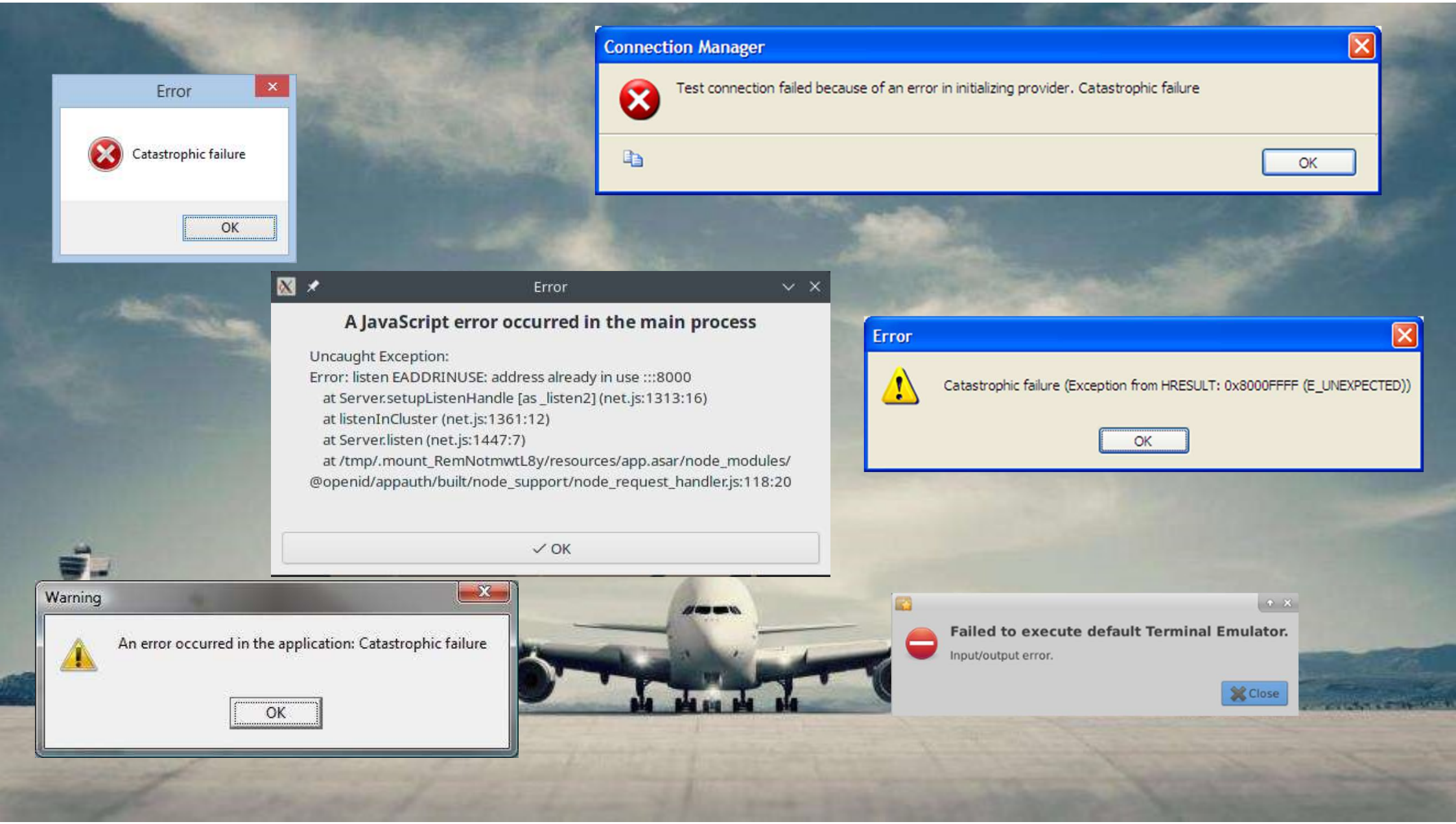
When Things Go Wrong in Software Development

