Computer Aided Disaster
What Went Wrong?

Going beyond requirements-based testing

Mike Elliott
mre@m79.net
714 374-6453

AFTI F-16 Flight 44 – Edwards AFB

- 4 asynchronous DFCS
- Byzantine Generals
- Each decided others failed
- “The number of test conditions becomes so large that conventional testing would require a decade to complete . . . creating an untestable design”

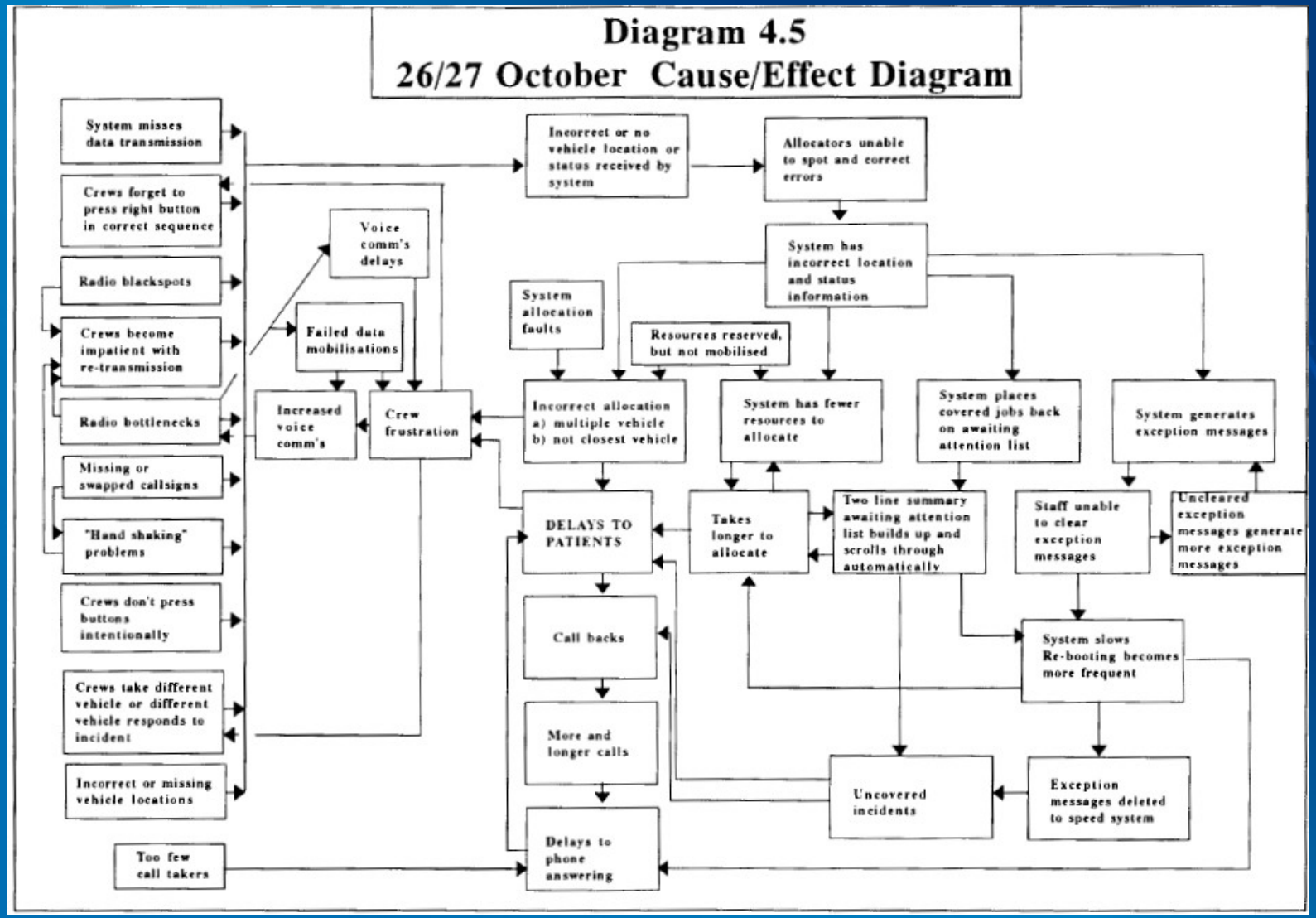
Patriot Missile Failure - Dhahran

- February 25, 1991
- 28 fatal
- 24 bit mantissa @ 10 Hz
- ~100 hours = ~0.34 seconds
- Scud speed ~= 1676 m/sec
- 600 meters difference
- Outside “range gate”
- Upgrade to some software parts, not others

