CERTIFICATION

OF

FLIGHT CRITICAL SYSTEMS

Herbert Hecht
SoHaR Incorporated
herb@sohar.com

Michael Gomez
Northrop Grumman Corp.
m.gomez@ngc.com

AC 25.1309-1A/AMJ 25.1309

- *…condition which would prevent the continued safe flight and landing of the airplane [must be] extremely improbable< 1 × 10-9 per flight hour*
- *…conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions [must be] improbable. < 1 × 10-5 per flight hour, less for severe conditions*

*"In general, the means of compliance described in this AC are not directly applicable to **software assessments** because it is not possible to assess the number and kinds of software errors, if any, that remain after the completion of system design, development and test."*

Refers for software to RTCA DO-178B

SOFTWARE CERTIFICATION
DO-178B

1. SYSTEM ASPECTS
2. SOFTWARE LIFE CYCLE
3. SOFTWARE PLANNING PROCESS
4. SOFTWARE DEVELOPMENT PROCESS
5. SOFTWARE VERIFICATION PROCESS
6. SOFTWARE CONFIGURATION M'GMNT PROCESS
7. SOFTWARE QUALITY ASSURANCE PROCESS
8. CERTIFICATION LIAISON PROCESS

.....

NOT TRACEABLE TO FAR 25.1309

FROM Y2K EFFORTS

"The main line software code usually does its job. Breakdowns typically occur when the software exception code does not properly handle abnormal input or environmental conditions – or when an interface does not respond in the anticipated or desired manner."

C. K. Hansen, *The Status of Reliability Engineering Technology 2001*, Newsletter of the IEEE Reliability Society, January 2001

4-UNIVERSITY EXPERIMENT

TEST RESULTS W/ ACCELEROMETER. FAILURES

PROGRAM TO FURNISH ORTHOGONAL OUTPUT FROM 6 NON-ORTHOGO-NAL ACCELEROMETERS

PROGRAM SHOULD TOLERATE UP TO **THREE** ACCELEROMETER FAILURES

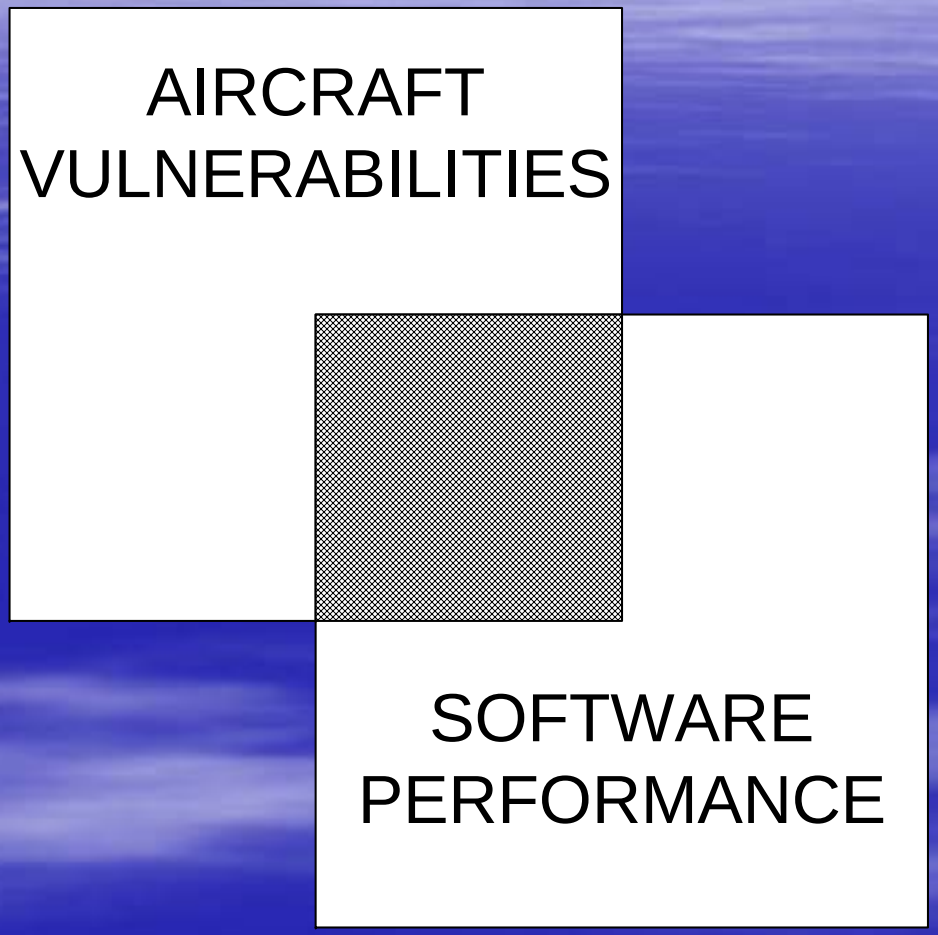
No. accel. failed	Total tests	Tests failed	Failure fraction
1	**134,135**	**1,268**	**0.01**
2	**101,151**	**12,921**	**0.13**
3	**143,509**	**83,022**	**0.58**

