Non-Standard HA Scenario (Trading Chain)

In case that switch between Primary and Mirror instances of a trading chain partition requires manual intervention, it will be handled via a non-standard HA scenario.

In case of Non-Standard HA event the impacted Instruments / Contracts are in state Halted, and order entry is not allowed.

In the unlikely event of a disruptive incident on the trading chain partition that follows a non-standard HA scenario clients will be provided with details via Market Status, including the expected time of availability of the Mirror, as well as the associated conditions and instructions.

Steps of the Standard HA Mechanism

- Exchange experiences disruptive incident which affects Primary instance of the partition & Mirror instance takes over the role of Primary instance

  In case of a disruptive incident all instruments of the partitions become effective active on the Mirror instance of the partition.
- Mirror generates **Synchronization Time** (51) / (FIX U51) messages
- Mirror triggers processing of Cancel on Disconnect (COD) mechanism for all messages / instruments hosted on the partition
- Clients reconnect to the Mirror
  - Clients will be able to reconnect transparently, without changing the IP address, port or partition ID to the Mirror instance. All other identifiers, including Symbol Indices of instruments remain the same as well. Order book event data between the Primary and Mirror instances is continuously synchronized to ensure minimum amount of data loss.
- Exchange sends messages facilitating resynchronization after the failover
  - In some cases when partition Primary instance fails over to the Mirror the message sequence number may be intentionally increments by 1000**. This is being done specifically for cases of HA to guarantee delivery of full scope of messages for resynchronization and to reduce number of unexpected rejections of client Logon attempts.

*** Please review details on the intentional increment value parameter in section "High Availability (HA)". The latest values of this increment are provided in the section "Segment-Wide Configuration Settings".*

  - Resending of messages by the trading partition depends on the sequence number identified by the client upon re-connection, which may resend messages that have already been received by the clients. Clients are responsible for managing any duplicates that may occur as a result of resending of messages.
  - Interaction with the throttling mechanism: In case of disconnection, messages in throttling queue are dropped as if never received.

  The various cases of behavior by the OEG depend on the sequence number sent by the client in the **Logon** (100) / (FIX A) message when reconnecting to the partition, and are described below.

  The cases listed below are identified using the following messages and fields.

  SBE:

  In Message **Logon** (100) field *Last Message Sequence Number* compared to field *Message Sequence Number* from any last messages sent by the OEG to client

	Sent by Client		Compared to by Exchange
Comparison	Field *Last Message Sequence Number* in **Logon** (100) message	= < >	Field *Message Sequence Number* from any last messages sent by the OEG to client

  FIX:

  In Message **Logon** (A) field *NextExpectedMsgSeqNum* (tag: 789) compared to field *MsgSeqNum* (34) incremented by 1 from any last messages sent by the OEG to client.

Exchange replies the same value provided in the *NextExpectedMsgSeqNum* (789) in the *MsgSeqNum* (34) of the **Logon** (A) messages sent by OEG to the client in case of successful connection.

	Sent by Client		Compared to by Exchange
Comparison	Field *NextExpectedMsgSeqNum* (tag: 789) in **Logon** (A) message	= < >	Field *MsgSeqNum* (34) from any last messages sent by the OEG to client

- Logon that does NOT Trigger a Resend of Messages Generated Before the Disruptive Incident
  - No messages are sent for resynchronization of missed events
  - **Synchronization Time** (51) / (FIX U51) messages are sent, followed by
  - **Kill** (05) / (FIX 8) messages, if any, that were generated by CoD mechanism are sent
- Logon that Triggers Resend of Messages Generated Before the Disruptive Incident
  - Exchange sends out messages associated to the market events that are known to the Exchange. Messages sent start from the number identified in the client's Logon message ending with the last known message of the session, and the resent FIX messages have the field *PossDupFlag* (43) is set with value **Y** (Possible duplicate)
  - **Synchronization Time** (51) / (FIX U51) messages are sent.

    Clients are required to manage the rules associated to the time provided in these messages as identified in the guidelines section.
  - followed by **Kill** (05) / (FIX 8) messages, if any, that were generated by CoD mechanism are sent
- Logon that is Rejected

  This case includes the possible intentional increment of message sequence number
  - Exchange sends a rejection [**Logon Reject** (102) / (FIX 5)] message and drops the connection
  - In order to assist clients in managing this case, Optiq provides the following facilities:
    - In SBE, the **Logon Reject** (102) message sent in this case will provide the field *Logon Rejection Code* is set to 3 (Invalid sequence number) and the field *Last Message Sequence Number* is set to the expected value, which is the max value that the client should set in their next logon
    - In FIX, the field *LastMsgSeqNumProcessed* (369), in the **Logout** (5) message, provides the last MsgSeqNum value received and processed by the OEG, and can be used as the indication of sequence number that may be used for resynchronization.
- Logon with "start of day" message sequence number

  This case follows the normal mechanism used for the trading session start-up, with the message sequence number sent as zero (0) for SBE or one (1) for FIX.
  - **Instrument Synchronization List** (50) / (FIX U50) message is sent, providing mapping between Resynchronization IDs and instruments assigned to them
  - OEG sends out any messages associated to the market events from the start of the trading session, and ending with the last known message of the session
  - **Synchronization Time** (51) / (FIX U51) messages are sent.

    Clients are required to manage the rules associated to the time provided in these messages as identified in the guidelines section.
  - followed by **Kill** (05) / (FIX 8) messages, if any, that were generated by CoD mechanism are sent

Other Messages

- As part of the resynchronization client's OE session will receive TCS messages (Cash markets) that were sent during the failover, if any.
- MDG sends out the Snapshot messages, and follows processes defined for HA and start-up
  - Clients have the opportunity to resynchronize their systems with the MDG messages
  - Order and quotes cancelled (killed) by CoD mechanism are not resent via Market Data (MDG).
- Any data that has been received via the Drop Copy accesses is fully stored in Exchange system and was sent to the clearing partners

Guidelines for Client Recovery (HA)

In case of a High Availability failover clients are advised to implement conservation measures listed below:

- If client Logon is rejected due to a sequence number sent to OEG being higher than the one known by the OEG, client is advised to discard any messages with the number that is out of range, and re-connect with the sequence number provided in exchange's response. To determine the sequence number provided exchange in response, and expected to be used in the next Logon are as follows:
  - For SBE
    - In **Logon Reject** (102) message exchange provides a field *Last Message Sequence Number*.

      This is the values expected to be provided by the client in the **Logon** (100) message in the field *Last Message Sequence Number*
  - For FIX
    - In the **Logout** (5) message exchange provides a field *MsgSeqNum* (34).

      In the next Logon message client should populate this value incremented by one (+1) in the field *NextExpectedMsgSeqNum* (789)

- Following a successful connection to the OEG
  - **Messages Sent to OEG (by client)**
    - Using standard resynchronization mechanism customer application must be able to detect any gaps in sequence numbers, that would be issued in one of the cases as identified above based on the Logon message. Please refer to the section "Sequence Number Management & Rejection" in the *Euronext Markets – Optiq OEG Client Specifications – FIX 5.0 Interface* document.
    - Discard any messages sent to OEG that have a message sequence number that is higher than the one replied by the exchange.
  - **Messages Received from the OEG**
    - Process any messages that may be issued by resynchronization, if the sequence number provided in the Logon is in the case requiring this, and there are events requiring resynchronization.
    - **IMPORTANT**: Discard any messages received from the OEG before the disruptive incident, in which the *Book IN Time* / *BookINTime* (tag 21002) is superior to the timestamp provided in the field *Last Book IN Time* / *LastBookInTime* (tag 20031) of the **Synchronization Time** (51) / (FIX U51) messages for the associated instruments.

