SIDC OPSCOM report on Critical Incident

Experienced on 27th of February 2023

External version

05/07/2023

Executive summary

The report informs the Stakeholders on global critical incident at SIDC that happened on the 27th February 2023 resulting in a XBID network outage. The incident involved a switch failure in the XBID primary data center that triggered an immediate failover to the redundant secondary switch. However, the redundancy mechanism failed to promptly detect the malfunctioning system, and the lack of alert capability on the connected servers hindered any immediate reaction on the server side resulting in a XBID application core failover.
The issue resulted in 52 minutes of unexpected outage in the XBID operation.

List of contents

1. Introduction

This report serves to fulfill 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. 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. Finally, in Chapter 6, the mitigation measures to resolve the issue, and the lessons learnt are presented.

2. 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.

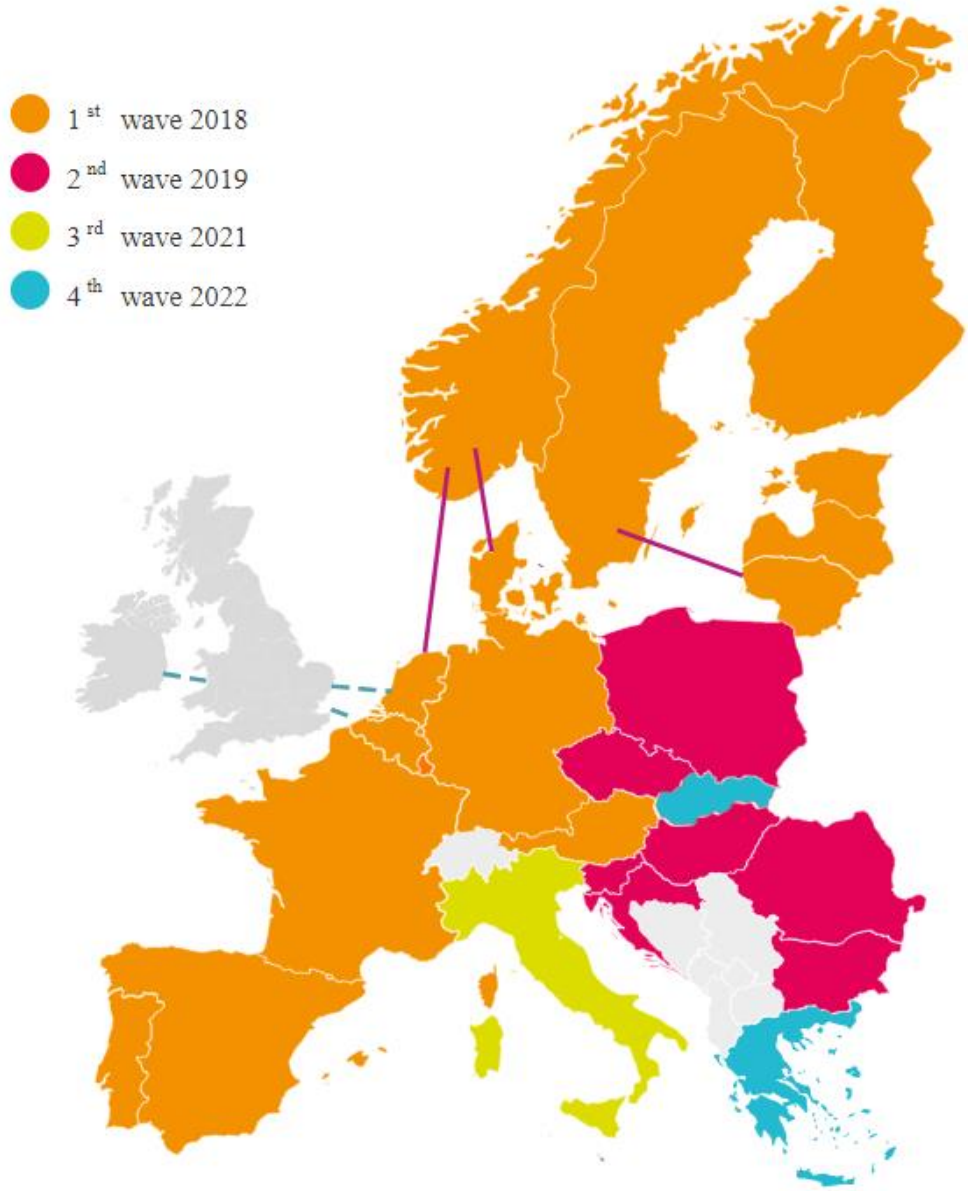
An integrated intraday market makes intraday trading more efficient across Europe by:

- 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 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 forth wave, added Slovakia and Greece in November 2022. The picture below depicts all current countries in SIDC



