The Strategic Implications of Safety-Critical Software and Cyber-Security on ATM Operations

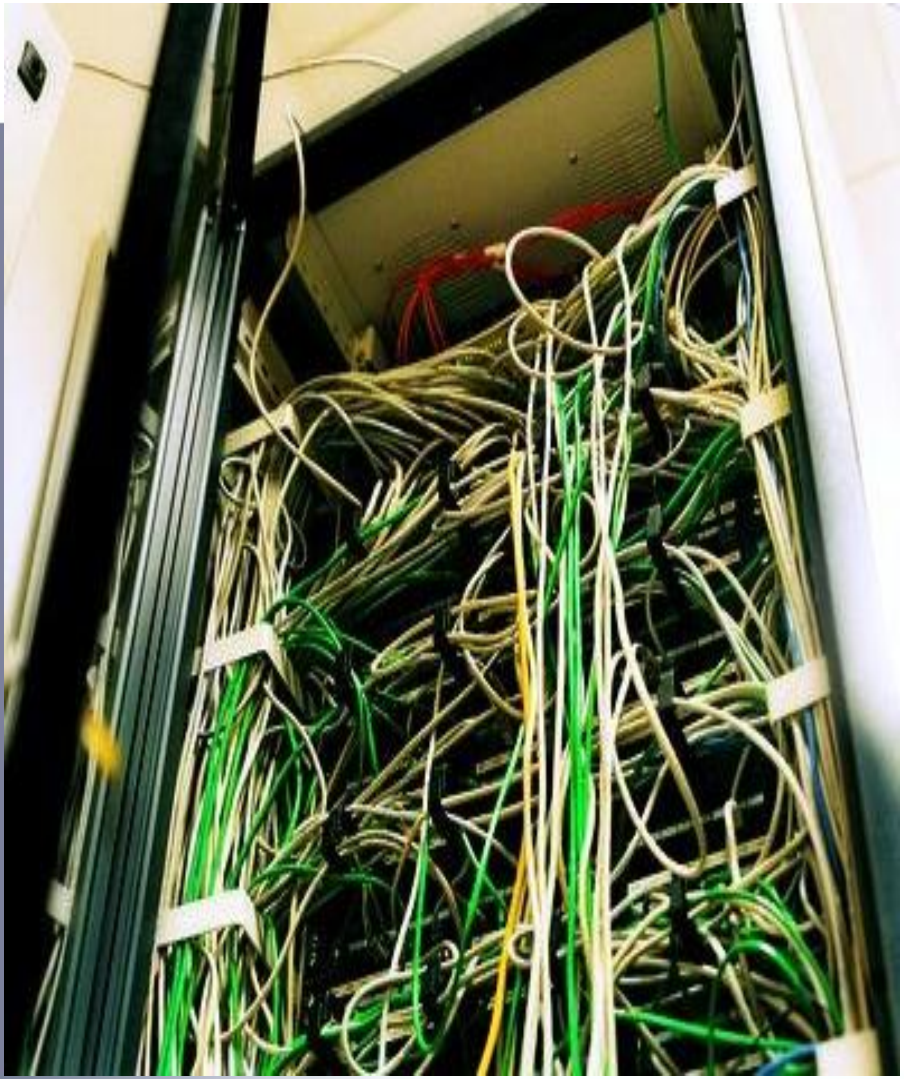
Prof. Chris Johnson,
School of Computing Science, University of Glasgow, Scotland.
http://www.dcs.gla.ac.uk/~johnson

Cyprus, 28th February 2012.