Seminário MECT

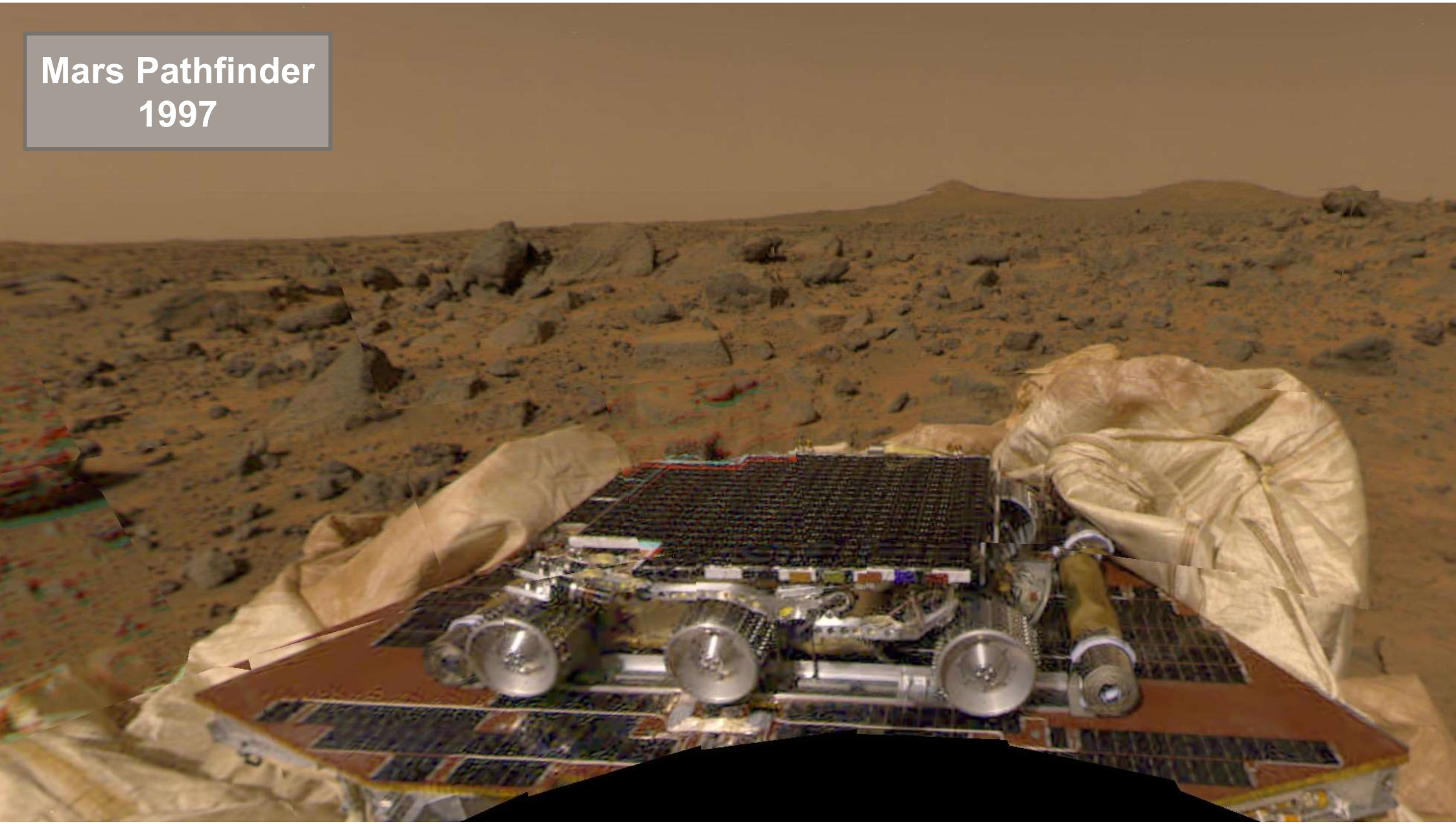
Date: 02/01/2024

CRITICALSOFTWARE.COM

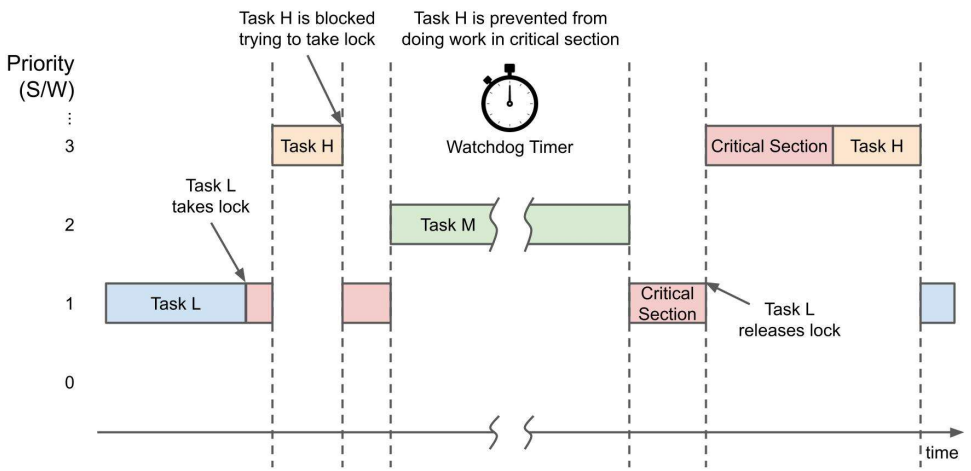

Error
Catastrophic failure
OK
Connection Manager
Test connection failed because of an error in initializing provider. Catastrophic failure
OK
Error
A JavaScript error occurred in the main process
Uncaught Exception:
Error: listen EADDRINUSE: address already in use :::8000
at Server.setupListenHandle [as _listen2] (net.js:1313:16)
at listenInCluster (net.js:1361:12)
at Server.listen (net.js:1447:7)
at /tmp/.mount_RemNotmwtL8y/resources/app.asar/node_modules/
@openid/appauth/built/node_support/node_request_handler.js:118:20
✓ OK
Error
Catastrophic failure (Exception from HRESULT: 0x8000FFFF (E_UNEXPECTED))
OK
Warning