ECKHARDT, CAGLAYAN ET AL., *AN EXPERIMENTAL EVALUATION OF SOFTWARE REDUNDANCY,* TSE, 7/91

WHAT CAN BE LEARNED?

- EXCEPTION CONDITIONS, AND PARTICULARLY MULTIPLE EXCEPTION CONDITIONS, ARE LIKELY TO BE OMITTED
  - IN PROGRAM DESIGN
  - IN PROGRAM TESTING
- TEST CASES INVOLVING MULTIPLE EXCEPTIONS ARE
  - MORE DIFFICULT TO CONSTRACT
  - MUCH MORE PRODUCTIVE IN DETECTING PROGRAM WEAKNESSES

THE CRITICAL AREA

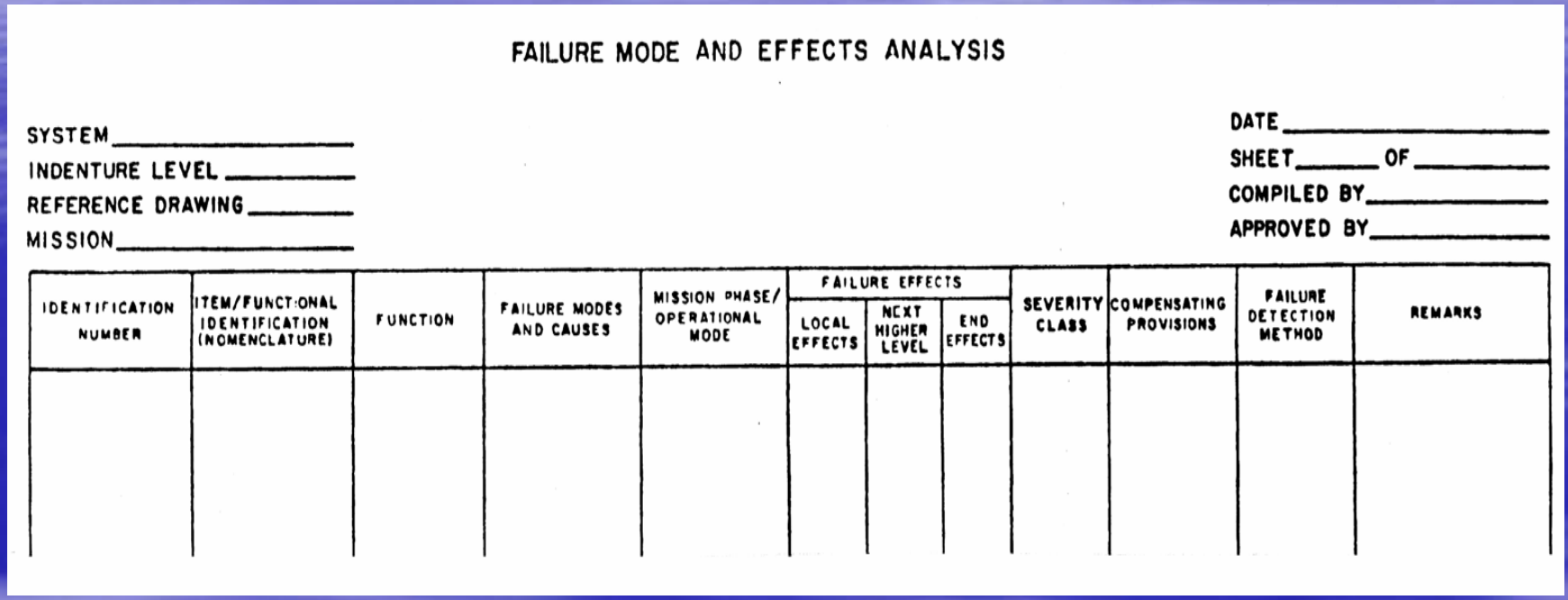


REQUIRED: INVOLVE SYSTEM ENGINEERING

FMEA AS THE BRIDGE

- SYSTEM ENGINEERING:
  - END LEVEL FAILURE EFFECTS
  - SEVERITY
- BOTH
  - DETECTION METHODS
  - COMPENSATION (MITIGATION)
- SOFTWARE ENGINEERING
  - FAILURE MODES
  - LOW LEVEL FAILURE EFFECTS

FMEA WORKSHEET



FAILURE MODE AND EFFECTS ANALYSIS

SYSTEM _____
INDENTURE LEVEL _____
REFERENCE DRAWING _____
MISSION _____

DATE _____
SHEET _____ OF _____
COMPILED BY _____
APPROVED BY _____

