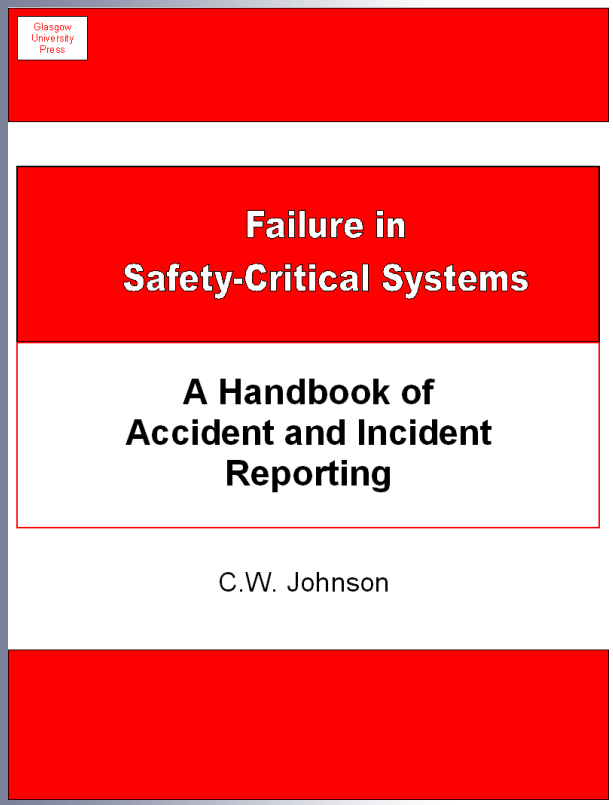
Review of Accident and Incident investigation Models and Alternative Techniques from Various Industries…

Prof. Chris Johnson, Marco Sarconi and Yvon Le Saint
School of Computing Science, University of Glasgow, Scotland.
http://www.dcs.gla.ac.uk/~johnson

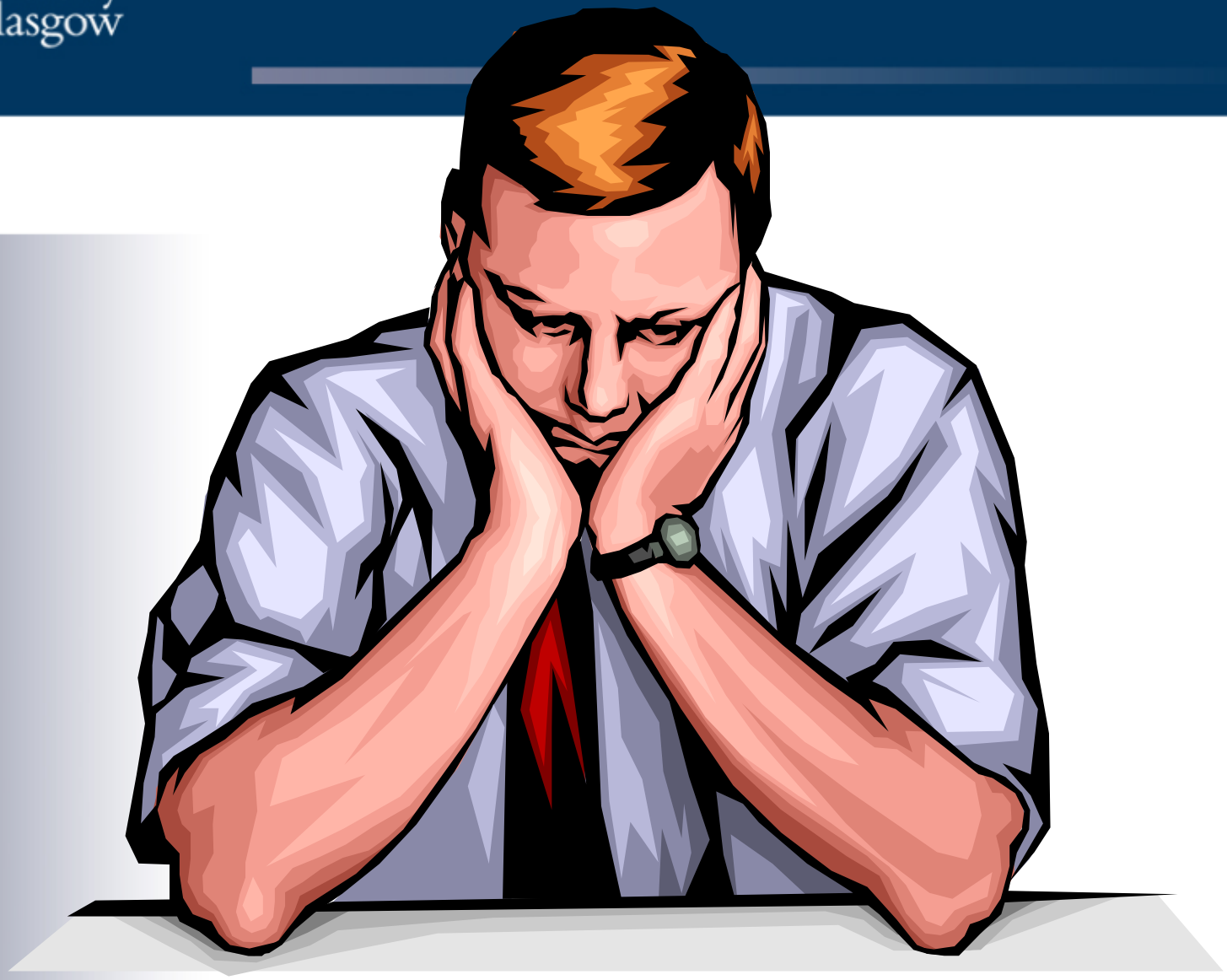
21st November 2013.

Previous Expertise



- Experience in:
  - Accident/Incident analysis in rail & aviation;
  - Reviewing Accident Methodologies (ERA, ENISA, EUROCONTROL, USAF, NASA)
  - Transfer of tools and techniques in Healthcare, Aerospace, and Military etc.
- http://www.dcs.gla.ac.uk/~johnson

University of Glasgow

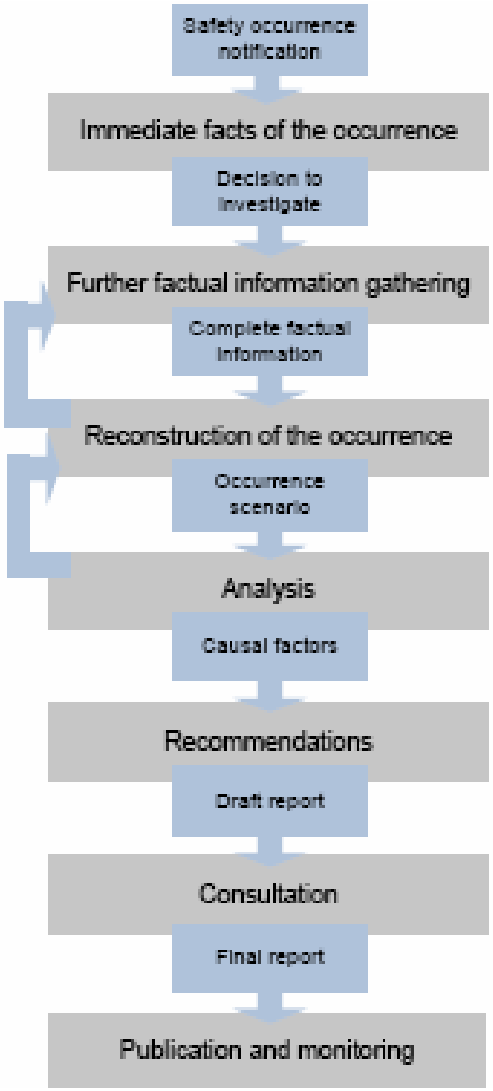


University of Glasgow

Overview

- Introduction and background.
- Part One:
  - On the Need for ATM Engineering Incident Reports.
- Part Two:
  - The Impact of the CyberSecurity Directive (2013).
- Part Three:
  - ATM Sub-orbital debris and AIRPROX models.