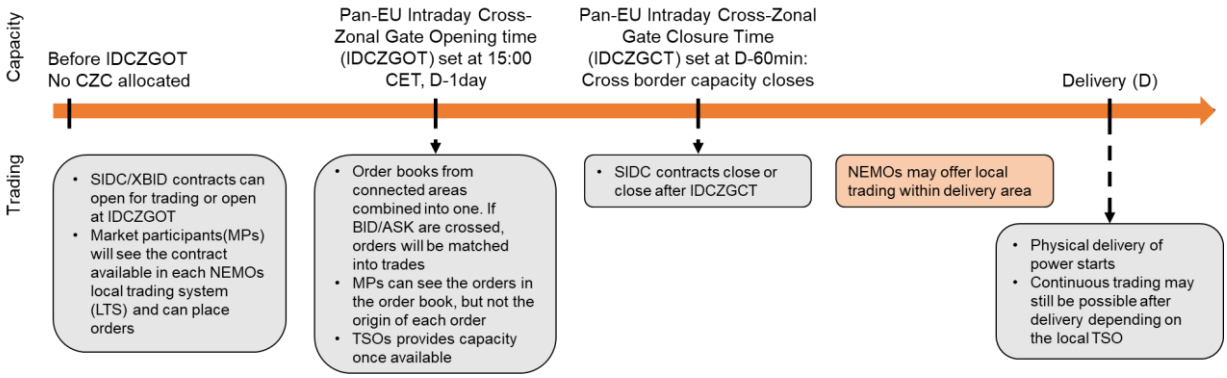
See for more information the following websites:

- 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 describes normal operational process and how the incidents are resolved following incident management process.

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 the communications channels connecting them. An incident that requires triggering an IC 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 Market 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 Participants, 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 (IC), the fallback solution to be applied following the procedures, e.g. closing and re-opening of Interconnectors, closing and restarting of market or delivery area(s) or trading service and corresponding local procedures.

The IC 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 Systems and Shipping Agent default. Any other incident only can trigger the IC when the incident fulfils the pre-defined criteria. In order to prevent the IC 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 Market Coupling processes, an Incident Committee (IC) needs to be started, which will be convened by the IC SPOC.

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

At the start of the IC 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 IC the parties also decide on communication to the Market Participants deemed necessary.

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

5. Incident Description

Incident was reported after a message from XBID core failover was received and SOB WebGUI was impossible to access.

5.1 Timeline

System failure	**2023/02/27 00:35**
Triggering of Incident Committee	**2023/02/27 00:49**
System recovered	**2023/02/27 01:16**
Green light from Supplier	**2023/02/27 01:18**
Green light from all parties to start trading	**2023/02/27 01:18**
Restart of trading	**2023/02/27 01:27**

5.2 Course of Event

On 27/02/2023 at 00:35, a switch in the primary Data Center of XBID system crashed. Normally, the secondary Data Center should take over immediately. However, the redundancy mechanism in charge of switching from the Primary Data Center to the Secondary did not work as expected, and the XBID system was down, and market automatically halted.

At 00:47 an Incident Committee was opened and NEMOs and TSOs confirmed that the XBID systems were down. Supplier confirmed that they were investigating the issue, and trying to ensure that it was safe to restart the XBID system core instances. At 01:16, the Supplier announced that the system was stable and it was safe to restart the market. Once NEMOs and TSOs performed the necessary checks and confirmed that the connection between the Local Trading Solutions and the XBID system worked well, it was agreed to set the system to trading at 01:27. Therefore, at 01:27 the market was successfully set back to trading and at 01:30, with the approval of every NEMO and TSO, the Incident committee call was closed.

5.3 Root Cause

After thorough analysis, it's been discovered that the reason for both the crash of the Primary Data Center and the failure of the redundancy mechanism, was a Network outage. One system out of a 2 system active/active cluster malfunctioned in a way that the redundancy mechanism did not notice immediately. As connected servers are not able to alert on partially dropped traffic, there is no way of reacting to this situation on the server side. Consequently, the redundancy system did not activate and therefore the XBID system went down.

5.4 Impact

Downtime	52 minutes
Critical business process impacted	XBID Server Disconnection
Procedural impact	N/A

Mitigation measures and lessons learnt

To ensure successful restoration of the operations the following measures have been taken:

Supplier's Short-term Solution	XBID Core was restored
Supplier's Long-term Measures	Fix was not possible as connected servers are not able to alert on partially dropped traffic, there is no way of reacting to this situation on the server side.

	Supplier rearranged the setup of the cluster network connectivity to ensure redundancy mechanism works properly, and as soon as one core fails, the other one can take over
SIDC Project Lessons Learned	**NA**