EUROCONTROL

Network Manager outage on 3 April 2018

Summary brief

INTRODUCTION

On the 3rd of April the Network Manager suffered an outage of its technical system affecting primarily its ATFM and CCAMS operational services. On the 4th of April the Director General asked for an investigation, independent from NM, to take place, led by DATM (Philippe Merlot) and the Head of Engineering Division MUAC (Peter Naets).

This resulted in the Technical Problem Report NM 2018 01; this was presented to the European Commission, EASA, the Network Management Board and Permanent Commission members and is available via this link:

https://www.eurocontrol.int/sites/default/files/publication/files/technical-problem-report-nm-2018-01.pdf

EASA decided to perform an unscheduled audit which took place on the 18th and 19th of April. Their conclusions can be found in para 6 of this paper.

The ATFM Procedural Contingency Plan was activated which included precautionary reductions in sector capacities and lower departure rates from airports. Provisional figures show average additional departure delays of 10 mins compared to the average expected departure delay of 3 mins between 1230 and 1800UTC.

CAUSE OF THE OUTAGE

In preparation for the introduction of the new NM software release (NM22), routine system acceptance tests were scheduled for the morning of 3rd April 2018. For such testing purposes, a new environmental database (containing static airspace data such as definition of airspaces. aerodromes, route, points, etc.) was needed. For this, an automated script is routinely used, with the objective to initialise all the systems in the target domain by uploading a new set of data (environment and flight) in all systems. One of the first steps in the script is to erase the content of the existing databases in the operational test domain only.

A configuration variable linked to this script had been erroneously changed, two weeks earlier, to point to a system instance in the operational domain instead of the operational test domain. This erroneous manipulation led to a change made in the operational system instead of the operational test system. This mistake in itself was not sufficient to allow for the deletion in the operational environment. The spread to the operational environment was possible due to the existence of a vulnerability (backdoor) in the barriers that were supposed to prevent access to the operational domain from the operational test domain. This backdoor was introduced as an exception through an approved change request in 2002 as it was then needed for a particular type of testing/validation that could have not been performed otherwise.

The script contains additional protection that prevents its execution from the operational domain. However, since the script was launched from the operational test domain instead, that protection did not work either. Finally, the operational systems have an additional protection to prevent accidental deletion of their live databases. This protection is limited to the airspace data only and not to the flight data.

The Operational systems by NM have resilience implemented locally in Haren and a contingency site exists in Bretigny with a hot standby function for IFPS, ENV and CCAMS and cold standby for ETFMS. The resilience characteristics of the system mitigate failures except for common mode failures of software or data corruption. Given the data replication from one site to the other, data corruption that might occur on the Haren site, can also have impact on the Bretigny site.

In conclusion the script was able to delete the live flight data from the operational systems. The simultaneous deletion of all flights from the live databases of all operational instances was the trigger for the system outage that generated the service disruption at the Eurocontrol Network Manager on 3rd April 2018.

At the time the automated script was launched, no one was aware of these potential threats to the operational systems.

