



University
of Glasgow

Degraded Modes of Operations in Software Engineering

Prof. Chris Johnson,
School of Computing Science, University of Glasgow, Scotland.
<http://www.dcs.gla.ac.uk/~johnson>



**No entry for heavy
goods vehicles.
Residential site only**

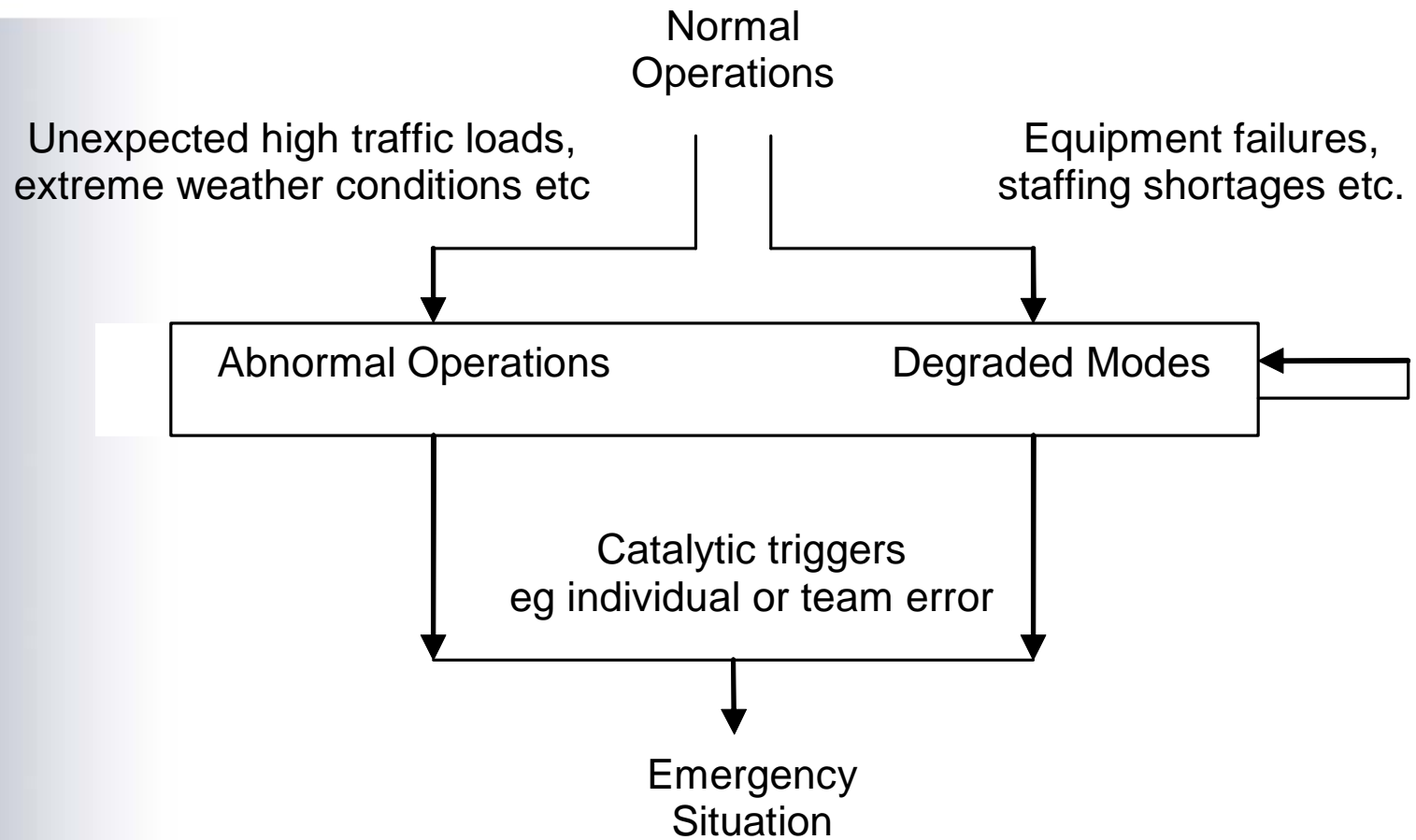


**Nid wyf yn y swyddfa
ar hyn o bryd. Anfonwch
unrhyw waith i'w gyfieithu.**

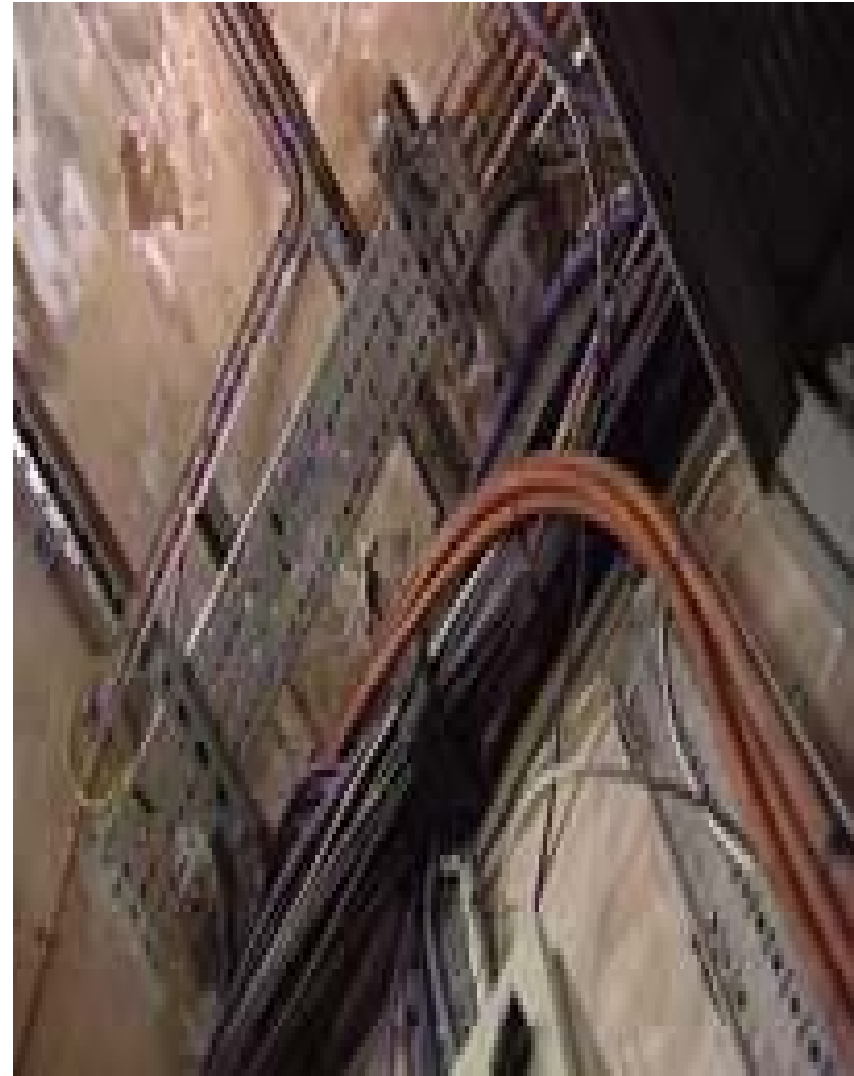




What are Degraded Modes



Aging, Complex Critical Infrastructures...





- Staff struggle to maintain levels of service.
- Software failures force ad hoc solutions:
 - violate safety requirements;
 - Not supported by risk assessments.
- Lead to major failures if not addressed.



- Power Supply Station near ACC:
 - Transformer and Generator.
- PS Switching boxes in ACC.
- Equipment installed 30 years ago:
 - Procure new kit.
- Installation affects comms ACC/PS



14:25 UTC: Alarm Remote Control Unit
In PS Station from UPS in ACC.

- Technician to ACC, checks UPS:
 1. Warning on UPS display:
<Power Supply is out of tolerance >
 2. UPS operates on battery supply
 3. UPS autonomy - **13 minutes**



14:30: Technician returns to PS Station.

- Informs Technical Supervisor about problem
- Calls Head of department is **not** accessible.

14:32: In ACC again, Technician detects

- **UPS autonomy - 6 minutes**
- Makes **erroneous decision** to switch PS to 2nd UPS;
- Switches 1st UPS to bypass configuration
- Generator voltage direct to Users, no stabilization;
- Under voltage but no over voltage protection.



Time	Destination
15:45	CANCELLED
15:50	CANCELLED
16:00	CANCELLED
16:00	CANCELLED
16:10	CANCELLED
16:10	CANCELLED
16:10	CANCELLED
16:15	CANCELLED
16:20	CANCELLED
16:30	CANCELLED
16:30	CANCELLED
16:30	CANCELLED
16:40	CANCELLED
16:40	CANCELLED
16:40	CANCELLED
16:50	CANCELLED
16:50	CANCELLED

14:35 UTC - In a few minutes collapse of:

- three quarters of Radar Data Displays,
- one half of Flight Data Displays,
- all radar inputs in DPS,
- Controller Working Positions for Voice Comms
- and AFTN connection with ARO & NOTAM.