DEPARTURES 28.12.2010
09:58 ВЫЛЕТ DEPARTURES 28.12.2010
09:58 ВЫЛЕТ DEPARTURES 28.12

SHCO

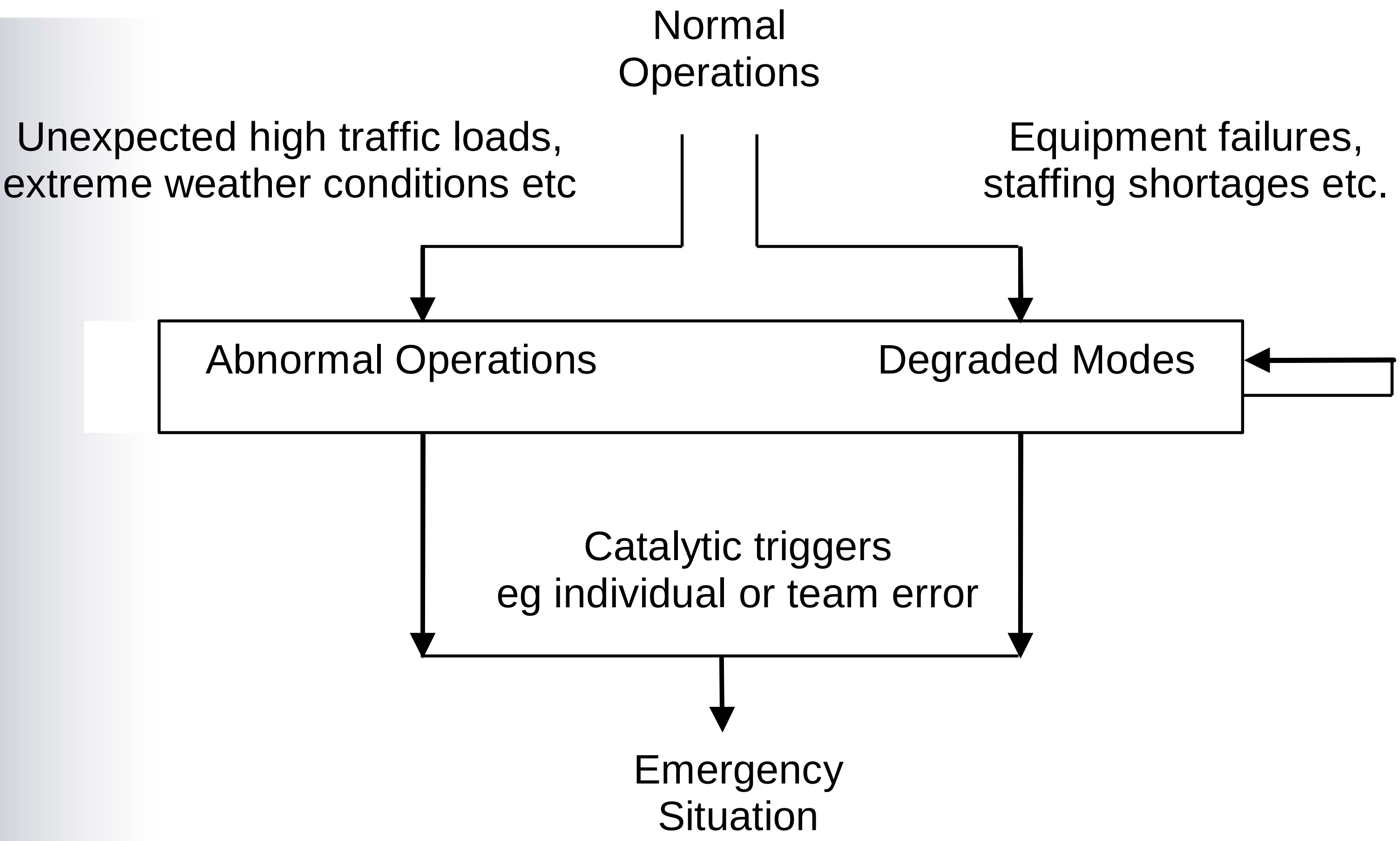
Aging, Complex Critical Infrastructures...



PCMMU
LEFT AUDIO
LEFT COMM
GPC STATUS
CABIN PRESS
CYRO
SENSOR A
EVENT TIME
39:50
MAIN ENGINE STATUS
WINDOW JETTISON HANDLE PIN
REMOVE BEFORE JETTISON

2
3
SVMF
103848
Desc
Reach Mechanism Assembly Auxiliary
PN SED33101307-308
SN MC0002 shelf 4 C
AVIU
Digital CC Video Power Ctl (15 FT)
Digital Video Tape
PDV-184ME DVCAM Video Tape
VPU Plug Patch
EXT COMM
POWER
OFF

What are Degraded Modes



Normal Operations

Unexpected high traffic loads, extreme weather conditions etc

Equipment failures, staffing shortages etc.

Abnormal Operations

Degraded Modes

Catalytic triggers
eg individual or team error

Emergency Situation

Introduction to Degraded Modes

- Staff struggle to maintain levels of service.
- Failures lead to ad hoc solutions:
  - violate safety requirements;
  - Not supported by risk assessments.
- Key causes in Linate and Überlingen.
- Major concern with economic stringency:
  - Lack of technical competency in regulation?

Anatomy of the Incident (1)

14:25 UTC: Alarm Remote Control Unit

Technician to ACC, checks UPS

<Power Supply is out of tolerance >

UPS autonomy - 13 minutes

14:30: Technician returns to PS Station.

Calls Head of department is **not** accessible.

14:32: In ACC again, Technician sees

UPS autonomy - 6 minutes

Makes error switch PS to 2nd UPS;

Under voltage but no over voltage protection.