London Ambulance Service

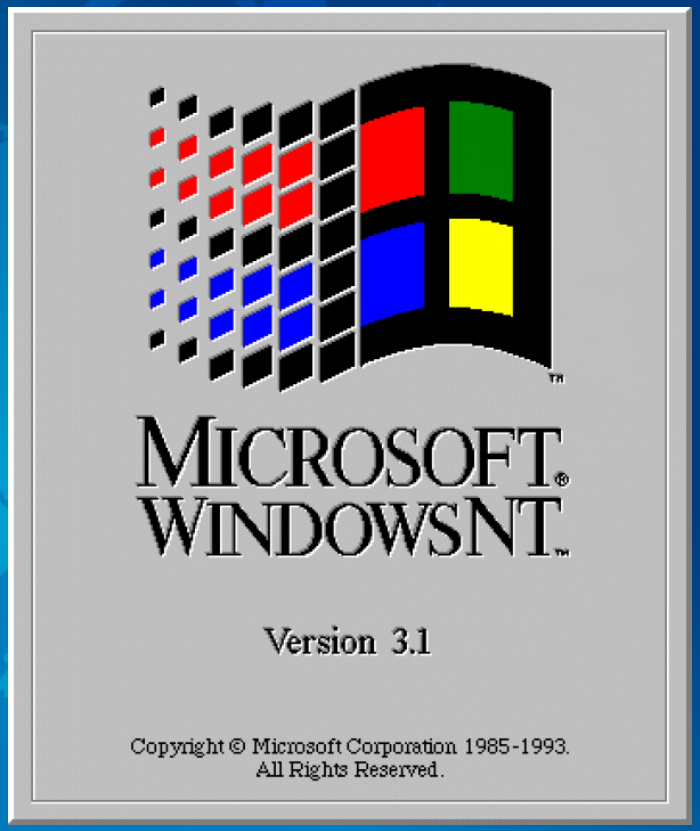
- October 26 – 27, 1992
- Computer-aided dispatch
- 10 – 20 fatalities (est.)
- Unqualified vendor
- Hostile stakeholders
- System overwhelmed
- Exception msgs. generated exception msgs.
- Backup specified but not present

Diagram 4.5
26/27 October Cause/Effect Diagram



Windows NT & LANMAN - Redmond

- Claimed 5000 yrs to crack
- mudge and hobbit
- L0pht Heavy Industries
- Win95 needed LANMAN
- NT 128 characters
- LANMAN 14 characters
- Break 7 chars in LM hash, not 14
- L0phtcrack 5 days
- Freely downloadable



- User's password converted to upper case,
- Null padded or truncated to 14 bytes, split into two 7-byte halves
- Values used to create 2 DES keys, one per half
- Each key encrypts the string **KGS!@#$%**
- Two cyphertext values concatenated to form 16 bit value.