Note

While quote related messages may be part of the resynchronization messages, they are assumed to be no longer present in the market

- In this document when it is identified that one timestamp (t1) is superior to another (t2), it must be read that the numerical value of t1 is higher than that of t2, as timestamps are provided in numerical format of nanoseconds since Epoch

  For Example:
  t1 is the value in the field *Book In Time* in **Ack** (03) / (FIX 8) message. The message is received before the Synchronization Time (51) message, and its value is = 11:22:33.123456789
  In SBE this value would be represented as 1516962153000640611
  In FIX this value would be represented as 20180126-11:22:33.123456789
  t2 is the value in field *Last Book IN Time* in **Synchronization Time** (51) / (FIX U51), and its value is = 11:22:33.000111333
  In SBE this value would be represented as 1516962153000346644
  In FIX this value would be represented as 20180126-11:22:33.000111333

  As such
  t1 is **superior** to t2
  numerically represented as follows:
  In SBE
  t1 (1516962153000640611) **>** t2 (1516962153000346644)
  In FIX
  t1 (20180126-11:22:33.123456789) **>** t2 (20180126-11:22:33.000111333)

  - Process cancellations, if any, triggered by the Cancel on Disconnect mechanism
  - Customer applications must be able to identify and discard any duplicate messages / events
- Resynchronize with the MDG messages
- Proceed with trading on the Mirror

Detecting Duplicates in COB messages

In case of a High Availability one of the client conservation measures is identification of the duplicate messages. Clients may detect duplicate Outbound messages (sent by the OEG to the client) using the following combination of fields in the messages listed below:

Trading Event	SBE		FIX	
	Message	Fields	Message	Fields
Trade	Fill (04)	- Firm ID - Symbol Index - EMM - Execution ID - Order Side	ExecutionReport (8)	- DeliverToCompID (tag 128) - SecurityID (tag 48) - EMM (tag 20020) - ExecID (tag 17) - Side (tag 54)
Order Creation	Ack (03)	- Firm ID - Symbol Index - EMM - Order ID - Order Side - Ack Type	ExecutionReport (8)	- DeliverToCompID (128) - SecurityID (48) - EMM (20020) - OrderID (37) - Side (54) - OrdStatus (39) - ExecType (150)
Order Modification / Replacement	Ack (03)	- Firm ID - Symbol Index - EMM - Order ID - Client Order ID - Order Side	ExecutionReport (8)	- DeliverToCompID (128) - SecurityID (48) - EMM (20020) - OrderID (37) - ClOrdID (11) - Side (54)

Trading Event	SBE		FIX	
	Message	Fields	Message	Fields
		- Ack Type		- OrdStatus (39) - ExecType (150)
Quotes	Quote related messages may be part of the resynchronization messages, but they are assumed to be no longer present in the market			

Notes

- *Order Id / OrderID (31) field is being used for the identification of duplicates, because Client Order ID / ClOrdID (11) field is no longer checked by the exchange for uniqueness.*
- *In case of multiple modification messages, Client order id is expected to be different for the different messages attempting to modify the same order. In this case Client Order ID may be used to detect duplicates, or differentiate the different messages submitted*

6.3.1.2 Recovery of a Single, Stand-Alone Partition, in a Mono-Partition Segment

In a segment that is hosted on a single partition, an HA event of the partition means that the whole segment experiences an HA event.

The granularity of that event, as well as all the steps, behavior and messages associated to it, would be the same as described in the section "General Methodology of HA Mechanism (Single Partition)".

6.3.1.3 Recovery of a Single Partition in a Multi-Partition Situation

In a segment that is hosted on multiple partitions an HA event of the partition means that the other partitions within the segment may continue their trading activity.

As partitions are cross-linked (meshed) the partitions that remain active will receive messages resulting from the HA event. While **Synchronization Time** (51) / U51 messages will be sent in all cases to all partitions, messages resulting from CoD will be sent to the cross-linked partitions only if there are orders that are in scope of the mechanism.

The granularity of the event, as well as all the steps, behavior and messages associated to it, would be similar to the one description provided in section "General Methodology of HA Mechanism (Single Partition)", and the main differences for the case of multi-partition situation are provided below.

Messages upon reconnection to Mirror

The messages resent by the OEG will be sent to the OE session / partition which owned the order directly before the disconnection. This means that if multiple OE sessions reconnect to multiple failed over partitions, each will receive only messages that it owns, and there should be no duplicate Order or Trade messages sent to this and other OE sessions / partitions.

Behavior of cancellation messages triggered by CoD mechanism in this case is described in the dedicated section of this document. For details clients should review section "Multiple Meshed (cross-linked) partitions & associated cases".

TCS messages (Cash markets)

TCS unsolicited messages are sent to all partitions in the segment. Upon reconnection to the mirror partition, client's OE session will receive TCS messages that were already sent to other OE session / partitions during the failover. TCS messages are not in scope of Cancel on Disconnect service.

6.3.1.4 Recovery of Multiple Partitions in a Multi-Partition Situation

In a segment that is hosted on multiple partitions an HA event may occur on more than one partition within the segment, however the remaining partitions may continue their trading activity.

As partitions are cross-linked (meshed) the partitions that remain active will receive messages resulting from the HA event. While **Synchronization Time** (51) / U51 messages will be sent in all cases to all partitions, messages resulting from CoD will be sent to the cross-linked partitions only if there are orders that are in scope of the mechanism.

In case all partitions of a segment experience a disruptive incident, the full scope of the segment is impacted, however this will not automatically trigger a business continuity event (i.e. a system will not failover to the DR environment).

In case client sends a correctly technically and functionally formatted message from one of the available partitions, to a partition that is failing over and before its Mirror is available, the OEG of the active partition would send a **Reject** (07) / (FIX 8) message with status "System Unavailable" (*Error code: 5002*).

- Please note that such a message may be caused by different events, and should be investigated for root cause.

The granularity of the event, as well as all the steps, behavior and messages associated to it, would be similar to the one description provided in section "General Methodology of HA Mechanism (Single Partition)", and the main differences for the case of HA for multiple partitions within a segment are provided below.

Messages upon reconnection to Mirror

As identified above, the Resynchronization ID is unique across the Optiq segment. This ensures that the information provided of the time of last known state by the OEG doesn't contain duplicates, in case of a disruptive incident affective multiple partitions.

Behavior of cancellation messages triggered by CoD mechanism in this case is described in the dedicated section of this document. For details clients should review section "Multiple Meshed (cross-linked) partitions & associated cases".

TCS messages (Cash markets)

TCS unsolicited messages are sent to all partitions in the segment. Upon reconnection to the mirror partition, any OE sessions belonging to a Logical Access enabled to send and receive TCS messages will receive TCS messages that were already sent to the OE session / partitions during the failover. TCS messages are not in scope of Cancel on Disconnect service.

6.3.2 Recovery for Drop Copy

Drop Copy gateways follow recovery and resynchronization processes defined by the FIX protocol. Similarly to the trading OEG, cases of resynchronization of drop copy depend on the message sequence number provided by the client in the Logon message. Section below provides information on drop copy behavior and guidelines to clients for cases of exchange or client recovery.

Please note, as Drop Copy is available in FIX protocol only, only FIX references are provided for messages, fields, and values.

6.3.2.1 Recovery Following Drop Copy High Availability Event

Drop Copy partitions are individual gateways that are not cross-linked between themselves and there is only one DC gateway to which a DC access can connect to. Failure of a Primary instance of single DC gateway means all DC accesses associated to it can't receive messages targeted for it from other DC gateways until a restarted instance of this DC gateway becomes again available.

In the unlikely event that Drop copy gateway experiences a disruptive incident, and provided that the trading partition which is the source of the messages received by drop copy didn't experience a disruptive incident, data of all events that occurred will be queued for the DC gateway, and can be resent to the client upon the DC gateway instance availability.

Additionally, any data that has been received as a resend of message via the Drop Copy accesses is fully stored in Exchange system and was sent to the clearing partners.

Clients may detect that the drop copy experienced a disruptive incident when they observe an unexpected drop of connection by the Drop copy gateway.

- Please note that an unexpected drop in connection may be caused by different events
- If following this client is not able to reconnection to the Drop copy gateway they should review standard cases of network and connectivity failure, as well as consult the Exchange Market Status page

In some cases when a DC gateway instance fails, and when the restarted instance becomes available the message sequence number may be intentionally increments by 1000**. This is being done specifically for cases of HA to guarantee delivery of full scope of messages for resynchronization and to reduce number of unexpected rejections of client Logon attempts. Clients need to be prepared to manage this intentional increment if and when it occurs.

*** Please review details on the intentional increment value parameter in section "High Availability (HA)". The latest values of this increment are provided in the section "Segment-Wide Configuration Settings".*

As for the OEG, resending of messages by the drop copy depends on the sequence number identified by the client upon re-connection, which may resend messages that have already been received by the clients. Clients are responsible for managing any duplicates that may occur as a result of resending of messages.