IDENTIFICATION NUMBER	ITEM/FUNCTIONAL IDENTIFICATION (NOMENCLATURE)	FUNCTION	FAILURE MODES AND CAUSES	MISSION PHASE/ OPERATIONAL MODE	FAILURE EFFECTS			SEVERITY CLASS	COMPENSATING PROVISIONS	FAILURE DETECTION METHOD	REMARKS
					LOCAL EFFECTS	NEXT HIGHER LEVEL	END EFFECTS				

IDENTIFICATION

CAUSES AND EFFECTS

DISPOSITION

IDENTIFICATION

- IDENTIFICATION NUMBER, E. G. 1.2.1.4
  - MAJOR COMPONENT 1
  - ASSEMBLY 2
  - SUBASSEMBLY 1
  - PART 4
- ITEM (PART NAME)
- FUNCTION

FAILURE CAUSES AND EFFECTS

- FAILURE MODE AND CAUSE
  - FAILURE MODE (FUNCTIONAL) E. G., NO OUTPUT
  - FAILURE CAUSE (ENGINEERING) E. G., 1. OXIDE FAILURE 2. BOND BREAKAGE
- MISSION PHASE, OPERATIONAL MODE
- EFFECTS
  - LOCAL
  - NEXT HIGHER LEVEL
  - END EFFECTS
- SEVERITY CLASSIFICATION BASED ON END EFFECTS

DISPOSITION

- FAILURE DETECTION METHOD
  - CAN BE AT SEVERAL LEVELS
- COMPENSATION PROVISIONS
  - REDUNDANCY, RETRY, BACK-UP MODE
- REMARKS
  - WHAT IS THE EFFECT IF BACK-UP FAILS