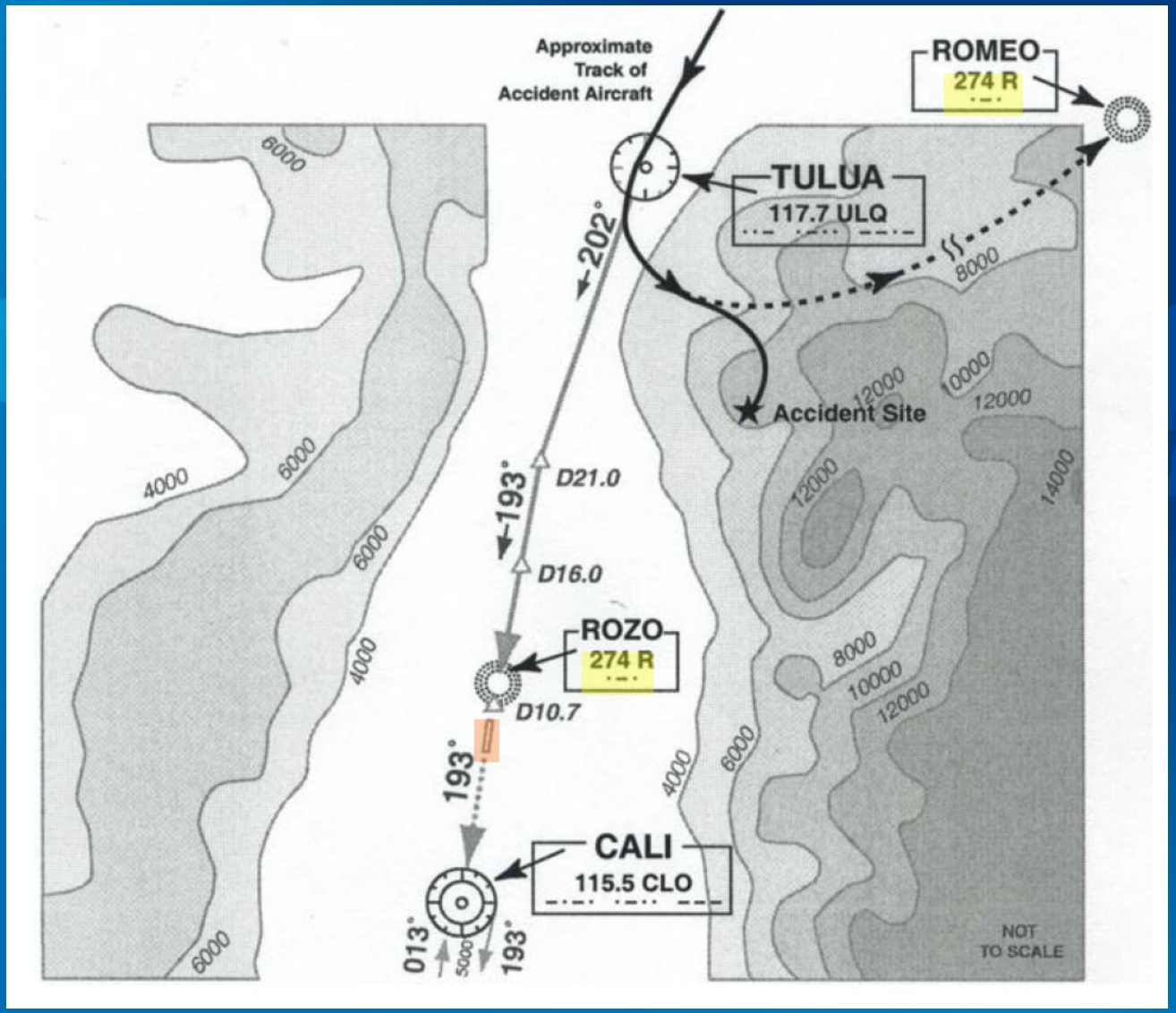
Lufthansa 2904 – Okęcie (Warsaw)

- September 14, 1993
- D-AIPN – Airbus A320-211
- EDDF – EPWA 11
- 2 fatal, 51 serious
- Thunderstorm, wind shear
- Right bank on landing
- 170 Kt, 770m on runway
- 9 sec. to left gear contact
- 12 tons & altitude < 3m
- Wheel rotation > 72kt

Lufthansa Airbus A.320-211 D-AIPN at Frankfurt 27 May 1990 , © Werner Fischdick

American 965 – Alfonso B. Aragón (Cali)

- December 20, 1995
- N651AA - Boeing 757-223
- KMIA – SKCL
- 160 fatal, 4 survivors
- 2 hours late – runway 01
- Cleared for 19 straight in
- Spoilers deployed
- TULUA VOR missed
- ROZO / ROMEO NDB (R)
- *El Deluvio*