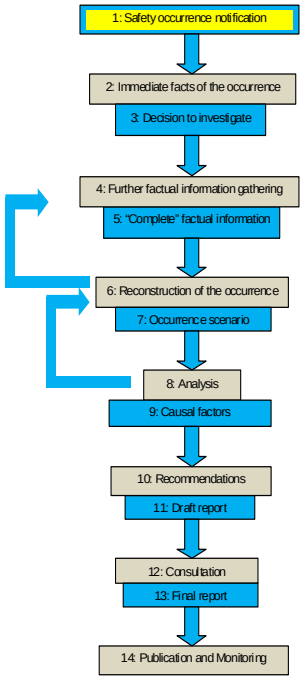
Guiding Principles: Support All Phases



ERA Generic Occurrence Investigation Process

Identifying Tools, Methods and Techniques

Accident Analysis Framework,
Accimaps (Rasmussen)
Accident Investigation Training Course (UK Rail)
Adverse Incident Tracking System, see AITS
Adverse Event Reporting System, (US Food and Drugs Administration)
Australian Incident Monitoring System, see AIMS
ATSB Aviation Safety Action Programme
Aviation Safety Reporting System (ASRS, National Transportation Safety Board)
ABCA Coalition Operations Lessons Learned Database,
Australian Office of Transport Safety Investigations, Confidential Safety Reporting Information Scheme
Barrier Analysis,
Bayesian Analysis
Bayesian Networks
Bias,
Biomechanical models
Canadian National Defence General Accident Information System, and Safety Digest,
Case-based reasoning
Causal trees
Counterfactual reasoning
Cause-context summaries
Cause-Consequence Models[1]
CD-ROM
Chain of events
Change Analysis
Chat Rooms
Checklists
Confidential Incident Reporting System (CIRS)
Cockpit Voice Recorders,
Composite Risk Management (CRM)
Computerised Accident Incident Reporting System (CAIRS)
Conclusion, Analysis and Evidence diagrams, (CAE)
Confidential Human Factors Incident Reporting Programme (CHIRP)
Confidential Incident Reporting and Analysis System (CIRAS)
consequence assessment
Cooperative Compliance Programme (OSHA's)
CREAM
Cryptography
Current Reality Tree
Databases
Data Mining
Data Recorders
Data Reporting Analysis and Corrective Action System (DRACAS)
Decision Theory
DesktopVR
Dynamic Querying
Decision Trees
Domino Theory
Eindhoven Classification Model,
Electronic mail
Enhanced Cognitive Interviews for Rail Investigations
European Space Agency Alert System,
EUROCONTROL Risk Assessment Worksheets
Event trees
Events and Causal Factor Charts (ECF)
Failure Modes, Effects and Criticality Analysis (FMECA)
Failure Reporting, Analysis and Corrective Actions (FRACAS)
Fault trees
Fax machines
Five Whys
Flight Operations Quality Assurance programmes
Flowchart
Formal methods
FRA Highway-Rail Crossing Web Accident Prediction System,
FRA Confidential Close Call
GEMS, Generic Error Modelling
Generic Occurrence Classification
Global Aviation Information Network (GAIN)
Goal Structured Notation (GSN)



HAZOPS
HEIDI
Heinrich Ratio
Human Reliability Analysis
Iceberg model
Incident Analysis Method for Railway Safety Management
International Nuclear Event Scale
Japanese Maritime Incident Reporting System
Joint Center for Lessons Learned
Kepner-Tregoe Problem Analysis
Kjellen's criteria
Latent failure
Likelihood Assessment
Logic,
Causal Logic, Deontic Logic, Explanatory Logic,
First Order Logic, Modal Logic, Temporal Logic,
Major Hazard Incidents Data Service (MHIDAS)
Management Oversight and Risk Trees (MORT)
Manufacturer and User Facility Device Experience database (MAUDE)
Multilinear Events Sequencing (MES)
MTO (human, technology and organisation) Japanese Rail Accident Method
National Patient Safety Agency, see NPSA National Patient Safety Database
Non-Compliance Analysis
PARDIA (WBA)
Performance Shaping Factors
Petri Nets
Peturbation Theory, P-Theory (part of MES/STEP)
Physical Reconstructions
Prevention and Recovery Information System for Monitoring and Analysis (PRISMA)
PRISMA-Rail
Precursor Indicator Model
QuicktimeVR
Rail-Program for Risk Informed Safety Managements
Railway Technical Research Institute (RTRI) type accident analysis method
Rail Data Recorders
Reason Root Cause Analysis Tools
Safety Cases
Safety Management Information System
Sequentially Timed and Events Plotting (STEP)
SHELL
Simulations
Skills, Knowledge, Rules (Rasmussen)
Skybrary Accident Information and Safety Information System
SMORT
Safety by Organisational Learning (SOL)
Systems Theoretic Accident Model and Processes (STAMP)
Systemic Causal Analysis Technique (SCAT)
Systematic Accident Scenario Analysis (SASA)
Systemic Safety Management System[1]
Taproot[1]
Theory of Constraints (TOC, Zotov, …)
Time-lines
Toulmin's Argumentation Structures
Technique for the Retrospective and Predictive Analysis of Cognitive Errors: TRACEr-rail version
Tripod
Tripod-Beta, Tripod-Delta
US Air Force Automated Security Incident Measurement
US Army 5 stage model
US Air Force 8-Step Problem Solving Methods
Virtual Reality
VRML
Why Because Analysis (WBA)
Witness Guidelines, (US Department of Justice)
Westrum's Taxonomy
World Wide Web
Worst Plausible Outcome
Yellow Book (Guidance on UK Rail Accident Analysis)

Distribution of Techniques

- Step 1: Safety occurrence notification (22 out of 130)
- Step 2: Immediate facts of the occurrence (17 out of 130)
- Step 3: Decision to investigate
- Step 4: Further factual information gathering (28 out of 130)
- Step 5: Complete factual information
- Step 6: Reconstruction of the occurrence (30 out of 130)
- Step 7: Occurrence scenario
- Step 8: Analysis (67 out of 130)
- Step 9: Causal factors
- Step 10: Recommendations (33 out of 130)
- Step 11: Draft report
- Step 12: Consultation (20 out of 130)
- Step 13: Final report
- Step 14: Publication and Monitoring (23 out of 130)

