ANATOMY OF A NO-EQUIPMENT-FAILED (NEF) ICNS SYSTEM MALFUNCTION:

THE CASE OF SINGAPORE AIRLINES SQ-327 RUNWAY EXCURSION

Lance Sherry, Center for Air Transportation Systems Research at George Mason University, Fairfax, Va.

Robert Mauro, Decision Research Inc., Eugene, Oregon

Abstract

Complex systems-of-systems are characterized by emergent behavior resulting from the interaction of behaviorally complex, distributed, autonomous sub-systems or agents. Although the individual sub-systems (e.g. Instrument Landing System, aircraft) are certified to high levels of reliability (e.g. 10-7), the interactions between the sub-systems is typically not explicitly, exhaustively, tested or certified. As a consequence, there can emerge scenarios in which a sub-system can find itself commanded into unsafe operating regimes without a failure of any sub-system or agent.

This paper describes a No Equipment Failed Malfunction (NEFM) analysis of the Singapore Airlines SQ-327 runway excursion that occurred November 3, 2011 at Munich airport. In the sequence of events of the incident, all the equipment operated as designed (i.e. no equipment failed) and the operators each performed according to their approved Standard Operating Procedures. The analysis highlights: (1) the need for comprehensive testing of the interaction between agents that can lead to scenarios resulting in rare hazardous outcomes, and (2) the vulnerability of designing human operators to monitor these complex system interactions and respond in a timely and appropriate manner. The need for comprehensive system-of-system sequential scenario testing, including exhaustive combinatorics using super computers, and the need for crowd-sourcing through voluntary reporting and safety management systems to address these issues is discussed.

1 INTRODUCTION

Complex systems are defined by the emergent behavior of the system that results from the interaction of behaviorally complex sub-systems or agents. In many cases, the sub-systems are geographically distributed and operate autonomously. Although the individual sub-systems may be tested and certified for high levels of reliability (e.g. 10-7), it is possible that the interaction between the sub-systems occurs in such a way that the emergent behavior allows the system to migrate into an unsafe operating regime. This may occur even when all of the sub-systems are behaving nominally and no equipment has failed.

In a review of the Three Mile Island nuclear power plant accident, organizational psychologist, Charles Perrow (1984) revolutionized the concepts of safety and risk for technologically advanced systems. He specifically identified the potential for systems composed of tightly coupled, behaviorally complex sub-systems to interact in such a way that could lead to hazardous outcomes without any equipment failures. Furthermore, he pointed out that adding technology to monitor system safety may simply add to the behavioral complexity of the system.

Perrow suggested that increasingly sophisticated systems would inevitably be prone to failures, however well they were managed. He posited that society might do better to contemplate a radical rethinking of the degrees of complexity that society should allow engineers to design.

On November 3, 2011, 34 years after the Three Mile Island Nuclear Power Plant accident and 27 years after Perrow published the book *Normal Accidents: Living with High-Risk Technologies,* Singapore Airlines SQ-327 experienced a runway excursion while landing on Runway 08R at Munich airport. An analysis of the accident described in this paper shows that none of the high reliability, autonomous, distributed, Integrated Communication Navigation Surveillance (ICNS) systems failed.

The incident scenario was initiated when two agents in the system-of-systems were legitimately operating under different "modes of operation" [1]. In this rare circumstance, the interaction between two systems (e.g. departing aircraft and Localizer) pushed a third system (i.e. arriving aircraft) into an unsafe operating regime. The human operators, tasked with supervision of the operations and monitoring for rare hazardous events, were unable to intervene in a timely manner – in part because they were inhibited by the behavior of the automation.

A system analysis was conducted using the No Equipment Failed Malfunction (NEFM) framework [2]. NEFMs are characterized by: (1) divergent sub-system/agents "modes of operations", (2) moded input devices, (3) semantically overloaded display graphic objects, (4) masked trajectories, (5) context sensitive control modes, and (6) human operator intervention performance within a limited available operational time window (AOTW).

The analysis of the SQ-327 runway excursion identified two main vulnerabilities of this ICNS system-of-systems: (1) divergent sub-system/agent "modes of operation." The synchronization of the distributed autonomous agents depends entirely on the harmonization of segregated "standard operating procedures." Because these procedures are not completely integrated, the system can easily devolve into non-synchronized operations, as it did in this event. (2) The safe operation of the system-of-systems depends on the ability of human operators to monitor the complex interactions between system components and respond in a timely and appropriate manner when anomalies occur in the presence of a moded input device and a short AOTW [3].

This analysis highlights the need for: (1) comprehensive testing of the interaction between agents that can lead to rare hazardous outcomes, and (2) the design of the procedures to account for available operational time windows for reasonable human intervention response times. This paper outlines three approaches to address these issues: (1) combinatorial evaluation of the states of system-of-systems, (2) crowd-sourcing of testing through voluntary reporting and safety management systems of revenue service operations, and (3) human performance simulation for procedures [3].

This paper is organized as follows: Section 2 provides an overview of the sub-systems and agents involved in Munich airport operations. Section 3 describes the incident scenario in a No-Equipment-Failed Malfunction (NEFM) framework. Section 4 discusses the results of the analysis. Section 5 provides a conclusion with implications of the analysis.