Approximate
Track of
Accident Aircraft
ROMEO
274 R
TULUA
117.7 ULQ
202°
8000
Accident Site
12000
10000
12000
14000
193°
D21.0
D16.0
ROZO
274 R
D10.7
193°
CALI
115.5 CLO
013°
5000
193°
NOT
TO SCALE
6000
4000
6000
6000
4000
6000
4000
8000
10000
12000
6000

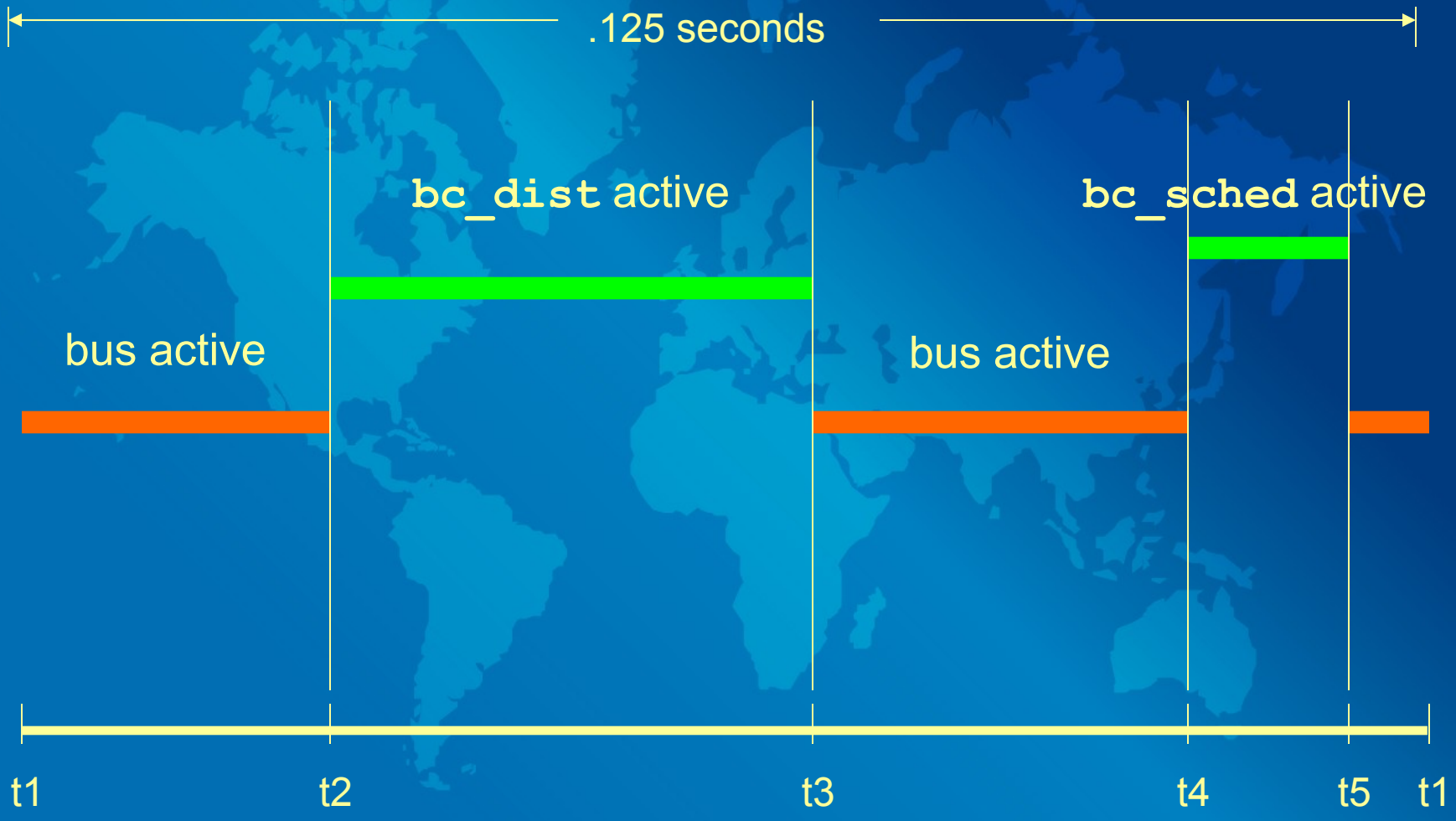
Ariane 501 – Kourou CSG

- June 4, 1996
- $500 million – uninsured
- Complete loss of guidance
- Convert from 64 to 16 bit
- Used once in Ariane 4
- Unnecessary for Ariane 5
- SRI not used after T–9
- Ran until T+50
- Exception not handled

