AIRNAV IRELAND

AI for Anomaly Detection in Air Traffic Management Systems

Callum Winship

22 April 2025

1. Why it matters?
2. How does it work?
3. How has it been tested?

AIRNAV IRELAND

ATM System Function

Ensure the **safe**, orderly and efficient flow of air traffic.

It does this by:

- Providing real-time information to pilots and controllers
- Coordinating take-offs, landings and transitions
- Preventing collisions between aircraft

AIRNAV IRELAND

The Problem

```
081109 203807 222 INFO dfs.DataNode$PacketResponder: PacketResponder 0 for block blk_-6952295868487656571 terminating
081109 204005 35 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.73.220:50010 is added to blk_7128370237687728475 size 67108864
081109 204015 308 INFO dfs.DataNode$PacketResponder: PacketResponder 2 for block blk_8229193803249955061 terminating
081109 204106 329 INFO dfs.DataNode$PacketResponder: PacketResponder 2 for block blk_-6670958622368987959 terminating
081109 204132 26 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.43.115:50010 is added to blk_3050920587428079149 size 67108864
081109 204324 34 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.203.80:50010 is added to blk_7888946331804732825 size 67108864
081109 204453 34 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.250.11.85:50010 is added to blk_2377150260128098806 size 67108864
081109 204525 512 INFO dfs.DataNode$PacketResponder: PacketResponder 2 for block blk_572492839287299681 terminating
081109 204655 556 INFO dfs.DataNode$PacketResponder: Received block blk_3587508140051953248 of size 67108864 from /10.251.42.84
081109 204722 567 INFO dfs.DataNode$PacketResponder: Received block blk_5402003568334525940 of size 67108864 from /10.251.214.112
081109 204815 653 INFO dfs.DataNode$DataXceiver: Receiving block blk_5792489080791696128 src: /10.251.30.6:33145 dest: /10.251.30.6:50010
081109 204842 663 INFO dfs.DataNode$DataXceiver: Receiving block blk_1724757848743533110 src: /10.251.111.130:49851 dest: /10.251.111.130:50010
081109 204908 31 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.110.8:50010 is added to blk_8015913224713045110 size 67108864
081109 204925 673 INFO dfs.DataNode$DataXceiver: Receiving block blk_-5623176793330377570 src: /10.251.75.228:53725 dest: /10.251.75.228:50010
081109 205035 28 INFO dfs.FSNamesystem: BLOCK* NameSystem.allocateBlock: /user/root/rand/_temporary/_task_200811092030_0001_m_000590_0/part-00590. blk_-1727475099218615100
081109 205056 710 INFO dfs.DataNode$PacketResponder: PacketResponder 1 for block blk_5017373558217225674 terminating
081109 205157 752 INFO dfs.DataNode$PacketResponder: Received block blk_9212264480425680329 of size 67108864 from /10.251.123.1
081109 205315 29 INFO dfs.FSNamesystem: BLOCK* NameSystem.allocateBlock: /user/root/rand/_temporary/_task_200811092030_0001_m_000742_0/part-00742. blk_-7878121102358435702
081109 205409 28 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.111.130:50010 is added to blk_4568434182693165548 size 67108864
081109 205412 832 INFO dfs.DataNode$PacketResponder: Received block blk_-5704899712662113150 of size 67108864 from /10.251.91.229
081109 205632 28 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.74.79:50010 is added to blk_-4794867979917102672 size 67108864
081109 205739 29 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.38.197:50010 is added to blk_8763662564934652249 size 67108864
081109 205742 1001 INFO dfs.DataNode$PacketResponder: Received block blk_-5861636720645142679 of size 67108864 from /10.251.70.211
081109 205746 29 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.74.134:50010 is added to blk_74538
```

AIRNAV IRELAND

2. How does it work?

AIRNAV IRELAND

Experience Report: Deep Learning-based System Log Analysis for Anomaly Detection

Zhuangbin Chen
The Chinese University of Hong Kong
Hong Kong, China

Jinyang Liu
Wenwei Gu
The Chinese University of Hong Kong
Hong Kong, China

Yuxin Su*
Sun Yat-sen University
Zhuhai, China

Jieming Zhu
Huawei Noah's Ark Lab
Shenzhen, China

Yongqiang Yang
Huawei Cloud BU
Beijing, China

Michael R. Lyu
The Chinese University of Hong Kong
Hong Kong, China

[1]

ABSTRACT

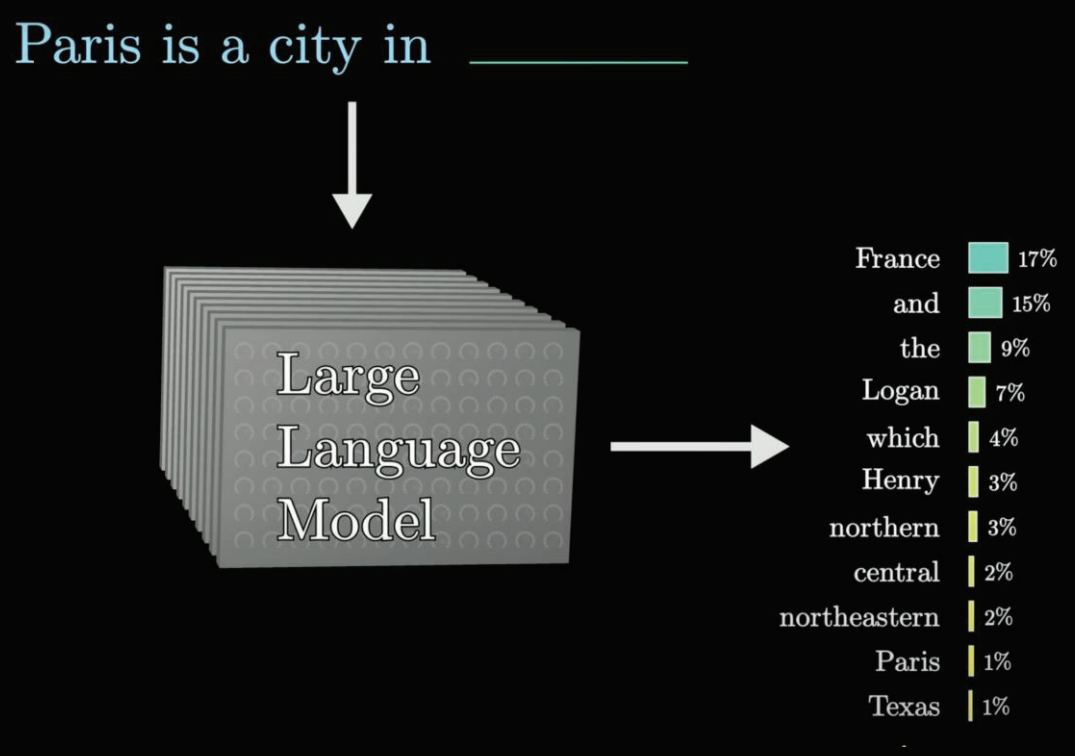
Logs have been an imperative resource to ensure the reliability and continuity of many software systems, especially large-scale distributed systems. They faithfully record runtime information to facilitate system troubleshooting and behavior understanding. Due to the large scale and complexity of modern software systems, the volume of logs has reached an unprecedented level. Consequently, for log-based anomaly detection, conventional manual inspection methods or even traditional machine learning-based methods become impractical, which serve as a catalyst for the rapid development of deep learning-based solutions. However, there is currently a lack of rigorous comparison among the representative log-based anomaly detectors that resort to neural networks. Moreover, the re-implementation process demands non-trivial efforts, and bias can be easily introduced. To better understand the characteristics of different anomaly detectors, in this paper, we provide a comprehensive review and evaluation of five popular neural networks used by six state-of-the-art methods. Particularly, four of the selected methods are unsupervised, and the remaining two are supervised. These methods are evaluated with two publicly available log datasets, which contain nearly 16 million log messages and 0.4 million anomaly instances in total. We believe our work can serve as a basis in this field and contribute to future academic research and industrial applications.

Models

Model	Paper reference
Unsupervised models	
LSTM	[CCS'17] Deeplog: Anomaly detection and diagnosis from system logs through deep learning, by Min Du, Feifei Li, Guineng Zheng, and Vivek Srikumar. [University of Utah]
LSTM	[IJCAI'19] LogAnomaly: unsupervised detection of sequential and quantitative anomalies in unstructured logs by Weibin Meng, Ying Liu, Yichen Zhu et al. [Tsinghua University]
Transformer	[ICDM'20] Self-attentive classification-based anomaly detection in unstructured logs, by Sasho Nedelkoski, Jasmin Bogatinovski, Alexander Acker, Jorge Cardoso, and Odej Kao. [TU Berlin]
Autoencoder	[ICT Express'20] Unsupervised log message anomaly detection, by Amir Farzad and T Aaron Gulliver. [University of Victoria]
Supervised models	
Attentional BiLSTM	[ESEC/FSE'19] Robust log-based anomaly detection on unstable log data by Xu Zhang, Yong Xu, Qingwei Lin et al. [MSRA]
CNN	[DASC'18] Detecting anomaly in big data system logs using convolutional neural network by Siyang Lu, Xiang Wei, Yandong Li, and Liqiang Wang. [University of Central Florida]