2 INTEGRATED COMMUNICATIONS, NAVIGATION, SURVEILLANCE (ICNS) SYSTEMS FOR AIRPORT OPERATIONS

The No Equipment Failed Malfunction (NEFM) Framework requires a list of sub-systems/agents and their properties, Section 2, and the interaction between the sub-systems/agents, Section 3.

Takeoff and Approach/Landing operations include the following systems and agents:

1. Runway
2. Weather
3. Instrument Landing System (including Localizer and Glideslope)
4. Air Traffic Control Operations and Procedures
5. Departing Aircraft
6. Arriving Aircraft (including Flight-crew, Automation, and Standard Operating Procedure)

2.1 Runway

The Munich airport has two parallel runways (08R/26L and 08L/26R). Each runway is 4,000 meters (13,120 ft) long and 60 meters (200 ft) wide. Runway 08R supports landings from the East and departures to the West. Runway 08R is equipped with an Instrument Landing System (ILS). The characteristics of the ILS for 08R is described in the next section. The current two-runway system operates at maximum capacity during peak hours such that requests for additional slots from airlines have been denied.

2.2 Weather

Up until 45 minutes before the incident, fog and low visibility (i.e. 2000' to 3000') prevailed at the airport. The visibility improved to 650' at the time of the incident. There was a slight easterly wind at 8 knots. Ceilings were 300' partially descending to 200' with a light mist. Temperature and dewpoint were 4 degrees C with barometric pressure at 1.011 hPa.

2.3 Instrument Landing System

Instrument Landing Systems (ILS) provide electronic signals from a ground location adjacent to the runway to the arriving aircraft. The signal provides vertical and horizontal guidance to arriving aircraft to allow the aircraft to locate and land on the runway in poor visibility conditions.

The ILS has two component functions: a glideslope to guide the aircraft on a 3 degree descent to the runway, and a localizer to guide the aircraft on the runway center-line. The localizer guides the aircraft to the runway and also provides guidance during the rollout once the aircraft has landed. Roll-out guidance is only available if the equipment and runways are certified for all-weather operations in accordance with CAT III operations (see below). Roll-out guidance was available at Munich. The signal is decoded on the flight deck and displayed on a Course Deviation Indicator (see Figure 1). The ILS signal typically can extend up to 6 nautical miles from the runway and 3000' Above Ground Level (AGL).

Localizer

The localizer is composed of a signal generator and a set of antennas that broadcast a signal down the runway, providing left/right guidance to the line the aircraft up with the runway center-line. The Localizer antenna is located at the far end of the runway (see Figure 1). The antenna array consists of a row of dipole antennas which are located at right angles and symmetrically to the runway. In general, the antennas are located about 300 m to 400 m beyond the end of the runway**.**

Munich Runway 08R was equipped with an ILS certified for Cat I/II/III operations. The localizer antennas for runway 08R were moved from 350 m to 1,000 m beyond the runway threshold to prevent localizer interferences through reflections off departing Airbus A380 flights (see Figure 2). The position change of the LOC antenna required modification of the ILS operation. The broadcast antenna diagram had to be pooled better by about 3.6° to ensure the required accuracy for CAT II and CAT III approaches which required an increase in energy supply by approximately 0.1 W.

The change in the position of the Localizer antenna at Munich affected the separation requirements for approaching and departing aircraft. To prevent signal interference caused by departing aircraft passing through the ILS signals, the separation between departing and approaching aircraft had to be increased for Category II/III approaches.

ILS Signal Disturbances and Airport ILS Critical/Sensitive Areas

The electromagnetic waves of the Localizer

Figure 1: Localizer antenna at runway end (left) and Course Deviation Indicator in cockpit (right).

propagate in a straight line. These signals can be disturbed by metallic surfaces which exhibit electromagnetic characteristics. Sources of interference include: buildings such as terminals, hangars, antenna support and masts, aircraft and other vehicles on the ground, and aircraft flying ahead in the area of the approach path or above the approach path. The disturbances can change the direction of the wave (i.e. Refraction), bend the waves (i.e. Diffraction), or diffuse and propagate the wave in different directions (i.e. Diffusion and Reflection).

To avoid interference with the ILS signals, airports have designated ILS Critical and Sensitive Areas. In these areas, the presence of vehicles and aircraft is restricted during instrument landing operations to prevent the disturbances to the ILS signals guiding approaching aircraft.

One of the main sources of disturbance is the result of aircraft taking off and overflying the localizer.

ILS Signal Monitoring in the Cockpit

It is essential that any failure of the ILS to provide safe guidance be detected immediately by the pilot. The autopilot flight director system can detect ILS signal interferences. When signal interference is detected, the autopilot disregards the ILS signals and switches in the attitude stabilizing mode which is based on data from the on-board inertial navigation system. A failure indication ('failure flag') is also displayed on the instruments of aircraft using the ILS.

However, brief interferences with ILS signals occur relatively frequently. These generally only last for short periods of time (i.e. < 10 seconds) and so no error is indicated. If the interferences last longer the flight director mode is downgraded e.g. from LAND3 (i.e. Cat III) to LAND2 (iI.e. Cat II).

SQ-327 monitoring did not indicate any disturbance.