Anatomy of the Incident (2)

14:35 UTC, In 10 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 -

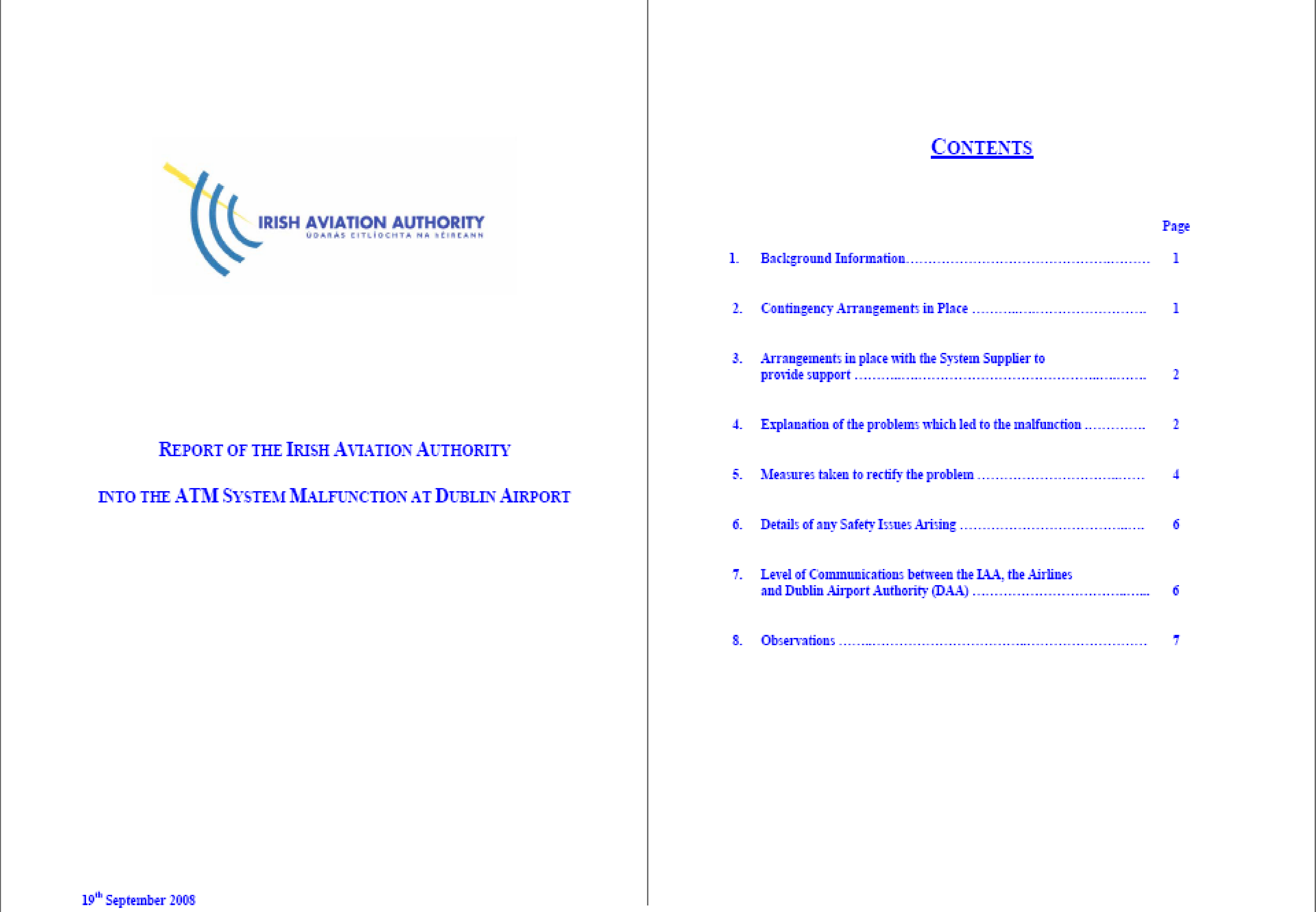
Technical Supervisor “We just need 30 minutes”.

14:45 UTC close FIR, CFMU traffic zero.

ANA
13
17
18
ANA

Edsger W Dijkstra (1930-2002)

Testing can prove the presence of errors, but not their absence.



IRISH AVIATION AUTHORITY
ÚDARÁS EITLÍOCHTA NA hÉIREANN

Report of the Irish Aviation Authority into the ATM System Malfunction at Dublin Airport

19th September 2008

Contents

http://www.iaa.ie/files/2008/news/docs/20080919020223_ATM_Report_Final.pdf

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.

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," University of Glasgow

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

June 2007, 2008 and 2009…

- 2007: Atlanta FDPS switch configuration:
  - Salt Lake City fallback fails, cascading demand.
  - Manually data entry, 18+ hours to diagnose…
- 2008: Software failure in Atlanta again:
  - Processes flight plans for Eastern US.
  - 566 flight delays+
- 2009: Salt Lake City router circuit fault:
  - comms with Atlanta, plus 21 radar centres;
  - Bad weather adds 17 hours to restore…
  - Network owned/operated by Harris Corp.