TIMELINE

10:26	ETFMS Outage. CHMI outage reported by EDYYUAC (Maastricht UAC) and LOWACC (Vienna ACC).
10:30 - 10:48	The Technical Operations Manager on duty (TOM) is notified and the responsible for the Level 2 application support is called. A possible network issue is discarded as reason for the problem and focus of the technical investigation is on ETFMS. Later on the Level 3 technical support in charge of software investigation is also called (ETFMS L3 LSE at 10:48).
10:41 - 10:54	NMOC enters the disruption phase in accordance with the NMOC Contingency Manual. NOM Manager on call is notified of the outage. Acting Head NTS is informed on the situation.
10:58	It is confirmed that ETFMS Database is empty and ETFMS is stopped at 11:01 to attempt a restore from recorded data.
11:01	The first NOP headline news is published announcing the provisional start of the Contingency Plan at 12:26UTC (the latest time of the previously allocated departure slots).
11:15	A first management briefing is held and it is concluded that system restore will not be possible in a short timeframe (within the next 20 minutes) and the need to apply the Contingency Plan is confirmed.
11:28	Transponder code (CCAMS) contingency activated but with no flight in the system there is a risk of code duplication. It is concluded that CCAMS contingency is unusable and CCAMS RED level is declared.
11:45	At this time it is realised that there is a problem with the IFPS database as well and a the LSE Level 3 for IFPS is called for additional support. Several options to restore the flight plan database in the IFPS and ETFMS systems were analysed and eventually it was decided to follow a conservative recovery approach to prevent any additional unwanted effects.
12:03	Airspace users are informed that all FPLs filed before 10:26 UTC were lost in the system and may need to be re-sent to IFPS. Later, at 12:53, NM requests all airspace users to refile all FPLs sent before 10:26UTC.
12:13	ETFMS is reinitialised with flights incoming after 10:28. 12:26 Contingency Plan is officially started.
13:00	The cause of the technical failure is identified and confirmed.
13:15	NM Teleconference (174 participants). Additional teleconferences and contacts, notably with NATS, DHMI and Turkish Airlines take place later in the day to alleviate some of the restrictions established in the Contingency Plan.
15:20	NM opens access to its flow management system, whilst remaining in Procedural Contingency mode. At this time ETFMS is considered safe enough to allow access to airspace users in order to verify their flight plans but it is not yet used for flow purposes. The system is gradually rebuilding the full air traffic situation and is declared fully operational at 18:00.
16:58	NM announces that the Procedural Contingency will remain valid until 1800UTC and ETFMS will return to normal operations from 1800UTC. This was preceded by a coordination telco with the ANSPs.
17:23	NM announces that CCAMS will be restarted at 2200UTC. Although CCMAS was fully restored at this stage, the later re-activation measure was a safety precaution to ensure that the transition is done during a period of low traffic to mitigate the risk of duplicated code allocations.
23:06	CCAMS back to normal.

SAFETY IMPACT AND RISKS

Mitigations were implemented in accordance with the NM Safety Base Line (NM Operations Safety Report "NOSR" v1.1 accepted by EASA on 13 Dec 2017).

The outage of ETFMS resulted in the application of the NM ATFM Procedural Contingency Plan which was correctly executed through all phases, thus ensuring a safe level of traffic throughout the European ATM Network. Once the NM ATFM Procedural Contingency Plan was implemented, coordination led by NMOC with ANSPs ensured that capacity was continuously optimised throughout the network. The return to using ETFMS was dependent on having a sufficient level of flight plans in the NM systems so that ETFMS would not give FMPs an incorrect, and potentially unsafe, picture by showing a lower traffic load against capacity than reality.

The deletion of the live flight data impacted IFPS and resulted in additional workload for the Airspace Users, which had to refile flight plans, and for the Air Traffic Service Units (ATSU), which had to manually enter flight details in their local systems.

The outage of CCMAS resulted in the application of the CCMAS Contingency plan (level RED). All ATS Units then started assigning predefined RED codes. It was identified that not all units confirmed the reception of the message and one unit did not switch to level RED immediately. Actions were taken to correct the situation through direct contacts with the concerned ANSPs. Apart from this, no operational issues were reported during the contingency period.

It can be concluded that safety has been maintained at all times during the outage and during the transition to normal operations.

MEASURES

The following measure were immediately taken by the Network Technical Systems teams in order to prevent the repetition of such a failure:

- Fixing of the faulty configuration variable used by the script that sets up the test condition in the OPS test system.
- Suspension of the process of testing and installation of the new NM 22.0 baseline until the fixing of the faulty configuration variable used by the script.
- Removal of the vulnerability (backdoor) between the Operational system and the OPS test system.

14 further measures to be implemented have been identified, of which the most important are:

- A thorough analysis of the current implementation of the separation to identify any vulnerabilities and address these.
- Implement a system change in future NM release (23) to enable recovery of the flight plan data from backup.
- Review the Common Cause Analysis of the existing NM Safety Baseline (NM Operations Safety Report) in order to identify possible system improvements and recovery procedures.
- Review the architecture of the NM systems to identify mitigations for common cause failures.
- Review the NM ATFM Procedural Contingency Plan with an aim to improve its clarity and optimise the applicable departure restriction rates.

EASA Unscheduled Audit

A separate and unscheduled EASA audit was performed on 18/19th April. At the time of completing this report, EASA, following a review of the timeline, interviews with relevant NM personnel and an assessment of the documentation provided, the EASA audit team has reached a number of conclusions in the areas of:

- Failure detection and contingency procedures.
- IT Control environment.
- Safety Management System.
- Staff Competence Assessment.

The Network Manager is responding to the identified weaknesses and areas for improvements through dedicated action plans which will be overseen by EASA to confirm their appropriateness and sufficiency to identify and mitigate the existing risks.

EUROCONTROL

www.eurocontrol.int