ILS Signal Monitoring at the Airport

Disturbances in the ILS signal are also monitored on the surface of the airport. If any deviation beyond strict limits is detected, either the ILS is automatically switched off or the navigation and identification components are removed from the carrier. In either case, the result is the same. Aircraft using the ILS detect the failure as described above.

Antenna, receiver, and signal analysis algorithms are located in the transmission zone of the Localizer signal. A Near Field Monitor is located some 10 m ahead of the localizer antennas. A Far Field Monitor is located in the approach flight path. The near field monitor monitors the localizer signal to detect possible corruption due to dysfunctional system components. The far field monitor monitors the localizer signal to detect possible corruption coming from the area of the runway and its surroundings, e. g. signal reflections. The far field monitor is mandatory for the all-weather operations CAT II and CAT III. An "Integral Monitor" evaluates the signal information on disturbances detected by the near field and the far field monitors and either shuts down the system or switches to the back-up transmitter.

With the increasing categories, ILS equipment is required to shut down faster since higher categories require shorter response times. For example, a Cat I localizer must shutdown within 10 seconds of detecting a fault, but a Cat III localizer must shut down in less than 2 seconds.

Munich Runway 08R ILS monitoring did not identify any ILS signal disturbance related to the approach and landing of SQ-327.

2.4 Air Traffic Control Operations and Procedures

The Departure and Approach Controller(s) are responsible for the sequencing and separation of departing and arriving flights. The separation is determined by the category of operations for the ILS which is determined by the weather operating conditions of the airport.

ILS Categories of Operations

ILS can be used for three Categories of operation. One difference between the ILS Categories is the height Above Ground Level (AGL) at which the Localizer signal is no longer directly used by the flight crew and flight deck automation to control the flight path.

Category I operations bring the aircraft below 300 feet AGL on the ILS signal. Prior to 200 ft above touchdown zone elevation (i.e. decision

height) the flight crew must have visual sighting of the runway. The Pilot in Command (PIC) flies the aircraft with manual stick & rudder commands the remainder of the way to the landing. To perform a Cat I approach, there must be either a visibility not less than 2,625 feet (800 m) or a runway visual range not less than 1,800 feet (550 m).

Category II operations allow for visual sighting of the runway lower than 200 feet above touchdown zone elevation but not lower than 100 feet, and a runway visual range not less than 1,150 feet (350 m). The aircraft is flown manually by the PIC for the landing.

Category III operations allow for the use of automation through the landing. There are three levels of Category III. Cat IIIA - allows for a precision instrument approach and landing with a decision height lower than 100 feet above touchdown zone elevation, or no decision height; and a runway visual range not less than 655 feet. Cat IIIB - allows for a precision instrument approach and landing with a) a decision height lower than 50 feet above touchdown zone elevation, or no decision height; and a runway visual range less than 2,625 feet but not less than 165 feet. CatIIIc - allows for a precision instrument approach and landing with no decision height and no runway visual range limitations. A Category III C system is capable of using the aircraft's autopilot to land the aircraft and can also provide guidance along the runway surface.

In each case, a suitably equipped aircraft and appropriately qualified crew are required. For example, Cat IIIc requires a fail-operational system, along with a Landing Pilot (LP) who holds a Cat IIIc endorsement in their logbook. Cat I does not require an endorsement. Cat I relies only on altimeter indications for decision height, whereas Cat II and Cat III approaches use radar altimeter to determine decision height.

Munich Runway 08R was equipped to operate under all three categories of operation. SQ—327 was equipped for all three Categories of ILS. The Captain on SQ-327 had the endorsement for a Cat III approach.

Departure and Arrival Separation Requirements

The separation is determined by the category of operations. For example, when Category II/III approaches are in effect for arriving aircraft, additional time is required between departures and arrivals to ensure that the departing aircraft do not interfere (i.e. block) the Localizer signal generated by antennae located at the end of the departure runway. Also departure queues and taxi-ing aircraft must be kept clear of the ILS Critical and Sensitive Areas.

For Cat I landing, the separation between departing and arriving aircraft can be reduced because the arriving aircraft are flying with visual sighting of the runway below 200 ft and are not reliant on the Localizer signal.

The change of the position of the Localizer antenna for runway 08R affected the separation of approaching and departing aircraft. To prevent interference with the ILS signal, separation was increased for Category II/III approaches to ensure that the departing aircraft would be above or beyond the antennae when approaching aircraft were nearing the surface.

The pilot is not required to ask for clearance to conduct an approach for Cat II and Cat III when the appropriate weather conditions apply.

2.5 Departing Aircraft

The departing aircraft follows ATC instructions. The time period in which the departing aircraft interferes with the Localizer signal is determined by location and timing of the clearance into the ILS Critical and Sensitive Areas, location and timing of the takeoff roll, takeoff roll acceleration, rotate speed and climb rate.

2.6 Arriving Aircraft Airline Cockpit Operations and Procedures

The arriving aircraft follows ATC instructions. The time period in which the arriving aircraft is subject to Localizer interference is determined by location and timing of the clearance for the approach, approach speed, rate of descent, flare and touchdown. Also critical is the decision on the category of approach to execute.

