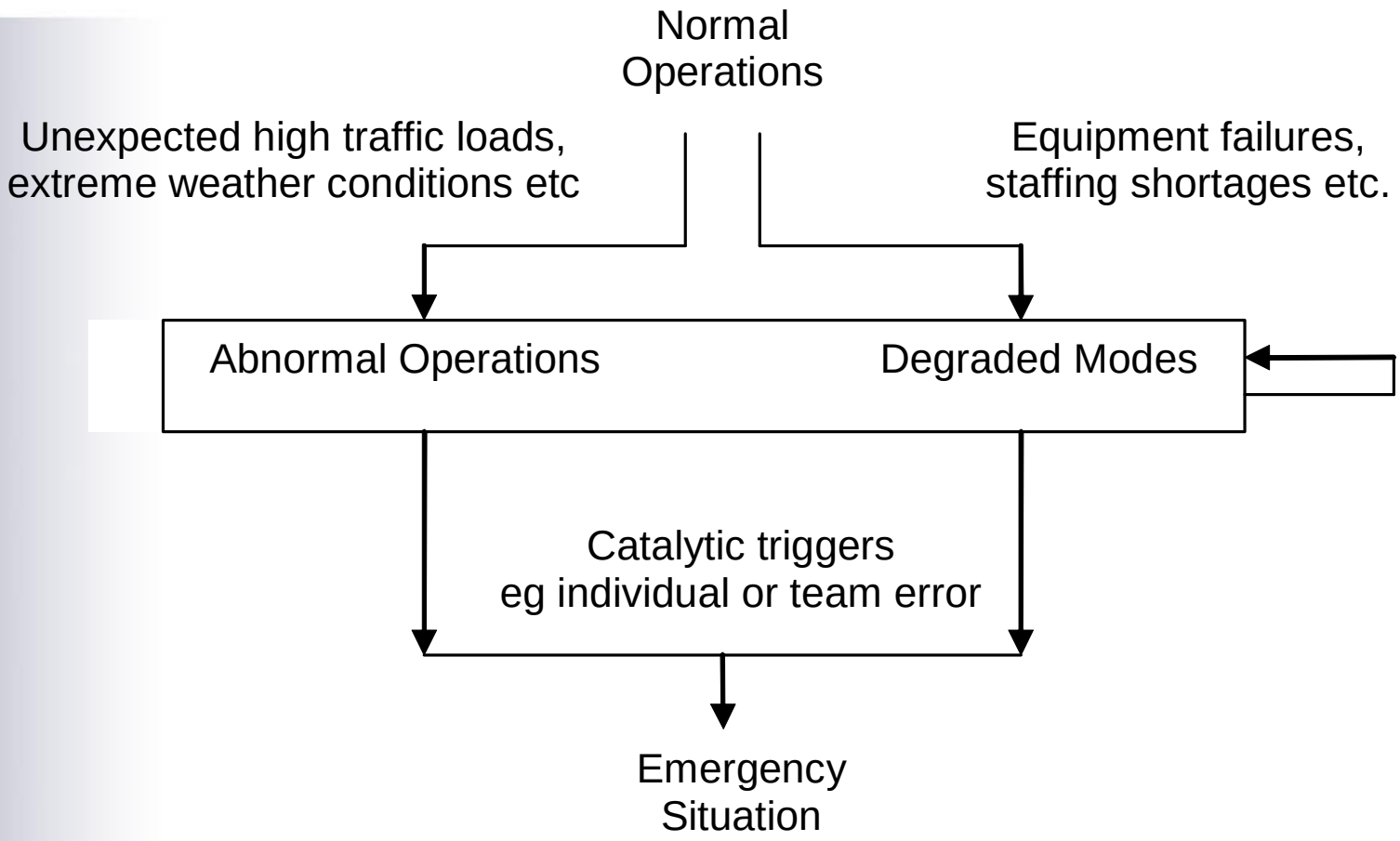
Degraded Modes of Operations for Operational Engineering (SW related issues)

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

ES2 WS3-11, Bled, Slovenia, September 2011


WINDOW JETTISON HANDLE PIN
REMOVE BEFORE JETTISON

What are Degraded Modes



University of Glasgow

Aging, Complex Critical Infrastructures...

University of Glasgow

Introduction to Degraded Modes

- 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.

UPS Case Study

- 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

Anatomy of the Incident (1)

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

Anatomy of the Incident (2)

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.

Anatomy of the Incident (4)

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.

IRISH AVIATION AUTHORITY
ÚDARÁS CITLÍOCHTA NA hÉIREANN

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

Dublin Airport Overview

- 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.

Dublin Airport - Contracting

- 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?

University of Glasgow

Secondary Response

- 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.