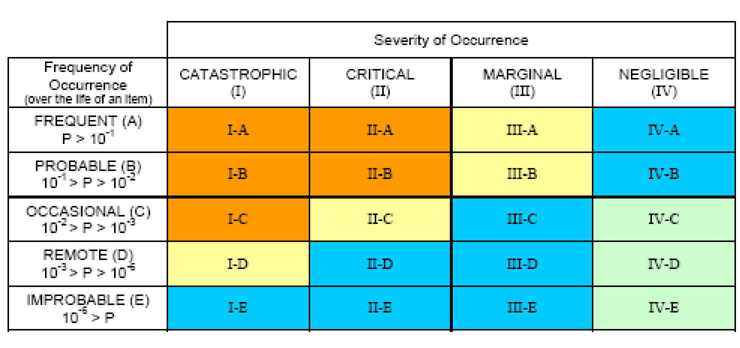
Media and Politicians

- “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...’”

Potential Solutions?

MIL-STD 882D



	Severity of Occurrence			
Frequency of Occurrence (over the life of an item)	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

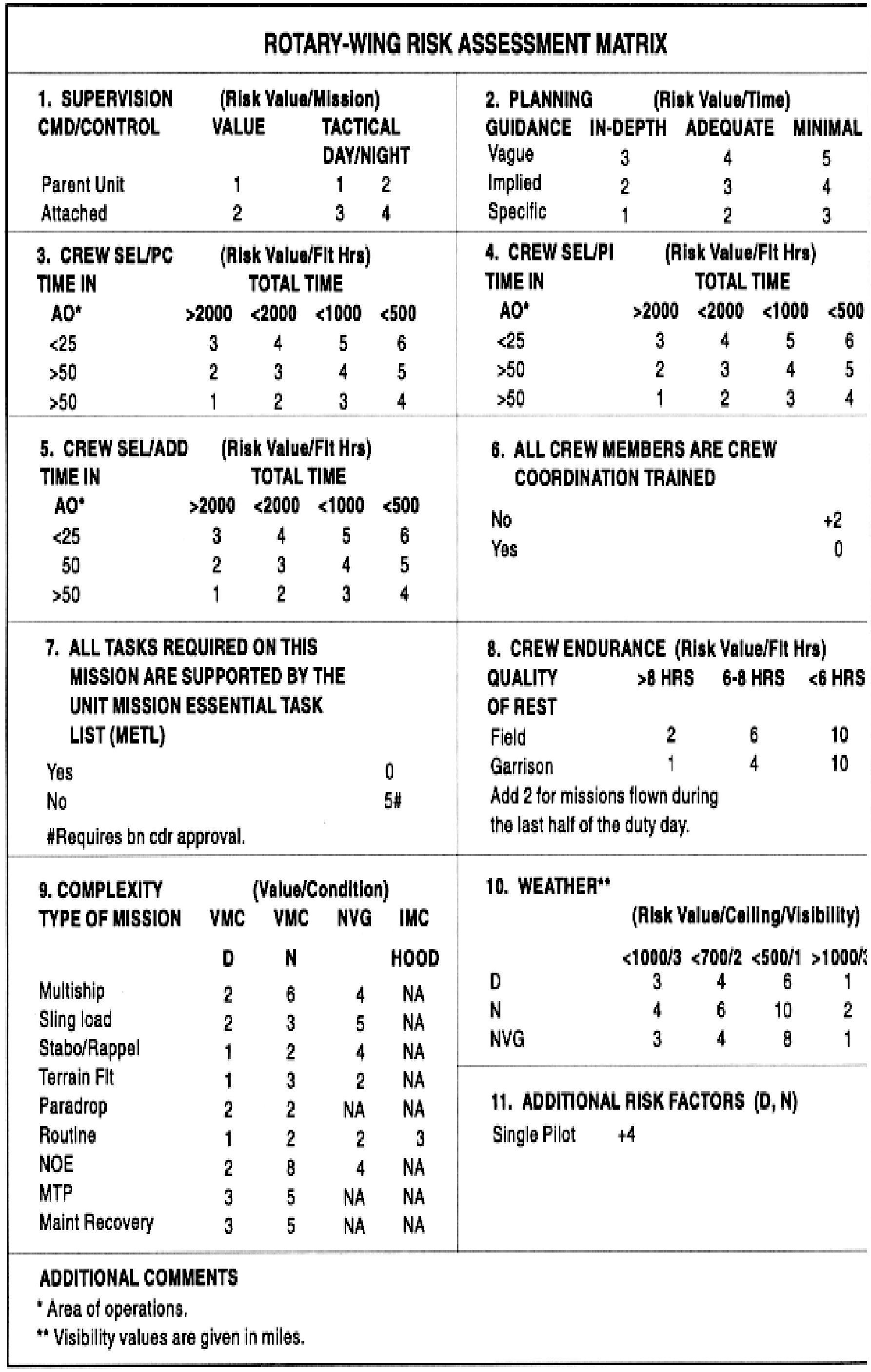
1. Document the approach:
2. Identify potential system hazards:
3. Assess severity and probability:
4. Identify mitigation measures:
5. Implementation of mitigation
6. Verify intended risk reduction:
7. Communicate residual risks:
8. Risk management after deployment;