Choice of Category of Approach

To maintain proficiency, flight crews will frequently perform CAT II/III autoland landings under CAT I conditions. Singapore Airlines B777

SOPs authorize Cat III under CAT I conditions with the following restrictions:

"Flight crews must remember that the ILS critical areas are not protected when the weather is above 800 foot ceiling and/or 2 mile visibility. As a

Table 1: No Equipment Failed Malfunction (NEFM) Sequence of Events

No Equipment Failed (NEF) Accident Scenario			
Analysis Framework		**Events**	**Description**
Operational Context		1, 2a, 2b, 3a, 3b, 4a, 4b, 5	Airport operating CAT III up to 45 minutes before event. Departure delays create need to get departures out. Ceiling increased to 300' AGL 45 minutes before. ATC operating airport at CAT I. Arriving aircraft operating CAT III landing. • Arriving aircraft provided weather data • Arriving aircraft provided clearance for Approach • Arriving aircraft cleared to Land • Departing aircraft provided departure clearance • Departing aircraft provided departure clearance
Triggering Event	**Sensor Discrepancy/ Pilot Entries**	6, 7, 8	Localizer signal disrupted by departing aircraft
	Effect on Automation	9	Autoland remains engaged
	Inappropriate Command	9	Autoland commands left bank at 50'-30' AGL
	Trajectory into Unsafe Operating Regime	10, 11	Aircraft no longer lined-up on center-line
Pilot Intervention #1	**Sensor Discrepancy/ Pilot Entries**	12	Localizer signal disrupted Wheels-on Pilot selects TOGA Switch to initiate Go Around
	Effect on Automation	13, 14	Autopilot remains engaged Autopilot switches to Roll-out Mode
	Inappropriate Command	15	Autopilot commands roll-out based on disrupted Localizer signal
	Trajectory into Unsafe Operating Regime	16	Aircraft rolls-out out left of runway
Pilot Intervention #2	**Sensor Discrepancy/ Pilot Entries**	17	Pilots apply rudder pedal pressure to steer aircraft back on to runway Localizer signal disrupted
	Effect on Automation	18	Autopilot remains engaged Autopilot Roll-out Mode remains engaged
	Inappropriate Command	19	Autopilot Commands roll-out based on disrupted Localizer signal and over-rides pilot rudder pedal commands
	Trajectory into Unsafe Operating Regime	20	Aircraft continues to roll-out out left of runway
Pilot Intervention #3	**Sensor Discrepancy/ Pilot Entries**	21	Pilots increase rudder pedal pressure to steer aircraft back on to runway exceeding pressure required to disengage autopilot. Localizer signal remains disrupted
	Effect on Automation	22	Autopilot dis-engaged Autopilot Roll-out Mode remains engaged
	Inappropriate Command	23	Pilot rudder pedal commands take effect
	Trajectory into Unsafe Operating Regime	24	Aircraft swings across runway and comes to stop on right side of runway

result, ILS beam bends may occur because of vehicle or aircraft interference. *Sudden and unexpected flight control movements may occur at a very low altitude or during the landing and rollout when the autopilot attempts to follow the beam bends*." (BFU, 2018, Section 1.17.2.1).

"At ILS facilities where critical areas are not protected, flight crews should be alert for this possibility and guard the flight controls (control wheel, rudder pedals and thrust levers) throughout automatic approaches and landings. *Be prepared to disengage the autopilot and manually land or go-around*."

"The Autopilot Flight Director System (AFDS) includes a monitor to detect significant ILS signal interference. If localizer or glideslope signal interference is detected by the monitor, the autopilot disregards erroneous ILS signals and remains engaged in an attitude stabilizing mode based on inertial data. Most ILS signal interferences last only a short period of time, in which case there is no annunciation to the flight crew other than erratic movement of the ILS raw data during the time the interference is present. No immediate crew action is required unless erratic or inappropriate autopilot activity is observed."

Under international regulations, it is at the discretion the flight crew to communicate to Air Traffic Control the intention to land under Cat II/III under Cat I conditions.

3 ANALYSIS OF THE SQ-327 RUNWAY EXCURSION

This analysis is based on the description of the incident from the Bundesstelle für Flugunfalluntersuchung/German Federal Bureau of Aircraft Accident Investigation BFU EX010-11 [1]. The NEFM sequence of events is summarized in Table 1.

Background

On November 3 2011, flight SQ-327 was enroute from Manchester, England to Munich, Germany. The flight had 147 passengers, 13 flight attendants and 2 pilots on board. The first-officer (35, ATPL, 3,681 hours total, 3,681 hours on type) was initially the Pilot in Command (PIC) during the flight from Manchester to Munich. To meet criteria for the approach, the Captain (45, ATPL, 12,416 hours total, 4,712 hours on type) became the PIC, the first officer became the Pilot Monitoring (PM). The Captain was an instructor pilot.

Both the Captain and the First Officer had enough flying experience on type, to be sufficiently familiar with the go-around procedure. These procedures were sufficiently described in the Flight Crew Training Manual (FCTM) and had been trained sufficiently in the simulator in accordance with effective regulations.

The incident occurred at Munich Airport (EDDM) at about 12:10L (11:10Z).

Sequence of Events

The NEFM sequence of events is summarized in Table 1. Under a specific operational context, there was a triggering event, followed by a sequence of three attempted flight crew interventions.

