MORT and Organisational Failures

Prof. Chris Johnson,

School of Computing Science, University of Glasgow.

johnson@dcs.gla.ac.uk

http://www.dcs.gla.ac.uk/~johnson
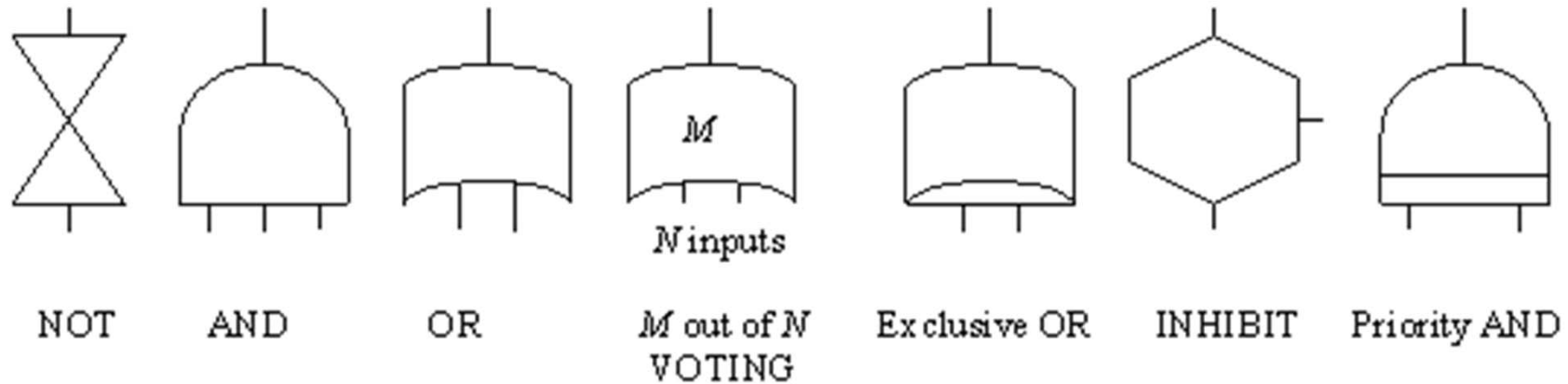
University of Glasgow

- **Organisational Failure.**
  - Are safety culture & standards sufficient?
  - Need high level management support.

- **MORT:**
  - Management Oversight & Risk Tree;
  - maps generic concerns for safety management.

- **Dublin Airport Case Study.**
  - Limits on what management can do?
  - Can they understand technical systems?

- **Standards supported by**
  - Safety Management Systems.

- **Safety culture defended by**
  - Safety Management Systems.

- **Without managerial support:**
  - safety culture will die;
  - standards will be abused.

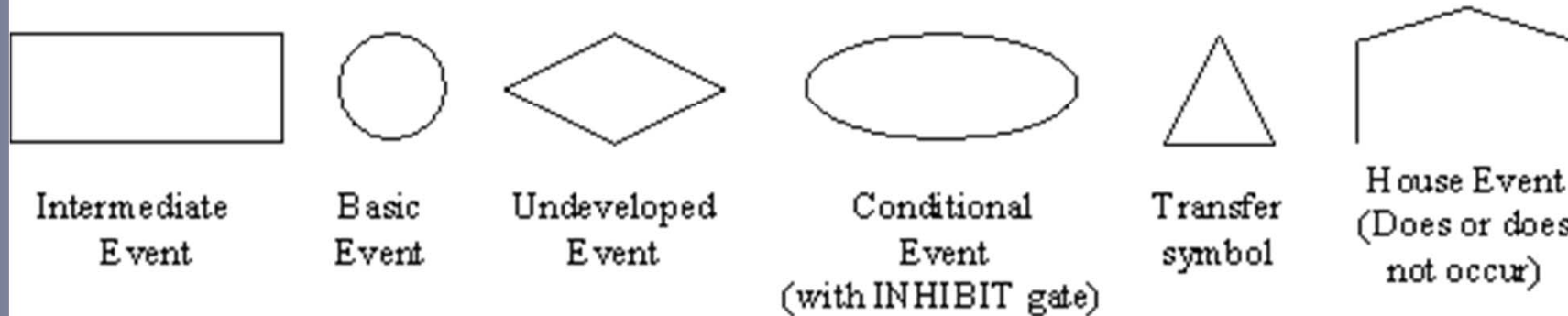- **Limits – financial not engineering background**