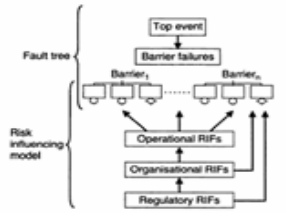
Template-Based Comparisons

B

Barrier Analysis

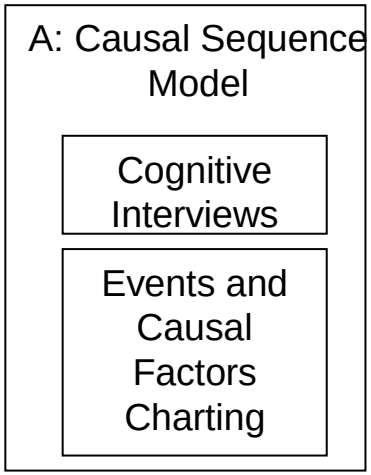
Evaluation Criteria	Assessment
Name of the method/tool/technique	Barrier Analysis
References to the method/tool/technique	W.A. Trost and R.J. Nertney, Barrier Analysis, August 1995, SCIE-DOE-01-TRAC-29-95, US Dept of Energy. http://www.jklld.net/trac29.pdf E. Albrechtsen and P. Hokstad, An Analysis of Barriers in Train Traffic Using Risk Influencing Factors, Page 25-31. In Safety and reliability: Proceedings of ESREL 2003, European Safety and Reliability Society, Annual Conference. Edited by T. Bedford, P. H. A. J. M. van Gelder
Other names or speciality names	Originally part of MORT analysis but now a more general technique.
Primary objective of the method/tool/technique: the original purpose or function of the method/tool/technique	Barriers are important for the understanding and prevention of accidents in two different, but related, ways. Firstly, the very fact that an accident has taken place means that one or more barriers have failed – either because they did not serve their purpose adequately or because they were missing or dysfunctional. The search for barriers that have failed should therefore be an important part of accident analysis. Secondly, once the aetiology of an accident has been determined and the causal pathways identified, barriers are used as a means to prevent that the same, or similar, accidents take place in the future. In order to facilitate this, the consideration of barrier functions should be a part of system design[2].
A description of the process which must be followed to apply the method/tool/technique –this description is a digest of information drawn from the references or subject matter experts	"Barrier Analysis" was written to support the total MORT Programme. It is a reminder to the system safety person or the accident investigator that there are three factors to be considered when evaluating an accident or a potential accident situation. Those three factors are (1) the energy or environmental condition present, (2) the target, the person or object of value and (3) the barrier and control, those things that are in place or should be in place to keep the energy and the targets apart". The following figure illustrates different types of barriers. Barriers Control: • Control of wanted energy flows; Examples: • Conductors • Approved work methods • Job training • Disconnect switch • Pressure vessel Safety: • Control of unwanted energy flows; Examples: • Protective equipment • Guardrails • Safety training • Work permit • Emergency plan

[2] http://www.it.uu.se/research/project/train/papers/AccidentAnalysis.pdf

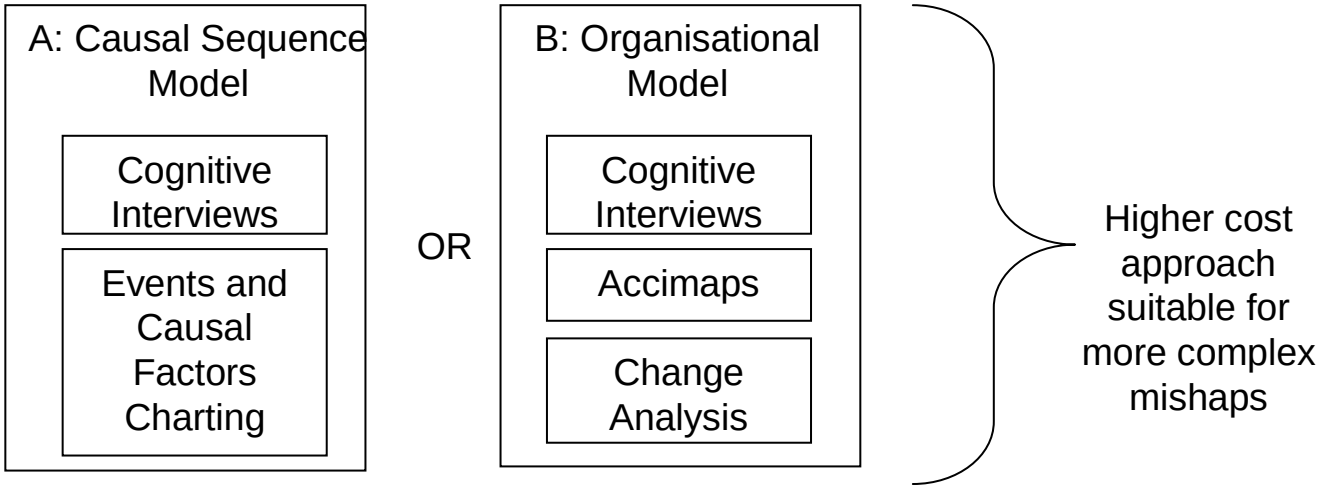
	
An indication for which of the phases in the generic occurrence investigation process (Figure 1) it could be applicable	Step 8: Analysis Step 9: Causal factors Step 10: Recommendations Step 11: Draft report
Has the method/tool/technique previously been applied in railway occurrence investigations, or could it be adapted to the railway context?	Yes, see citation above and similar examples in the ESREL collection.
Alternative, overlapping or complementary method/tool/technique, e.g. methods/tools/techniques that can be used preliminary or successively to the method/tool/technique	MORT, Fault Tree Analysis.
An indication whether the method/tool/technique is in use	Yes, it is in widespread use in many industries around the globe – taught as part of many engineering courses and as can be seen above has been integrated with fault tree analysis closing loops between incident investigation and hazard analysis/design.
Computer tools that can support application of the method/tool/technique	Barrier analysis is a conceptual approach that has been integrated into a number of different tools but the generic nature of the ideas mean the actual version implemented differs greatly from tool to tool.
Evidence of successful application of the method/tool/technique	Considerable evidence of successful use of the tool.
The required level of expertise to apply the technique: is it relatively easy to understand and use? Is specific training needed?	There are different flavours of Barrier Analysis – the basic concepts are easy to pick up but training is offered by a range of companies to use the approach in conjunction with other techniques such as MORT or FTA.
The degree to which the technique lends itself to reviewable documentation	In most instances the products of Barrier Analysis are easy to comprehend and can be represented in a range of visual forms, even for complex systems.
The consistency of the technique, such that if used on two occasions by independent investigators, reasonably similar results are derived	It remains a relative subjective approach – there are choices to be made both in the nature of appropriate barriers – technological, procedural etc and also where they might be deployed in design or where they failed in an accident hence some disagreement might be expected -
Any restrictions on application, e.g. problem scale, generality, accuracy, ease of use, cost, availability, maturity, use of resources, data requirements, etc.	Barrier analysis is amongst the most mature techniques for accident investigation and has many benefits in terms of the number of case studies and training courses.
Do the tools and techniques provide equal benefits for both small and large member states?	In this case, training investments for smaller organisations are probably justified in terms of the benefits reported by previous applications of the approach.
Do the tools and techniques provide support for all aspects of a failure (Human, organisational, technical) in equal measure or must they be integrated with other approaches?	In it's generic form Barriers take many forms – including procedural and organisational although there is controversy about how much we can rely on these and other human factors measures.
Can the tools and techniques provide credible support for the future requirements given increasing complexity and integration in railway operations?	Yes, barrier analysis remains a significant approach as a precursor to some more recent ideas in resilience engineering and so will most likely offer support into the