If the sequence number in client's message (value of tag *NextExpectedMsgSeqNum* (789) in client's **Logon** (A) message requires Drop Copy gateway to resend messages then:

- Resent messages will start from the Drop Copy message sequence value sent by client that triggered the resending, and continue until the last known stored message
- Resent messages will have the field *PossDupFlag* (43) is set with value **Y** (Possible duplicate)
- There is no message identifying "end of resending" of missed messages, however any messages that are sent after the last "stored" messages will not have *PossDupFlag* (43); *[which is equivalent to PossDupFlag (43) being set to **N** (Original transmission (default))]*
- As identified above, the sequence number may be intentionally incremented by 1000 **

*** Please review details on the intentional increment value parameter in section "High Availability (HA)". The latest values of this increment are provided in the section "Segment-Wide Configuration Settings".*

- Drop copy doesn't receive the synchronization messages that are used on the trading OEGs

The different cases of behavior by the Drop Copy gateway follow the standard FIX mechanisms, which depend on the sequence number sent by the client in the **Logon** (A) message when reconnecting to the Drop copy. The cases below mention the comparison to the sequence number of the outbound messages sent by drop copy, but the cases of message sequence number for the inbound messages is handled in the same manner as any other trading OEG.

- Logon that does NOT Trigger a Resend of Messages Generated Before the Disruptive Incident (DC gateway)
  - No messages are sent for resynchronization
- Logon that Triggers Resend of Messages Generated Before the Disruptive Incident (DC gateway)
  - Exchange sends out messages associated to the market events that are known to the drop copy gateway. Messages will be flagged as identified above.
- Logon that is Rejected (DC gateway)
  - Exchange sends as a rejection **Logout** (5) message with *SessionStatus* (1409) set to **10** (Received NextExpectedMsgSeqNum(789) is too high) and closes the connection
- Logon with message sequence number field *NextExpectedMsgSeqNum* (789) equal to one (1) (DC gateway)
  - DC gateway sends out any messages associated to the market events from the start of the trading session, and ending with the last known message of the session.

- In cases where the resynchronization messages will be sent, they will include the full scope of messages for the current trading session, and for which the DC Logical access is setup (e.g. order, trades, TCS). Messages from previous trading sessions are not queued in Drop Copy.

Timelines for HA (Drop Copy)

In the unlikely event of a disruptive incident Exchange expects the restarted instance of Drop Copy gateway to become available for client reconnection within 5 minutes following occurrence of the incident on the Primary instance. Clients are always informed of any disruptive incidents via the Market Status page.

In case a disruptive incident on Drop Copy is deemed by the Exchange as requiring more time for recovery or further individual actions by Market Operations - clients will be provided with additional details via Market Status with the expected time of availability of the restarted DC gateway instance, as well as the associated conditions and instructions to clients.

6.3.2.2 Drop Copy Behavior After Client Disconnection

After resolving the issue that caused the disconnection by the client from the DC gateway, clients may reconnect to the gateway.

The Drop Copy server stores all the messages that it receives throughout the trading day. Therefore, it can be used by a Drop Copy client to retrieve any messages that may have been missed while that client was not connected.

Upon client's re-connection to Drop Copy gateway resynchronization of drop copy messages will be handled in the same manner as the recovery of the DC gateway described above. It depends on the sequence numbers submitted by the DC Access in the **Logon** (A) message, and if the message sequence number received requires resending of the missed Drop Copy messages, the DC Access will receive all the missed messages.

As resending of messages by the drop copy depends on the sequence number identified by the client upon re-connection may result in resending of messages that have already been sent by the Exchange, clients are responsible for managing any duplicates that may occur as a result of this resending.

In cases where the resynchronization messages will be sent, they will include the full scope of messages for the current trading session, and for which the DC Logical access is setup (e.g. order, trades, TCS). Messages from previous trading sessions are not queued in Drop Copy gateway.

6.3.2.3 Message in Drop Copy After HA Event on a Trading Partition

Messages sent on recovery / resynchronization of clients with the OEG of a trading partition are not sent to the Drop Copy. However, copy of order messages are sent to the Drop Copy if client sends an **Ownership request** (U18) messages to the OEG.

6.3.3 Recovery After Client's System Unavailability or Network Disconnection from Optiq

For cases where client's system experiences a disruptive event and become unavailable or disconnects from Optiq the section below identifies functionalities available in the Exchange system to assist client in resynchronizing with the exchange after client's re-connection.

6.3.3.1 What Happens on Client Re-Connection

Resynchronization steps in case of client system unavailability are similar to the ones described for HA.

Upon client reconnection to the partition OEG sends information for the cases listed below, that depend on the information provided in the client's **Logon** (100) / (FIX A) message and follow similar behavior as the one described in section "Steps of the Standard HA Mechanism".

- Logon that does NOT Trigger a Resend of Messages Generated Before the Disruptive Incident
- Logon that Triggers Resend of Messages Generated Before the Disruptive Incident
- Logon that is Rejected
- Logon with message sequence number zero (0) for SBE [one (1) for FIX], normal mechanism similar to the trading session start-up

6.3.3.2 Resynchronization Guidelines for Client Unavailability or Disconnection

After a client reconnects to the trading chain after unavailability of their system, or disconnection from the trading chain that didn't result from a disruptive incident on the Exchange systems, the resynchronization mechanism followed is the same as those described in this document.

The exception being that in such a case **Synchronization Time** (51) / (FIX 51) messages are not sent.

Client's disconnection will result in triggering of the Cancel on Disconnect mechanism.

Segment with Multi-partitions

On a segment hosted on multiple partitions, and in the case of disconnection of an OE session, while another remains active, client may choose to continue with their trading activity through the remaining OE session. To receive information on all orders that are still in the book on the partition to which connection was lost, and to ensure receipt of all the unsolicited messages for such orders, clients can send an **Ownership Request** (18) / (FIX U18) message.

Behavior of cancellation messages triggered by CoD mechanism in this case is described in the dedicated section of this document. For details clients should review section "Multiple Meshed (cross-linked) partitions & associated cases".

For MDG:

As real-time and snapshot market data is available from two different multicast groups in case of client system failure, the backup client system should continue to process the real-time and snapshot data sent by the second multicast group.

6.3.4 Exchange Business Continuity

In the specific case of business continuity event affecting the Exchange's primary data center, trading activity would be switched to be done on the DR environment. Section below provides guidelines for the method used in case of Exchange business continuity event.

6.3.4.1 Business Continuity Event

A Business Continuity event occurs when Exchange switches client systems processing from the production environment to its back-up site (DR environment). The DR environment provides redundant standby systems to be used upon the failure of the Exchange Production environment.

A business continuity event occurring on the Exchange's trading system will encompass a whole market, including all the segments and partitions belonging to that market.

Clients are always informed of any disruptive incidents and events via the Market Status page. Start of use of the DR environment will being after being announced to the clients. Until such an announcement is made clients are not able to connect to the DR gateways (OEG or Drop copy).

The standing data on the DR environment is identical to the one used on the Production environment, and the same files used on EFS are provided for the DR environment as for the Production.

While the partition and DC gateway ID, Logical Access ID and assigned port remains unchanged between the Production and DR environments, to ensure business continuity the IP addresses between the environments for each partition are different and defined with the rest of the connectivity details. Please review section "Obtaining Connectivity Details" for more information.

In case of business continuity event Exchange trading system restarts in the DR environment with the last known context of trading events from the Production environment.

Overall mechanism of resynchronization is similar to the one described for High Availability events, with the following guidelines:

As identified for the HA events, in some cases when Production instance switches to the DR environment the message sequence number may be intentionally increments by 1000**. This is being done specifically to guarantee delivery of full scope of messages for resynchronization and to reduce number of unexpected rejections of client Logon attempts. Clients need to be prepared to manage this intentional increment if and when it occurs.

*** Please review details on the intentional increment value parameter in section "High Availability (HA)". The latest values of this increment are provided in the section "Segment-Wide Configuration Settings".*

The Resynchronization IDs for a partition and instruments assigned to them are identical between Production and DR environments, on the same segments and partitions. Clients may reuse the instrument list information obtained at the start of the session provided by message **Instrument Synchronization List** (50) / (FIX U50), or follow the same processes as for HA event to obtain these messages on the DR environment.

In case of Business Continuity event all segments and partition will be started in the suspended trading state, where all the Instruments / Contracts are Halted and order entry is not allowed.

As for the OEG, resending of messages by the OEG in the DR environment depends on the sequence number identified by the client upon re-connection, which may resend messages that have already been received by the clients.

As in Production, OEG will send out the **Synchronization Time** (51) / (FIX U51) messages to assist in resynchronization, using the same mechanism as identified elsewhere in this document. Clients are responsible for managing any duplicates that may occur as a result of resending of messages.