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:
  - “incompetence, complacency, cynicism”.
  - Documentation overwhelming;
  - Many trivial or irrelevant failure modes;
  - Supports only new procurements…



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	TOTAL TIME			
AO*	>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	TOTAL TIME			
AO*	>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	TOTAL TIME			
AO*	>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	VMC	NVG	IMC
	D	N		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

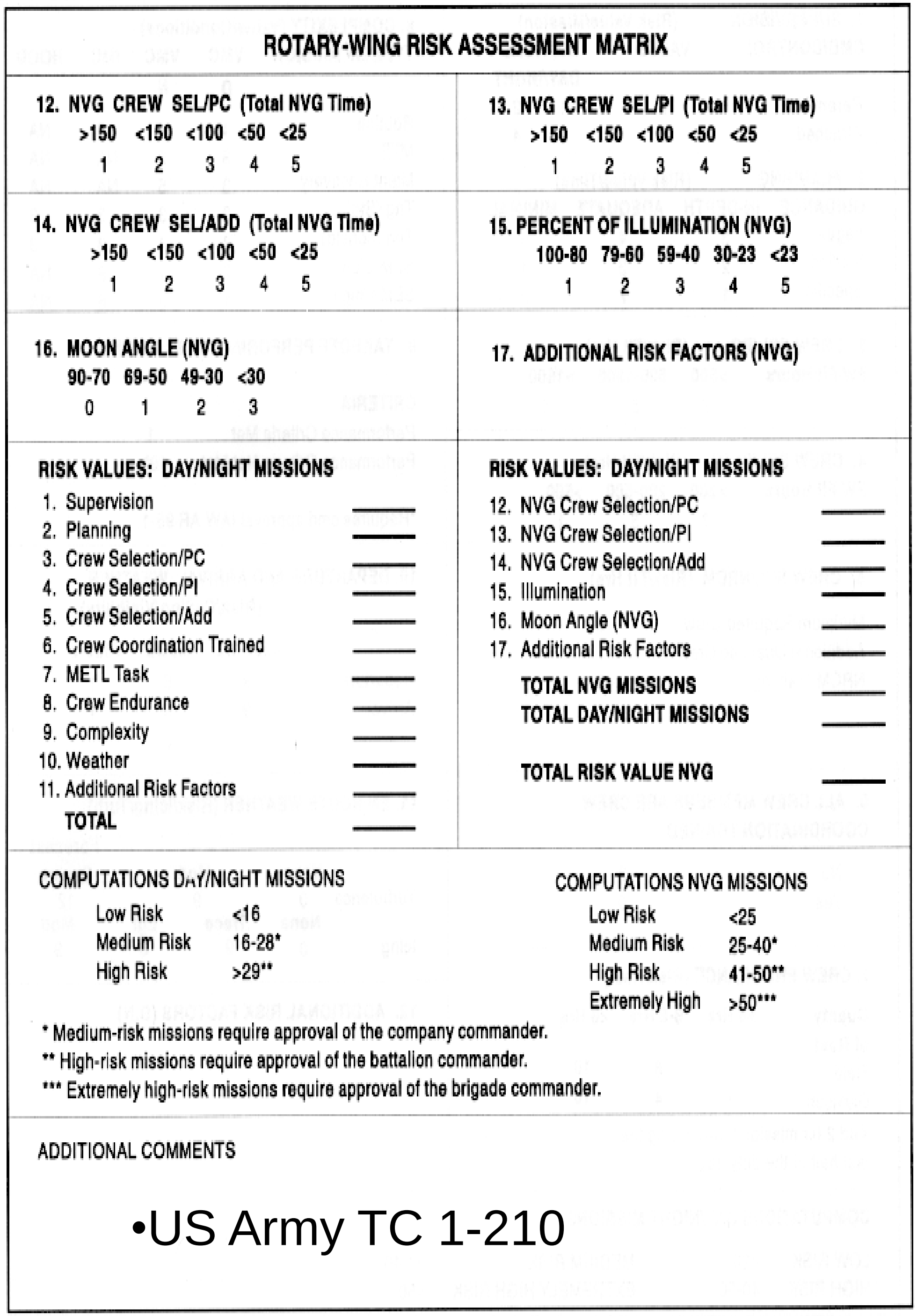
11. ADDITIONAL RISK FACTORS (D, N)

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.