Recommended Approaches

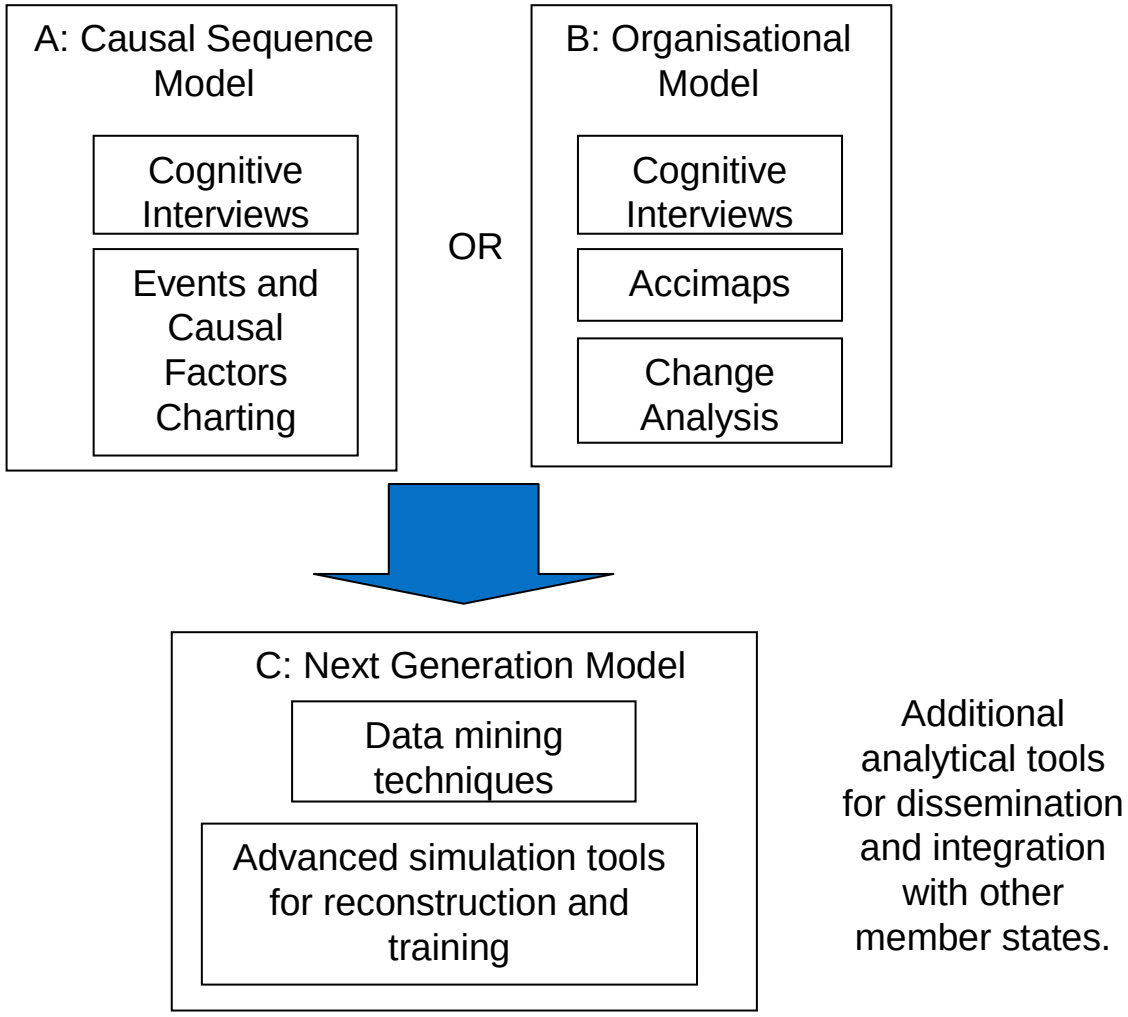
Low cost approach intended for simpler mishaps.



Recommended Approaches



Recommended Approaches



Additional analytical tools for dissemination and integration with other member states.

University of Glasgow

Edsger W Dijkstra (1930-2002)

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

University of Glasgow

Overview

- Introduction and background.
- Part One:
  - On the Need for ATM Engineering Incident Reports.
- Part Two:
  - The Impact of the CyberSecurity Directive (2013).
- Part Three:
  - ATM Sub-orbital debris and AIRPROX models.

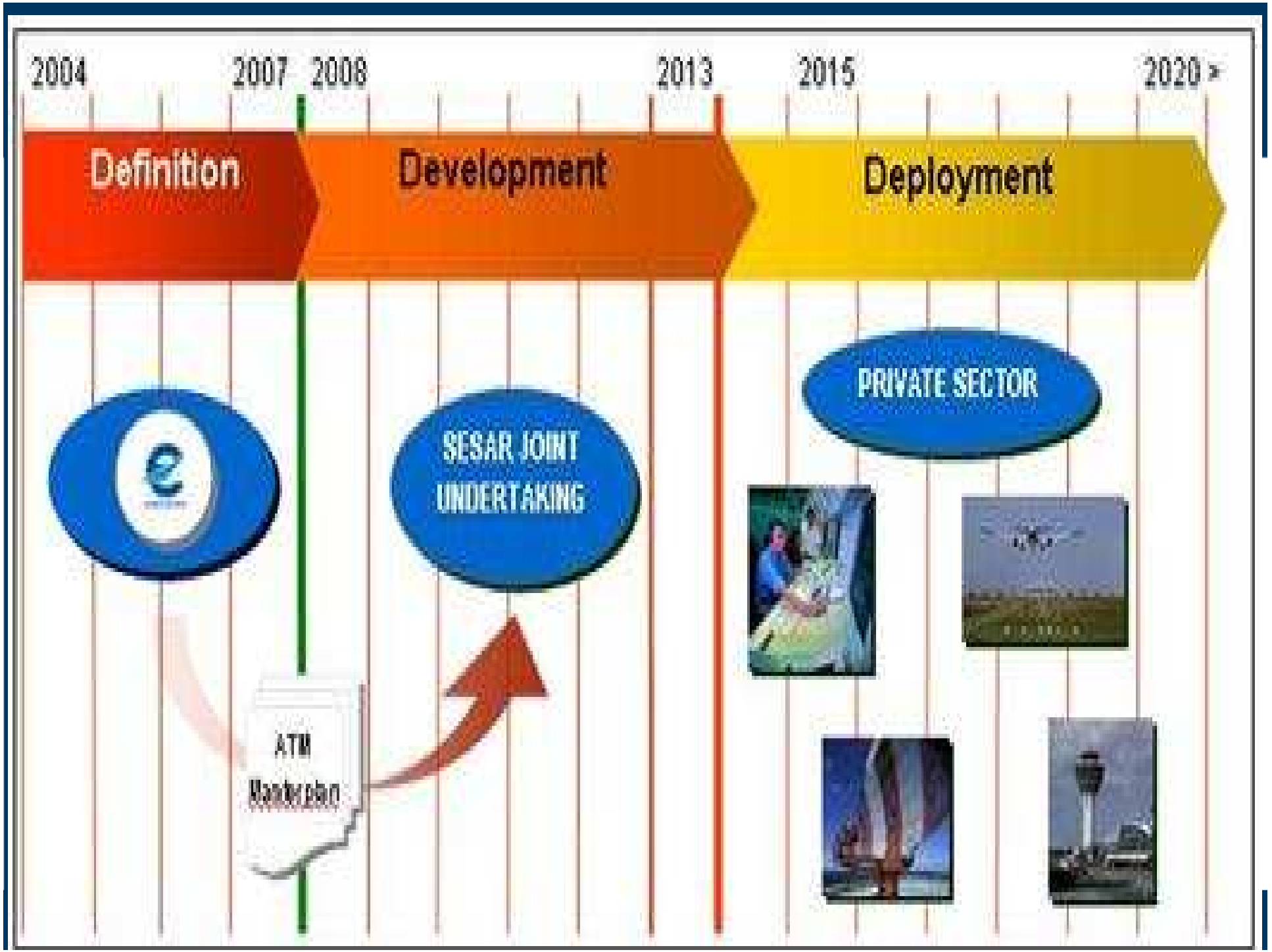
IRISH AVIATION AUTHORITY
ÚDARÁS CITLÍOCHTA NA hÉIREANN

REPORT OF THE IRISH AVIATION AUTHORITY

INTO THE ATM SYSTEM MALFUNCTION AT DUBLIN AIRPORT

19th September 2008

CONTENTS


2004
2007
2008
2013
2015
2020 >
Definition
Development
Deployment
SESAR JOINT UNDERTAKING
PRIVATE SECTOR
ATM Masterplan

Need ATM Engineering Incident Exchange

- 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

NextGen and SESAR as Root Causes?

- $2.1 Billion upgrade:
  - 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

Reliability in Cloud Infrastructures

- **Two months, 1 million users:** October 2009 T-Mobile's Sidekick users lost contacts, calendars, photos when Microsoft subsidiary Danger suffered a server failure.
- **Permanent data loss, over 6,300 users:** 1-4th July 2010, Evernote hardware failure, loss of data.
- **Four days, 35,000 users:** February 2011 Gmail accounts and Google Apps customers lost all the data in the accounts. Google had to resort to restoring backups from tapes, in an operation lasting 4 days.
- **Several hours, service-wide:** 6,11 and 15 August 2008, Google's enterprise e-mail system, Apps Premier Edition, outage affected nearly all users for 2 hours; some were affected for 24 hours.
- **30 minutes, service-wide:** September 2011, Google Docs, Google Docs List and Google went offline for 30 minutes, affecting all its users.
- **72 hours, as big as 70m users:** Millions of Blackberry users across Europe, Middle East and Africa suffered outage for 3 days in October 2011. Speculation is that most of global customer base (70m users) were affected at some point during 72 hours.