In the unlikely event of a business continuity event Exchange expects to be available for client re-connection in the DR environment within 2 hours following occurrence of the incident requiring switch to the DR.

Behavior of cancellation messages triggered by CoD mechanism in this case is the same as described in the dedicated CoD section in this document.

Public Messages

For public messages, standing data contains the IP addresses dedicated to the DR environment. Clients should ensure that all configurations for the DR environment are setup as described in the *Euronext Optiq Market Data Gateway Production or External User Acceptance Environment* document, and ready to use in case of a business continuity event.

The channels for market data are the same for both Production and DR environments, which allows to keep their configuration, and just change the source IP for the switch between the Production and DR environments.

Drop Copy in DR Environment

Messages and overall functional mechanisms of Drop Copy in the DR environment will operate in the same manner as in Production.

Upon switch of the activity from the Production to DR environment Drop Copy gateways will become available, when the DR environment is announced as available to clients by the Market operations. Until such an announcement is made, access to the DR environment is possible only for telnet testing on a predefined port.

In DR environment drop copy is made available with a full resynchronization from the start of the session as follows:

- FIX Sequence Number will restart from value 1. Client must reconnect using **Logon** (A) message with fields *MsgSeqNum* (34) set to 1 and *NextExpectedSeqNum* (789) set to 1.
- All Drop Copy messages will be resent, that were persisted for that day's trading session
- The resent Drop Copy messages, and those that start being sent from the re-start of trading on the DR environment are not distinguished by any flag

- The message will be sent without any Gap in sequence numbers, and will not have the same sequence numbers as provided originally in the Production drop copy during that session.
- Resynchronization ID and time messages are not sent for Drop Copy, and are not used for resynchronization processes in DR environment.
- As all Drop Copy messages from start of session will be resent:
  - Clients are advised to allocate sufficient time for processing of the messages. This time may vary depending on the amount of data that was processed by the drop copy during that associated trading session
  - Clients must ensure that they discard any duplicates in their own systems using the combination of fields present in the messages as listed below

Trading Event	FIX	
	Message	Fields
Trade	ExecutionReport (8)	- DeliverToCompID (tag 128) - SecurityID (tag 48) - EMM (tag 20020) - ExecID (tag 17) - Side (tag 54)
Order Creation	ExecutionReport (8)	- DeliverToCompID (128) - SecurityID (48) - EMM (20020) - OrderID (37) - Side (54) - OrdStatus (39) - ExecType (150)
Quotes	Quote related messages are not in scope of Drop Copy	

Note

Order Id / OrderID (31) field is being used for the identification of duplicates, because Client Order ID / ClOrdID (11) field is no longer checked by the exchange for uniqueness.

6.3.4.2 Regularly Scheduled Business Continuity Tests

Regularly scheduled business continuity tests use the Production and DR environments during off-market hours to confirm Exchange's and client's ability to handle a Business Continuity event.

These tests are communicated ahead of time, using the standard Exchange communication channels, and are accompanied by

- specific instructions to clients for each individual test event
- dependencies and expected timelines of an even

6.3.5 Handling & Automation following Synchronization Time (51) / (FIX U51) messages

6.3.5.1 Rules for handling various cases of message non-synchronization in case of HA or DR event

During re-synchronization processes it is possible that messages may be sent to the client:

- prior to the **Synchronization Time** (51) / (FIX U51) message and are considered as messages that were generated (and possibly sent) before the disruptive incident. As such they may need to be discarded during the resynchronization process
- after to the **Synchronization Time** (51) / (FIX U51) message and are considered as messages that are generated and sent after the disruptive incident (i.e. they should not be impacted by the disruptive incident and shouldn't be discarded)

6.3.5.2 Detecting the case with Synchronization Time messages:

- Reception of the **Synchronization Time** (51) / (FIX U51) messages serves as confirmation of the switch to the Mirror instance, or in case of a Business continuity event, to Disaster Recovery environment. This means a disruptive incident has definitively caused a failover of the Optiq system to the Mirror.

  Please note: While these messages are also sent on re-connection to the Disaster Recovery environment, clients are made aware of switch to DR by other means as the switch to DR requires use of a different set of IP addresses.
- In case of a multi-partition segment, and only in case of the HA event (switch to the Mirror instance), reception of the **Synchronization Time** (51) / (FIX U51) messages on one of the partitions may occur without client being disconnected, as it would indicate that an HA event has occurred on one of the other partitions

In this case clients must:

- Process any Application messages that may be issued by OEG for re-synchronization, as described in this doc (if any)
- **IMPORTANT**: Discard any messages received from the OEG prior to the receipt of the **Synchronization Time** (51) / (FIX U51) message in which the *Book IN Time* / *BookINTime* (tag 21002) is older (superior to) the timestamp provided in the field *Last Book IN Time* / *LastBookInTime* (tag 20031) of the **Synchronization Time** (51) / (FIX U51) messages for the associated instruments.
- Process cancellations, if any, triggered by the Cancel on Disconnect mechanism, which are sent after the **Synchronization Time** (51) / (FIX U51) message
- Customer applications must be able to identify and discard any duplicate messages / events, as identified elsewhere in this document
- Process any other “after the incident” messages

6.3.5.3 Guidelines for Handling of Synchronization Time (51) / (FIX U51) messages

Automation below addresses outbound application messages

- Ack[3], Wholesale Order Ack or QuoteAck

If a client previously received an **Ack** (03) / (FIX 8), **Wholesale Order Ack** (65) / (FIX U65) or **Quote Ack** (09) / (FIX b)[4] message with a *Book In Time* / *BookINTime* (tag 21002) superior to the *Last Book In Time* / *LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then the Ack notification must be ignored

  - The order (or Quote) is NOT present in the order book
  - Client may choose to re-send the message

- Cross Order message for Derivatives

[3] This is the case of Ack for all orders on the Cash segments, and Ack for COB orders only for the Derivatives segments, and doesn’t address the other cases where the Ack message is sent (e.g. Cross order or Request for Implied Execution)

[4] FIX message (b) for Quote Ack is applicable only for the Warrants segment of the Cash markets

If a client previously received an **Ack** (03) / (FIX 8) for a Cross Order message with a *Book In Time* / *BookINTime* (tag 21002) superior to the *Last Book In Time / LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then the Ack notification must be ignored

- The order is NOT present in the order book and wasn't processed
- Client may choose to re-send the Cross Order message

- Fill

Upon the reception of a **Synchronization Time** (51) / (FIX U51) message, if a client previously received a **Fill** (04) / (FIX 8) message with the *Trade Time / TransactTime* (tag 60) superior to the *Last Book In Time* / *LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then

- the trade is considered as it has never happened (i.e. the quantity has not been traded, and the order may still be present in the order book for further execution)
- this **Fill** (04) / (FIX 8) message must be fully reversed in client system
- and the Order is still in the book (i.e. the order quantity of the discarded Fill may still be present in the order book for further execution.)
  - The order may be subject to Cancel on Disconnect, but until a valid Kill messages for this order is processed (i.e. Kill message that isn't discarded by the resynchronization process), it is still in the book, and can be matched against other orders

- Kill

If a client previously received a **Kill** (05) / (FIX 8) message with a *Book In Time*/ *BookINTime* (tag 21002) superior to the *Last Book In Time* / *LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then the Kill notification must be ignored (meaning that the order may still present in the order book for further execution).

- The Order is still in the book
  - The order may be subject to Cancel on Disconnect, but until a valid Kill messages for this order is processed, it is still in the book, and can be matched against other orders
- Clients should assess if their CoD policy would automatically cancel the order on and if not, then they should re-submit the cancellation of that order

- Ownership Request Ack

If a client previously sent an **Ownership Request** (18) / (FIX U18) message before receiving **Synchronization Time** (51) / (FIX U51), then client should perform this operation again. Any **Ack** (03) / (FIX 8) messages resulting for the original **Ownership Request** (18) / (FIX U18) message should be processed as described above.

- Mass Cancel Ack

The instructions below are for clients that are (1) not using Cancel on Disconnect for all their orders and (2) sent **Mass Cancel** (13) / (FIX q) request immediately before the disruptive incident.

- If a client previously received two **Mass Cancel Ack** (14) / (FIX r) messages with the second one having *Total Affected Orders* set to zero (0) - there is no need resend the Mass cancel request upon re-connection
- In all other cases client should re-send the for the **Mass Cancel** (13) / (FIX q) request
- Any **Kill** (05) / (FIX 8) messages resulting for the original **Mass Cancel** (13) / (FIX q) message should be processed as described above.