Organisational Failure

- Increasing focus on management.

- Standards can be miss-applied?

- Incidents can be ignored?

- Management controls context of failure?

University of Glasgow

- Management Oversight and Risk Tree.

- Draws on management and safety.

- Based on fault-tree notation:
  - AND, OR gates;
  - Basic and intermediate events.

- Novel use of LogicWorks 8(

Fault Tree Gates
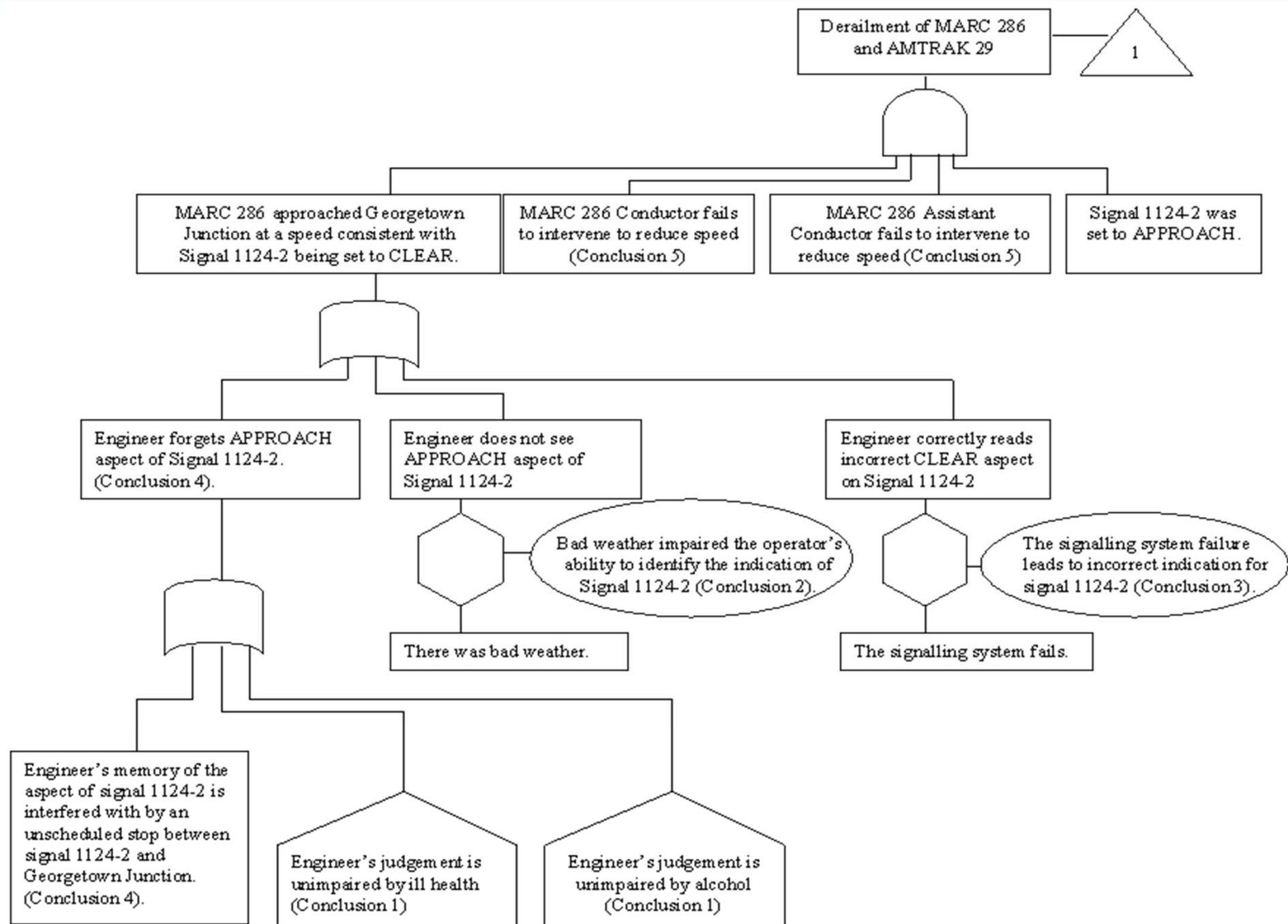
NOT AND OR *M* out of *N* VOTING Exclusive OR INHIBIT Priority AND