Operational Context

(1) Weather information at Munich, visibility 2,000 m, cloud base 300 ft at the time of the incident.

Prior to the incident, until 0920 UTC, Munich airport experienced fog and visibilities between 600 and 900 m. After 0940 UTC, visibility improved slowly to 2,000 m at the time of the landing. Prior to landing, the crew had received two aviation routine weather reports (METAR) via the Air Traffic Information Service (ATIS) at Munich. Information W of 1030 UTC and Information X of 1050 UTC: Light and variable wind from the East at 8 knots; visibility 2 km with light mist. Cloud base at 300 ft, partially descending to 200 ft. Temperature and dewpoint 4°C. Barometric air pressure 1,011 hPa. No significant weather changes expected.

(2a) At a visibility of 2 km and a cloud base of 300 ft, ATC was performing CAT I operations.

The visibility and cloud bases for the approach met the criteria for CAT I operations for 45 minutes prior to the incident. As a result, the controller

sought to reduce the departure delays that had accrued from the all-weather operations in the morning (CAT II/III) by rapidly allowing aircraft to depart. The controller was working on the edge of the separation minimum so that aircraft waiting to depart could do so quickly and traffic situation would become normal.

Although, the increased separation minima which are required for CAT II/III did not have to be applied, the "provision phase" for CAT II/III was still active and the departing aircraft and other traffic were held away from critical and sensitive zones for CAT II/III ILS operations. For this reason, it would have been possible with relatively little effort to change from CAT II/III to CAT I operations with the aircraft waiting for departure still stopped at the CAT II/III holding points.

(2b) In accordance with the airline Standard Operating Procedures (SOP), the Captain decided to use his approved discretion to conduct an automatic approach and Autoland.

According to the airline's SOP, based on the weather information from Munich, the Captain assumed the role of Pilot Flying (PF) and the co-pilot became Pilot Monitoring (PM).

At 1152:13 hrs, during descent to Flight Level (FL) 110, the crew contacted Munich approach control for the first time. The crew did not acknowledge receiving the valid ATIS Information X of 1150 hrs (1050 UTC). The crew received several instructions, such as heading and rate of descent, from the controller. At 1158:19 hrs the crew was advised to call Munich Director on frequency 118.825 MHz.

The crew did not inform the controller of the intended Autoland landing. Neither the FTSM nor the FCTM clearly required that ATC be notified.

(3a/b) The ICNS system was now operating in a non-synchronized configuration.

Air Traffic Control was conducting operations according to CAT I under the assumption that the arriving aircraft would be flown manually under VFR conditions below 200' AGL. The assumption was that any interference from departing aircraft on the ILS signal would have no impact on the flight path of arriving aircraft, because as the aircraft neared the runway they would be navigating visually.

However, SQ-327 was conducting operations according to CAT III. The flight crew was monitoring the approach and prepared to intervene to perform a Go Around. The assumption was that there would be sufficient time to identify the need to abort the landing, and initiate a Go Around should the need arise.

(4a) ATC cleared a BAE 146 Avro (Jumbolino) for takeoff. To expedite the departure, the aircraft was cleared to takeoff from the taxiway B4 intersection. As a consequence, the departing flight cleared the Localizer antenna at a lower altitude than it would have if it had been cleared from the runway threshold.

The separation between the landing and departing airplanes corresponded with the requirements for CAT I operations.

Because the localizer antenna for 08R had been moved from 350 m to 1,000 m beyond the runway threshold for 26L, a larger separation between arriving and departing aircraft was required to avoid interference with the ILS signal when all-weather operations under CAT II/III are in

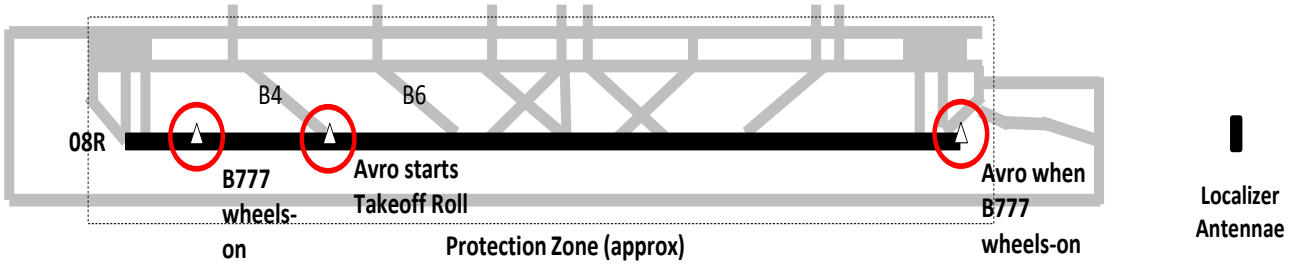

Figure 2: Location of Avro in front of the Localizer when the B777 touched down (BFU, 2019)

service. The larger distance of the localizer antenna to the runway required a stronger pooling of the signal which resulted in an increased energy supply (about 0.1 W) which increased the susceptibility to dysfunction slightly. These effects were taken into account when the antenna had been moved and the respective protection areas extended.

(4b) ATC cleared the SQ-327 for approach and then for landing. ATC assumed that the aircraft was performing Cat I operations.