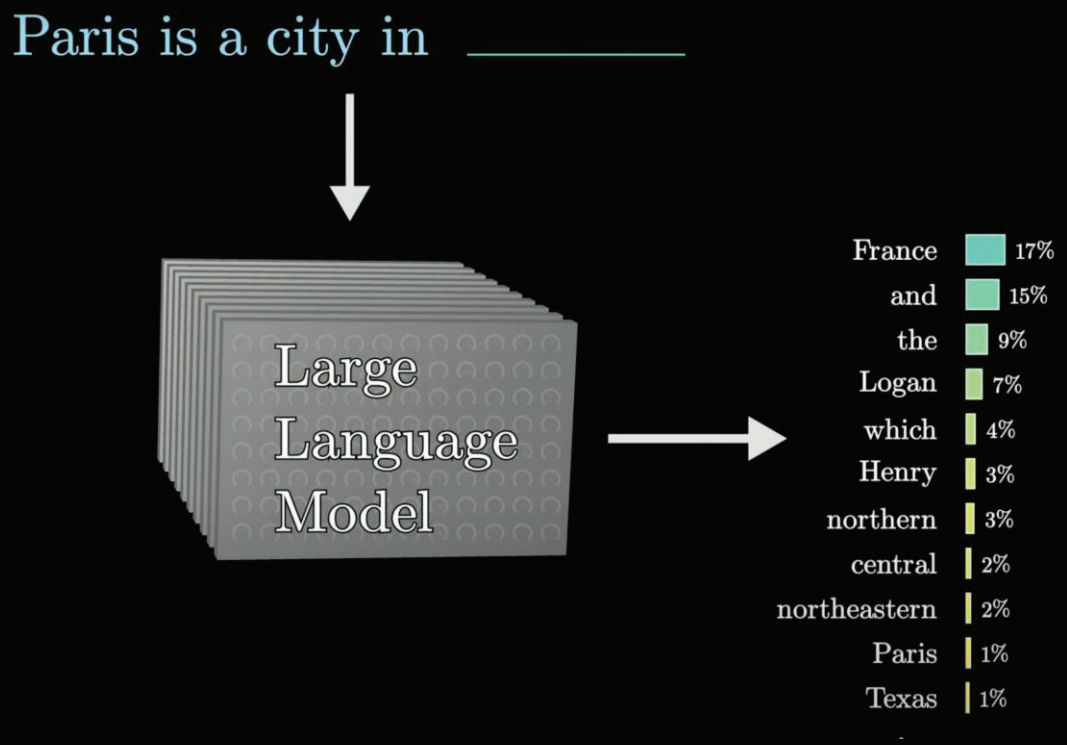
AIRNAV IRELAND

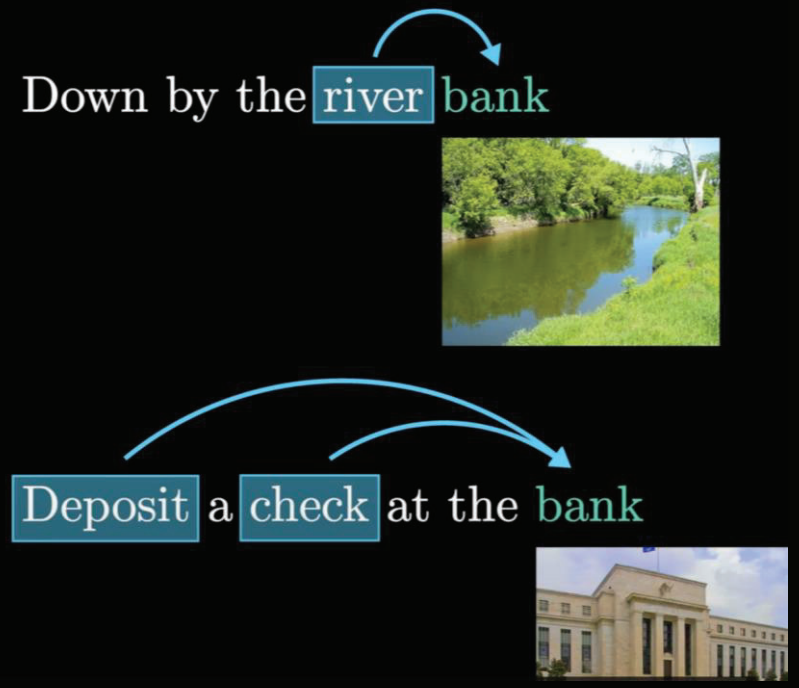
Transformer Model



[2]

Transformer Model



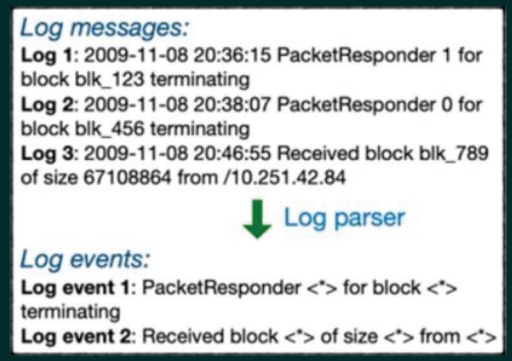


[2]