The Real Impact

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,"

The Real Impact

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,“

The Real Impact


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”.

http://www.herald.ie/news/oleary-more-disruption-if-iaa-doesnt-clean-up-act-1431408.html

Europe is Not Alone

University of Glasgow

June 2007

- 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 and November 2009

- 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.

November 2009

- 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

Media and Politicians

- “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...’”

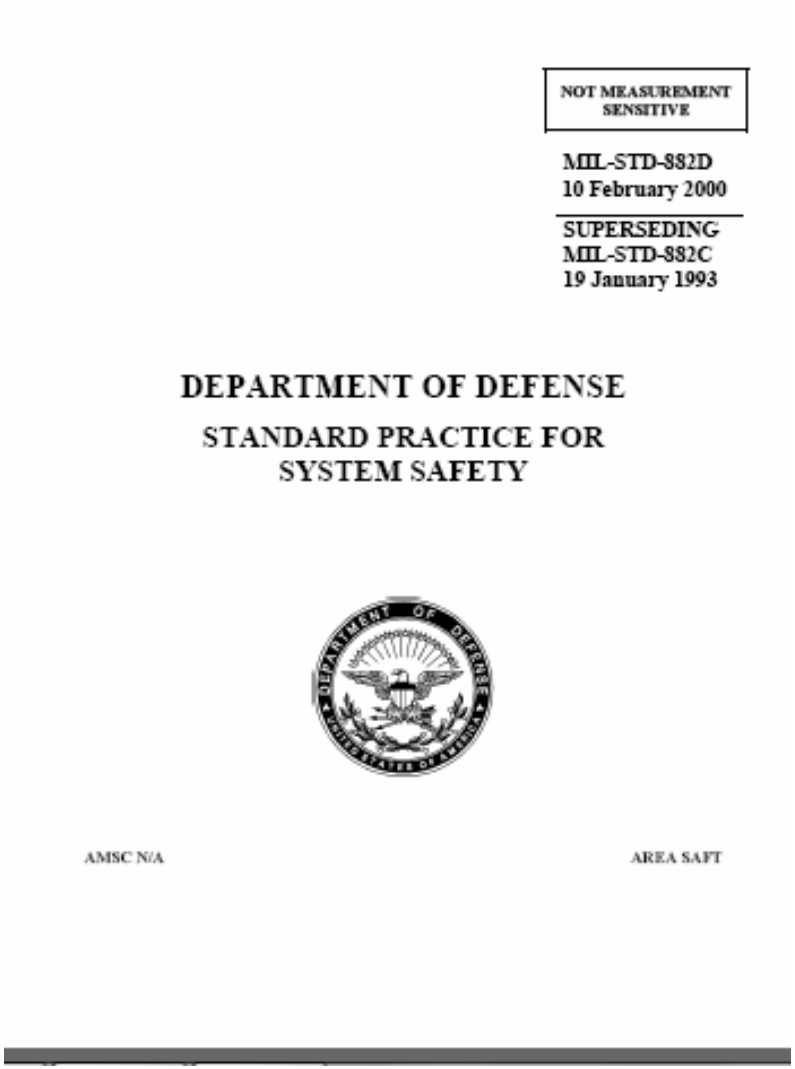
April 2010

- $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...

University of Glasgow

Potential Solutions?

“The Risk Assessment Blind Spot”



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

University of Glasgow

MIL-STD 882D

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;

Limits of Conventional Risk Assessment

- 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.

Rapid Risk Assessment Techniques

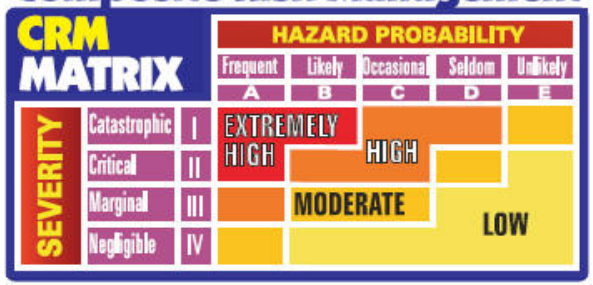
- Techniques to address operational risk:
  - Low cost, approximations, rules of thumb;
  - Where necessary should trigger HAZOPS etc.