An error occurred in the application: Catastrophic failure
OK
Failed to execute default Terminal Emulator.
Input/output error.
Close


Ariane 5
1996

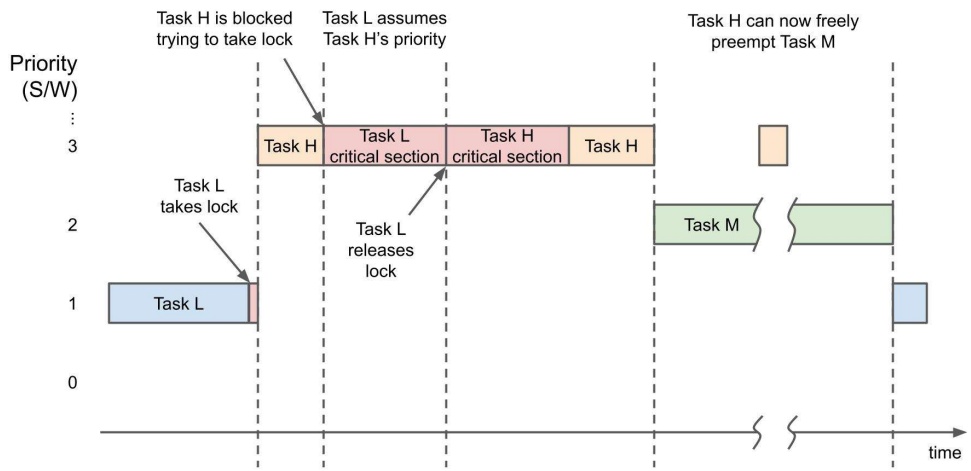
```
      L_M_BV_32 := TDB.T_ENTIER_32S ((1.0/C_M_LSB_BV) *
                                     G_M_INFO_DERIVE(T_ALG.E_BV));
      if L_M_BV_32 > 32767 then
         P_M_DERIVE(T_ALG.E_BV) := 16#7FFF#;
      elsif L_M_BV_32 < -32768 then
         P_M_DERIVE(T_ALG.E_BV) := 16#8000#;
      else
         P_M_DERIVE(T_ALG.E_BV) := UC_16S_EN_16NS(TDB.T_ENTIER_16S(L_M
      end if;

      P_M_DERIVE(T_ALG.E_BH) := UC_16S_EN_16NS (TDB.T_ENTIER_16S
                                     ((1.0/C_M_LSB_BH) *
                                     G_M_INFO_DERIVE(T_ALG.E_BH)))
   end LIRE_DERIVE;
```