14:40 UTC - Technical Supervisor tells ATC Supervisor needs 30 minutes.

14:45 UTC - ATC SUP decides to close FIR, CFMU told **traffic is zero**.





**REPORT OF THE IRISH AVIATION AUTHORITY
INTO THE ATM SYSTEM MALFUNCTION AT DUBLIN AIRPORT**

19th September 2008

CONTENTS

	Page
1. Background Information	1
2. Contingency Arrangements in Place	1
3. Arrangements in place with the System Supplier to provide support	2
4. Explanation of the problems which led to the malfunction	2
5. Measures taken to rectify the problem	4
6. Details of any Safety Issues Arising	6
7. Level of Communications between the IAA, the Airlines and Dublin Airport Authority (DAA)	6
8. Observations	7

- Busiest period of the year.
- Initial hardware failure:
 - Poor quality of service from LAN;
 - Slows flight data processing system.
- ATCOs cannot access data on radar targets:
 - including aircraft identification and type data.
- Capacity restrictions for safety reasons.





- ATM system provided by contractor:
 - maintained under annual service contract;
 - provide both hardware and software support;
 - On-site support for diagnosis and debugging.
- General question for SESAR?
 - ANSPs rely on subcontractors:
 - key areas of technical support ;
 - ‘it will take another 30 minutes...’
 - Is outsourcing a form of de-risking?

- ANSPs engineering staff correct symptoms;
 - Cannot identify root causes of the problem.
- Problem stemmed from double failure:
 - triggered by a faulty network interface card;
 - flooded network with spurious messages.
- Symptoms of the fault were masked;
 - recovery mechanisms in Local Area Network;
 - hard for engineers to identify component failure.



Michael O'Leary, CEO Ryanair

- "The problem here is that you have an autonomous semi-state monopoly which doesn't care about its customers or the disruption to passengers,"



Michael O'Leary, CEO Ryanair

- "The problem here is that you have an autonomous semi-state monopoly which doesn't care about its customers or the disruption to passengers,"
- "Send the buggers to Shannon, if it was a commercial company they would have done so,"



Michael O'Leary, CEO Ryanair

- "The problem here is that you have an autonomous semi-state monopoly which doesn't care about its customers or the disruption to passengers,"
- "Send the buggers to Shannon, if it was a commercial company they would have done so,"
- "They're not on top of the job. We're talking about 25 arrivals and departures per hour. The air traffic controllers should be capable of handling this volume of flights".



Europe is Not Alone





- Atlanta FDPS System software bug;
 - Switch data rate configuration error (again).
- Use of fallback system in Salt Lake City:
 - Cascading failure cannot cope with demand.
- ATCOs enter flight data manually;
 - Cannot cope with backlog, knock-on delays.
- 12 hours to diagnose problem;
 - 6 more to catch up with backlog eg New York.



- August 2008:
 - Software failure in Atlanta again.
 - Processes flight plans for Eastern US.
 - 566 flight delays+
- Press, media and political outrage....
- GAO reports into ATM service provision.



- Fault stems from Salt Lake City:
 - hardware fault on router circuit board;
 - Network interface affects comms with Atlanta;
 - Also affects comms with 21 regional radar centers.
- Network owned/operated by Harris Corp...
 - “We are working with the FAA to diagnose problem and explain the failure of backup systems...”
 - 5 hours to diagnose, 12+ to restore support;
 - ATCOs enter flight plans manually (workload);
 - Effects exacerbated by bad weather eg Chicago

- “Sisters Sharon Walker and Sheila James were taking their elderly mother to see their sister in St. Louis. Their 09.30 flight was delayed until 16:00...”
- “Sen. Charles Schumer said the country’s aviation system is ‘in shambles’...’the FAA needs to upgrade the system, these technical glitches that cause cascading chaos across the country are going to become a very regular occurrence...””





- \$2.1 Billion upgrade by Dec 2010:
 - En Route Automation Modernization.
- Faults lead to ‘missing’ flight plans;
 - Other aircraft change identity in flight;
 - Again cannot transfer flight data to Atlanta etc.
 - Undermines ATCO confidence in system;
 - ‘fallback’ original 20 year old IBM system
 - IBM contract expired, uses Jovial – rarely used.
- Test deployment to Salt Lake City:
 - FAA spend \$14 million, still not working.
 - Salt Lake City simple compared to Chicago...

Potential Solutions?