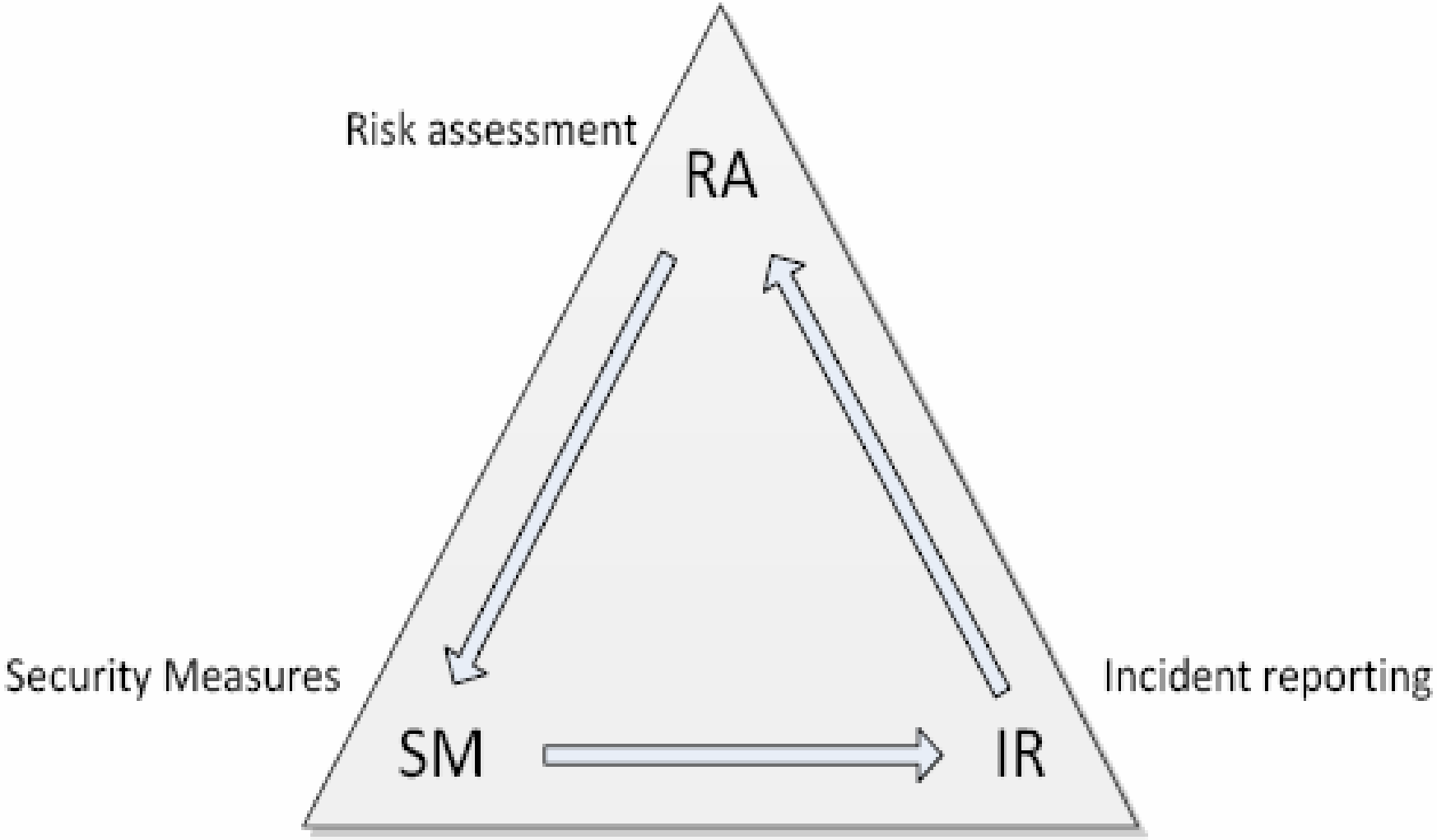
University of Glasgow

Overview

- Introduction and background.
- Part One:
  - On the Need for ATM Engineering Incident Reports.
- Part Two:
  - Impact of the proposed CyberSecurity Directive (2013).
- Part Three:
  - ATM Sub-orbital debris and AIRPROX models.

University of Glasgow

Security Governance Processes



University of Glasgow

How Not to Impress a Regulator

- Regulator receives radar data for airpprox.
- ANSP and regulator use same player.
- ANSP ROM contains conficker.
- Regulator warns ANSP:
  - They claim player is obsolete anyway…
  - `no further investigation' at this time?

GAO Review of FAA CyberSecurity

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

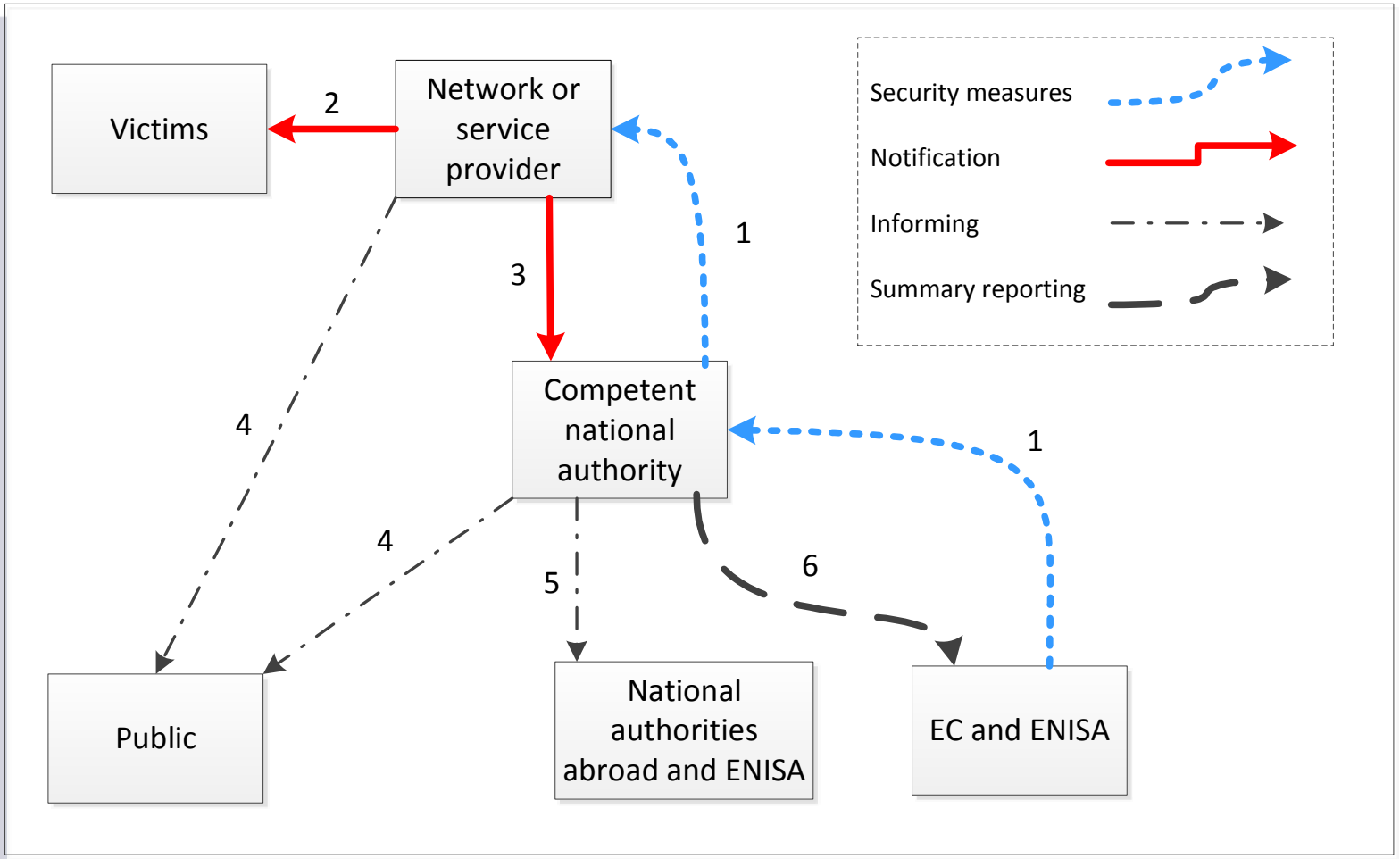
"performed the necessary analysis to determine system threats, vulnerabilities, and safeguards for only 3 of 90 operational ATC computer systems, or less than 4%".

