SIDC OPSCOM Report on Critical Incident Experienced on 21st of May 2024

27/08/2024

Executive Summary

This report informs stakeholders on the critical incident at SIDC/IDCT (Intraday Continuous Trading, part of Single Intraday Coupling) that happened on the 21st of May 2024, resulting in an XBID environment outage.

The cause of the issue was two Capacity Management Module (CMM) node instances running in parallel, competing with each other on which sends the data for publishing the capacity first.

The mentioned situation repeated twice on 21st of May in a short time interval, resulting in a total of 64 minutes of unexpected outage in the SIDC/IDCT operation.

While for the short-term XBID Core was restored, the issue was stopped from reoccurring by deploying a hotfix.

List of Contents

1. Introduction

This report serves to fulfil the obligation under CACM on reporting of unexpected downtimes of Market towards Stakeholders.

This report is structured as follows. In Chapter 2, SIDC is described. In Chapter 3, the normal operational process as covered in the operational procedures with respective timings is described. In Chapter 4, the incident management process applied when critical incident occurs is described. In Chapter 5, a description of the incident, including inter alia the timing, and the root cause are provided. Finally, in Chapter 6, the mitigation measures to resolve the issue and the lessons learnt are presented.

2. Single Intraday Coupling (SIDC)

SIDC creates a single EU cross-zonal intraday electricity market. In simple terms, buyers and sellers of energy (market participants) are able to work together across Europe to trade electricity continuously on the day the energy is needed.

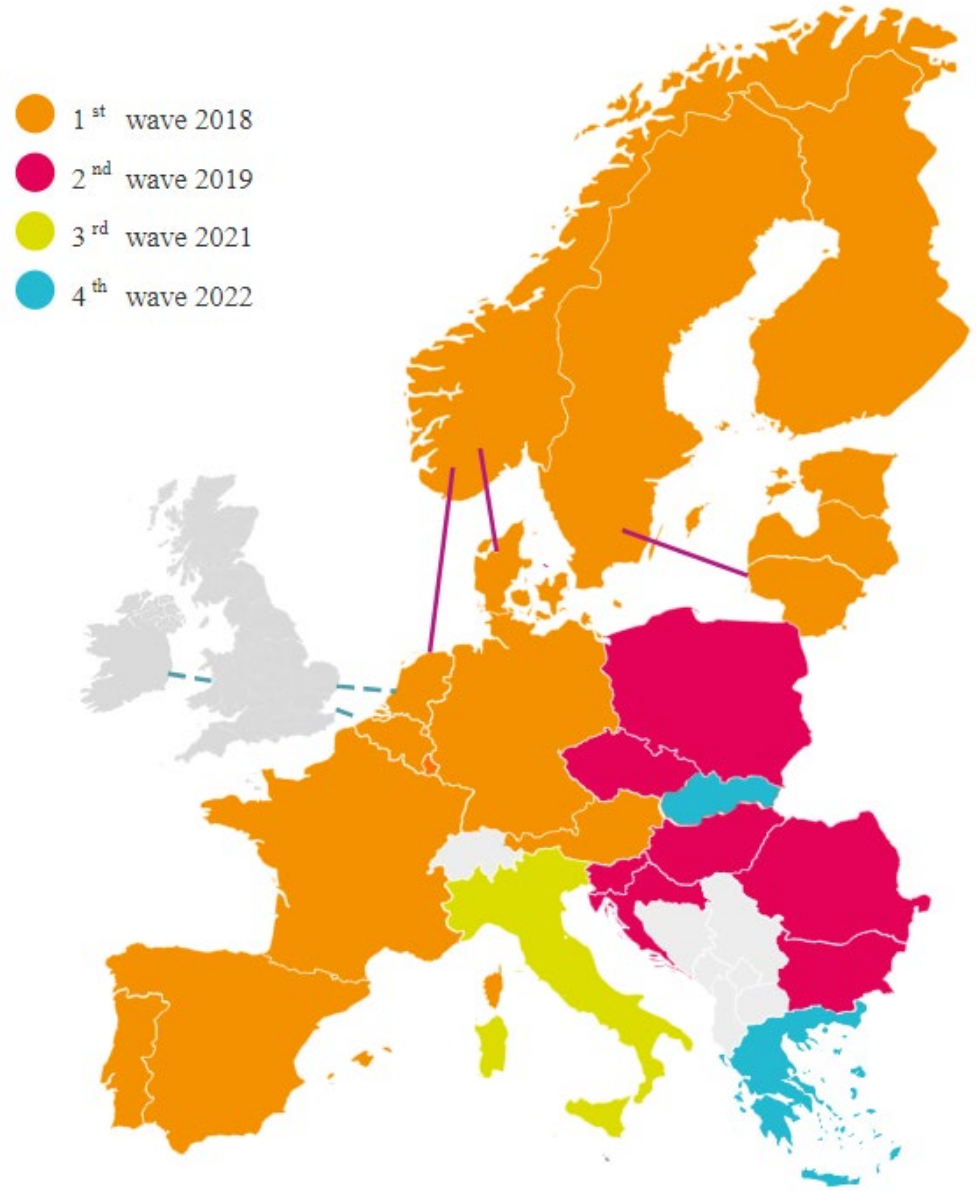
An integrated intraday market makes intraday trading more efficient across Europe by:

- promoting competition
- increasing liquidity
- making it easier to share energy generation resources
- making it easier for market participants to allow for unexpected changes in consumption and outages

As renewable intermittent production such as solar energy increases, market participants are becoming more interested in trading in the intraday markets. This is because it has become more challenging for market participants to be in balance (i.e. supplying the correct amount of energy) after the closing of the Day-Ahead market.

Being able to balance their positions before delivery time is beneficial for market participants and for the power systems alike by, among other things, reducing the need for reserves and associated costs while allowing enough time for carrying out system operation processes for ensuring system security.

The first go-live wave was in June 2018 and included 15 countries. A second go-live with seven further countries was achieved in November 2019, a third go-live including Italy in September 2021, and the latest go-live, the fourth wave, added Slovakia and Greece in November 2022. The picture below depicts all current countries in SIDC.



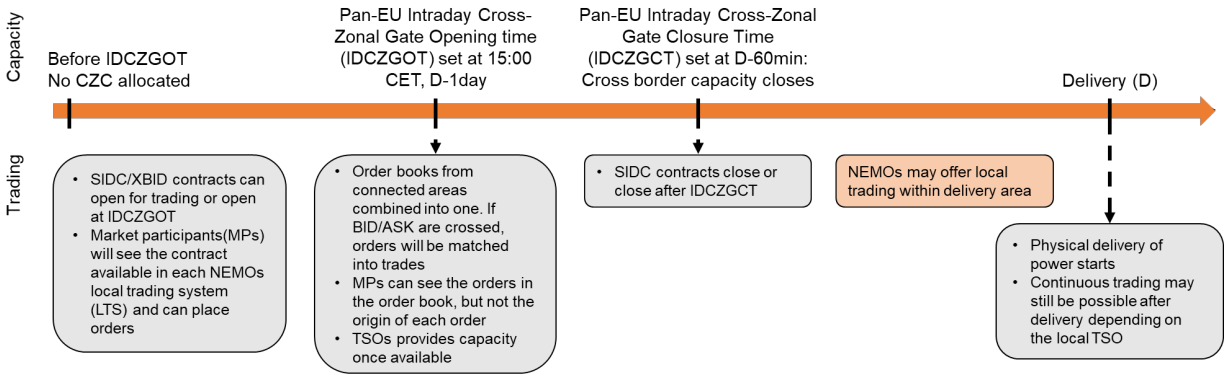
See for more information the following websites:

- ENTSO-E: https://www.entsoe.eu/network_codes/cacm/implementation/sidc/
- NEMO Committee: http://www.nemo-committee.eu/sidc

3. Normal Operational Process

This section depicts normal operational process where incidents are resolved following incident management process (as described in Chapter 4).

The normal operational process is described in the timeline below:



4. Incident Management Process

An incident is an unwanted event in the XBID system (SIDC's IT solution), local NEMO or TSO systems connected to XBID or a disturbance of the communication channels connecting these systems. An incident that requires triggering an Incident Committee call has the following characteristics: the issue(s) causing the incident cannot be solved through a (Local) Backup procedure and can thereby breach a deadline (e.g. gate closure or gate opening) of the Single Intraday Coupling.

The operational parties agreed to follow the Incident Management procedure to handle incidents. The Incident Management procedure assumes that communication to relevant 3rd parties (e.g. CCP, Shipping Agent, Explicit Participant, etc.) is done by the involved TSOs and NEMOs by following their local procedures.