Mars Pathfinder
1997

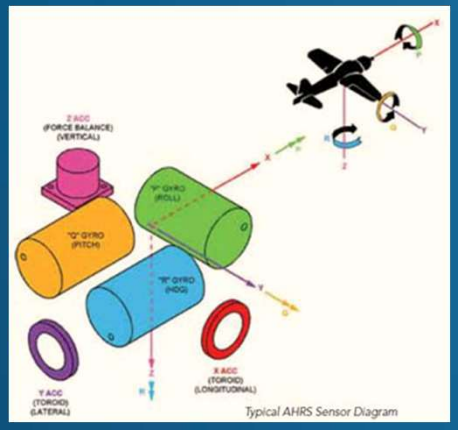
Unbounded Priority Inversion



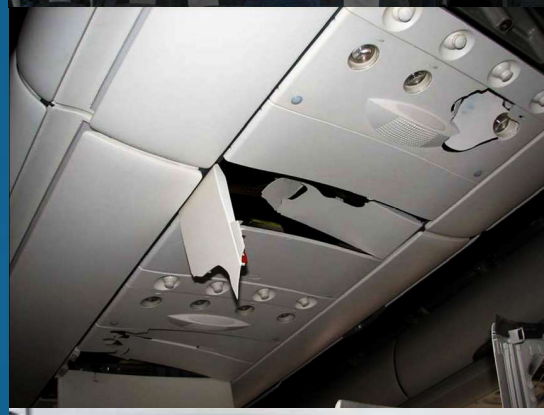
Priority Inheritance



Qantas QF72 (A330)
2008



Typical AHRS Sensor Diagram




Boeing 787
2015
787
BOEING

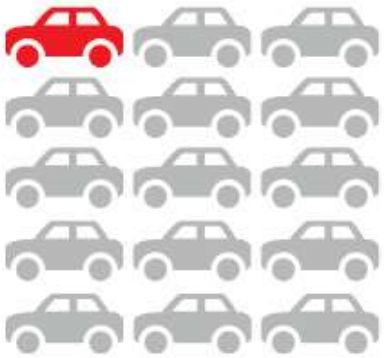

Airbus A400M