Intermediate Event Basic Event Undeveloped Event Conditional Event (with INHIBIT gate) Transfer symbol House Event (Does or does not occur)

Fault Tree Events

Derailment of MARC 286 and AMTRAK 29

1

MARC 286 approached Georgetown Junction at a speed consistent with Signal 1124-2 being set to CLEAR.

MARC 286 Conductor fails to intervene to reduce speed (Conclusion 5)

MARC 286 Assistant Conductor fails to intervene to reduce speed (Conclusion 5)

Signal 1124-2 was set to APPROACH.

Engineer forgets APPROACH aspect of Signal 1124-2. (Conclusion 4).

Engineer does not see APPROACH aspect of Signal 1124-2

Bad weather impaired the operator's ability to identify the indication of Signal 1124-2 (Conclusion 2).

Engineer correctly reads incorrect CLEAR aspect on Signal 1124-2

The signalling system failure leads to incorrect indication for signal 1124-2 (Conclusion 3).

There was bad weather.

The signalling system fails.

Engineer's memory of the aspect of signal 1124-2 is interfered with by an unscheduled stop between signal 1124-2 and Georgetown Junction. (Conclusion 4).

Engineer's judgement is unimpaired by ill health (Conclusion 1)

Engineer's judgement is unimpaired by alcohol (Conclusion 1)
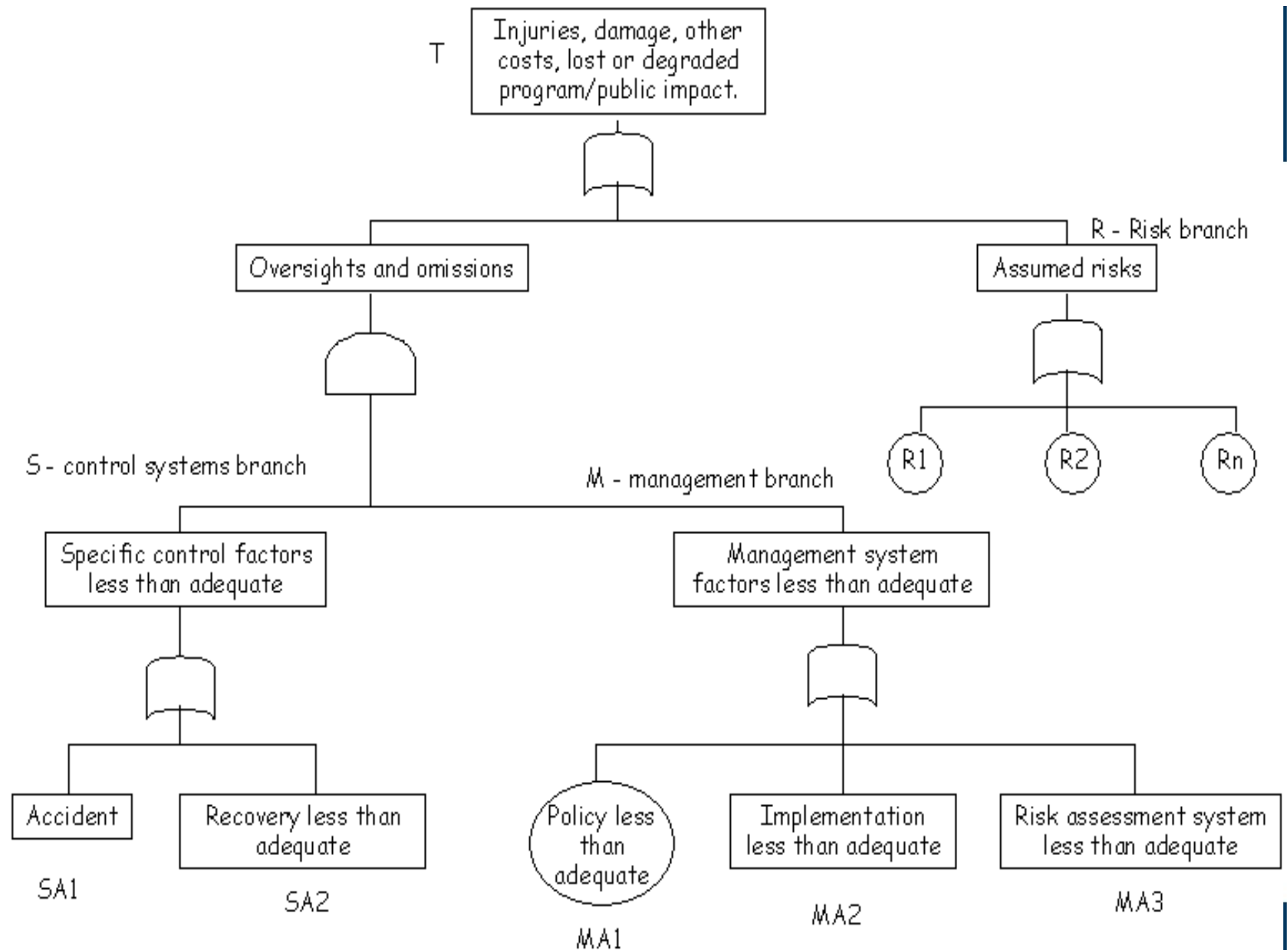
- Lets suppose we have an incident.

- Usually easy to spot direct causes?

- Operator error, system failure.

- How to identify managerial causes?

- MORT uses fault tree notation to provide a graphical checklist.