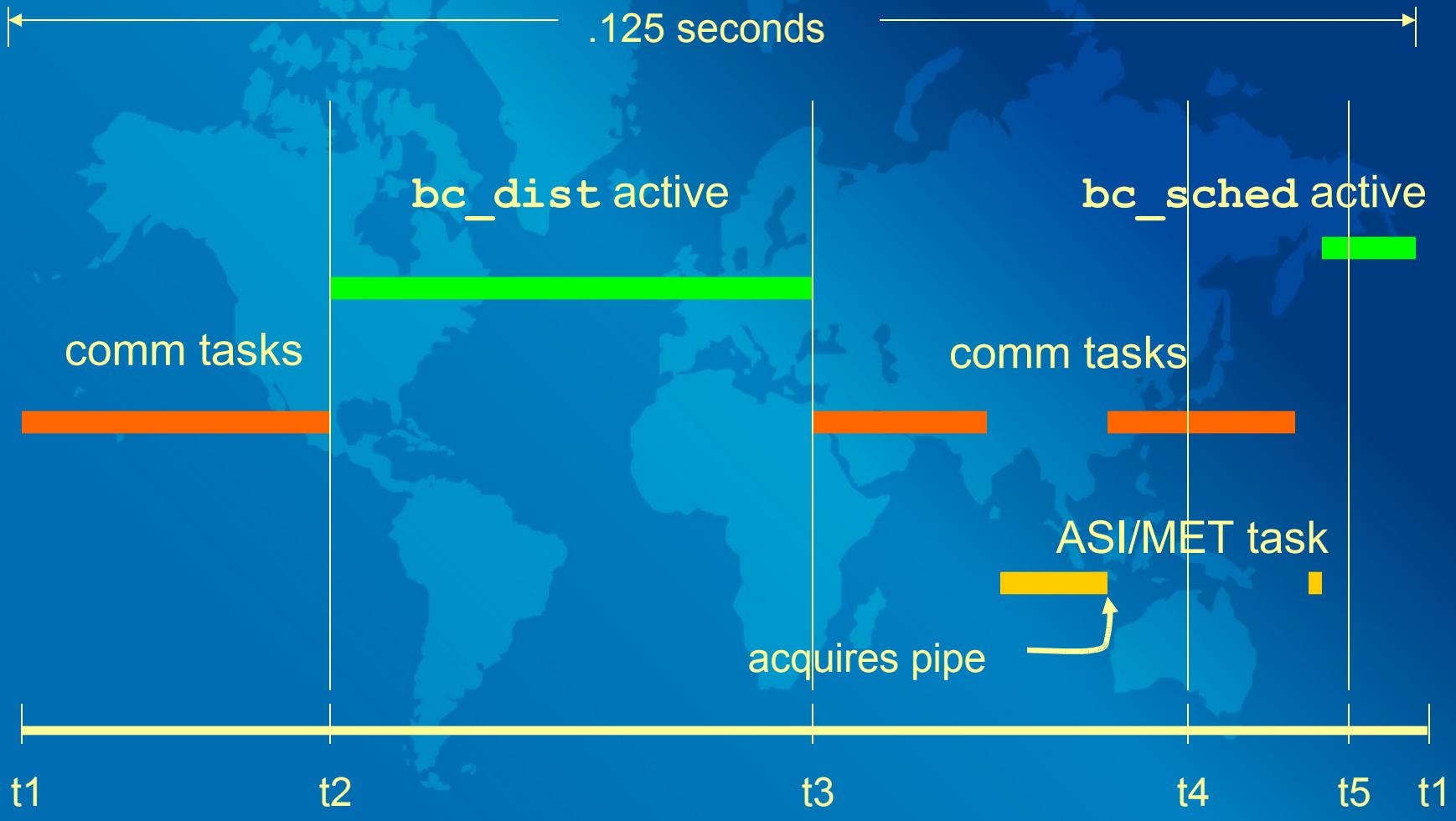
Mars Pathfinder - Mars

- July 4, 1997
- Dec. 4, 1996 - Delta II
- Software reset
- Antenna pointing success
- Bus monitoring tasks
- Communications tasks
- Meteorological tasks
- VxWorks port to RS6000
- Priority Inversion
- Fix uploaded successfully