Intrusion detection in 11 of 300 ATM facilities.

Article 13a of the Telecoms Directive (2009)

- Article 13a Electronic Telecommunications Framework Directive (2009/140/EC).
  - NRAs ensure ecomms providers guarantee security and resilience of electronic communication networks and services;
  - Providers of comms services must report significant incidents to competent authorities (NRAs);
  - NRAs must provide a summary of significant incidents to ENISA and the EC.

What Exists Today… System We Designed

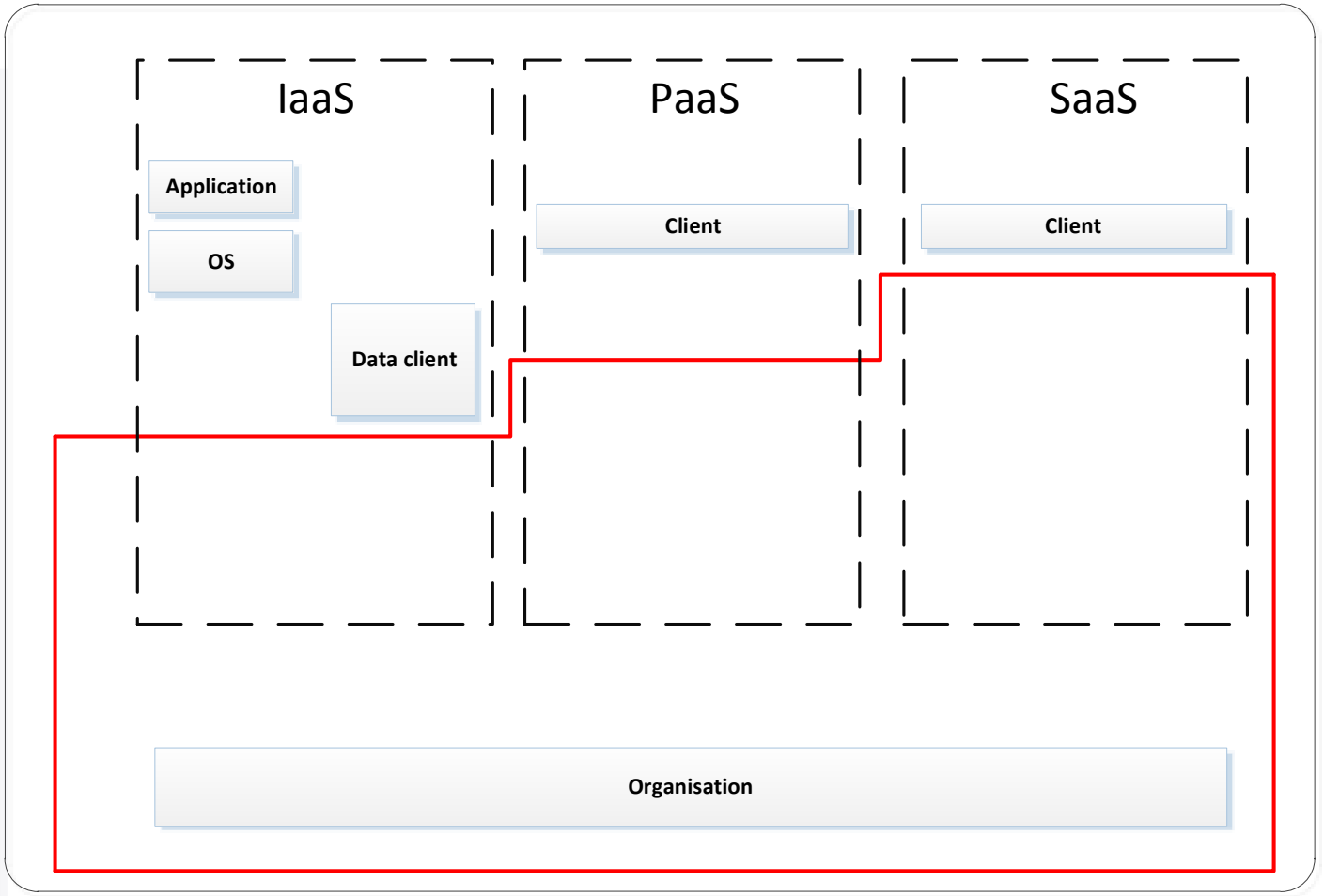


University of Glasgow

ENISA Critical Cloud Incident Reporting

enisa

Skyguide and the Virtual Center…



Proposed CyberSecurity Directive (2013)

- Article14 applies to:

(a) providers of information society services which enable the provision of other information society services;

(b) operators of critical infrastructure which is essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health.

Future Issues: Cyber Insurance: 1st Party Risk

- *First party risk:*
  - Loss or damage to digital assets;
  - Business interruption;
  - Cyber extortion;
  - Reputational damage;
  - Theft of money and digital assets.
- Third party cyber risks:
  - Security and privacy breaches;
  - Investigation of privacy breach;
  - Customer notification expenses;
  - civil damages/defamation;
  - Loss of third party data.