- Collar Breach Confirmation (Cash markets only)

For an order that is rejected when it breaches collars during the incident, and was not yet confirmed such order doesn't enter the book. Depending on when the collar breach occurs relative to the incident clients may observe two behaviors:

- Reception of an **Ack** (03) / (FIX 8) messages, followed by a **Reject** (07) / (FIX 9) message, which still indicates that order never entered the book
- Reception of no messages associated to it upon re-connection, even if it the order would normally be in scope of Cancel on Disconnect

- Reject
  - Rejection of new orders or quotes

    If a client previously received a **Reject** (07) / (FIX 9) message for a new order, or **Reject** (07) / (FIX AG) message for a new Quote, with a *Book In Time / BookINTime* (tag 21002) superior to the *Last Book In Time / LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then the original message is in the same state, it wasn't processed into the order book

  - Rejection of Liquidity Provider Command

    Reject of the liquidity provide command is sent via OEG using **Reject** (07) / (FIX Uy) messages. If a client previously received such a messages following submission of a Liquidity Provider command, with a *Book In Time / BookINTime* (tag 21002) superior to the *Last Book In Time / LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then the command wasn't processed, and the impacted instrument remains in its state before the Liquidity Provider command message was sent.

6.3.5.4 OEG messages for which no specific management required

- Ask For Quote (Warrants segment)

If a client previously received an **Ask For Quote** (33) / (FIX UL) message with a *Book In Time/ BookINTime* (tag 21002) superior to the *Last Book In Time / LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then instrument remains in non-tradeable state, as before the incident.

- In case of a disruptive incident no special additional processing is required for the Ask for Quote messages
- Until the Liquidity Provider is available with quotes on the instrument it will remain in non-tradeable state
- Client should send an **Quotes** (8) (FIX i) message, as for any other instrument on which they are the Liquidity Provider

- Request For Execution (Warrants segment)

If a client previously received a **Request for Execution** (34) / (FIX UM) message with a *Book In Time/ BookINTime* (tag 21002) superior to the *Last Book In Time / LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then message should be ignored.

- Client should complete the resynchronization of messages to assess if the RFE resulted in a trade or not
- Upon entry of quotes if there is a potential match that occurs after the Mirror is available, client should receive another Request For Execution message

- User Notification

User Notification (39) / (FIX CB) messages do not require special automated management. If User notification is sent to client to inform them of a suspension, then client will receive this message again, upon attempts to send any additional messages after the failover.

- MM Sign-In Ack (Derivatives Segments)

If a client previously received a **MM Sign-in Ack** (48) message with a *Book In Time*/ *BookINTime* (tag 21002) superior to the *Last Book In Time* / *LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then this acknowledgement message should be ignored.

  - The MM Sign-in is NOT present in the system
  - Client should re-submit the **MM Sign-in** (47) message to re-establish their market maker short code session.

- Security Definition Ack (Derivatives Segments)

If a client previously received a **Security Definition Ack** (61) message with a *Book In Time*/ *BookINTime* (tag 21002) superior to the *Last Book In Time* / *LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then such acknowledgement message should be ignored.

  - The Strategy is not created in the system
  - Client should re-submit **Security Definition Request** (60) message for creation of the security, and if it already exists system will reply with the Symbol Index that should be used for the strategy.

- MM Protection Ack (Derivatives Segments)

If a client previously received a **MM Protection Ack** (63) message with a *Book In Time*/ *BookINTime* (tag 21002) superior to the *Last Book In Time* / *LastBookInTime* (tag 20031) in message **Synchronization Time** (51) / (FIX U51), then this acknowledgement message should be ignored.

  - The MM Protection is NOT present in the system / is not set
  - Client should re-submit the **MM Protection Request** (62) to set their Market Maker Protection.

- Request for Implied Execution (Derivatives Segments)

As identified above, if an Ack is received for the **Request for Implied Execution** (66) (FIX U66) message (Ack Type = RFIE Ack) client should re-submit the Request for Implied Execution into the required strategy book.

- Quote Request

For the Fund segment (Cash markets): If disconnection occurred during the exchange of RFQ messages, recovery of trades of this process should follow steps described above for the **Fill** (04) / (FIX 8) message. Otherwise, client should re-submit a **Quote Request** (10) (FIX R) message to re-initialize the RFQ process.

For the Derivatives segments: Upon completion of resynchronization client should re-submit the **Quote Request** (10) (FIX R) message to request liquidity.

6.3.5.5 Handling of TCS specific messages (Cash markets)

The TCS specific outbound acknowledgement and rejection messages listed below are not managed via the timestamp **Synchronization Time** (51) / (FIX U51).

- Inbound messages

Any TCS specific inbound messages that did not receive an acknowledgement were not processed, and should be re-sent.

- Outbound messages

Any TCS specific outbound messages that may have been sent to the client, will be re-sent as part of standard re-synchronization.

6.4 EXAMPLE OF HA MESSAGES & SEQUENCES

Examples below are a sub-set of possible cases that could occur, and cover simple case of a disruptive incident, with Standard HA scenario, affecting trading chain of a segment with a single partition.

For readability purposes, only 1 Resynchronization ID and associated messages are identified in the examples, even though system should have multiple per partition.

6.4.1 Logon that does NOT Trigger a Resend of Messages Generated Before the Disruptive Incident

6.4.1.1 Case 1: All messages before the incident are processed and sent. No messages in difference before and after the incident

SBE Protocol

#	Received From Client / Inbound		Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:		
	New Order (01) #5 *Client Message Sequence Number* = **100**	>	
		<	**Ack** (03) for order #5 *Message Sequence Number* = **275**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20		
3	Client successfully reconnects to the Mirror		
	Logon (100) *Last Message Sequence Number* = **275**	>	
		<	**Logon Ack** (101) *Last Client Message Sequence Number* = **100**
4	No messages are sent for resynchronization of missed events. **Synchronization Time** (51) messages are sent		
		<	**Synchronization Time** (51) *Message Sequence Number* = **1276** *Resynchronization ID* = 0220xxxx *Last Book IN Time* = 11:22:33.123456789
5	One order (#2) in client's book was submitted during the session, and is set with "default" value for CoD, as such gets cancelled		
		<	**Kill** (05) for order #2 *Message Sequence Number* = **1277**
6	TCS message sent to client		
		<	**Declaration Notice** (42) *Message Sequence Number* = **1278**
7	Client discards message for order #5, because value in *Book In Time* of **Ack** (03) message for order #5 is superior to the value in *Last Book IN Time* in **Synchronization Time** (51) message		
8	Client resynchronizes with MDG identifying no differences		
9	Start trading on Mirror, with first message sent for order #6		
	New Order (01) #6 *Client Message Sequence Number* = **101**	>	
		<	**Ack** (03) for order #6 *Message Sequence Number* = **1279**

FIX Protocol

#	Received From Client / Inbound	Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:	
	NewOrderSingle (D) #5 >	
	MsgSeqNum (34) = **100**	
		< **ExecutionReport** (8) to ack order #5
		MsgSeqNum (34) = **275**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20	
3	Client successfully reconnects to the Mirror	
	Logon (A) >	
	MsgSeqNum (34) = **101**	
	NextExpectedMsgSeqNum (789) = **276**	
		< **Logon** (A)
		MsgSeqNum (34) = **1276**
		NextExpectedMsgSeqNum (789) = **102**
4	No messages are sent for resynchronization of missed events. However, due to intentional increment of sequence number it is required to perform Gap Fill	
		< **SequenceReset** (4) (For Gap fill)
		MsgSeqNum (34) = **276**
		NewSeqNo (36) = **1277**
5	**SynchronizationTime** (U51) messages are sent	
		< **SynchronizationTime** (U51)
		MsgSeqNum (34) = **1277**
		ResynchronizationID (20030) = 0220xxxx
		LastBookINTime (20031) = 11:22:33.123456789
6	One order (#2) in client's book was submitted during the session, and is set with "default" value for CoD, as such gets cancelled	
		< **ExecutionReport** (8) to cancel order #2
		MsgSeqNum (34) = **1278**
7	TCS message sent to client	
		< **TradeCaptureReportAck** (AR)
		MsgSeqNum (34) = **1279**
8	Client discards message for order #5, because value in *BookInTime* (21002) of **ExecutionReport** (8) message to acknowledge order #5 is superior to the value in *LastBookINTime* (20030) in **SynchronizationTime** (U51) message	
9	Client resynchronizes with MDG identifying no differences	
10	Start trading on Mirror, with first message sent for order #6	
	NewOrderSingle (D) #6 >	
	MsgSeqNum (34) = **102**	
		< **ExecutionReport** (8) to ack order #6
		MsgSeqNum (34) = **1280**