bc_dist & bc_sched



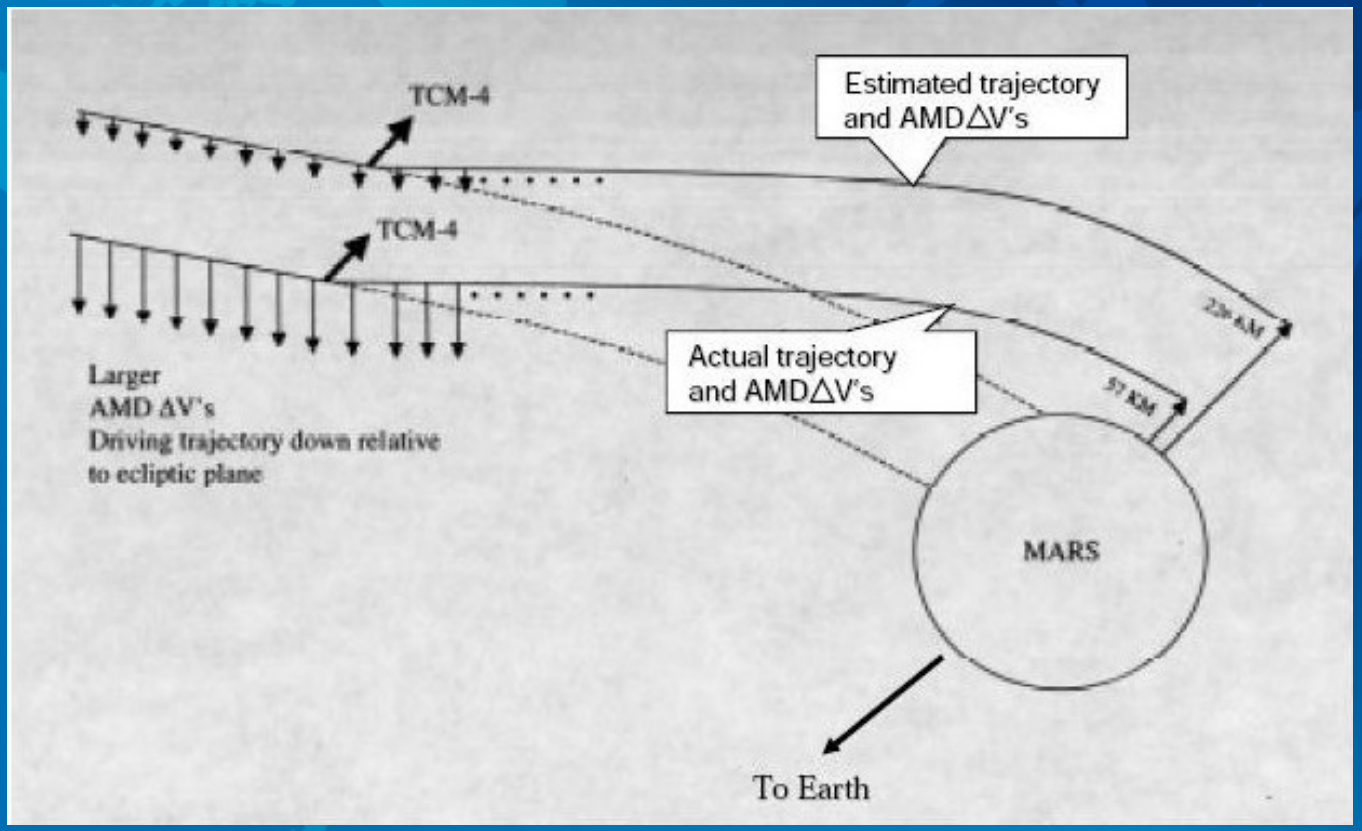
Priority inversion



Mars Climate Orbiter - Mars

- September 23, 1999
- Mars Surveyor Program
- Dec. 11 1998 Delta II 7425
- Skim Martian atmosphere
- English units used for thruster performance data
- Required to conform to MGS legacy interface
- 4.45 conversion – magic number