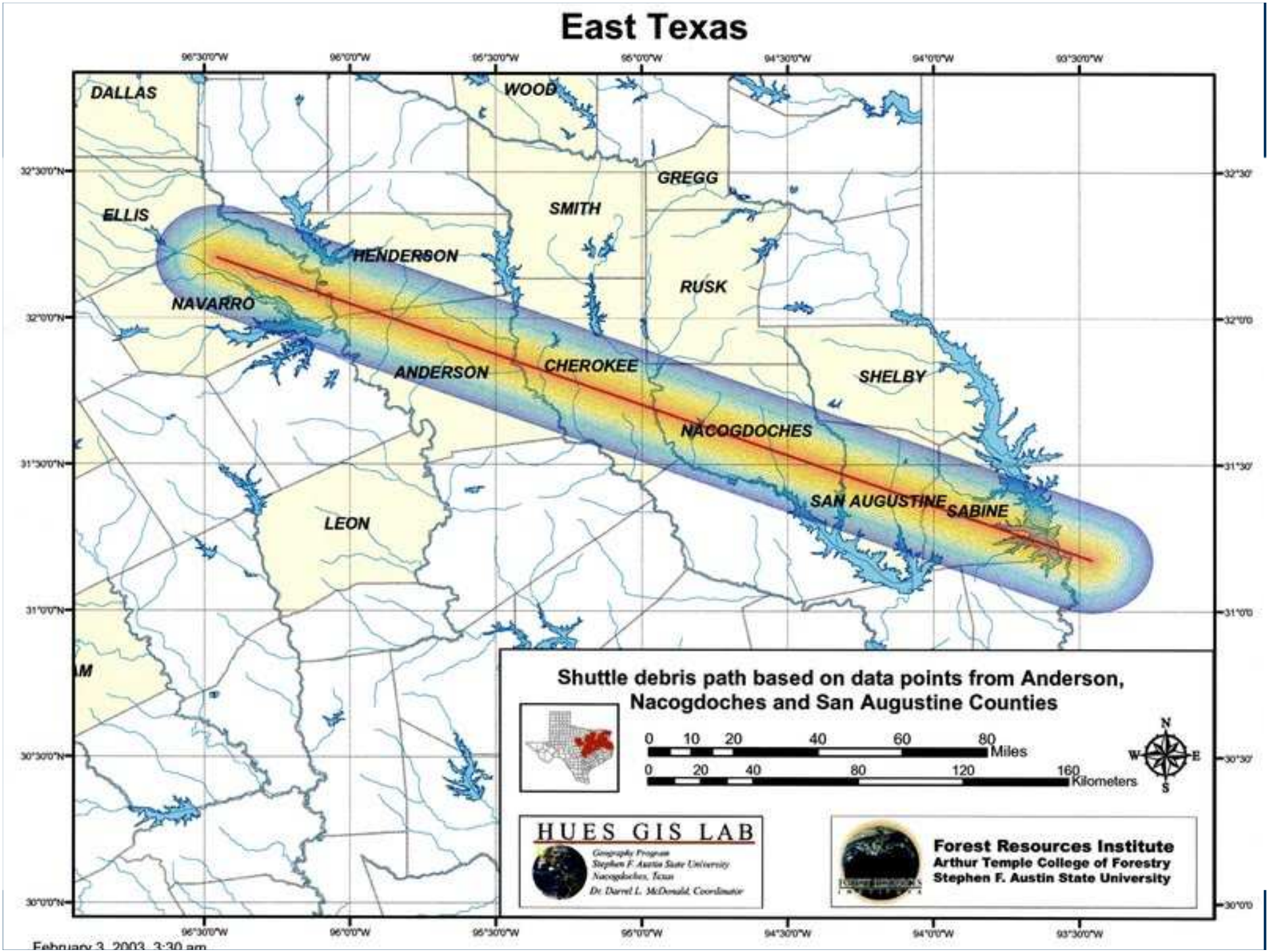
Future Issues: Cyber Insurance

- Cloud services face a number of concerns.
- Most existing policies will not cover them.
- Lack of information:
  - About customer apps/ data (3rd party?);
  - Little actuarial data (incident reporting).
- “Cyber hurricane”:
  - Multiple claims in single incident destroy market?

University of Glasgow

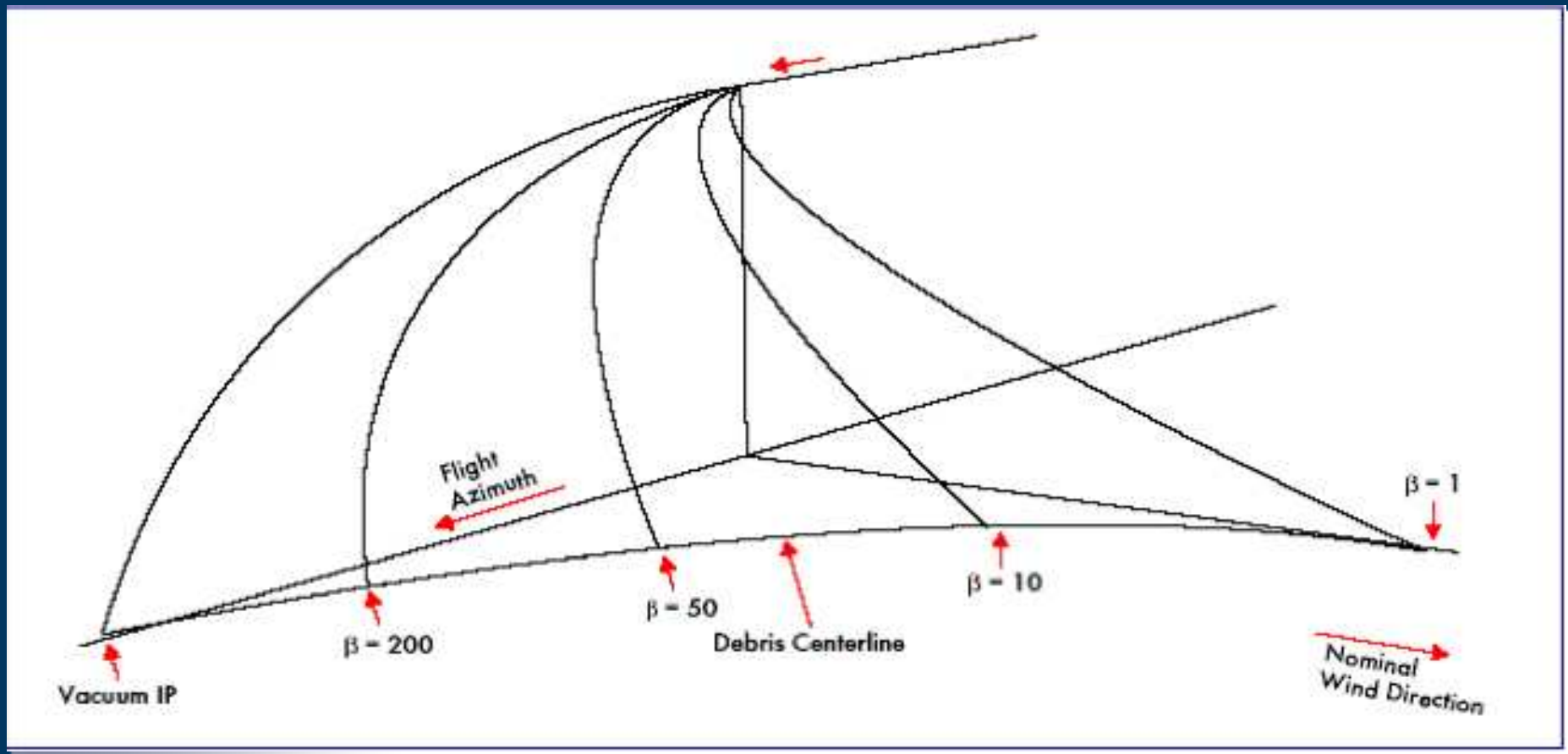
Overview

- Introduction and background.
- Part One:
  - On the Need for ATM Engineering Incident Reports.
- Part Two:
  - Impact of the proposed CyberSecurity Directive (2013).
- Part Three:
  - ATM Sub-orbital debris and AIRPROX models.


East Texas
DALLAS
WOOD
GREGG
SMITH
ELLIS
HENDERSON
RUSK
NAVARRO
ANDERSON
CHEROKEE
SHELBY
NACOGDOCHES
SAN AUGUSTINE
SABINE
LEON
Shuttle debris path based on data points from Anderson, Nacogdoches and San Augustine Counties
0 10 20 40 60 80 Miles
0 20 40 80 120 160 Kilometers
N
W
E
S
HUES GIS LAB
Geography Program
Stephen F. Austin State University
Nacogdoches, Texas
Dr. Darrel L. McDonald, Coordinator
Forest Resources Institute
Arthur Temple College of Forestry
Stephen F. Austin State University
February 3, 2003, 3:30 am