T	**Injuries, damage, other costs, lost or degraded program/public impact.**	R - Risk branch

Oversights and omissions

Assumed risks

S - control systems branch

M - management branch

R1 R2 Rn

Specific control factors less than adequate

Management system factors less than adequate

Accident

Recovery less than adequate

Policy less than adequate

Implementation less than adequate

Risk assessment system less than adequate

SA1

SA2

MA1

MA2

MA3

- **Illustrates problems of safety management.**
  - 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.**

REPORT OF THE IRISH AVIATION AUTHORITY

INTO THE ATM SYSTEM MALFUNCTION AT DUBLIN AIRPORT

19th September 2008

CONTENTS

- **ATM system provided by contractor:**
  - maintained under annual service contract;
  - provide both hardware and software support;
  - Preventative maintenance of components;
  - On-site support for diagnosis and debugging.

- **ANSP relies upon subcontractor:**
  - key areas of technical support ;
  - lacks sufficient in-house capability;
  - Is outsourcing a form of de-risking?

- **First symptoms observed:**
  - aircraft id & type not displayed by flight tracks;
  - but only for flights entering system...

- **ANSPs engineering staff correct symptoms;**
  - Cannot identify root causes of the problem.

- **Capacity restrictions to maintain safety levels;**
  - Above operating demands so little impact?