"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
5 steps
1 Identify Hazards
2 Assess Hazards
3 Develop Controls & Make Decisions
4 Implement Controls
5 Supervise & Evaluate

Composite Risk Management



Composite Risk Management

CRM MATRIX
HAZARD PROBABILITY
Frequent A
Likely B
Occasional C
Seldom D
Unlikely E
SEVERITY
Catastrophic I
Critical II
Marginal III
Negligible IV
EXTREMELY HIGH
HIGH
MODERATE
LOW

ROTARY-WING RISK ASSESSMENT MATRIX

1. SUPERVISION (Risk Value/Mission)

CMD/CONTROL	VALUE	TACTICAL DAY/NIGHT	
Parent Unit	1	1	2
Attached	2	3	4

2. PLANNING (Risk Value/Time)

GUIDANCE	IN-DEPTH	ADEQUATE	MINIMAL
Vague	3	4	5
Implied	2	3	4
Specific	1	2	3

3. CREW SEL/PC (Risk Value/Flt Hrs)

TIME IN AO*	TOTAL TIME >2000	<2000	<1000	<500
<25	3	4	5	6
>50	2	3	4	5
>50	1	2	3	4

4. CREW SEL/PI (Risk Value/Flt Hrs)

TIME IN AO*	TOTAL TIME >2000	<2000	<1000	<500
<25	3	4	5	6
>50	2	3	4	5
>50	1	2	3	4

5. CREW SEL/ADD (Risk Value/Flt Hrs)

TIME IN AO*	TOTAL TIME >2000	<2000	<1000	<500
<25	3	4	5	6
50	2	3	4	5
>50	1	2	3	4

6. ALL CREW MEMBERS ARE CREW COORDINATION TRAINED

No	+2
Yes	0

7. ALL TASKS REQUIRED ON THIS MISSION ARE SUPPORTED BY THE UNIT MISSION ESSENTIAL TASK LIST (METL)

Yes	0
No	5#

#Requires bn cdr approval.

8. CREW ENDURANCE (Risk Value/Flt Hrs)

QUALITY OF REST	>8 HRS	6-8 HRS	<6 HRS
Field	2	6	10
Garrison	1	4	10

Add 2 for missions flown during the last half of the duty day.

9. COMPLEXITY (Value/Condition)

TYPE OF MISSION	VMC D	VMC N	NVG	IMC HOOD
Multiship	2	6	4	NA
Sling load	2	3	5	NA
Stabo/Rappel	1	2	4	NA
Terrain Flt	1	3	2	NA
Paradrop	2	2	NA	NA
Routine	1	2	2	3
NOE	2	8	4	NA
MTP	3	5	NA	NA
Maint Recovery	3	5	NA	NA

10. WEATHER** (Risk Value/Ceiling/Visibility)

	<1000/3	<700/2	<500/1	>1000/3
D	3	4	6	1
N	4	6	10	2
NVG	3	4	8	1

11. ADDITIONAL RISK FACTORS (D, N)

Single Pilot	+4

ADDITIONAL COMMENTS

* Area of operations.

** Visibility values are given in miles.

ROTARY-WING RISK ASSESSMENT MATRIX

12. NVG CREW SEL/PC (Total NVG Time)

>150	<150	<100	<50	<25
1	2	3	4	5

13. NVG CREW SEL/PI (Total NVG Time)

>150	<150	<100	<50	<25
1	2	3	4	5

14. NVG CREW SEL/ADD (Total NVG Time)

>150	<150	<100	<50	<25
1	2	3	4	5

15. PERCENT OF ILLUMINATION (NVG)

100-80	79-60	59-40	30-23	<23
1	2	3	4	5

16. MOON ANGLE (NVG)

90-70	69-50	49-30	<30
0	1	2	3

17. ADDITIONAL RISK FACTORS (NVG)

RISK VALUES: DAY/NIGHT MISSIONS

1. Supervision _____
2. Planning _____
3. Crew Selection/PC _____
4. Crew Selection/PI _____
5. Crew Selection/Add _____
6. Crew Coordination Trained _____
7. METL Task _____
8. Crew Endurance _____
9. Complexity _____
10. Weather _____
11. Additional Risk Factors _____

TOTAL _____

RISK VALUES: DAY/NIGHT MISSIONS

12. NVG Crew Selection/PC _____
13. NVG Crew Selection/PI _____
14. NVG Crew Selection/Add _____
15. Illumination _____
16. Moon Angle (NVG) _____
17. Additional Risk Factors _____

TOTAL NVG MISSIONS _____

TOTAL DAY/NIGHT MISSIONS _____

TOTAL RISK VALUE NVG _____

COMPUTATIONS DAY/NIGHT MISSIONS

Low Risk	<16
Medium Risk	16-28*
High Risk	>29**

COMPUTATIONS NVG MISSIONS

Low Risk	<25
Medium Risk	25-40*
High Risk	41-50**
Extremely High	>50***

* Medium-risk missions require approval of the company commander.

** High-risk missions require approval of the battalion commander.

*** Extremely high-risk missions require approval of the brigade commander.

ADDITIONAL COMMENTS

- US Army TC 1-210

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	Equipment	Procedures
☐	☐	☐
Operational	Technical	Other
☐	☐	☐

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)

University of Glasgow

Last Word: Cyber-security of ATM Software

University of Glasgow

Any Questions?