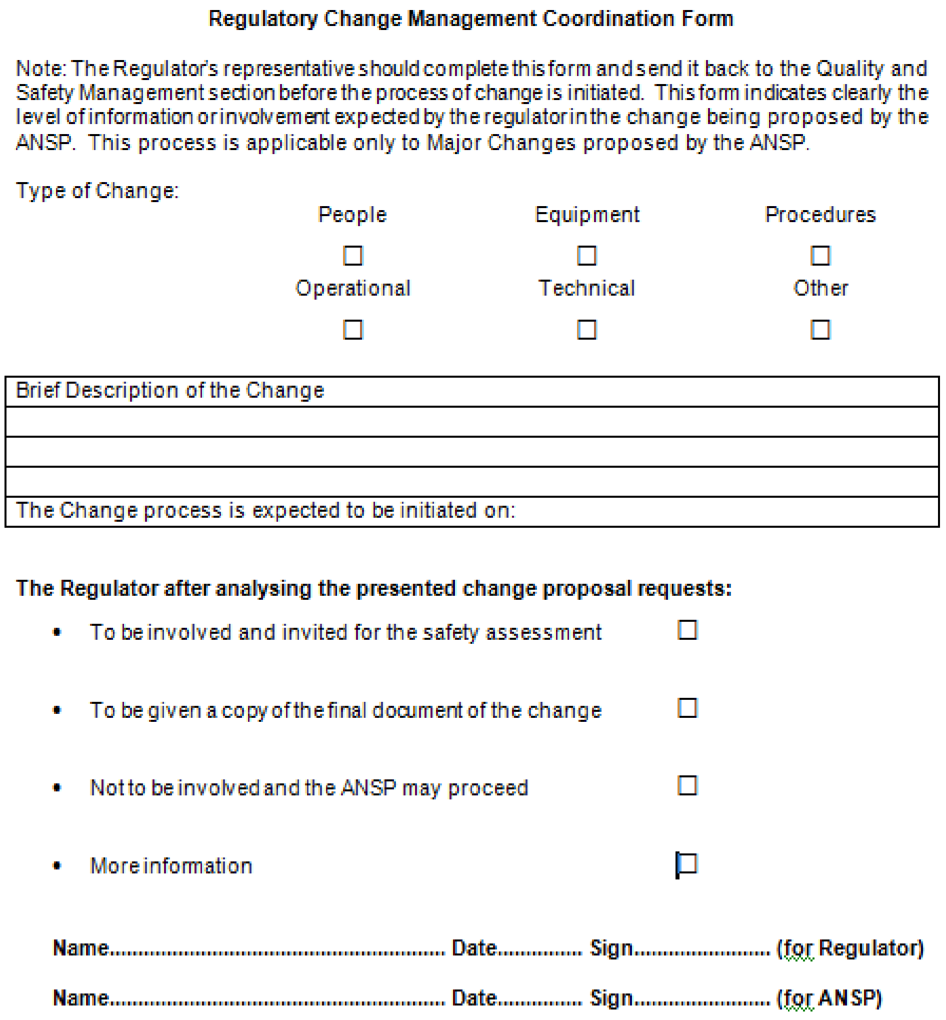
** High-risk missions require approval of the battalion commander.

*** 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)

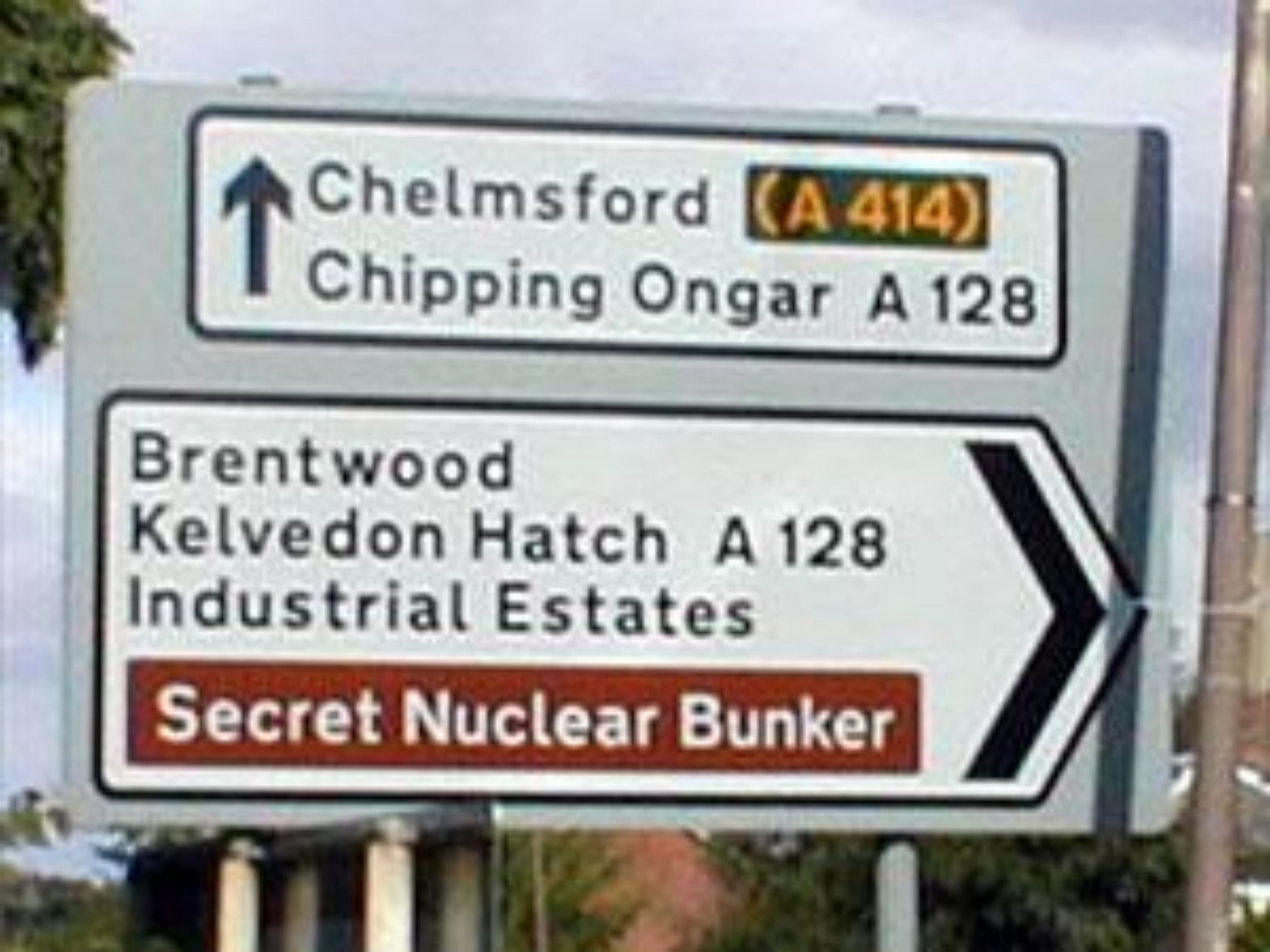
Name.. Date............... Sign......................... (for ANSP)