6.4.1.2 Case 2: Some client messages before the incident are missed by the Exchange and some are discarded by client based on Timestamp comparison

SBE Protocol

#	Received From Client / Inbound	Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:	
	New Order (01) #5 > *Client Message Sequence Number* = **100**	
	New Order (01) #6 > *Client Message Sequence Number* = **101**	
		< **Ack** (03) for order #5 *Message Sequence Number* = **275** *Book In Time* = **11:22:33.123456789**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20	
3	Client successfully reconnects to the Mirror	
	Logon (100) > *Last Message Sequence Number* = **275**	
		< **Logon Ack** (101) *Last Client Message Sequence Number* = **100**
4	Based on the field *Last Client Message Sequence Number* in the **Logon Ack** (101) message, it appears that Exchange missed client message 101 for order #6. Client should wait for **Synchronization Time** (51) to assess the status of the order	
5	Order #6 was never processed by the Exchange, and no messages are sent for resynchronization of missed events. **Synchronization Time** (51) messages are sent	
		< **Synchronization Time** (51) *Message Sequence Number* = **1276** *Resynchronization ID* = 0220xxxx *Last Book IN Time* = **11:22:33. 000111333**
6	No messages have been resent by the exchange before the **Synchronization Time** (51) message	
7	Client manages stale messages: As the value of *Book In Time* in **Ack** (03) message for order #5 is superior to the *Last Book IN Time* in **Synchronization Time** (51) message. Client discards this message.	
8	Client manages missed messages: As message 101 for order #6 was not resent, it was never processed by the Exchange. Client can choose to resend, or not, this message.	
8	Start trading on Mirror, with first message sent for order #6	
	New Order (01) #6 > *Client Message Sequence Number* = **101**	
		< **Ack** (03) for order #6 *Message Sequence Number* = **1277**

FIX Protocol

#	Received From Client / Inbound	Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:	
	NewOrderSingle (D) #5 > *MsgSeqNum* (34) = **100**	
	NewOrderSingle (D) #6 > *MsgSeqNum* (34) = **101**	
		< **ExecutionReport** (8) to ack order #5 *MsgSeqNum* (34) = **275** *BookINTime* (21002) = **11:22:33.123456789**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20	
3	Client successfully reconnects to the Mirror	
	Logon (A) > *MsgSeqNum* (34) = **102** *NextExpectedMsgSeqNum* (789) = **276**	
		< **Logon** (A) *MsgSeqNum* (34) = **1276** *NextExpectedMsgSeqNum* (789) = **101**
4	Based on the field *NextExpectedMsgSeqNum* (789) in the Logon from Exchange, it appears that Exchange missed client message 101 for order #6. Client should wait for **SynchronizationTime** (U51) message to assess status of their orders. It is strongly recommended not to resend the message for order #6. If time constraint does not allow to wait for **SynchronizationTime** (U51) client should send a **SequenceReset** (4) for Gap Fill. No messages are sent by the Exchange for resynchronization of missed events. **SequenceReset** (4) messages are exchanged to fill the gap. Exchange sends the message automatically based by the intentional increment	
		< **SequenceReset** (4) for Gap fill *MsgSeqNum* (34) = **276** *NewSeqNo (36)* = **1277**
	SequenceReset (4) for Gap fill > *MsgSeqNum* (34) = **101** *NewSeqNo* (36) = **103**	
5	**SynchronizationTime** (U51) messages are sent	
		< **SynchronizationTime** (U51) *MsgSeqNum* (34) = **1277** *ResynchronizationID* (20030) = 0220xxxx *LastBookINTime* (20031) = **11:22:33.000111333**
6	No messages have been resent by the exchange before the **SynchronizationTime** (U51) message	
7	Client manages stale messages: As the value of *BookInTime* (21002) in **ExecutionReport** (8) message for order #5 is superior to the *LastBookINTime* (20031) in **SynchronizationTime** (U51) message. Client discards this message.	
8	Client manages missed messages: As message 101 for order #6 was not resent, it was never processed by the Exchange. Client can choose to resend, or not, this message.	
10	Client performs other resynchronization steps, and starts trading on Mirror, with first message sent for order #6	
	NewOrderSingle (D) #6 > *MsgSeqNum* (34) = **103**	
		< **ExecutionReport** (8) to ack order #6 *MsgSeqNum* (34) = **1278**

6.4.2 Logon that Triggers Resend of Messages Generated Before the Disruptive Incident

6.4.2.1 Case 1: Client messages sent before the incident are sent before the Synchronization Time (51) message. Messages are checked using the Timestamps and some are discarded due to differences

SBE Protocol

#	Received From Client / Inbound	Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:	
	New Order (01) #5 > *Client Message Sequence Number* = **100**	
		< **Ack** (03) for order #5 *Message Sequence Number* = **275**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20	
3	Client successfully reconnects to the Mirror, but appears to have missed the Ack of order #5 sent at the moment of disruptive incident	
	Logon (100) > *Last Message Sequence Number* = **274**	
		< **Logon Ack** (101) *Last Client Message Sequence Number* = **100**
4	Exchange sends out messages associated to the market events that occurred before the incident, but based on the sequence number provided by client appears to be missed, starting from the number identified in the client's Logon message	
		< **Ack** (03) for order #5 (Resent for Resynchronization) *Message Sequence Number* = **275**
5	Once sending of messages for resynchronization of missed events is completed **Synchronization Time** (51) messages are sent	
		< **Synchronization Time** (51) *Message Sequence Number* = **1276** *Resynchronization ID* = 0220xxxx *Last Book IN Time* = 11:22:33.123456789
6	One order (#2) in client's book was submitted during the session, and is set with "default" value for CoD, as such gets cancelled	
		< **Kill** (05) for order #2 *Message Sequence Number* = **1277**
7	TCS message sent to client	
		< **Declaration Notice** (42) *Message Sequence Number* = **1278**
8	Client discards message for order #5, because value in *Book In Time* of **Ack** (03) message for order #5 is superior to the value in *Last Book IN Time* in **Synchronization Time** (51) message	
9	Client resynchronizes with MDG identifying no differences	
10	Start trading on Mirror, with first message sent for order #6	
	New Order (01) #6 > *Client Message Sequence Number* = **101**	
		< **Ack** (03) for order #6 *Message Sequence Number* = **1279**

FIX Protocol

#	Received From Client / Inbound	Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:	
	NewOrderSingle (D) #5 > *MsgSeqNum* (34) = **100**	
		< **ExecutionReport** (8) to ack order #5 *MsgSeqNum* (34) = **275**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20	
3	Client successfully reconnects to the Mirror, but appears to have missed the Ack of order #5 sent at the moment of disruptive incident	
	Logon (A) > *MsgSeqNum* (34) = **101** *NextExpectedMsgSeqNum* (789) = **275**	
		< **Logon** (A) *MsgSeqNum* (34) = **1276** *NextExpectedMsgSeqNum* (789) = **102**
4	Exchange sends out messages associated to the market events that occurred before the incident, but based on the sequence number provided by client appears to be missed, starting from the number identified in the client's Logon message	
		< **ExecutionReport** (8) to ack order #5 (Resent for Resynchronization) *MsgSeqNum* (34) = **275** *PossDupFlag* (43) = **Y**
5	Once sending of messages for re-synchronization of missed events is completed, due to intentional increment of sequence number it is required to perform Gap Fill	
		< **SequenceReset** (4) (For Gap fill) *MsgSeqNum* (34) = **276** *NewSeqNo* (36) = **1277**
6	**Synchronization Time** (U51) messages are sent	
		< **SynchronizationTime** (U51) *MsgSeqNum* (34) = **1277** *ResynchronizationID* (20030) = 0220xxxx *LastBookINTime* (20031) = 11:22:33.123456789
7	One order (#2) in client's book was submitted during the session, and is set with "default" value for CoD, as such gets cancelled	
		< **ExecutionReport** (8) to cancel order #2 *MsgSeqNum* (34) = **1278**
8	TCS message sent to client	
		< **TradeCaptureReportAck** (AR) *MsgSeqNum* (34) = **1279**
9	Client discards message for order #5, because value in *BookInTime* (21002) of **ExecutionReport** (8) message to acknowledge order #5 is superior to the value in *LastBookINTime* (20030) in **SynchronizationTime** (U51) message	
10	Client resynchronizes with MDG identifying no differences	
11	Start trading on Mirror, with first message sent for order #6	
	NewOrderSingle (D) #6 > *MsgSeqNum* (34) = **102**	
		< **ExecutionReport** (8) to ack order #6 *MsgSeqNum* (34) = **1280**