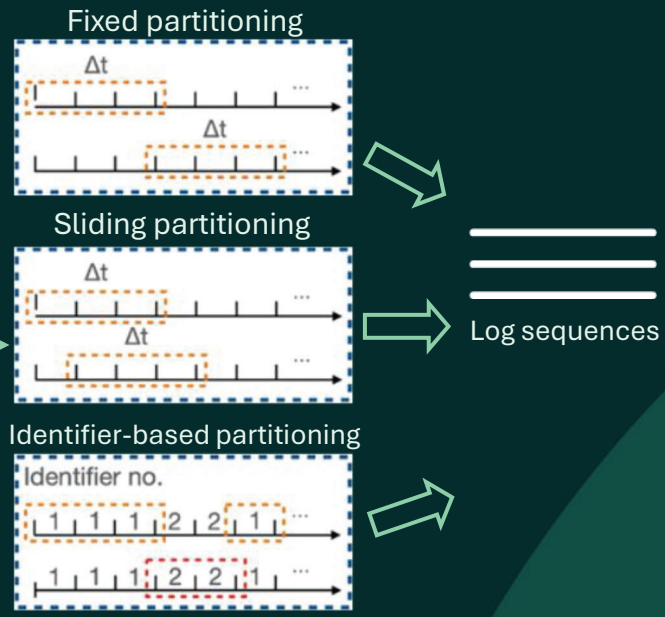
Pipeline

Raw Logs

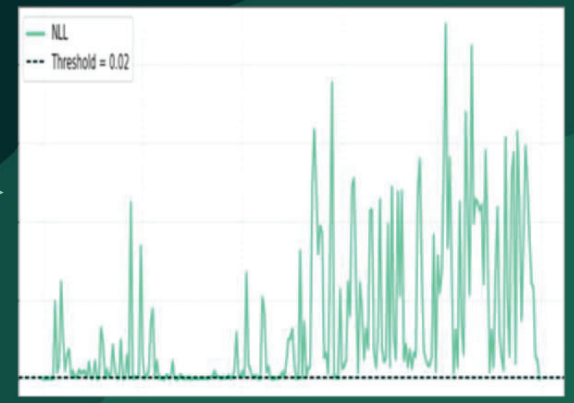
1. Log Collection



2. Log Parsing



3. Log Partition and Feature Extraction



4. Anomaly Detection

AIRNAV IRELAND

1. Log Collection

Flight Data Processing System

AIRNAV IRELAND

1. Log Collection

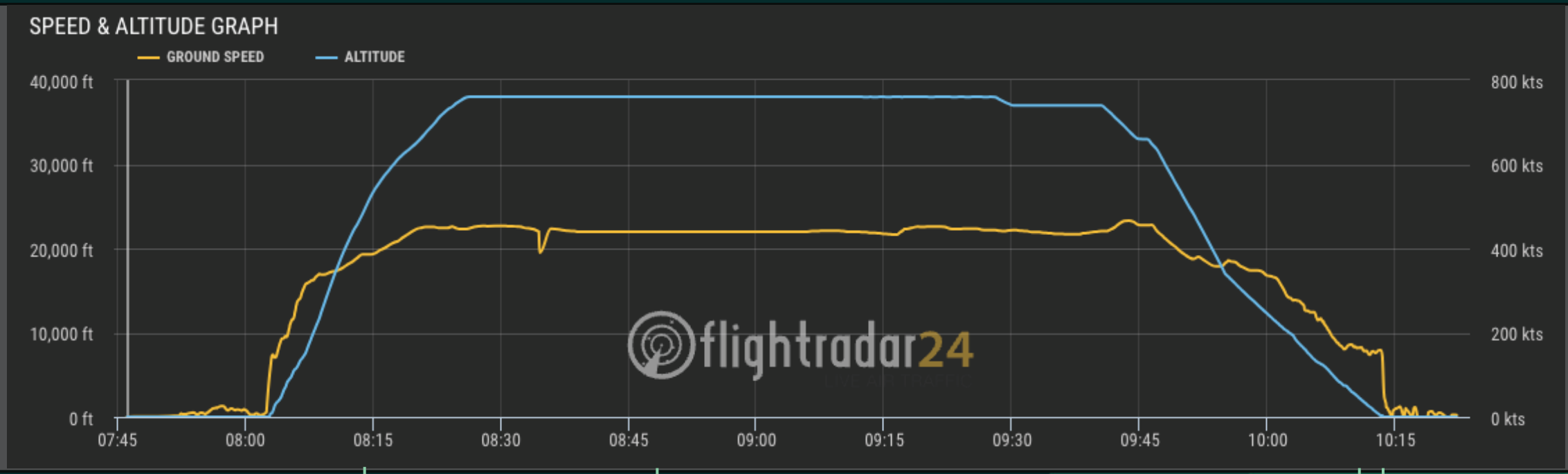
Flight Data Processing System

```
- 1136352584 2006.01.03 R14-M0-NA-C:J12-U11 2006-01-03-21.29.44.825539 R14-M0-NA-C:J12-U11 RAS KERNEL INFO 8 L3 EDRAM error(s) (dcr 0x0157) detected and corrected over 6263 seconds
- 1136352584 2006.01.03 R13-M1-N1-C:J06-U01 2006-01-03-21.29.44.857302 R13-M1-N1-C:J06-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 9 over 6263 seconds
- 1136352584 2006.01.03 R13-M1-N1-C:J06-U01 2006-01-03-21.29.44.938859 R13-M1-N1-C:J06-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 6263 seconds
- 1136352584 2006.01.03 R14-M0-N6-C:J02-U11 2006-01-03-21.29.44.971986 R14-M0-N6-C:J02-U11 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 15 over 6263 seconds
- 1136352585 2006.01.03 R14-M0-N6-C:J02-U11 2006-01-03-21.29.45.052402 R14-M0-N6-C:J02-U11 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 6263 seconds
- 1136352585 2006.01.03 R11-M1-N1-C:J02-U11 2006-01-03-21.29.45.076389 R11-M1-N1-C:J02-U11 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 19 over 6263 seconds
- 1136352585 2006.01.03 R11-M1-N1-C:J02-U11 2006-01-03-21.29.45.099259 R11-M1-N1-C:J02-U11 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 6263 seconds
- 1136353150 2006.01.03 R10-M0-N7-C:J17-U01 2006-01-03-21.39.10.653623 R10-M0-N7-C:J17-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 14 over 523 seconds
- 1136353150 2006.01.03 R10-M0-N7-C:J17-U01 2006-01-03-21.39.10.762810 R10-M0-N7-C:J17-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 523 seconds
- 1136353150 2006.01.03 R14-M0-N6-C:J02-U11 2006-01-03-21.39.10.786477 R14-M0-N6-C:J02-U11 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 15 over 523 seconds
- 1136353150 2006.01.03 R14-M0-N6-C:J02-U11 2006-01-03-21.39.10.808686 R14-M0-N6-C:J02-U11 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 523 seconds
- 1136353150 2006.01.03 R11-M1-N1-C:J02-U11 2006-01-03-21.39.10.829257 R11-M1-N1-C:J02-U11 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 19 over 523 seconds
- 1136353150 2006.01.03 R11-M1-N1-C:J02-U11 2006-01-03-21.39.10.851873 R11-M1-N1-C:J02-U11 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 523 seconds
- 1136353152 2006.01.03 R07-M0-NC-I:J18-U01 2006-01-03-21.39.12.525768 R07-M0-NC-I:J18-U01 RAS KERNEL INFO ciod: generated 1 core files for program /g/g0/hommes/bgl/dd3d.v1.5.1.1/dd3d
- 1136353489 2006.01.03 R10-M0-N7-C:J17-U01 2006-01-03-21.44.49.344693 R10-M0-N7-C:J17-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 14 over 311 seconds
- 1136353489 2006.01.03 R10-M0-N7-C:J17-U01 2006-01-03-21.44.49.454858 R10-M0-N7-C:J17-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 311 seconds
- 1136353489 2006.01.03 R06-M1-N6-C:J15-U01 2006-01-03-21.44.49.483320 R06-M1-N6-C:J15-U01 RAS KERNEL INFO 1 tree receiver 2 in re-synch state event(s) (dcr 0x019a) detected over 311 seconds
- 1136353489 2006.01.03 R06-M1-N6-C:J15-U01 2006-01-03-21.44.49.506202 R06-M1-N6-C:J15-U01 RAS KERNEL INFO 1 tree receiver 2 in re-synch state event(s) (dcr 0x019a) detected over 311 seconds
- 1136353489 2006.01.03 R16-M0-N1-C:J09-U11 2006-01-03-21.44.49.535821 R16-M0-N1-C:J09-U11 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 3 over 311 seconds
- 1136353489 2006.01.03 R16-M0-N1-C:J09-U11 2006-01-03-21.44.49.634008 R16-M0-N1-C:J09-U11 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 311 seconds
- 1136353489 2006.01.03 R11-M1-N1-C:J02-U11 2006-01-03-21.44.49.658061 R11-M1-N1-C:J02-U11 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 19 over 311 seconds
- 1136353489 2006.01.03 R11-M1-N1-C:J02-U11 2006-01-03-21.44.49.692336 R11-M1-N1-C:J02-U11 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 311 seconds
- 1136353491 2006.01.03 R07-M0-NC-I:J18-U01 2006-01-03-21.44.51.355472 R07-M0-NC-I:J18-U01 RAS KERNEL INFO ciod: generated 1 core files for program /g/g0/hommes/bgl/dd3d.v1.5.1.1/dd3d
- 1136353713 2006.01.03 R10-M0-N7-C:J17-U01 2006-01-03-21.48.33.696018 R10-M0-N7-C:J17-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 14 over 199 seconds
- 1136353713 2006.01.03 R10-M0-N7-C:J17-U01 2006-01-03-21.48.33.804788 R10-M0-N7-C:J17-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 199 seconds
- 1136353713 2006.01.03 R11-M1-N1-C:J02-U11 2006-01-03-21.48.33.838229 R11-M1-N1-C:J02-U11 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 19 over 199 seconds
- 1136353713 2006.01.03 R11-M1-N1-C:J02-U11 2006-01-03-21.48.33.860979 R11-M1-N1-C:J02-U11 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 199 seconds
- 1136353715 2006.01.03 R06-M0-N8-I:J18-U01 2006-01-03-21.48.35.537000 R06-M0-N8-I:J18-U01 RAS KERNEL INFO ciod: generated 4 core files for program /g/g0/hommes/bgl/dd3d.v1.5.1.1/dd3d
- 1136354112 2006.01.03 R30-M0-N7-C:J09-U01 2006-01-03-21.55.12.748683 R30-M0-N7-C:J09-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 26 over 44 seconds
- 1136354112 2006.01.03 R30-M0-N7-C:J09-U01 2006-01-03-21.55.12.911617 R30-M0-N7-C:J09-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 44 seconds
- 1136355991 2006.01.03 R30-M0-N7-C:J09-U01 2006-01-03-22.26.31.850290 R30-M0-N7-C:J09-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 26 over 1433 seconds
- 1136355991 2006.01.03 R30-M0-N7-C:J09-U01 2006-01-03-22.26.31.939688 R30-M0-N7-C:J09-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 1433 seconds
- 1136357856 2006.01.03 R30-M0-N7-C:J09-U01 2006-01-03-22.57.36.445161 R30-M0-N7-C:J09-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 26 over 1379 seconds
- 1136357856 2006.01.03 R30-M0-N7-C:J09-U01 2006-01-03-22.57.36.560272 R30-M0-N7-C:J09-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 1379 seconds
- 1136359842 2006.01.03 R30-M0-N7-C:J09-U01 2006-01-03-23.30.42.694714 R30-M0-N7-C:J09-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 26 over 570 seconds
- 1136359842 2006.01.03 R30-M0-N7-C:J09-U01 2006-01-03-23.30.42.866235 R30-M0-N7-C:J09-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 570 seconds
- 1136361180 2006.01.03 R30-M0-N7-C:J09-U01 2006-01-03-23.53.00.974027 R30-M0-N7-C:J09-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 26 over 1243 seconds
- 1136361181 2006.01.03 R30-M0-N7-C:J09-U01 2006-01-03-23.53.01.075070 R30-M0-N7-C:J09-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 1243 seconds
- 1136362361 2006.01.04 R66-M0-N0-C:J17-U11 2006-01-04-00.12.41.783700 R66-M0-N0-C:J17-U11 RAS KERNEL INFO instruction cache parity error corrected
- 1136362947 2006.01.04 R30-M0-N7-C:J09-U01 2006-01-04-00.22.27.730707 R30-M0-N7-C:J09-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 26 over 1111 seconds
- 1136362947 2006.01.04 R30-M0-N7-C:J09-U01 2006-01-04-00.22.27.835655 R30-M0-N7-C:J09-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 1111 seconds
- 1136364256 2006.01.04 R31-M0-N9-C:J02-U01 2006-01-04-00.44.16.569273 R31-M0-N9-C:J02-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 7 over 992 seconds
- 1136364256 2006.01.04 R31-M0-N9-C:J02-U01 2006-01-04-00.44.16.675438 R31-M0-N9-C:J02-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 992 seconds
- 1136364389 2006.01.04 R30-M0-N7-C:J09-U01 2006-01-04-00.46.29.136026 R30-M0-N7-C:J09-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 26 over 1138 seconds
- 1136364389 2006.01.04 R30-M0-N7-C:J09-U01 2006-01-04-00.46.29.242192 R30-M0-N7-C:J09-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 1138 seconds
- 1136366055 2006.01.04 R31-M0-N9-C:J02-U01 2006-01-04-01.14.15.302535 R31-M0-N9-C:J02-U01 RAS KERNEL INFO 1 ddr error(s) detected and corrected on rank 0, symbol 7 over 934 seconds
- 1136366055 2006.01.04 R31-M0-N9-C:J02-U01 2006-01-04-01.14.15.410091 R31-M0-N9-C:J02-U01 RAS KERNEL INFO total of 1 ddr error(s) detected and corrected over 934 seconds
- 1136366157 2006.01.04 R16-M1-N2-C:J04-U11 2006-01-04-01.15.57.297425 R16-M1-N2-C:J04-U11 RAS KERNEL INFO 1 torus processor sram reception error(s) (dcr 0x02fc) detected and corrected over
```