2010-Present (SESAR and NextGen)

- $2.1 Billion En Route Automation Modernization
- Faults lead to ‘missing’ flight plans;
  - Again cannot transfer flight data to Atlanta etc.
  - Undermines ATCO confidence in system;
  - IBM fallback contract expired, Jovial…20 years old…
- Test deployment to Salt Lake City:
  - FAA spend $14 million, still not working.
  - Salt Lake City simple compared to Chicago...

Paranoia? ATM and the CyberThreat

- Before, specialized infrastructures but now:
  - EGNOS: Smart Grids, Trains, ATM...
  - VOIP: Fire dispatch, space, ATM…
  - LINUX: NHS, UK Military, ATM…
- My students take these systems to pieces…
  - 4 recent viruses in ACC’s on recent tour…
- Paranoia?



Chelmsford (A 414)
Chipping Ongar A 128
Brentwood
Kelvedon Hatch A 128
Industrial Estates
Secret Nuclear Bunker

NASA/ESA/USAF Space Station Resilience

“Go But You Will Never Work Here Again…”

China, GhostNet and Shadow, March 2009

- Trojan horse onto victim's machine;
  - Information forwarded to control servers;
  - reporting back to Chinese sources.
- Use of social media and Gmail:
  - Use of TOR annonymity server…
- Chinese government:
  - ATM as 'dual use' infrastructure;
  - promotes 'active defence' in cybersecurity;
  - UK and US govts both active in this area.

W32.STUXNET, March 2010

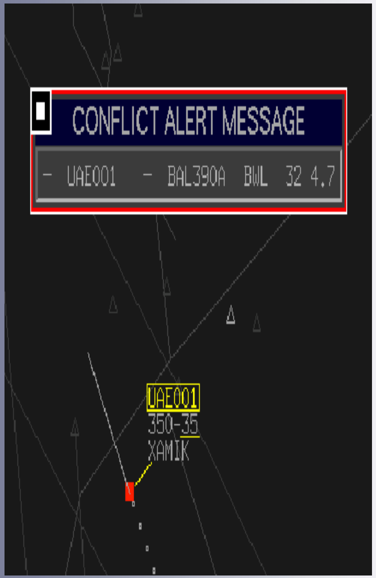
- W32.Stuxnet multi-component malware
  - Attacks Programmable Logic Controllers (PLCs);
- Stuxnet has up to 4 zero-day exploits:
  - ATM very vulnerable to this…
  - Unusual range of languages (C/C++) team?
  - Used 2 legit Taiwanese digital signatures…
- Command & control servers identified:
  - Located in Malaysia and Denmark;
  - 155 countries, 40,000 IP addresses.

W32.STUXNET, March 2010

- Monitors frequency of attached
  - attacks systems operating 807-1210 Hz.
- Triggers a state machine to hide ‘sabotage’;
  1. Wait13 days;
  2. Set maximum frequency to 1410 Hz;
  3. Wait 27 days
  4. Set maximum frequency to 2 Hz;
  5. Set maximum frequency to 1064 Hz;
  6. Go to 1.
- Clever… pathological failure modes.

keylogger:
Predator and Reaper GCS
Creech Airforce Base

GAO Review of FAA CyberSecurity



CONFLICT ALERT MESSAGE

- UAE001 - BAL390A BWL 32 4.7

“The FAA is ineffective in all areas including operational systems information security, future systems modernization security, management structure, policy implementation”.