2015

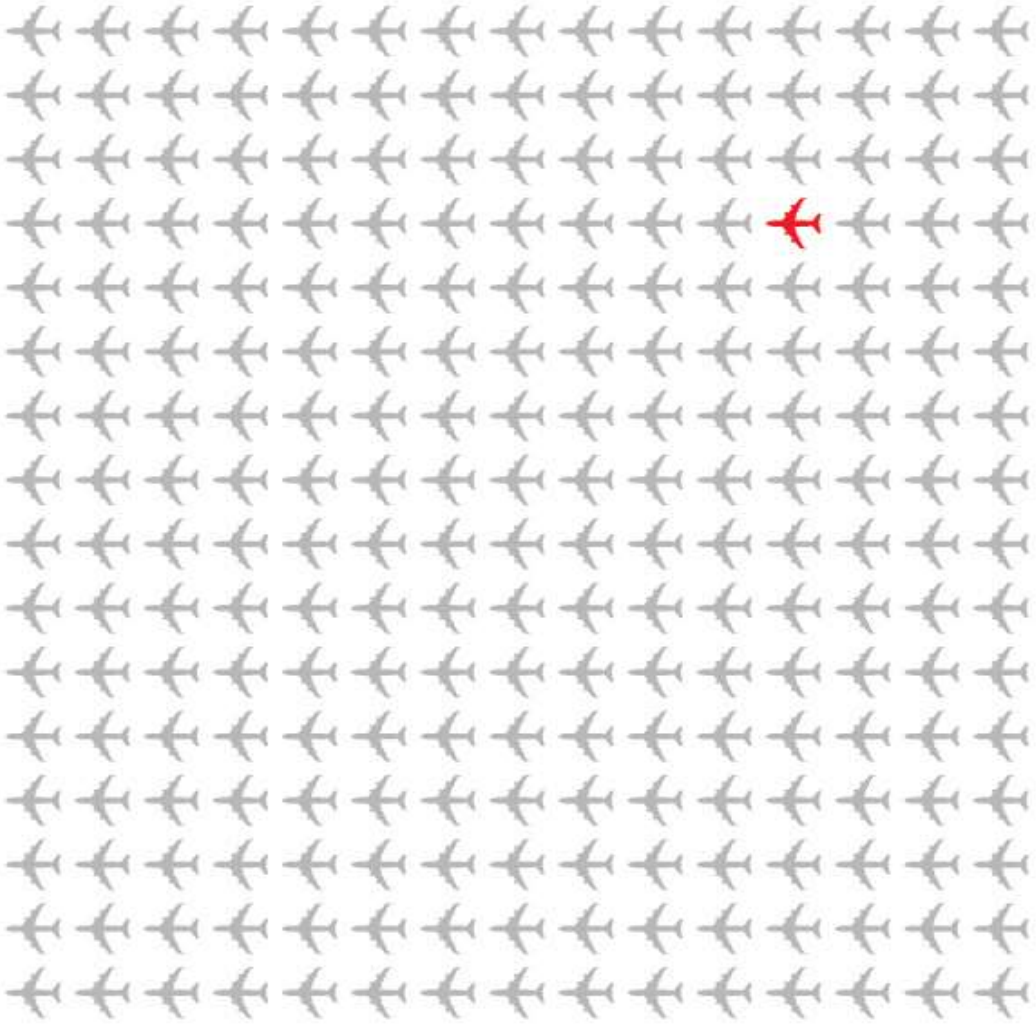
Boeing 737 MAX
2018 & 2019

TUI Airways
2020

Your odds of dying in a car accident are **1 in 114.**

Your odds of dying in a plane crash are **1 in 9,821.**





Source: Security Boulevard

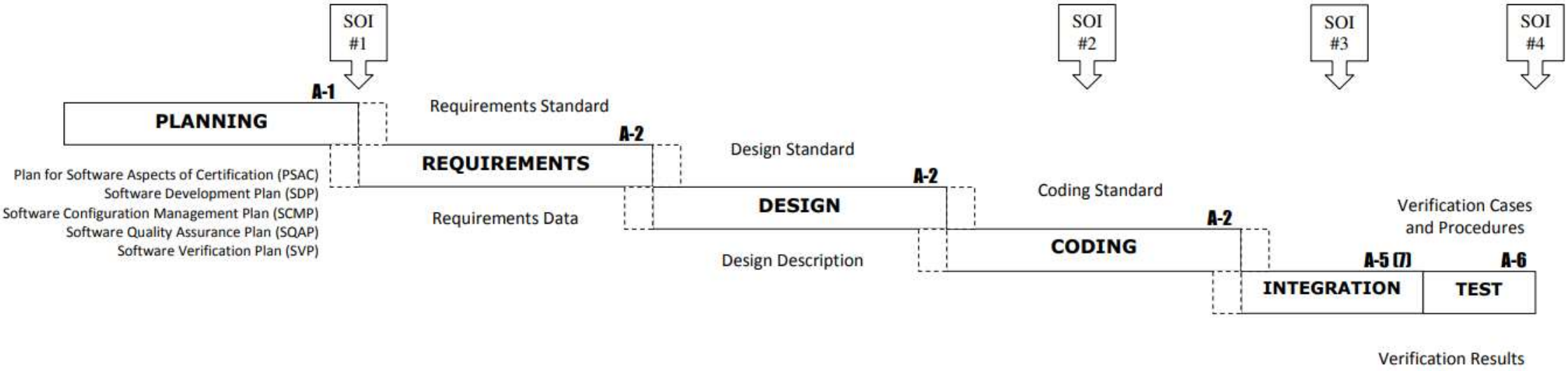
What is done to avoid it?