Extracted in batches each day

AIRNAV IRELAND

2. Log Parsing



08:03:18: DEPARTURE

08:47:02: ATC_FLIGHT_ATTRIBUTES_UPDATE

10:10:19: CHANGE_OF_FREQUENCY

10:13:59: AMAN_UPDATE

AIRNAV IRELAND

3. Log Partition and Feature Extraction

05:41:14: FILED_FLIGHT_PLAN_CREATION
05:59:24: FLIGHT_PLAN_SEARCH
05:59:30: FLIGHT_ATTRIBUTES_UPDATE
05:59:33: EXTERNAL_MESSAGE_SENDING
...
08:03:18: DEPARTURE
08:43:13: SSR_CODE_ASSIGNMENT
08:47:02: ATC_FLIGHT_ATTRIBUTES_UPDATE
08:47:03: MESSAGE_TRANSMISSION_REPORT
08:57:53: NOTIFICATION
09:02:49: TRAFFIC_LOAD_MONITORING
09:09:07: FLIGHT_ATTRIBUTES_UPDATE
09:09:07: EXTERNAL_MESSAGE_SENDING
09:42:07: INBOUND_COORDINATION_INITIATION
09:42:17: AREA_CONFLICT_DATABASE_STATUS
09:42:17: OUTBOUND_COORDINATION_INITIATION
...
10:05:58: APPROACH_CLEARANCE
10:06:03: AUTOMATIC_POSITION_REPORT
10:06:38: MESSAGE_TRANSMISSION_REPORT
10:10:19: CHANGE_OF_FREQUENCY
10:13:59: AMAN_UPDATE
...
10:33:09: TERMINATION
10:33:13: AREA_CONFLICT_DATABASE_STATUS
10:51:11: TIMEOUT_STATUS

AIRNAV IRELAND

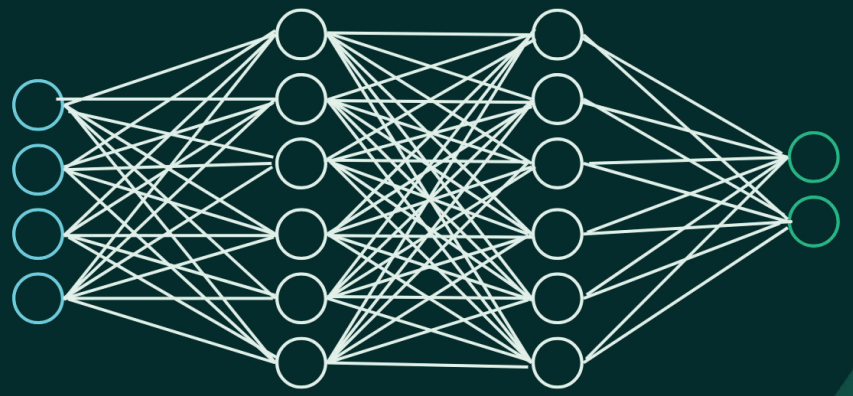
3. Log Partition and Feature Extraction

05:41:14: FILED_FLIGHT_PLAN_CREATION	27
05:59:24: FLIGHT_PLAN_SEARCH	34
05:59:30: FLIGHT_ATTRIBUTES_UPDATE	30
05:59:33: EXTERNAL_MESSAGE_SENDING	25
...	...
08:03:18: DEPARTURE	22
08:43:13: SSR_CODE_ASSIGNMENT	90
08:47:02: ATC_FLIGHT_ATTRIBUTES_UPDATE	12
08:47:03: MESSAGE_TRANSMISSION_REPORT	60
08:57:53: NOTIFICATION	64
09:02:49: TRAFFIC_LOAD_MONITORING	99
09:09:07: FLIGHT_ATTRIBUTES_UPDATE	30
09:09:07: EXTERNAL_MESSAGE_SENDING	25
09:42:07: INBOUND_COORDINATION_INITIATION	46
09:42:17: AREA_CONFLICT_DATABASE_STATUS	7
09:42:17: OUTBOUND_COORDINATION_INITIATION	10
...	...
10:05:58: APPROACH_CLEARANCE	68
10:06:03: AUTOMATIC_POSITION_REPORT	6
10:06:38: MESSAGE_TRANSMISSION_REPORT	13
10:10:19: CHANGE_OF_FREQUENCY	60
10:13:59: AMAN_UPDATE	16
...	...
10:33:09: TERMINATION	97
10:33:13: AREA_CONFLICT_DATABASE_STATUS	7
10:51:11: TIMEOUT_STATUS	98

AIRNAV IRELAND

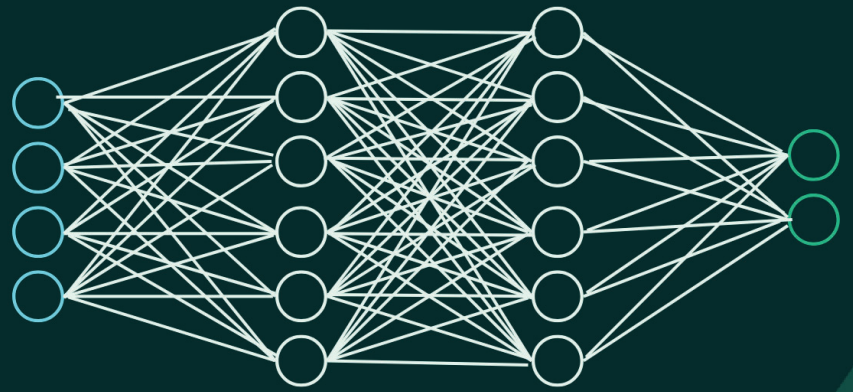
4. Anomaly Detection

27
34
30
25
...
22
90
12
60
64
99
30
25
46
7
10
...
68
6
13
60
16
...
97
7
98



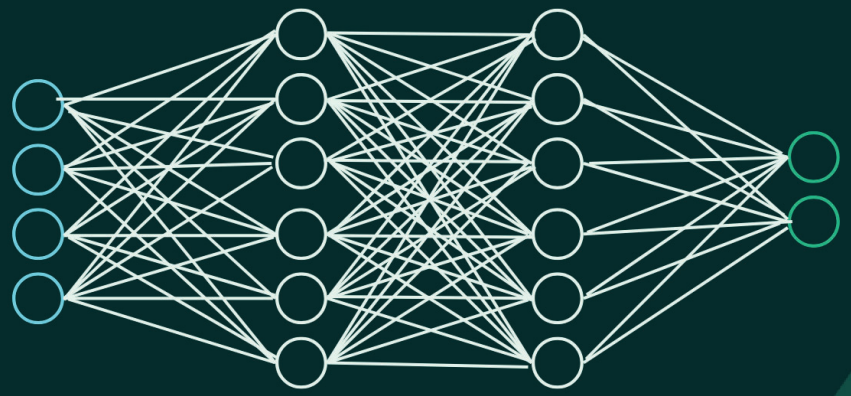
AIRNAV IRELAND

4. Anomaly Detection



AIRNAV IRELAND

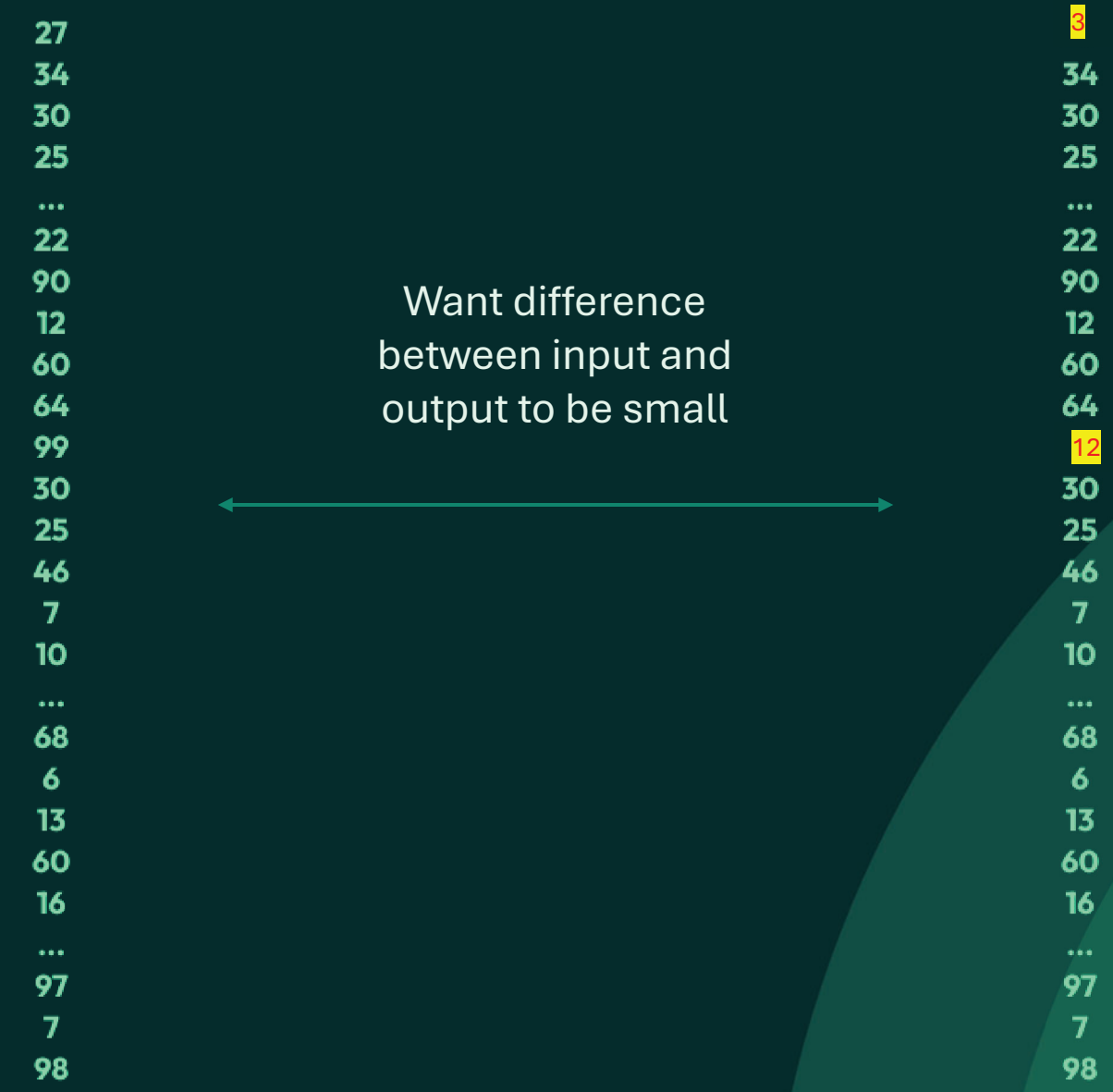
4. Anomaly Detection



3
34
30
25
...
22
90
12
60
64
12
30
25
46
7
10
...
68
6
13
60
16
...
97
7
98

AIRNAV IRELAND

4. Anomaly Detection



AIRNAV IRELAND

4. Anomaly Detection

27	3
34	34
30	30
25	25
...	...
22	22
90	90
12	12
60	60
64	64
99	12
30	30
25	25
46	46
7	7
10	10
...	...
68	68
6	6
13	13
60	60
16	16
...	...
97	97
7	7
98	98