NOT MEASUREMENT
SENSITIVE

MIL-STD-882D
10 February 2000

SUPERSEDING
MIL-STD-882C
19 January 1993

DEPARTMENT OF DEFENSE
STANDARD PRACTICE FOR
SYSTEM SAFETY



AMSC N/A

AREA SAFT

Frequency of Occurrence (over the life of an item)	Severity of Occurrence			
	CATASTROPHIC (I)	CRITICAL (II)	MARGINAL (III)	NEGLIGIBLE (IV)
FREQUENT (A) $P > 10^{-1}$	I-A	II-A	III-A	IV-A
PROBABLE (B) $10^{-1} > P > 10^{-2}$	I-B	II-B	III-B	IV-B
OCCASIONAL (C) $10^{-2} > P > 10^{-3}$	I-C	II-C	III-C	IV-C
REMOTE (D) $10^{-3} > P > 10^{-6}$	I-D	II-D	III-D	IV-D
IMPROBABLE (E) $10^{-6} > P$	I-E	II-E	III-E	IV-E

1. Document the approach:
2. Identify potential system hazards:
3. Assess severity and probability:
4. Identify mitigation measures:
5. Implementation of mitigation
6. Verify intended risk reduction:
7. Communicate residual risks:
8. Risk management after deployment;



- Haddon-Cave report:
“If risk assessment has been conducted with proper skill, care and attention, the catastrophic fire risk ... would have been spotted”.
- Risk assessment:
 - no substitute for ‘sound judgement’.
 - “incompetence, complacency, cynicism”.
 - Documentation overwhelming;
 - Many trivial or irrelevant failure modes;
 - Few combined failures across functions;
 - Most help for large-scale procurements.

- Techniques to address operational risk:
 - Low cost, approximations, rules of thumb;
 - Where necessary should trigger HAZOPS etc.

“When engineering analysis and risk assessments are condensed to fit on a standard form or overhead slide, information is inevitably lost”.

- On the other hand:
 - You cannot capture everything...
 - Limited time, limited training, present threats.

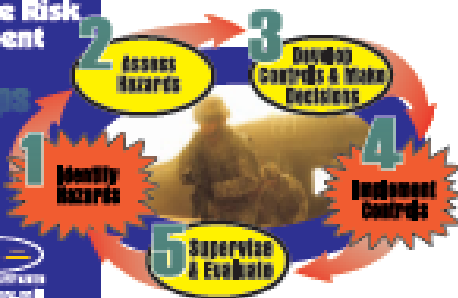
Composite Risk Management Process



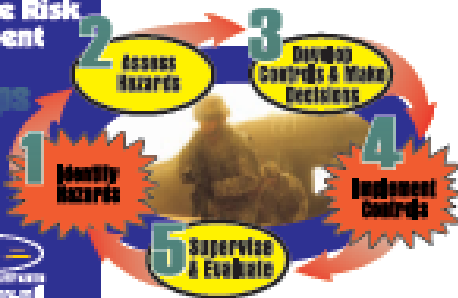
Composite Risk Management Process



Composite Risk Management Process



Composite Risk Management Process



Composite Risk Management Process



Composite Risk Management Process



Composite Risk Management Process



Composite Risk Management Process



Composite Risk Management Process



Composite Risk Management Process



Composite Risk Management Process



Composite Risk Management Process



Wider Applications: MATS Forms...

Regulatory Change Management Coordination Form

Note: The Regulator's representative should complete this form and send it back to the Quality and Safety Management section before the process of change is initiated. This form indicates clearly the level of information or involvement expected by the regulator in the change being proposed by the ANSP. This process is applicable only to Major Changes proposed by the ANSP.

Type of Change:

People <input type="checkbox"/>	Equipment <input type="checkbox"/>	Procedures <input type="checkbox"/>
Operational <input type="checkbox"/>	Technical <input type="checkbox"/>	Other <input type="checkbox"/>

Brief Description of the Change
The Change process is expected to be initiated on:

The Regulator after analysing the presented change proposal requests:

- To be involved and invited for the safety assessment
- To be given a copy of the final document of the change
- Not to be involved and the ANSP may proceed
- More information

Name..... Date..... Sign..... (for Regulator)

Name..... Date..... Sign..... (for ANSP)



Any Questions?

Time	Destination
15:45	CANCELLED
15:50	CANCELLED
16:00	CANCELLED
16:00	CANCELLED
16:00	CANCELLED
16:10	CANCELLED
16:10	CANCELLED
16:10	CANCELLED
16:15	CANCELLED
16:20	CANCELLED
16:30	CANCELLED
16:30	CANCELLED
16:30	CANCELLED
16:40	CANCELLED
16:40	CANCELLED
16:40	CANCELLED
16:50	CANCELLED
16:50	CANCELLED