At 1158:42 hrs the crew of SQ-327 contacted Munich ATC Director and received heading and descent instructions for the Instrument Landing System (ILS) approach to runway 08R.

At 1200:43 hrs the crew received the approach clearance to runway 08R "[…] descend 5,000 feet cleared ILS zero eight." At 1203:23 hrs the crew was instructed to reduce speed to 170 kt and contact Munich Tower on 120.500 MHz.

At 1204:37 hrs the crew contacted Munich Tower. At 1208:47 hrs the crew received the latest wind information and was cleared to land: "[…] one three zero degrees, seven knots runway zero eight right, cleared to land".

(5a) When the BAE 146-RJ85 received its take-off clearance from the intersection with taxiway B4, the B777 was about 2.9 NM from the runway 08R threshold and 3.4 NM behind the BAE 146-RJ85.When the Boeing 777-300 was about 2.1nm from touchdown, the BAe 146-RJ85 began its takeoff run. When the Boeing 777-300 crossed the runway threshold, the Jumbolino was climbing out still short of the runway end (Figure 2).

(6) As the B777 flew above the runway 08R threshold, the BAE 146-RJ85 was in front of the localizer antenna and interfered with the localizer signal. The BAE 146-RJ85 was significantly lower in front of the localizer antenna compared to other airplanes having taken off earlier due to having taken off from the taxiway B4 intersection and its lower climb rate. This resulted in a significantly greater localizer interference.

(7) The flight data recorder on SQ-327 showed that all three ILS receivers recorded localizer signal deviations in both directions. All three receiver antennas on the airplane received identical signals from the localizer on the ground so that no malfunction was indicated.

(8) No monitoring systems identified a signal error. Neither the near nor the far field monitor recorded a dysfunction of the ILS due to the short duration of the interference.

(9) The B777 followed the disturbed localizer signal with engaged autopilot.

(10) The airplane dipped the left wing shortly before touch-down and was no longer aligned with the runway center-line.

(11) The airplane touched down with the left landing gear approximately 420 m beyond the runway threshold at 132 knots with a bank angle of 3.5°. The aircraft veered to the left and about 7

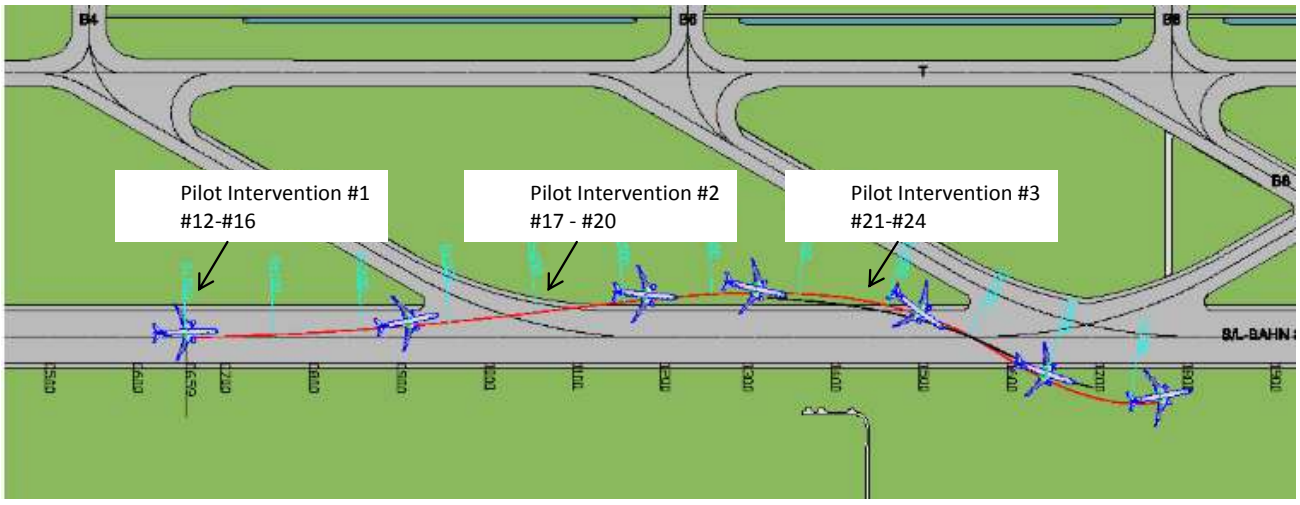

Figure 3: Three pilot interventions during roll-out

seconds later veered off the runway to the left.

Pilot Intervention #1: Go Around

(12) With the aircraft in the Flare, the PIC decided to abort the approach and perform a Go Around. He called out: "Okay, flaps twenty" and pushed the TOGA (Takeoff and Go Around) Switch to initiate an automated Go Around. In anticipation of the automated Go Around, he then retracted the spoilers, which had been automatically deployed at the touchdown (Figure 3).

(13) The flight data recorder showed that the ground spoilers extended about 2 seconds prior to the autopilot changing to ROLL-OUT and retracted 10 seconds later. The extension was command by the automation for the Cat III autoland. The retraction was the manual intervention by the PIC.

(14) However, the TOGA switch and the associated autopilot Go-Around mode were deactivated according to the logic programmed in the autopilot by the initial ground contact (i.e. weight-on-wheels).