If there is a big difference across multiple logs - it may suggest an anomaly

AIRNAV IRELAND

3. How has it been tested?

AIRNAV IRELAND

Test Cases

1. Generated Anomalies
2. Individual Anomalies
3. Systemic Anomalies

AIRNAV IRELAND

1: Generated Anomalies

Normal Test Set

+

Injected Anomalies (~10%)

AIRNAV IRELAND

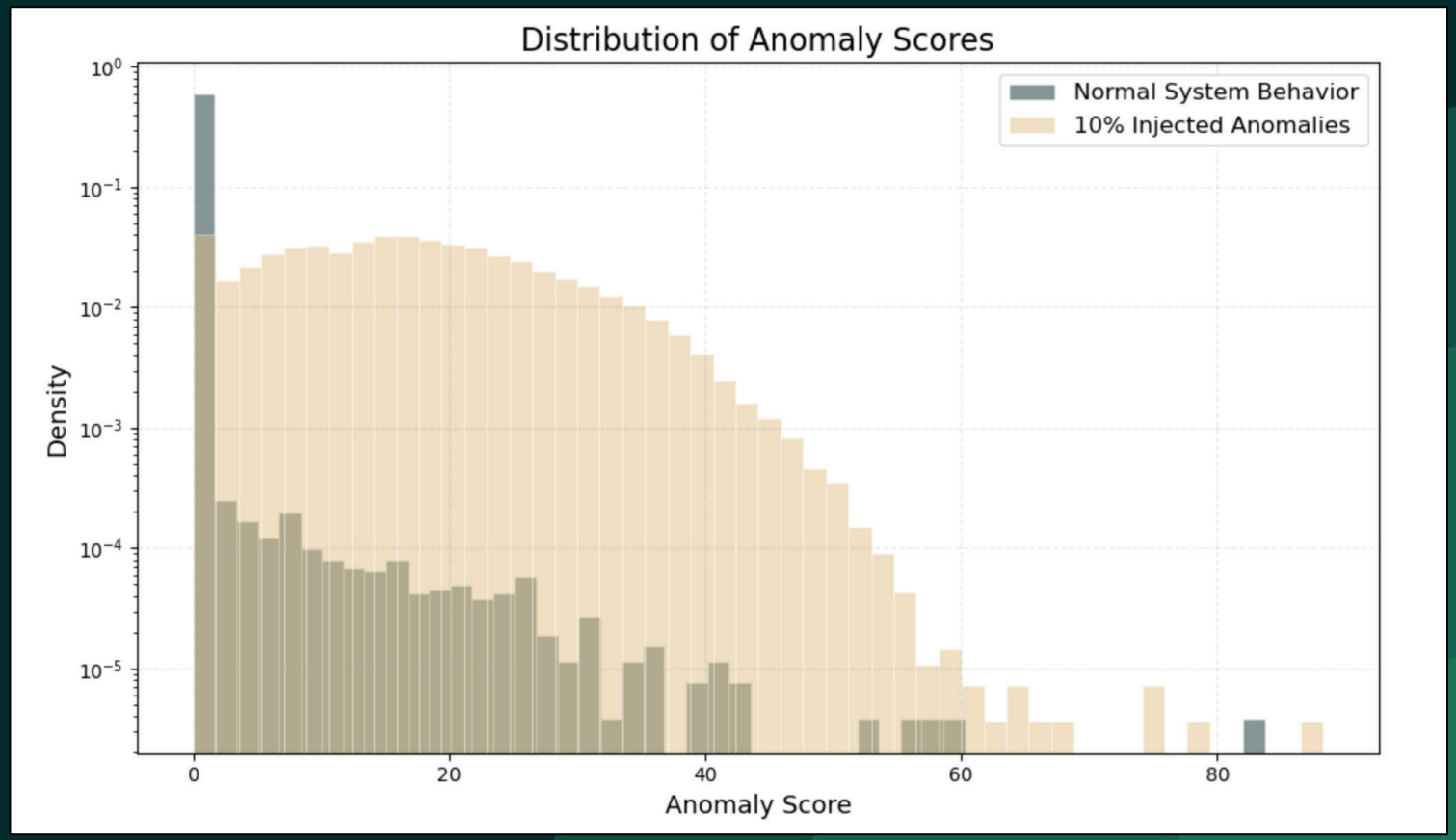
1: Generated Anomalies

Normal Test Set

Flagged 7,609 sequences as anomalies **(5%)**

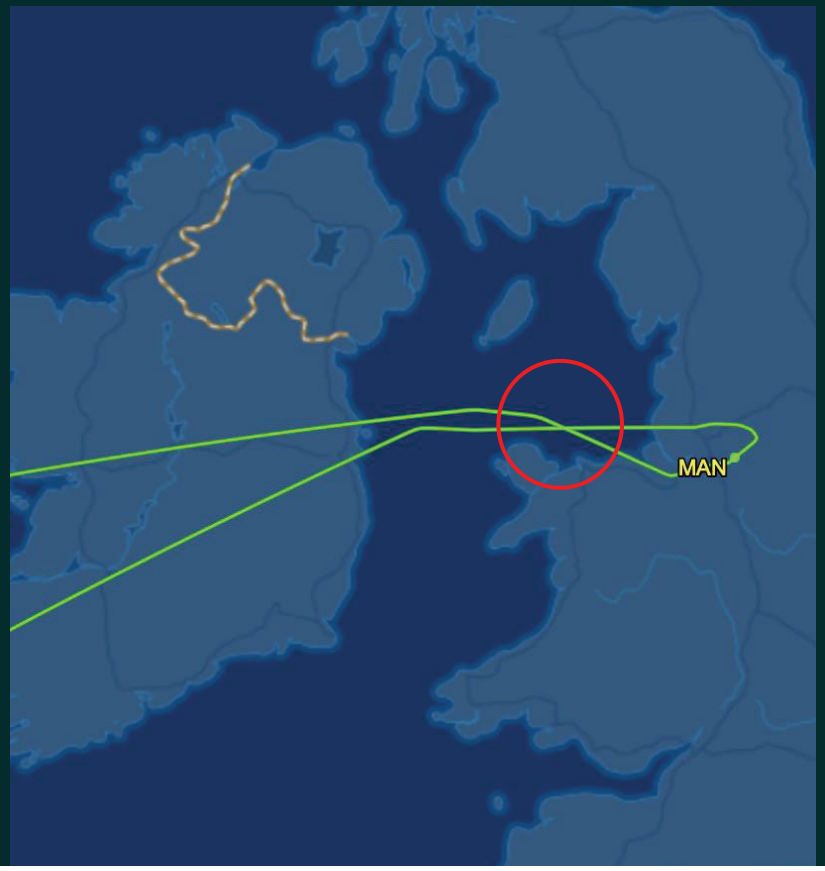
Injected Anomalies (~10%)