Define guidance for airborne software development (aka DO-178C)

COMMITTEE MEMBERSHIP

Michael Deltz	Gentex Corporation
Jean-Luc Delamaide	EASA
Hervé Delseny	Airbus
Patrick Desbiens	Transport Canada
Mike DeWalt	Certification Services, Inc./FAA
Mansur Dewshi	Ultra Electronics Controls
Bernard Dion	Esterel Technologies
Antonio Jose Vitorio Domiciano	Embraer
Kurt Doppelbauer	TTTech
Cheryl Dorsey	Digital Flight
Rick Dorsey	Digital Flight
John Doughty	Garmin International
Vincent Dovydaitis III	Foliage Software Systems, Inc.
Georges Duchein	DGA
Branimir Dulic	Transport Canada
Gilles Dulon	SAGEM DS Safran Group
Paul Dunn	Northrop Grumman Corporation
Andrew Eaton	UK CAA
Brian Eckmann	Universal Avionics Systems Corporation
Vladimir Eliseev	Sukhoi Civil Aircraft Company (SCAC)
Andrew Elliott	Design Assurance
Mike Elliott	Boeing Company
Joao Esteves	Critical Software

SOFTWARE DEVELOPMENT PROCESS



SOFTWARE DEVELOPMENT OBJECTIVES

100

Table A-5 Verification of Outputs of Software Coding & Integration Processes

	Objective		Activity	Applicability by Software Level				Output		Control Category by Software Level			
	Description	Ref	Ref	A	B	C	D	Data Item	Ref	A	B	C	D
1	Source Code complies with low-level requirements.	6.3.4.a	6.3.4	●	●	○		Software Verification Results	11.14	②	②	②	
2	Source Code complies with software architecture.	6.3.4.b	6.3.4	●	○	○		Software Verification Results	11.14	②	②	②	
3	Source Code is verifiable.	6.3.4.c	6.3.4	○	○			Software Verification Results	11.14	②	②		
4	Source Code conforms to standards.	6.3.4.d	6.3.4	○	○	○		Software Verification Results	11.14	②	②	②	
5	Source Code is traceable to low-level requirements.	6.3.4.e	6.3.4	○	○	○		Software Verification Results	11.14	②	②	②	
6	Source Code is accurate and consistent.	6.3.4.f	6.3.4	●	○	○		Software Verification Results	11.14	②	②	②	
7	Output of software integration process is complete and correct.	6.3.5.a	6.3.5	○	○	○		Software Verification Results	11.14	②	②	②	
8	Parameter Data Item File is correct and complete	6.6.a	6.6	●	●	○	○	Software Verification Cases and Procedures Software Verification Results	11.13 11.14	① ②	① ②	② ②	② ②
9	Verification of Parameter Data Item File is achieved.	6.6.b	6.6	●	●	○		Software Verification Results	11.14	②	②	②	

APPROVED FOR FLIGHT

Civil presumption of innocence principle:

"one is considered innocent unless proven guilty"

Aerospace presumption of innocence principle: *"one is considered guilty unless proven innocent"*

Boeing 777X

using CRITICAL Software technology


BOEING
777
34L-16R


January 25, 2020

LUNA NG/B

using CRITICAL Software technology

Boeing 787-10

using CRITICAL Software technology

Airbus A350-800/-1000

using CRITICAL Software technology

THANK YOU!

CRITICALSOFTWARE.COM