(15) The Autopilot did not command a Go Around, instead the Autopilot continued to follow the Localizer signal commanding a track to the left of the runway. The aircraft moved toward the left runway edge and veered off the runway with a speed of 123 kt (KIAS) about 944 m beyond the threshold in the area of taxiway B4.

(16) The airplane rolled through the grass north of runway 08R.

Pilot Intervention #2: Manually Steer aircraft on to Runway

(17) At this point, the PIC decided against a manual go-around procedure. Instead, the PIC started to use the rudder pedals and nose wheel steering to try to bring the aircraft back onto the runway (Figure 3).

(18) The autopilot was not disconnected at this time because the PIC had been prepared for an automatic go-around.

(19) Because the Autopilot remained engaged, manual rudder commands by the PIC were over-ridden by the Autopilot ground roll-out mode.

(20) For about 400 m, the airplane rolled through the grass north of runway 08R in a slightly curved right hand turn. The largest lateral deviation from the runway was reached at about 1,242 m beyond the threshold; speed was 109 kt KIAS.

Pilot Intervention #3: Manually Steer aircraft on to Runway

(21) PIC and PM apply rudder pedals and nose wheel steering to bring aircraft back onto runway (Figure 3).

(22) Manual force applied to rudder pedals causes Autopilot disconnect.

(23) Due to the sudden disconnection of the autopilot and the rudder full deflection induced by the pilots, the airplane turned back around the yaw axis by about 40° to the right, re-entered the runway close to the intersection with taxiway B6, about 1,566 m beyond the threshold.

(24) The airplane crossed the runway at about 45° to the approach direction at 71 knots and came to rest at the right side of the runway in the grass south of and parallel to runway 08R. Because of the gravel runway shoulder area and the long dry weather, the airplane did not sink in very far and remained almost undamaged. The passengers and the crew could leave the airplane without injuries via attached stairways.

4 DISCUSSION

The complex interaction of the ICNS system "started the fire" when two agents in the system were operating under different "modes of operation." Air Traffic Control, *operating the airport under Cat I*, released a flight for takeoff that interfered with the Localizer signal. The arriving flight SQ-327, *operating under Cat 2/3, had selected to use a completely automated (Cat II/III) landing*.

Both agents performed their tasks according to their Standard Operating Procedures. ATC was operating according to standard Cat I procedures under Cat I conditions. Under Cat II/Cat III conditions the separation requirements between landing and departing aircraft are greater than under Cat I conditions because the pilots cannot navigate visually.

The arriving aircraft was allowed to fly a Cat III approach under the prevailing conditions, as long as the pilots monitored for disrupted ILS signals. Then they could continue the landing using visual references or perform a Go Around if necessary.

However, due to the intersection departure combined with the displaced ILS antenna system, the disrupted ILS signal occurred when the arriving aircraft was closer to the ground than would have been expected, giving the pilots very little time to react.

At this point, the surprised flight crew did what they were trained to do. First, they attempted to initiate a go-around by hitting the TOGA switch, using the automation to quickly and effectively move the aircraft away from the ground. However, the crew were surprised again. By this time, the aircraft had touched down and the automation had disabled the TOGA switch.

The crew was now confronted with overwhelming visual cues that the aircraft was veering off the runway and they reverted to their basic pilot training and tried to correct the aircraft's trajectory using rudder pedal steering.

They were surprised again when this proved ineffective because the autopilot was still in control of the aircraft. There is some indication that the pilot flying may have tried unsuccessfully to disconnect the autopilot, but sufficient pressure on the rudder pedals finally disconnected the autopilot and returned the aircraft to manual control.

This incident exhibited the features of a NEFM as follows:

Divergent Modes of Operation

Had ATC been informed of the arriving aircraft's intention to perform a Cat III Autoland under Cat I conditions, the controllers might have held the departing aircraft using Cat III standards. However, there is no requirement that arriving flight crews inform ATC of their intentions, given that they should be able to complete the landing safely without ATC intervention.

Reduced Margin of Safety

In this case, the margin of safety was reduced by the geometry of the Munich runway 08 ILS system. The ILS was operating as designed and had been adjusted to provide appropriate guidance to arriving aircraft. However, the effects of possible interactions between aircraft in the new geometry had not been fully realized or at least they had not been communicated to ATC and were not incorporated into the ATC standard operating procedures for Munich airport.

Pilot Flying: The Safety Barrier

Under these conditions, all of the designed safety barriers were effectively removed, save one – the ability of pilot flying to react quickly and effectively enough with the available operational time window (AOTW) to an unexpected event very low to the ground. In this case, this final barrier failed as one would expect.

Hidden Critical Decision Point

Analogous to the V_1 speed decision point during takeoff, after which the aircraft is obliged to rotate due to insufficient remaining runway length, the transition to ROLL-OUT mode is a critical decision point in the approach and land sequence. When the Autopilot transitions to ROLL-OUT the spoilers are automatically deployed and the automation is committed to a roll-out. Further the automated Go Around mode and the associated TOGA switches are disabled. For this reason, a crew call-out is important to mark the transition to the next procedure (i.e. roll-out) and to know which control modes are/are not available .