Flagged 156,645 sequences as anomalies **(99.97%)**



AIRNAV IRELAND

2: Individual Anomalies

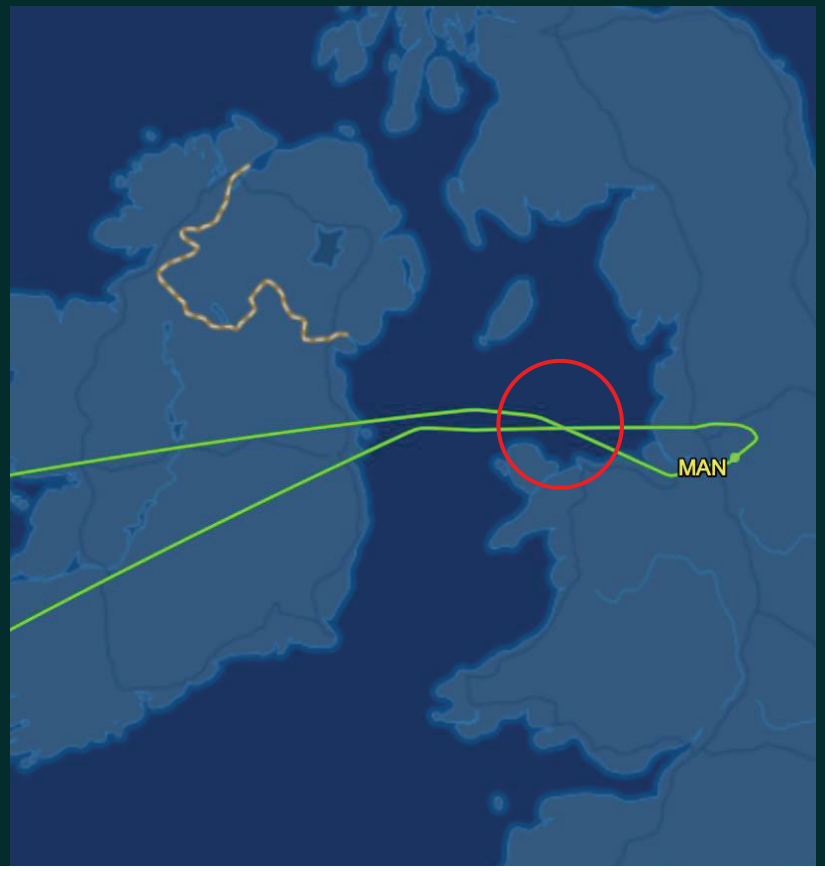


Rank 1: Seq index=1621, score=339.9786

	timestamp	token_id	event_name	nll
0	2025-03-26T09:12:28	47	FILED_FLIGHT_PLAN_CREATION	0.001284
1	2025-03-26T10:35:17	50	FLIGHT_ATTRIBUTES_UPDATE	0.000363
2	2025-03-26T10:35:17	45	EXTERNAL_MESSAGE_SENDING	0.002083
3	2025-03-26T10:35:17	84	MESSAGE_TRANSMISSION_REPORT	0.020233
4	2025-03-26T11:47:16	130	SSR_CODE_ASSIGNMENT	0.001055
5	2025-03-26T11:51:09	130	SSR_CODE_ASSIGNMENT	0.001102
6	2025-03-26T13:47:15	130	SSR_CODE_ASSIGNMENT	1.958709
7	2025-03-26T13:50:59	91	NOTIFICATION	0.166538
8	2025-03-26T13:59:24	35	CPDLC_LOGGED	0.365191
9	2025-03-26T14:56:58	69	INBOUND_NOTIFICATION	2.467011
10	2025-03-26T14:57:36	69	INBOUND_NOTIFICATION	1.010990
11	2025-03-26T14:57:57	21	AUTOMATIC_POSITION_REPORT	0.208507
12	2025-03-26T14:57:58	51	FLIGHT_CONFLICT_DATABASE_STATUS	0.592912
13	2025-03-26T14:59:37	21	AUTOMATIC_POSITION_REPORT	0.748035

AIRNAV IRELAND

2: Individual Anomalies



Rank 1: Seq index=1621, score=339.9786

	timestamp	token_id	event_name	nll
0	2025-03-26T09:12:28	47	FILED_FLIGHT_PLAN_CREATION	0.001284
1	2025-03-26T10:35:17	50	FLIGHT_ATTRIBUTES_UPDATE	0.000363
2	2025-03-26T10:35:17	45	EXTERNAL_MESSAGE_SENDING	0.002083
3	2025-03-26T10:35:17	84	MESSAGE_TRANSMISSION_REPORT	0.020233
4	2025-03-26T11:47:16	130	SSR_CODE_ASSIGNMENT	0.001055
5	2025-03-26T11:51:09	130	SSR_CODE_ASSIGNMENT	0.001102
6	2025-03-26T13:47:15	130	SSR_CODE_ASSIGNMENT	1.958709
7	2025-03-26T13:50:59	91	NOTIFICATION	0.166538
8	2025-03-26T13:59:24	35	CPDLC_LOGGED	0.365191
9	2025-03-26T14:56:58	69	INBOUND_NOTIFICATION	2.467011
10	2025-03-26T14:57:36	69	INBOUND_NOTIFICATION	1.010990
11	2025-03-26T14:57:57	21	AUTOMATIC_POSITION_REPORT	0.208507
12	2025-03-26T14:57:58	51	FLIGHT_CONFLICT_DATABASE_STATUS	0.592912
13	2025-03-26T14:59:37	21	AUTOMATIC_POSITION_REPORT	0.748035
43	2025-03-26T15:07:13	88	NEXT_DATA_AUTHORITY_SENDING_CLEARANCE	0.023101
44	2025-03-26T15:07:13	84	MESSAGE_TRANSMISSION_REPORT	4.465286
45	2025-03-26T15:07:13	28	CONTACT_REQUEST_SENDING_CLEARANCE	0.027929
46	2025-03-26T15:07:18	21	AUTOMATIC_POSITION_REPORT	0.036422
47	2025-03-26T15:07:18	21	AUTOMATIC_POSITION_REPORT	0.038133
48	2025-03-26T15:07:19	86	NEXT_AUTHORITY_NOTIFICATION	0.066941
49	2025-03-26T15:07:43	83	MESSAGE_LOGICAL_ACKNOWLEDGEMENT_TIMEOUT	3.369866
50	2025-03-26T15:08:23	51	FLIGHT_CONFLICT_DATABASE_STATUS	0.470909
133	2025-03-26T15:49:43	112	RESPONSIBILITY_ASSUMPTION	0.256783
134	2025-03-26T15:49:45	123	SECTOR_TRANSFER_INITIATION	0.320647
135	2025-03-26T15:49:51	80	MANUAL_TRANSFER	4.863237
136	2025-03-26T15:49:54	123	SECTOR_TRANSFER_INITIATION	6.325871
137	2025-03-26T15:49:54	123	SECTOR_TRANSFER_INITIATION	4.908521
138	2025-03-26T15:49:54	123	SECTOR_TRANSFER_INITIATION	3.170274
139	2025-03-26T15:49:57	112	RESPONSIBILITY_ASSUMPTION	3.881701
140	2025-03-26T15:49:58	123	SECTOR_TRANSFER_INITIATION	3.696013
141	2025-03-26T15:50:00	80	MANUAL_TRANSFER	0.537795
142	2025-03-26T15:50:07	80	MANUAL_TRANSFER	0.645526

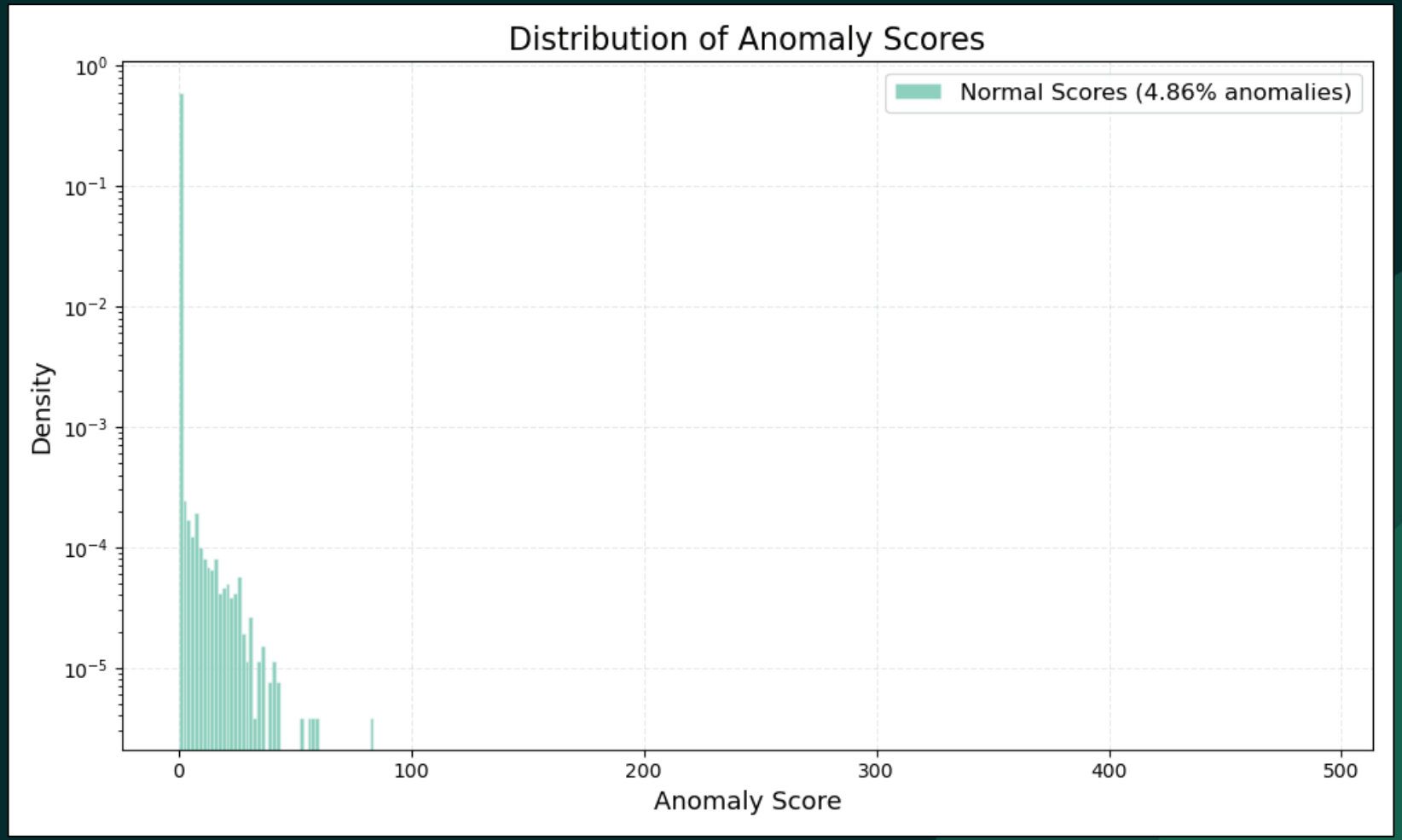
AIRNAV IRELAND

3: Systemic Anomalies

In July 2023, one of the FDP systems experienced a catastrophic failure due to a software bug.