As a general principle, the Incident Management procedure describes the handling of incidents, which includes the operation of the Incident Committee and the fallback solution to be applied following the procedures, e.g. closing and re-opening of Interconnectors, closing and restarting of market area(s), delivery area(s) or trading service.

The Incident Committee is only to be triggered for the management of a critical or major incident of the XBID system, critical or major incident of a Transit Shipping Agent System and Shipping Agent default. Any other incident can only trigger the Incident Committee when the incident fulfils the pre-defined criteria. In order to prevent the Incident Committee call to be triggered for incorrect reasons, the parties perform an initial internal check and a cross check with other parties on the incident before raising the incident as a central issue.

As soon as an incident occurs that impacts any of the Single Intraday Coupling processes, an Incident Committee needs to be started, which will be convened by the IC SPOC.

Participants to the Incident Committee identify the issue(s), assess and agree on potential solutions. The IC SPOC tracks all relevant information on the incident, the discussions during the Incident Committee and the decision taking place during the Incident Committee call.

At the start of the Incident Committee the IC SPOC and/or the incident reporter presents the issue. The parties discuss actions already taken by the affected party and immediate actions deemed necessary. The parties further consider correct classification of the incident.

The parties discuss potential solutions for the incident, where needed on recommendation of the service provider. Once a solution has been identified the parties decide on the application of the agreed solution.

During the Incident Committee the parties also decide on communication to the Market Participants deemed necessary.

Within typically 2 hours after closing the Incident Committee the IC SPOC will create/finalize the IC report and make the IC report available to all NEMOs and TSOs. The involved parties need to review, and if applicable, update the IC report.

5. Incident Description

Incidents were reported after an automated message from XBID Core failover was received and Shared Order Book (SOB) WebGUI went down. This situation has been repeated twice during 21st of May.

5.1 Timeline

System failure	2024/05/21 14:00	2024/05/21 14:46
Triggering of Incident Committee	2024/05/21 14:09	2024/05/21 14:48
System recovered	2024/05/21 14:01	2024/05/21 14:47
Green light from Supplier	2024/05/21 14:23	2024/05/21 14:58
Green light from all parties to start trading	2024/05/21 14:24	2024/05/21 15:06
Restart of trading	2024/05/21 14:35	2024/05/21 15:15

5.2 Course of Event

On 21/05/2024 at 14:00 SOB WebGUI went down and automated XBID failover to Core2 was performed.

At 14:09 first Incident Committee was triggered where the service provider confirmed that XBID correctly switched to Core2 and that the issue in Core1 was caused by validation error linked to

specific customer incoming file. The service provider informed that they required additional time to check with the specific customer causing the issue. Additionally, during the Incident Committee call, the service provider was asked about the stability of Core2 to reopen the market, indicating that additional time was needed to check it.

At 14:35, once the service provider gave green light to reopen the market and NEMOs and TSOs agreed, the market successfully was set back to trading.

At 14:46 same situation happened again, SOB WebGUI went down again, and a second Incident Committee took place. The service provider indicated that the root cause of the new incident was the same. Additionally, the service provider indicated that XBID system was healthy, and it was safe to reopen the market if the specific customer who caused the issue could avoid delivery of the respective file. The specific customer confirmed the respective file would not be uploaded again to avoid another Core down.

At 15:15 the market was successfully set back to trading based on specific customer confirmation and service provider advice; the Incident Committee call was closed.

5.3 Root Cause

The initial findings of the service provider showed that the specific files, sent from a specific TSO, triggered validation error which might have caused the Core to crash. However, after deeper analysis, the service provider found the issue was linked to the auto publish of capacity.

The service provider clarified when the two CMM node instances are running in parallel, they compete with each other which CMM node sends the data set for publishing to the core and which CMM node should not send any data set for publishing to the core. Instead, the other CMM node sent an empty data set for publishing to the core causing this situation to crash the XBID System.

5.4 Impact

Downtime	64 minutes
Critical business process impacted	XBID Server Disconnection
Procedural impact	N/A

5.5 Mitigation Measures and Lessons Learnt

To ensure successful restoration of the operations and prevent the issue happening again, the following measures have been taken:

Supplier's Short-term Solution	XBID Core was restored

Supplier's Long-term Measures	To avoid the issue experienced, only a single node of CMM was running. However, the other node remained as a backup, which is also viable and can be activated in case of failure of the primary node. The long-term solution to fix the issue was to apply a hotfix.
SIDC Project Lessons Learned	**NA**