Moded Input Devices

The TOGA switches on the Throttle Levers were disabled when the Autopilot transitioned to ROLL-OUT mode. The status of the TOGA switches is not annunciated on the flight deck. For example there is no green/red LED lights indicating whether the switches are able/disabled.

Achilles Heel: Fail-Safe Sensor Monitoring

The weak link in the chain for any automation system is the sensors and the sensor monitoring.

Determining what it the truth and using this measure to assess the performance of sensors and select the valid combination of sensors is a complex process. This process is even more complex when the sensor selection must be made based on time-series data within the allowable operational time window (AOTW) of the hazard [3].

5 CONCLUSIONS

Synchronization of Sub-System Intentions

This accident was a product of a system-of-systems failure. Every part of the system was operating as designed. The accident occurred due to the failures to synchronize the procedures followed by the sub-systems and for these subs-systems to communicate their intentions with each other. There is no procedure that guarantees the synchronization of the ATC, airline, and technical components of the system-of-systems and there is no organizational oversight that is responsible for ensuring this synchronization.

But how would one devise a synchronization procedure? What would an oversight organization do to ensure that these sorts of accidents do not occur? Because of their nature, the conditions that produce system-of-system accidents in very safe systems like commercial aviation in the developed world are rare. They occur only when multiple sub-systems concurrently enter into inimical states. Determining when these might occur based on knowledge of the range of operating conditions, the standard operating procedures of the sub-systems, the capabilities and limitations of the components is not a simple task.

There are several possible approaches to address the NEFM class of issues:

1 Super Computer Agent-based Simulation for Rare-events

First, one could attempt to model the entire system-of-systems in a computerized agent-based simulation and allow the simulation to run continuously exploring all of the possible combinations (Table 2). Given the extremely large number of possible combinations, one could use some basic rules for guiding the search order, but there would be no guarantee that the system could be comprehensively explored before changes to the system were introduced that would necessitate repeating the entire endeavor. Methods for rare-event simulation are discussed in [4]

Table 2 Combinatorics for Simulation

Sub-system	Random Variable
Arriving Aircraft	Probability of Cat II/III
	Initial Altitude
	Start of Approach Distance
	Approach Speeds
	Landing Speed
	Weight on Wheels Timing (and TOGA Switch Disable)
	Pilot select TOGA Switch
Departing Aircraft	Timing of Runway Entry
	Location of Runway Entry
	Takeoff Roll Acceleration
	Rotate Speed
	Rate of Climb
Localizer	Effect of Departing Aircraft on Localizer Signal
	Far-field Monitor
	Near-field Monitor

2 Voluntary Reporting

Second, one could attempt to conduct comprehensive searches of voluntary safety reports (e.g., ASRS, ASAP, ATSAP) using machine algorithms to locate problems. These could be guided by a principled risk matrix (e.g., events close to the ground are generally more dangerous than those at altitude). This would require more investment and coordination between these databases than presently exists.

A preliminary search in the ASRS data-bae identified that “localizer interference,” although rare, is not uncommon. Of course in the case of the ASRS reports the human operator intervened and there was no “incident/accident report.”

3 Flight Operations Data Analysis

Third, one could perform comprehensive searches using a global data repository of combined automated data gathered from aviation sources including Flight Data Monitoring (FDM)/Flight Operations Quality Assurance (FOQA), surveillance track data, weather data, NOTAMs, etc. As in the previous cases, this would require relying on machine learning and substantial computing resources.

Final Thoughts

Not long ago, none of these options for addressing this class of NEFM would have been possible. All of these, though difficult and costly and in some cases politically handicapped, are now not only conceivable but practical. The disasters averted would be worth the costs incurred.

References

[1]Bundesstelle für Flugunfalluntersuchung German Federal Bureau of Aircraft Accident Investigation (2019) Investigation Report: 3 November 2011, Munich. BFU EX010-11. Bundesstelle für Flugunfalluntersuchung Hermann-Blenk-Str. 16 38108 Braunschweig www.bfu-web.de

[2] Sherry, L., R. Mauro, J. Trippe (2019) Design of a Primary Flight Display to Avoid Decelerating Below the Minimum Safe Operating Speed. Journal Aviation Psychology and Applied Human Factors. Issue 1, 2019.

[3] Kourdali, H. L. Sherry (2017) Available Operational Time Window (AOTW): A Method for Evaluating and Monitoring Airline Procedures. Journal of Cognitive Engineering and Decision Making. August 31, 2017

[4] Shortle, J., C-H. Chen (2013) Sensitivity analysis of rare-event splitting applied to cascading blackout models. Winter Simulation Conference - (WSC 2013) Washington, DC, USA http://ieeexplore.ieee.org/document/6721467

Acknowledgements

Technical contributions from George Donohue, John Shortle, Paulo Costa, Tom Clemmons, Brett Berlin, Oleksandra "Sasha" Donnelly, Seungwon Noh (Center for Air Transportation Research at George Mason University). Immanuel Barshi, Michael Feary, Dorrit Billman (NASA), Randall Mumaw (San Jose State University).

Email Addresses

lsherry@gmu.edu

mauro@decisionresearch.org.

2019 Integrated Communications Navigation and Surveillance (ICNS) Conference

April 9-11, 2019