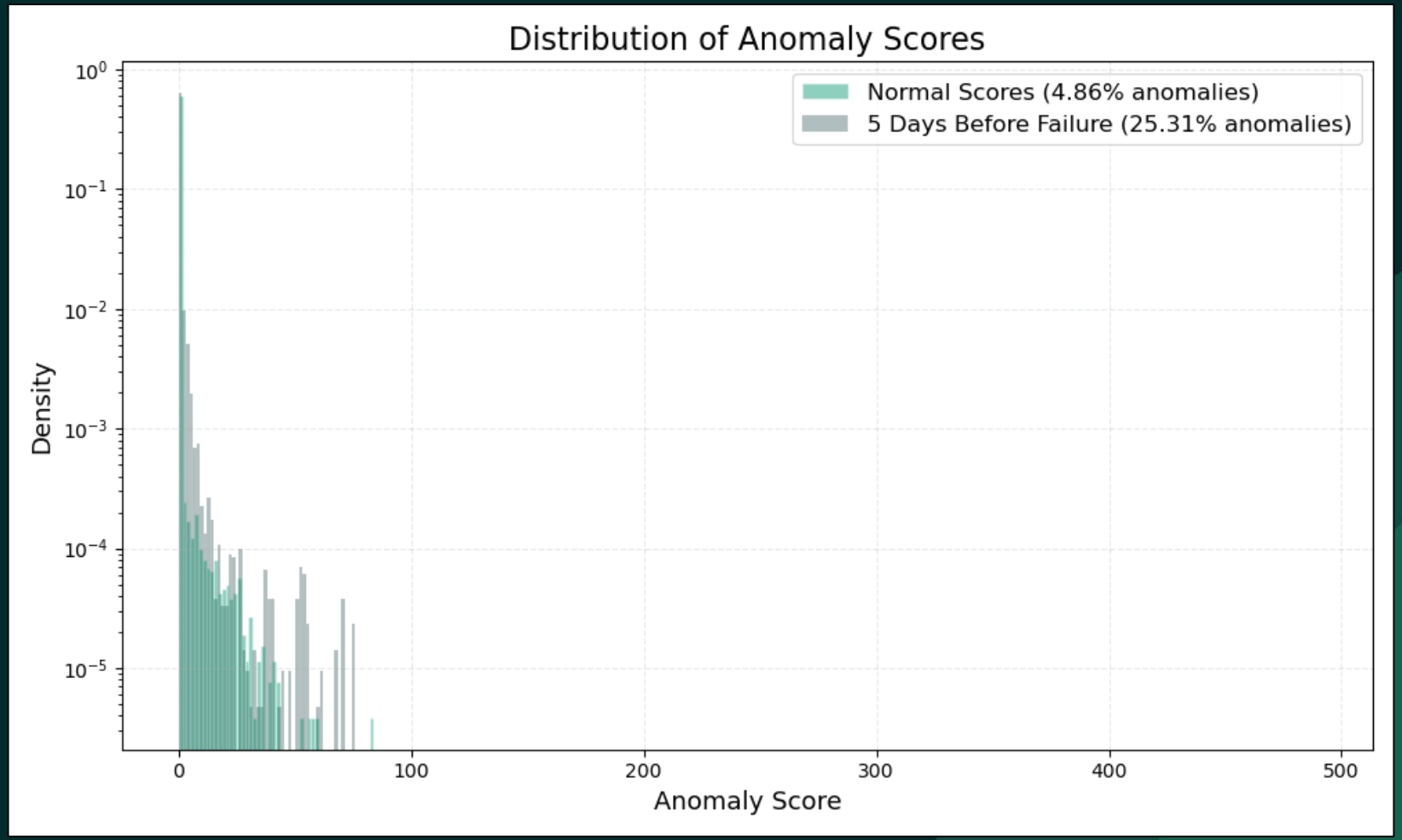
AIRNAV IRELAND

3: Systemic Anomalies



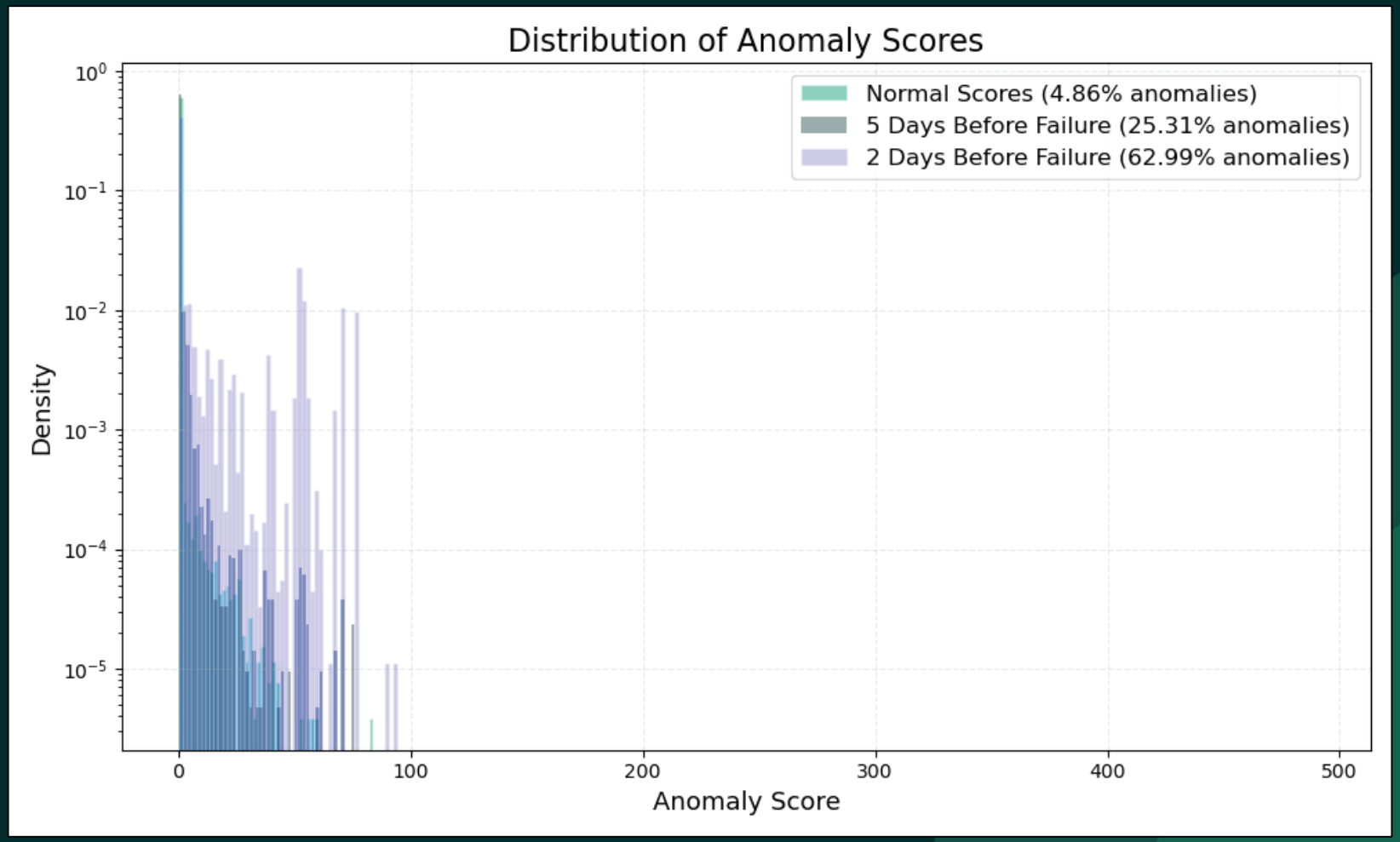
AIRNAV IRELAND

3: Systemic Anomalies



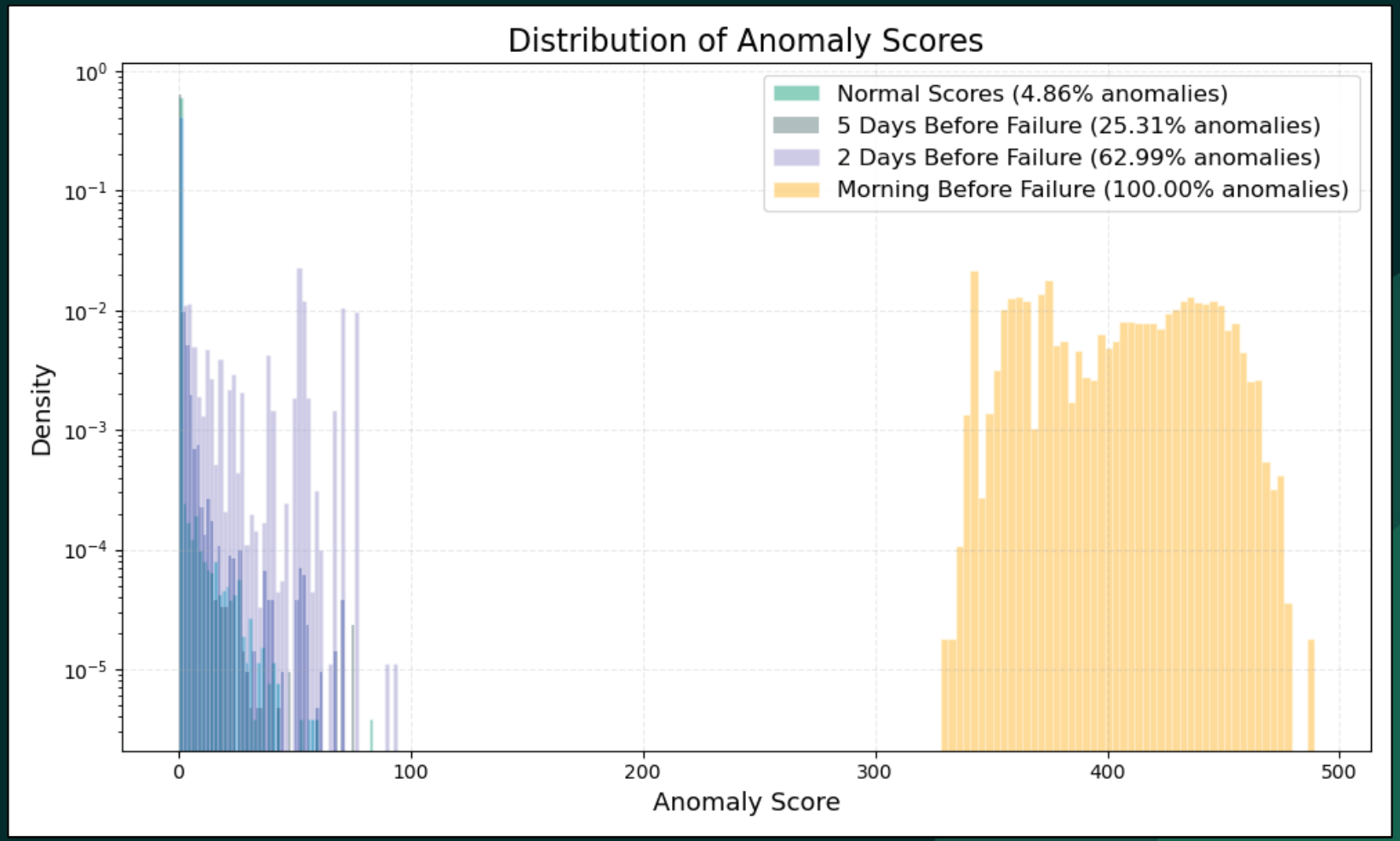
AIRNAV IRELAND

3: Systemic Anomalies



AIRNAV IRELAND

3: Systemic Anomalies



AIRNAV IRELAND

Use Cases

Detect anomalies in operational system (daily reports)

Test new software releases

AIRNAV IRELAND

Solution

```
081109 203807 222 INFO dfs.DataNode$PacketResponder: PacketResponder 0 for block blk_-6952295868487656571 terminating
081109 204005 35 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.73.220:50010 is added to blk_7128370237687728475 size 67108864
081109 204015 308 INFO dfs.DataNode$PacketResponder: PacketResponder 2 for block blk_8229193803249955061 terminating
081109 204106 329 INFO dfs.DataNode$PacketResponder: PacketResponder 2 for block blk_-6670958622368987959 terminating
081109 204132 26 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.43.115:50010 is added to blk_3050920587428079149 size 67108864
081109 204324 34 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.203.80:50010 is added to blk_7888946331804732825 size 67108864
081109 204453 34 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.250.11.85:50010 is added to blk_2377150260128098806 size 67108864
081109 204525 512 INFO dfs.DataNode$PacketResponder: PacketResponder 2 for block blk_572492839287299681 terminating
081109 204655 556 INFO dfs.DataNode$PacketResponder: Received block blk_3587508140051953248 of size 67108864 from /10.251.42.84
081109 204722 567 INFO dfs.DataNode$PacketResponder: Received block blk_5402003568334525940 of size 67108864 from /10.251.214.112
081109 204815 653 INFO dfs.DataNode$DataXceiver: Receiving block blk_5792489080791696128 src: /10.251.30.6:33145 dest: /10.251.30.6:50010
081109 204842 663 INFO dfs.DataNode$DataXceiver: Receiving block blk_1724757848743533110 src: /10.251.111.130:49851 dest: /10.251.111.130:50010
081109 204908 31 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.110.8:50010 is added to blk_8015913224713045110 size 67108864
081109 204925 673 INFO dfs.DataNode$DataXceiver: Receiving block blk_-5623176793330377570 src: /10.251.75.228:53725 dest: /10.251.75.228:50010
081109 205035 28 INFO dfs.FSNamesystem: BLOCK* NameSystem.allocateBlock: /user/root/rand/_temporary/_task_200811092030_0001_m_000590_0/part-00590. blk_-1727475099218615100