6.4.2.2 Case 2: Client messages sent before the incident are sent before the Synchronization Time (51) message. Messages are checked using the Timestamps and all are valid

SBE Protocol

#	Received From Client / Inbound	Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:	
	New Order (01) #5 > *Client Message Sequence Number* = **100**	
	New Order (01) #6 > *Client Message Sequence Number* = **101**	
		< **Ack** (03) for order #5 *Message Sequence Number* = **275**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20	
3	Client successfully reconnects to the Mirror	
	Logon (100) > *Last Message Sequence Number* = **275**	
		< **Logon Ack** (101) *Last Client Message Sequence Number* = **100**
4	Based on the value in the field *Last Client Message Sequence Number* of the **Logon Ack** (101) message, it appears that Exchange missed client's message 101 for order #6. Client should wait for **Synchronization Time** (51) message to assess the status of their orders.	
5	Exchange sends out messages associated to the market events occurred before the incident but based on the sequence number provided by client. In this example it is illustrated by ack of message 101 for order #6	
		< **Ack** (03) for order #6 *Message Sequence Number* = **1276** *Book In Time* = **11:22:33.000111333**
6	Once sending of messages for re-synchronization of missed events is completed **Synchronization Time** (51) messages are sent	
		< **Synchronization Time** (51) *Message Sequence Number* = **1277** *Resynchronization ID* = 0220xxxx *Last Book IN Time* = **11:22:33.123456789**
6	Client compares the data between messages received before **Synchronization Time** (51) messages to assess the status of their orders. As *Book In Time* of **Ack** (03) message for order #6 is superior to the *Last Book IN Time* in message **Synchronization Time** (51) no messages have to be discarded	
7	Client performs other resynchronization steps, and starts trading on Mirror, with first message sent for order #7	
	New Order (01) #7 > *Client Message Sequence Number* = **102**	
		< **Ack** (03) for order #7 *Message Sequence Number* = **1278**

FIX Protocol

#	Received From Client / Inbound		Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:		
	NewOrderSingle (D) #5 *MsgSeqNum* (34) = **100**	>	
	NewOrderSingle (D) #6 *MsgSeqNum* (34) = **101**	>	
		<	**ExecutionReport** (8) to ack order #5 *MsgSeqNum* (34) = **275**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20		
3	Client successfully reconnects to the Mirror		
	Logon (A) *MsgSeqNum* (34) = **102** *NextExpectedMsgSeqNum* (789) = **276**	>	
		<	**Logon** (A) *MsgSeqNum* (34) = **1276** *NextExpectedMsgSeqNum* (789) = **101**
4	Based on the field *NextExpectedMsgSeqNum* (789) of the Exchange's Logon, it appears that Exchange missed client message 101 for order #6. Client should wait for **SynchronizationTime** (U51) message to assess status of their orders. It is strongly recommended not to resend the message for order #6. If time constraint does not allow to wait for **SynchronizationTime** (U51) client should send a **SequenceReset** (4) for Gap Fill. Exchange sends **SequenceReset** (4) to fill the gap caused by the automatic increment and sends out messages associated to the market events occurred before the incident. In this example it includes **ExecutionReport** (8) of message 101 for order #6		
		<	**SequenceReset** (4) for Gap Fill *MsgSeqNum* (34) = **276** *NewSeqNo* (36) = **1277**
		<	**ExecutionReport** (8) to ack order #6 *MsgSeqNum* (34) = **1277** *BookINTime* (21002) = **11:22:33.000111333**
5	As advised, while awaiting the **SynchronizationTime** (U51) message client sends **SequenceReset** (4) message for GapFill		
	SequenceReset (4) for Gap Fill *MsgSeqNum* (34) = **101** *NewSeqNo* (36) = **103**	>	
6	**SynchronizationTime** (U51) messages are sent		
		<	**SynchronizationTime** (U51) *MsgSeqNum* (34) = **1278** *ResynchronizationID* (20030) = 0220xxxx *LastBookINTime* (20031) = **11:22:33.123456789**
7	Client compares the data between messages received before **SynchronizationTime** (U51) messages to assess the status of their orders. As *BookInTime* (21002) of **ExecutionReport** (8) for order #6 is superior to the *LastBookINTime* (20031) in message **SynchronizationTime** (U51) no messages have to be discarded		
8	Client performs other resynchronization steps, and starts trading on Mirror, with first message sent for order #7		
	NewOrderSingle (D) #7 *MsgSeqNum* (34) = **103**	>	
		<	**ExecutionReport** (8) to ack order #7 *MsgSeqNum* (34) = **1279**

6.4.3 Logon that is Rejected

Please note that while this case could occur during a disruptive incident, it isn't specific to HA events

SBE Protocol

#	Received From Client / Inbound		Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:		
	New Order (01) #5 *Client Message Sequence Number* = **100**	>	
		<	**Ack** (03) for order #5 *Message Sequence Number* = **275**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20		
3	Client sends a Logon to the Mirror and gets rejected due to inconsistent sequence number		
	Logon (100) *Last Message Sequence Number* = **20000**	>	
		<	**Logon Reject** (102) *Logon Reject Code = 3 (Invalid sequence number)* *Last Client Messages Sequence Number* = **100** *Last Message Sequence Number* = **1275**
	Connection is not established. Client can use the value provided in the field *Last Message Sequence Number* provided in the **Logon Reject** (102) messages. This is the max value that the client should set in their next logon.		

FIX Protocol

#	Received From Client / Inbound		Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:		
	NewOrderSingle (D) #5 *MsgSeqNum* (34) = **100**	>	
		<	**ExecutionReport** (8) to ack order #5 *MsgSeqNum* (34) = **275**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20		
3	Client send a Logon to the Mirror and gets rejected due to inconsistent sequence number		
	Logon (A) *MsgSeqNum* (34) = **101** *NextExpectedMsgSeqNum* (789) = **20000**	>	
		<	**Logout** (5) *SessionStatus* (1409) = **10** (ReceivedNextExpectedMsgSeqNum(789) is too high) *MsgSeqNum* (34) = **1275** *LastMsgSeqNumProcessed* (369) = **100**
	Connection is not established. Client can use the value provided in the field the *MsgSeqNum* (34). This is the max value that the client should set in the field *NextExpectedMsgSeqNum* (789) for the resynchronization in their next logon.		

6.4.4 Logon with “Start of day” message sequence number

SBE Protocol

#	Received From Client / Inbound	Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:	
	New Order (01) #5 > *Client Message Sequence Number* = **100**	
		< **Ack** (03) for order #5 *Message Sequence Number* = **275**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20	
3	Client successfully reconnects to the Mirror, with the “Start of Day” messages sequence number	
	Logon (100) > *Last Message Sequence Number* = **0**	
		< **Logon Ack** (101) *Last Client Message Sequence Number* = **100**
4	Exchange resends all messages from the beginning of the day, starting with the **Instrument Synchronization List** (50) message, which provides mapping between Resynchronization IDs and instruments assigned to them	
		< **Instrument Synchronization List** (50) (Resent for Resynchronization) *Message Sequence Number* = **1** *Resynchronization ID* = 0220xxxx *Symbol Index = 1xxxxxxxx1* *EMM = 1* *Symbol Index = 1xxxxxxxx2* *EMM = 1* *Symbol Index = 1xxxxxxxx3* *EMM = 1* *Symbol Index = 1xxxxxxxx4* *EMM = 1*
		< Other messages from start of date till last know message are resent They are not indicated for readability purposes
		< **Ack** (03) for order #4 (Resent for Resynchronization) *Message Sequence Number* = **275**
5	Once sending of messages for resynchronization of missed events is completed **Synchronization Time** (51) messages are sent	
		< **Synchronization Time** (51) *Message Sequence Number* = **1275** *Resynchronization ID* = 0220xxxx *Last Book IN Time* = 9786453123
6	One order (#2) in client’s book was submitted during the session, and is set with “default” value for CoD, as such gets cancelled	
		< **Kill** (05) for order #2 *Message Sequence Number* = **1276**
7	TCS message sent to client	
		< **Declaration Notice** (42) *Message Sequence Number* = **1277**
8	Client discards message for order #5, because value in *Book In Time* of **Ack** (03) message for order #5 is superior to the value in *Last Book IN Time* in **Synchronization Time** (51) message	
9	Client performs other resynchronization steps, and starts trading on Mirror, with first message sent for order #6	
	New Order (01) #6 > *Client Message Sequence Number* = **101**	
		< **Ack** (03) for order #6 *Message Sequence Number* = **1278**