- **Problem stemmed from double failure:**
  - triggered by a faulty network interface card;
  - flooded network with spurious messages;
  - delayed FDPS updates on network.

- **Symptoms of the fault were masked;**
  - recovery mechanisms in Local Area Network;
  - made it hard for engineering teams to identify initial component failure.
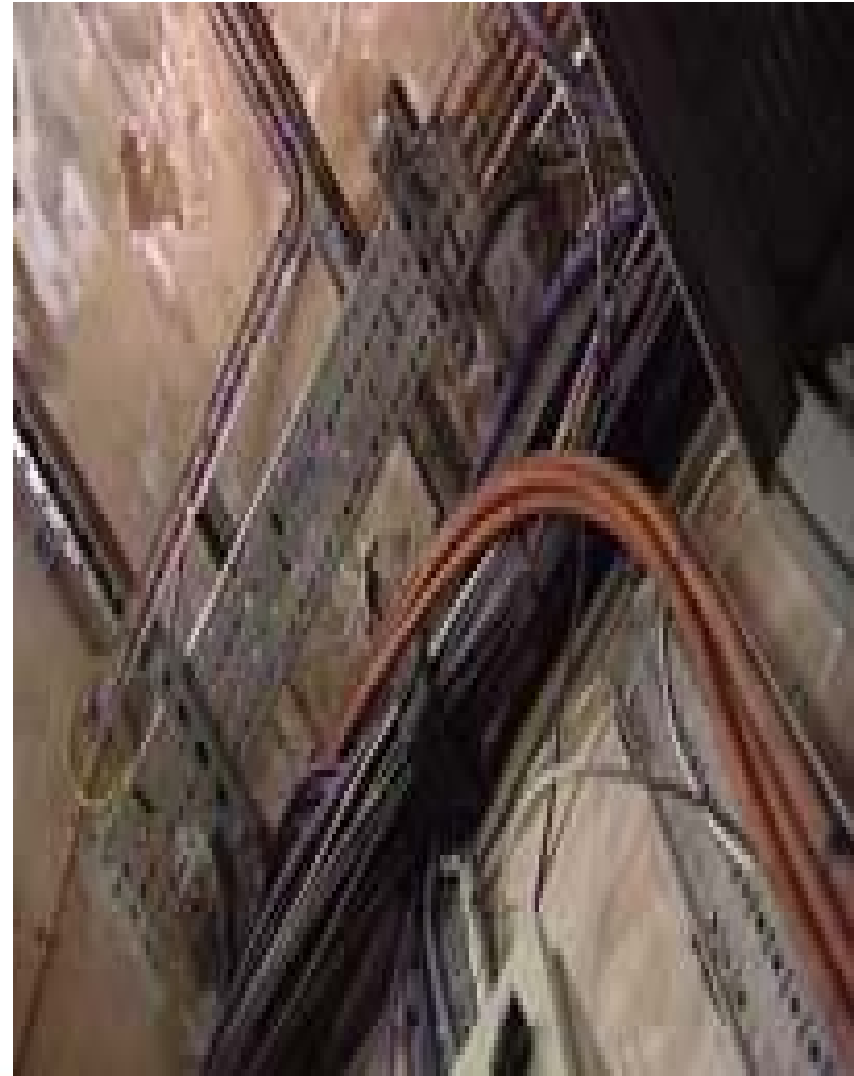
- ## Do management understand:
  - Computational problems?
  - Basics of safety (eg risk assessment)?
  - Consequences of technical issues?
  - Relaibility links to sub-contractors…

- ## The Ryanair effect:
  - Organizational damage enormous;
  - They are well managed and successful;
  - Things will only get more complex (SESAR).

- ## Organisational Failure.
  - Are safety culture & standards sufficient?
  - Need high level management support.

- ## MORT:
  - Management Oversight & Risk Tree;
  - maps generic concerns for safety management.

- ## Dublin Airport Case Study.
  - Limits on what management can do?
  - Can they understand technical systems?