081109 205056 710 INFO dfs.DataNode$PacketResponder: PacketResponder 1 for block blk_5017373558217225674 terminating
081109 205157 752 INFO dfs.DataNode$PacketResponder: Received block blk_9212264480425680329 of size 67108864 from /10.251.123.1
081109 205315 29 INFO dfs.FSNamesystem: BLOCK* NameSystem.allocateBlock: /user/root/rand/_temporary/_task_200811092030_0001_m_000742_0/part-00742. blk_-7878121102358435702
081109 205409 28 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.111.130:50010 is added to blk_4568434182693165548 size 67108864
081109 205412 832 INFO dfs.DataNode$PacketResponder: Received block blk_-5704899712662113150 of size 67108864 from /10.251.91.229
081109 205632 28 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.74.79:50010 is added to blk_-4794867979917102672 size 67108864
081109 205739 29 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.38.197:50010 is added to blk_8763662564934652249 size 67108864
081109 205742 1001 INFO dfs.DataNode$PacketResponder: Received block blk_-5861636720645142679 of size 67108864 from /10.251.70.211
081109 205746 29 INFO dfs.FSNamesystem: BLOCK* NameSystem.addStoredBlock: blockMap updated: 10.251.74.134:50010 is added to blk_74538
```

AIRNAV IRELAND

Thank You

References

[1] Z. Chen, J. Liu, W. Gu, Y. Su, and M. R. Lyu, “Experience Report: Deep Learning-based System Log Analysis for Anomaly Detection,” Jan. 2022, arXiv:2107.05908 [cs]. [Online]. Available: http://arxiv.org/abs/2107.05908

[2] 3Blue1Brown, “Large Language Models explained briefly,” YouTube, Nov. 20, 2024. https://www.youtube.com/watch?v=LPZh9BOjkQs&list=PLZHQObOWTQDNU6R1_67000Dx_ZCJB-3pi&index=5 (accessed Jan. 18, 2025).

AIRNAV IRELAND

4. Anomaly Detection

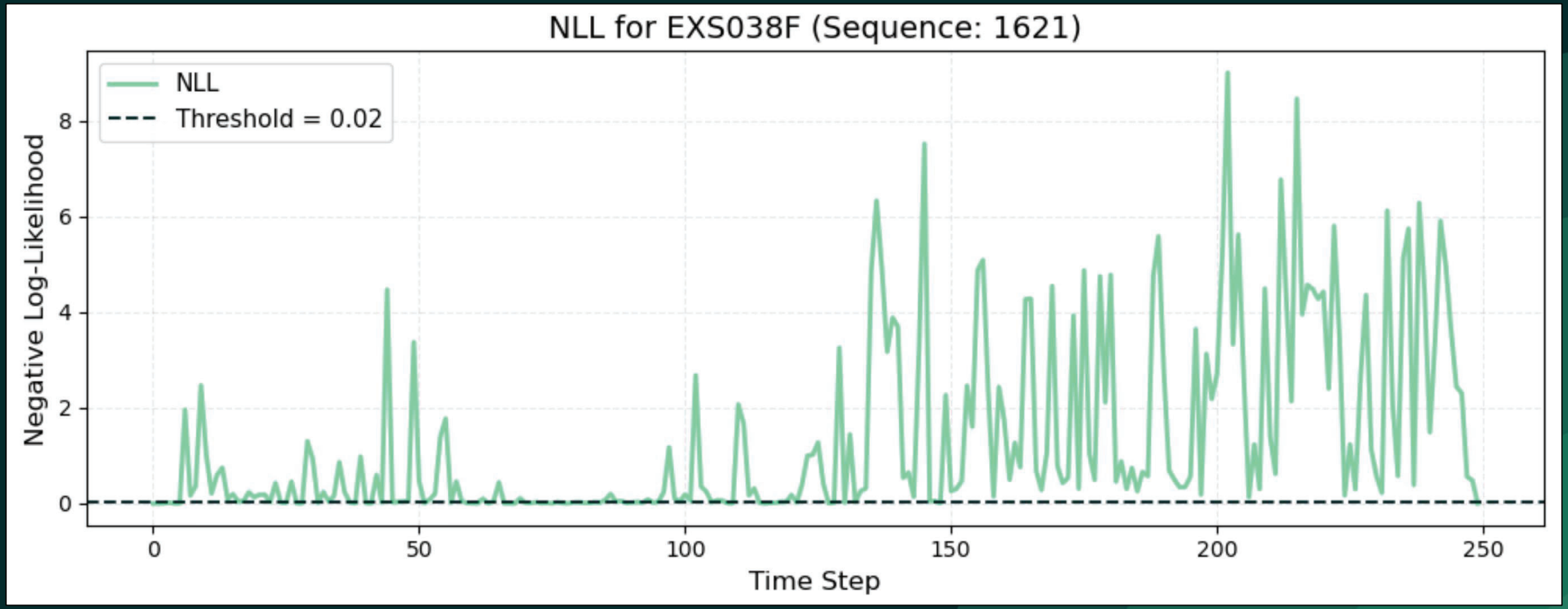
```
Step 7: current=91 -> true_next=35 (p=0.8466), nll=0.1665
   🔷 Top-3 predictions: ['35 (p=0.8466)', '45 (p=0.0178)', '75 (p=0.0129)']
```

```
Step 8: current=35 -> true_next=69 (p=0.6941), nll=0.3652
   🔷 Top-3 predictions: ['69 (p=0.6941)', '67 (p=0.0371)', '50 (p=0.0350)']
```

```
Step 9: current=69 -> true_next=69 (p=0.0848), nll=2.4670 ⚠ High NLL!
   🔷 Top-3 predictions: ['123 (p=0.7980)', '69 (p=0.0848)', '21 (p=0.0368)']
```

AIRNAV IRELAND

2: Individual Anomalies



AIRNAV IRELAND