FIX Protocol

#	Received From Client / Inbound	Sent by Exchange / Outbound
1	Prior to disconnection the last messages exchanged are:	
	NewOrderSingle (D) #5 > *MsgSeqNum* (34) = **100**	
		< **ExecutionReport** (8) to ack order #5 *MsgSeqNum* (34) = **275**
2	Exchange experiences disruptive incident on segment: Funds (2) Partitions ID: 20	
3	Client successfully reconnects to the Mirror, with the "Start of Day" messages sequence number	
	Logon (A) > *MsgSeqNum* (34) = **101** *NextExpectedMsgSeqNum* (789) = **1**	
		< **Logon** (A) *MsgSeqNum* (34) = **1275** *NextExpectedMsgSeqNum* (789) = **102**
4	Exchange resends all messages from the beginning of the day, starting with the **Instrument Synchronization List** (U50) message, which provides mapping between Resynchronization IDs and instruments assigned to them	
		< **InstrumentSynchronizationList** (U50) (Resent for Resynchronization) *MsgSeqNum* (34) = **2** *PossDupFlag* (43) = **Y** *ResynchronizationID* (20030) = 0220xxxx *SecurityID* (48) = 1xxxxxxxx1 *EMM* (20020) = 1 *SecurityID* (48) = 1xxxxxxxx2 *EMM* (20020) = 1 *SecurityID* (48) = 1xxxxxxxx3 *EMM* (20020) = 1 *SecurityID* (48) = 1xxxxxxxx4 *EMM* (20020) = 1
		< Other messages from start of date till last know message are resent, which may include SequenceReset for Gap fill They are not indicated for readability purposes
		< **ExecutionReport** (8) to ack order #5 (Resent for Resynchronization) *MsgSeqNum* (34) = **275** *PossDupFlag* (43) = **Y**
5	Once sending of messages for re-synchronization of missed events is completed, due to intentional increment of sequence number it is required to perform Gap Fill	
		< **SequenceReset** (4) (For Gap fill) *MsgSeqNum* (34) = **275** *NewSeqNo* (36) = **1276**
6	Once resending and Gap fill is completed **SynchronizationTime** (U51) messages are sent	
		< **SynchronizationTime** (U51) *MsgSeqNum* (34) = **1276** *ResynchronizationID* (20030) = 0220xxxx *LastBookINTime* (20031) = 9786453123
7	One order (#2) in client's book was submitted during the session, and is set with "default" value for CoD, as such gets cancelled	
		< **ExecutionReport** (8) to cancel order #2 *MsgSeqNum* (34) = **1277**
8	TCS message sent to client	
		< **TradeCaptureReportAck** (AR) *MsgSeqNum* (34) = **1278**
9	Client discards message for order #5, because value in *BookInTime* (21002) of **ExecutionReport** (8) message to acknowledge order #5 is superior to the value in *LastBookINTime* (20030) in **SynchronizationTime** (U51) message	
10	Client performs other resynchronization steps, and starts trading on Mirror, with first message sent for order #6	
	NewOrderSingle (D) #6 > *MsgSeqNum* (34) = **102**	
		< **ExecutionReport** (8) to ack order #6 *MsgSeqNum* (34) = **1279**

APPENDIX A: REVISION HISTORY

SUMMARY OF CHANGES

Version	Change Description
2.2.0	Update to combine all connectivity related topics in a single document. Updates for migration of Derivatives markets to Optiq. ▪ Updated list of Associated Documents, Introduction and Glossary to include information related to the added sections and services. ▪ Added section 2.3.1 “Functional Access Role (Derivatives markets)” ▪ Added sections: 5 “OEG Throttling” & 6 “High Availability and Business Continuity: Functional Overview”. This replaces the dedicated documents for these functionalities for Cash and Derivatives markets.
2.1.1	▪ Corrected PROD IP for EQD Partition 120 from 212.197.194.32 to 212.197.194.35
2.1.0	▪ Added section 4 dedicated to Cancel on Disconnect functionality. This replaced the dedicated file for this functionality for Cash and Derivatives markets for migration of Derivatives markets to Optiq. ▪ Document renamed “Euronext Markets – Optiq OEG Connectivity Specifications” ▪ Section 1.1 “Glossary” – updated with terms specific to Cancel on Disconnect (CoD) ▪ Content of Cancel on Disconnect section (compared to dedicated document) update for migration of Derivatives Markets onto Optiq ▪ Updates throughout section 4 for Cancel on Disconnect to remove specific mention of Cash markets where the functionality / rules apply to all markets ▪ In section 4.1.4 “Kinematics of Cancel on Disconnect – added diagram of the case for the Derivatives markets ▪ In section 4.2 “HOW TO ACTIVATE OR DISABLE CANCEL ON DISCONNECT” – changed the note on Drop Copy to be triggered by Ownership Request message in place of Open Order Request
2.0.0	Release for migration of Derivatives markets to Optiq - Document renamed as “Euronext Markets – Connectivity Configuration Specifications” - Updates throughout the document to remove specific mention of Cash markets where the functionality / rules apply to all markets - In section 2.4 “CONNECTIVITY INFORMATION & INSTRUMENT REFERENTIAL” • Added information about the Derivative standing data • Removed unused Drop Copy partitions from the example for Cash standing data • Added example for the Derivatives standing data files - In section 2.5 “SEGMENTS” – Updated the Derivatives segments and target partition allocation - In section 2.6 “DETERMINING THE “SHORTEST PATH” FOR INDIVIDUAL ORDERS” - updated to clarify individual order messages, and no cross-partition sending for Quotes - In section 2.7.2 “Segment & Partition IP Information” – added new Derivatives segments, and associated IP addresses for partitions, renamed EUA environments to their new names - In section 2.8 “Ports & Port Ranges” – updated references to the Derivative segments and Block - In section 2.10.1 “IP Addresses for Drop Copy per Environment” • Removed unused Drop Copy instances for the Cash markets • Added IP addresses for the new Derivatives DC gateways - In section 2.12 “OBTAINING OR MODIFYING A LOGICAL ACCESS” – updated links to the forms for ordering Logical accesses, and associated information. - In section 3.4 “INTENTIONAL INCREMENT OF SEQUENCE NUMBER” – updated list of Derivatives segments and the value for the Derivatives segments
1.1.1	- Correction of the IP address in Production for the Fixed Income (Bonds) segment, partition 30, corrected to be 212.197.194.17 - Added a note on existing practice of padding of firm id fields to its full length in section 2.11 “Login Overview”
1.1.0	- Added sections “Drop Copy” & “Trade Confirmation System (TCS)” - Added connectivity details for TCS and Drop Copy in section “Segment & Partition IP Information” - Removed section “Work in Progress” - Updated example of the XML for connectivity information in section “2.4 Connectivity Information & Instrument Referential” with the Drop Copy information - Renamed section 2.4.2 from “GIS” to “Indices” - Update section “2.9 Note For Migration to Optiq Testing”, with guideline for Prod and DR IP addresses

Version	Change Description
	- Added clarification in section “2.7.1 IP Ranges per Environment“ on the values within the range of IP addresses - Corrected references to field “PartitionID” from “PartitionsID” in sections “2.7.2 Segment & Partition IP Information” and “2.11 Login Overview” - Added TCS specifications to the section “Associated documents” - Added section “Cases of Disconnection Initiated by Exchange” - Added section “3.4 Intentional Increment of Sequence Number”
1.0.0	First Release for Optiq

DOCUMENT HISTORY

REVISION NO.	DATE	AUTHOR	CHANGE DESCRIPTION
2.2.0	September 2019	Euronext	Update to add High Availability (HA) / Business Continuity (DR); and OEG Throttling functionalities into the document
2.1.1	July 2019	Euronext	Correction update
2.1.0	May 2019	Euronext	Update to add Cancel on Disconnect functionality into the document
2.0	April 2019	Euronext	Release for migration of Derivatives markets to Optiq
1.1.2	March 2019	Euronext	Release for migration of Euronext Block to Optiq
1.1.1	January 2018	Euronext	Corrections of the seconds release
1.1.0	January 2018	Euronext	Second Release
1.0.0	August 2017	IT Solutions - DCO	First Release