“FAA is similarly ineffective in managing systems security for its operational systems and is in violation of its own policy”.

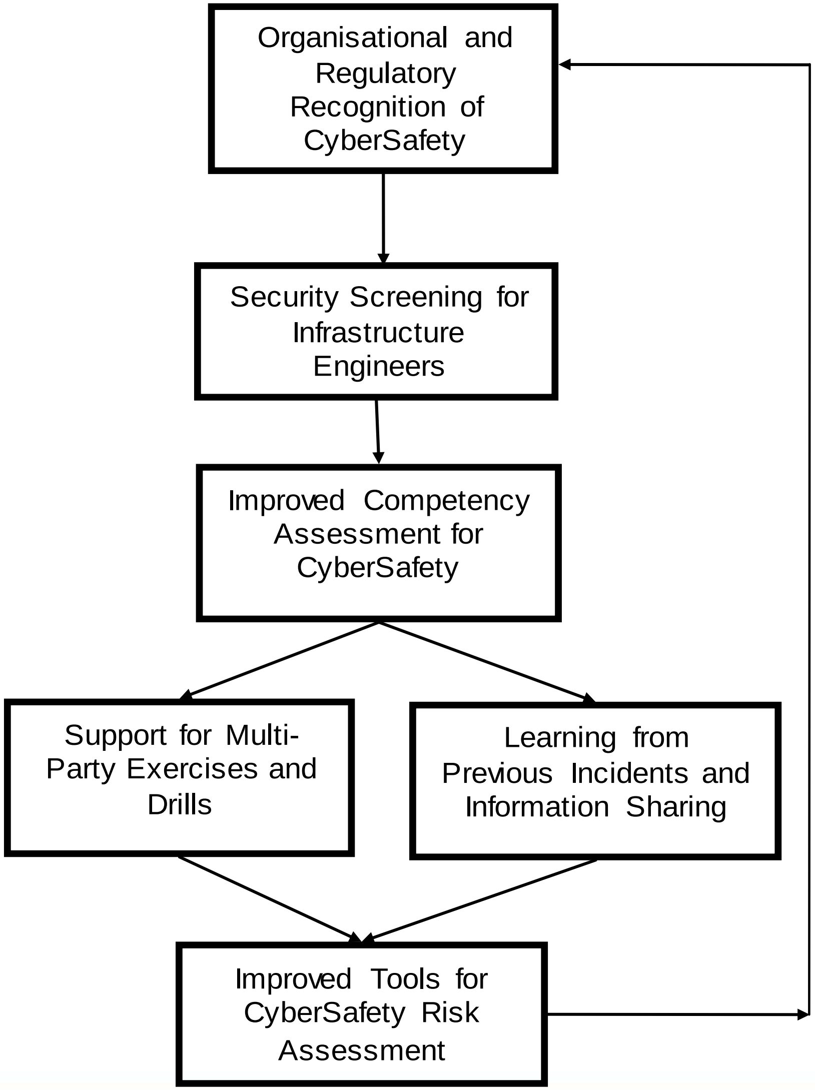
“They have performed the necessary for only 3 of 90 operational ATC computer systems, or less than 4%”

Paranoia?

- Coordinated attacks possible?
  - ATM is a dual-use infrastructure;
  - Chinese ‘active defense’;
  - Anonymity and plausible deniability.
- Who pays for security:
  - Private-public partnership?
- Many policies only exist on paper.
- Huge problem with complacency.

A Roadmap for CyberSafety

A Roadmap for CyberSafety



Organisational and Regulatory Recognition of CyberSafety
Security Screening for Infrastructure Engineers
Improved Competency Assessment for CyberSafety
Support for Multi-Party Exercises and Drills
Learning from Previous Incidents and Information Sharing
Improved Tools for CyberSafety Risk Assessment

Roadmap for CyberSecurity

- Some potential actions:

1. Contact CERTs/ENISA/NRAs;
2. Audit security policy and hold a drill;
3. Screening for staff and contractors;
4. Improve training and competency;
5. Assess safety risk of security violation…

Role for ENISA/EASA/EUROCONTROL…

enisa

European Network and Information Security Agency

ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR

November 2011

- Europe lags behind the United States
  - no surveys of ATM security practices;
  - 50-60% ACCs in last 12 months;
  - Virus in primary/secondary systems.

Summary

- ATM system complexity under SESAR:
  - Eg Software cannot be tested ‘completely’.
  - Bugs will remain and we must still be safe.

- Degraded modes, solution:
  - Rapid low cost risk assessment not just at procurement.

- Cyber-security, solution:
  - Act now, improve audit, training and drills.

Any Questions?