Schematic MCO Encounter Diagram



Mars Polar Lander - Mars

- December 3, 1999
- Mars Surveyor Program
- Jan. 3, 1999 Delta II 7425
- Entry, deployment, landing
- Sensors for surface contact
- Thrust off <50ms
- False signal at deployment
- Sensors enabled at 40m
- Engine shutdown
- 22 m/sec impact (est.)

Lufthansa – Frankfurt am Main

- March 20, 2001
- D-AIPW – Airbus A320-211
- EDDF
- Turbulence after rotation
- Left wing dipped 22˚ 0.5m
- FO: “I have control”
- FL 120 – reversed in roll
- Return to Frankfurt
- Elevator Aileron Computer
- Crossed pins during repair

Air Transat 236 – Santa Maria Oceanic

- August 24, 2001
- C-GITS – Airbus A330-243
- CYYZ – LPPT
- Terceira Lajes AFB
- Chafing fuel line
- Automatic fuel balancing
- ECAM anomalous oil system
- Dead-stick landing 80 nm
- Fuel on board = fuel at takeoff – fuel used

Virgin Atlantic 201 – Dutch airspace

- February 8, 2005
- G-VATL Airbus A340-642
- VHHH – EGLL (EHAM)
- Both FCMCs reset
- ECAM “FCMC2 FAULT”
- Engine 1 flameout
- 25000 kg remaining
- Master / slave

InGen security breach – Isla Nublar

- Jurassic Park
- August 12, 1989
- Trapdoors in system not detected
- Chief programmer stole frozen embryos
- Electric fences deactivated to facilitate escape and several important plot complications

USAF/USN - USS Ranger

- April 1, 2007
- USAF C-17 P234
- USS Ranger (CV-4)
- Block 22 (AAWS) too late
- Catapult inadequate
- Air Force inexperience
- Multiple suns
- Photoshop too pervasive
- Got to lighten-up

Untested requirements

- Windows NT password cracking
  - 5000 years – 5 days (1997)
- LAS computer aided dispatching
  - Backup specified but not present
  - General release of product with no live testing
- Mars Polar Lander crash
  - Leg deployment triggered engine shutoff
  - Reproducible after the fact

Human factors minimized

- System doesn’t work the way operators think
  - American 965 December 20, 1995
  - ROMEO is not ROZO – even though they’re both “R”
- Error messages are inadequate
  - Virgin Atlantic 201 February 8, 2005
  - FCMC2 FAULT does not mean “flameout imminent”

Unnecessary Requirements

- Ariane 5 aborted launch
  - Maiden flight June 4, 1996 – 37 seconds after launch
  - Software reuse error without requirement
- Mars Climate Orbiter
  - English units mixed with SI
  - Conformance to obsolete interface

Boundary conditions

- Mars Pathfinder software reset
  - Landed July 4, 1997
  - Priority inversion
- Patriot Missile failure to track
  - 10 Hz cumulative time
  - 32 bits into 24 bits

Missing requirements

- Side stick rewired improperly
  - Lufthansa A320 EDDF March 20, 2001
  - Fly by wire system failed to detect during pre-flight
- Ignore sensory input on deployment
  - Mars Polar Lander December 3, 1999
  - Leg extension not the same as touchdown
- Fuel equation not computed
  - Air Transat 236 August 24, 2001
  - `fuel remaining = starting - used`

Misguided requirements

- Airport runway overrun
  - Lufthansa 2904 EPWA September 14, 1993
  - Unable to apply spoilers, reverse thrust, wheel brakes

Untestable requirements

- AFTI – F16
  - Experimental version of the General Dynamics F16
  - Early (1978) Digital Flight Control System (DFCS)