University of Glasgow

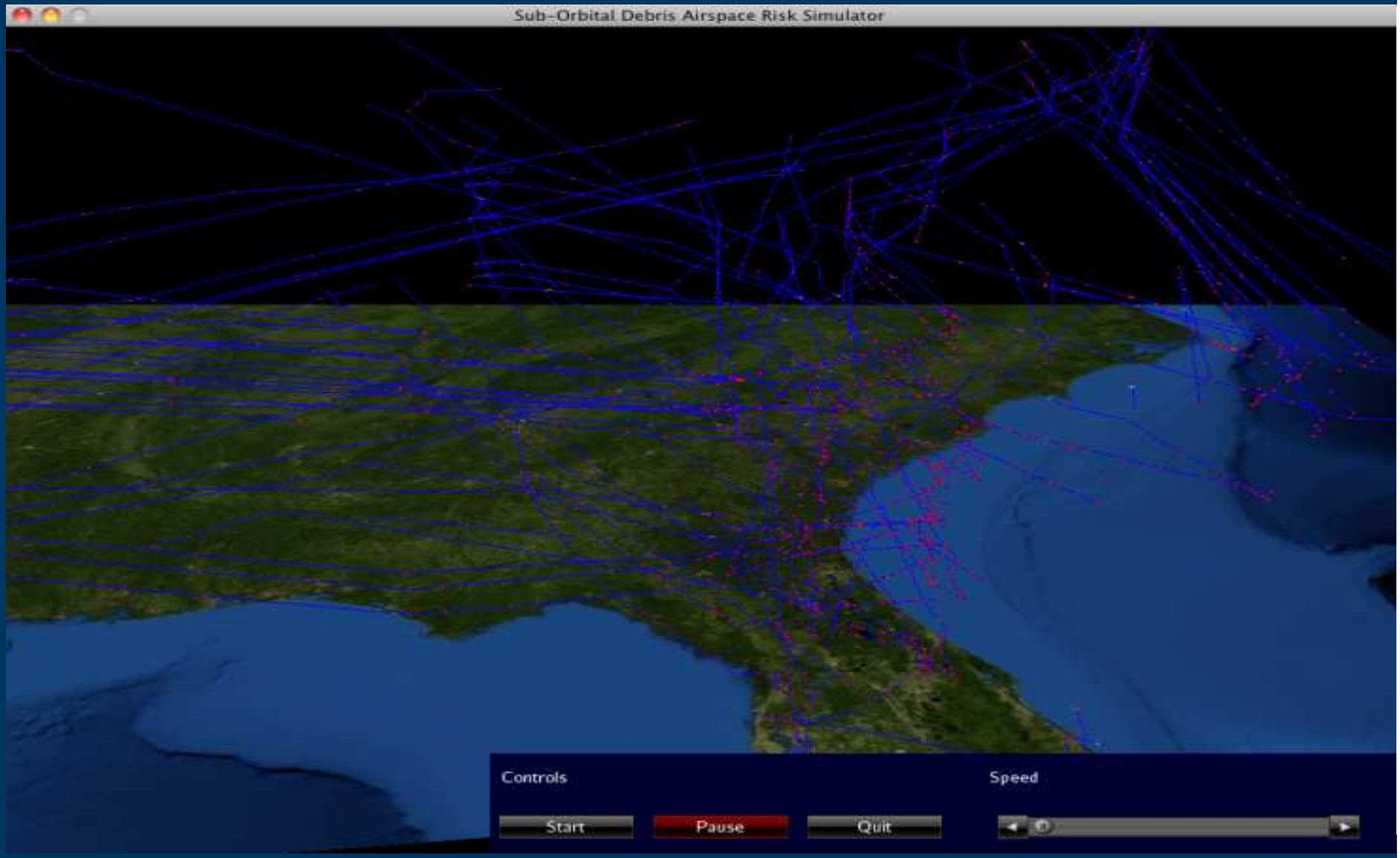
Debris Model



- The influence of the ballistic coefficient, β , and wind upon debris impact points (CAIB Report, 2003).

University of Glasgow

Visualization



University of Glasgow

Present Work

University of Glasgow

Present Work

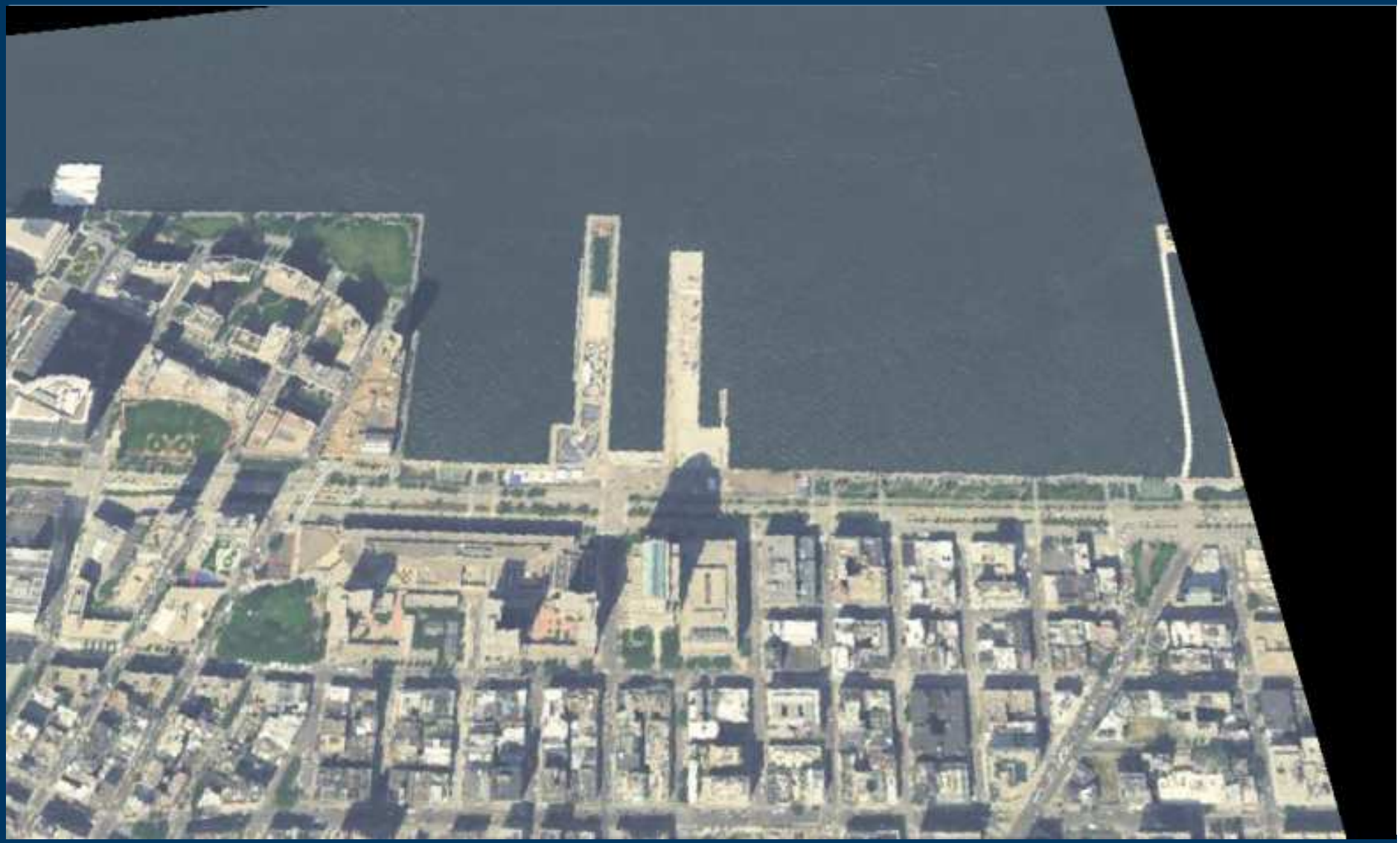
University of Glasgow

Present Work

- 4 October 1992, El Al Flight 1862.
  - Boeing 747 El Al cargo plane;
  - Hits Groeneveen and Klein-Kruitberg flats.
- 43 killed:
  - 3 crew, non-revenue passenger in a jump seat,
  - 39 people on the ground
- Worst aviaition accident in Netherlands:
  - plane exploded, starts large fire after the crash.

University of Glasgow

Present Work



University of Glasgow

Overview

- Introduction and background.
- Part One:
  - On the Need for ATM Engineering Incident Reports.
- Part Two:
  - Impact of the proposed CyberSecurity Directive (2013).
- Part Three:
  - ATM Sub-orbital debris and AIRPROX models.

University of Glasgow

Any Questions?