SIDC OPSCOM Report on the Critical Incident Experienced on 6th September 2025

31.10.2025

1. Executive Summary

This report provides information to stakeholders regarding a critical incident that occurred on 6th September 2025, affecting the Single Intra-Day Coupling (SIDC) market. Following scheduled maintenance on the XBID system, market parties were unable to connect to some of the XBID components. This led to a downtime of the continuous intraday electricity market lasting 8 hours and 20 minutes. When combined with the planned maintenance window of 2 hours and 30 minutes, the total interruption to XBID cross-border continuous trading was 10 hours and 50 minutes. The root cause was identified as a network infrastructure issue managed by the XBID Service Provider. Once resolved, normal market operations resumed.

2. Introduction

This report serves to fulfil the obligation under CACM Regulation on reporting unexpected market downtime towards stakeholders.

The report is structured as follows. In Chapter 3, SIDC is described. In Chapter 4, the normal operational process, as covered in the operational procedures with respective timings, is described. In Chapter 5, the incident management process applied when critical incidents occur is described. In Chapter 6, a description of the incident, including inter alia the timing and the root cause, is provided. Finally, in Chapter 7, the mitigation measures to resolve the issue and the lessons learnt are presented.

3. Single Intraday Coupling

The Single Intraday Coupling (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:

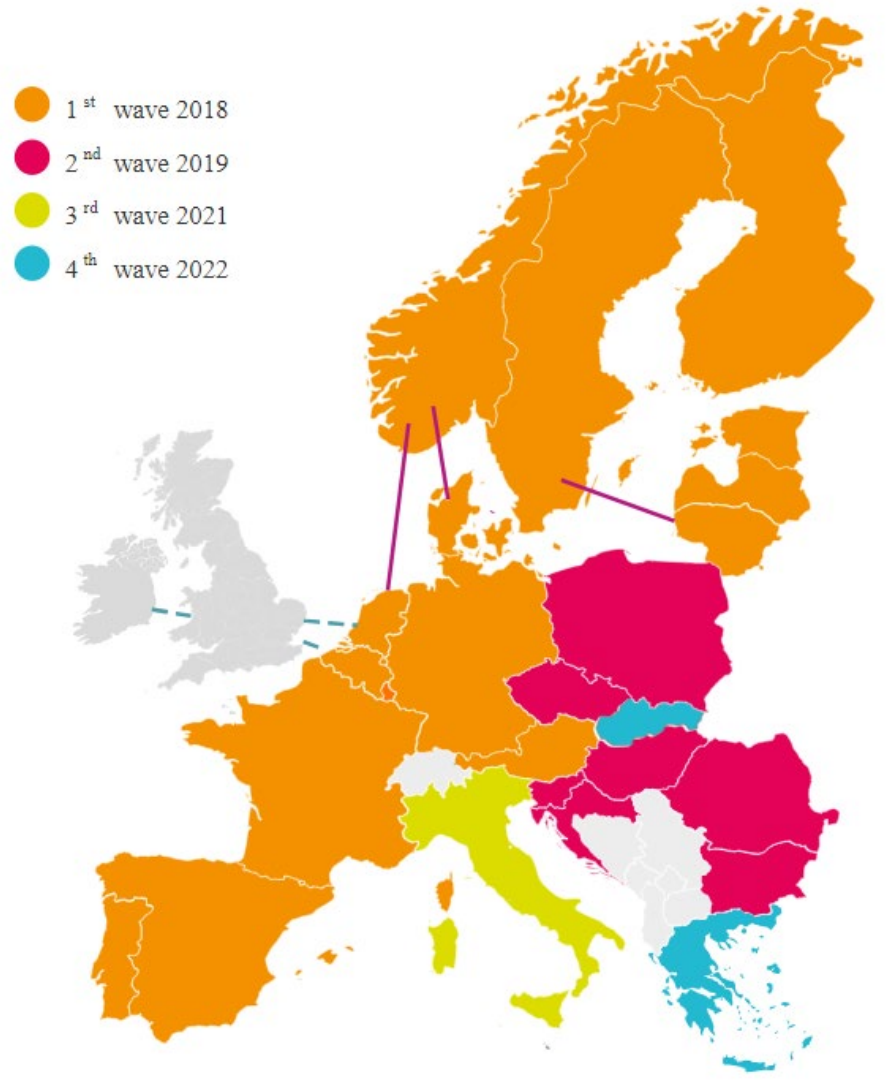
- promoting competition
- increasing liquidity
- making it easier to share energy generation resources
- making it easier for market participants to allow for unexpected changes in consumption and outages

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 until one hour 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 to ensure 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 took place 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:



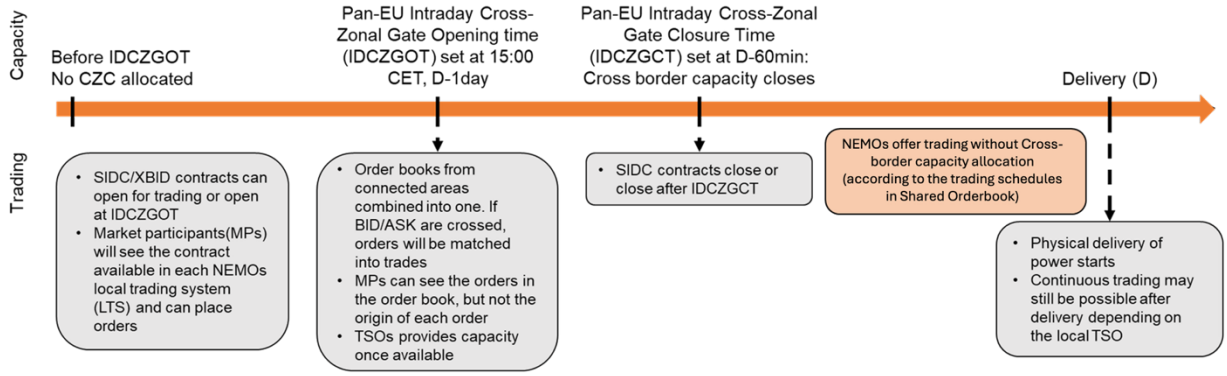
See for more information the following websites:

- ENTSO-E
- NEMO Committee

4. Normal Operational Process

This section outlines the normal operational process whereby incidents are resolved following the incident management process (as described in Chapter 5.

The normal operational process is described in the timeline below:



5. 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 the triggering of 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 undertaken by the involved TSOs and NEMOs 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 or 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 being incorrectly triggered, 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, 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 reached 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 what communication to the market participants is 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.

6. Incident Description

This report informs stakeholders of a critical incident affecting the Single Intra-Day Coupling (SIDC) market on 6th September 2025, resulting in a downtime for the continuous intraday electricity market of 8 hours and 20 minutes. The incident occurred following scheduled maintenance performed by the XBID Service Provider. After the maintenance window, parties experienced connectivity issues with several XBID components, leading to an extended market outage. The issue was resolved by the service provider and normal operations resumed.

6.1 Timeline

NEMO Central Admin, following the detection of the critical incident, initiated the Incident Committee Conference Call ("ICCC").

System failure	2025/09/06 09:27
System recovered	2025/09/06 17:30
Green light from supplier	2025/09/06 17:30
Green light from all parties to start trading	2025/09/06 17:37
Restart of trading	2025/09/06 17:50

6.2 Course of Event

On 6th September 2025, at 07:00 CEST, scheduled maintenance began on the XBID system.

09:27 CEST: The XBID Service Provider gave the green light for parties to reconnect, but issues were encountered with the Shipping Module, CMM connectivity, and later with the Shared Order Book (SOB). Parties were present in a Maintenance call with software provider and addressing the issue before raising an Incident Committee Call.

10:46 CEST: The incident was formalized by triggering an Incident Call according to procedures.

10:59 CEST: Service Provider attempts resolution by restarting affected components.

13:07 CEST: DBAG indicated the root cause was still unknown and continued troubleshooting.

15:25 CEST: DBAG considered involving additional support and the incident was escalated to the Market Coupling Steering Committee (MCSC).

16:46 CEST: Core failover was initiated by DBAG.

17:23 CEST: Multiple parties confirmed system components were available.

17:37 CEST: 17:50 was agreed as the market reopening time.

17:50 CEST: The market was set to trading and operations resumed.

Some parties reported residual connectivity issues, which were addressed in follow-up actions.

6.3 Root Cause

According to the Root Cause Analysis provided by the XBID Service Provider, the incident was caused by a bug in the network infrastructure provided by a third party. The problem was not related to the XBID application itself.

No evidence of external interference or cyberattack was found.

The bug has been identified and measures have been taken to ensure it does not happen again.

The incident was resolved after network components were restored and system connectivity was re-established.

6.4 Impact

Downtime	8 hours and 20 minutes
Critical business process impacted	XBID trading
Procedural impact	N/A

7. Mitigation Measures and Lessons Learned

To ensure a successful restoration of operations, the following measures were taken:

Supplier's Short-Term Solution	The XBID Service Provider restored network infrastructure and confirmed system availability.
Supplier's Long-Term Measures	Preventative Actions 1. Update of maintenance runbook (script used for maintenance actions) for cases of disruptive infrastructure changes. 2. Enhanced pre-maintenance coordination: • Joint planning and impact assessments across teams to ensure alignment and readiness. • Clear escalation paths and fallback procedures defined in advance for high-impact changes. 3. Defined rollback strategy as part of impact assessment and change planning. For future similar infrastructure changes, a rollback or contingency plan will be explicitly documented and reviewed during pre-maintenance coordination. This includes evaluating technical feasibility, risk thresholds and fallback procedures to ensure service continuity. 4. Enhance endpoint monitoring and visibility of endpoint connectivity across critical services. This will enable faster detection of session disruptions and support proactive

	troubleshooting during infrastructure changes.
SIDC Project Lessons Learnt	**N/A**