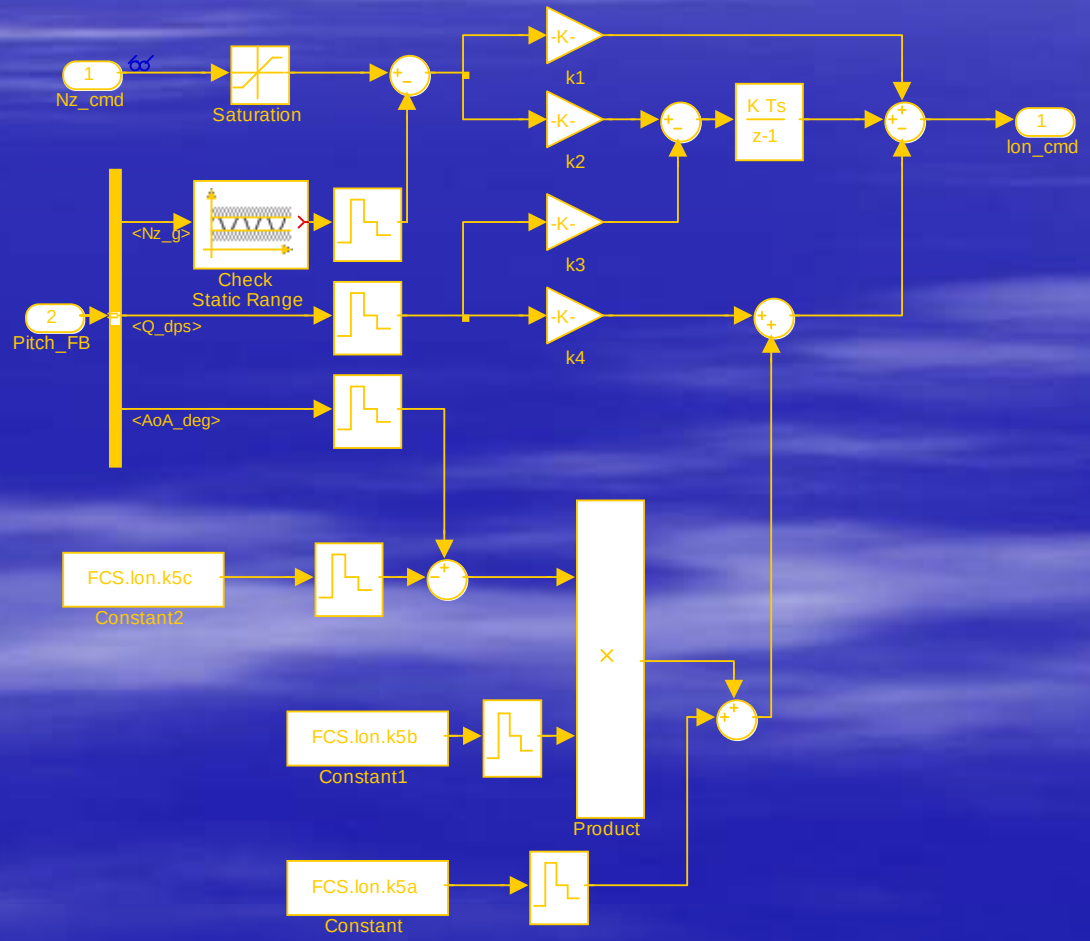
MOCET

- Model-based Certification Tool
- Computer Aided generation of FMEA
- Evaluation of robustness provisions
- TPNs for exploration of timing problems

LONGITUDINAL CONTROL

Longitudinal FCS

Generate longitudinal command for psuedo longitudinal surface

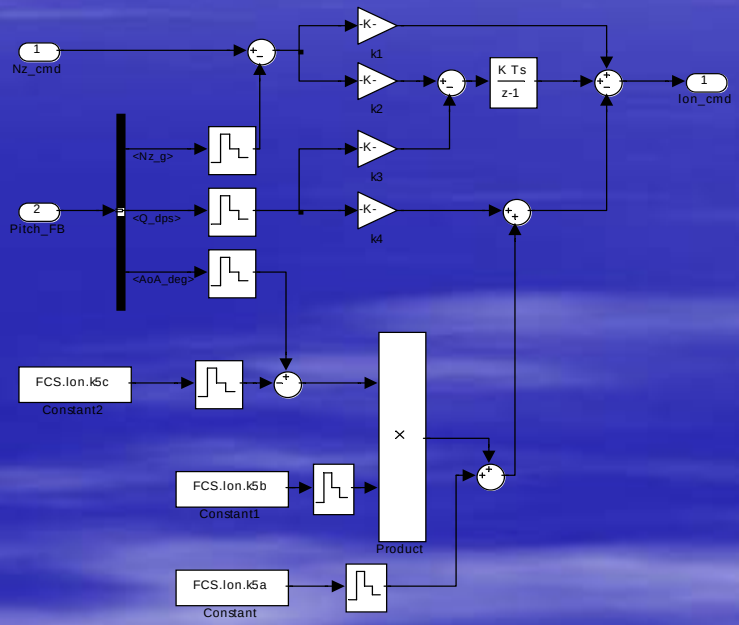


MODEL STRUCTURE

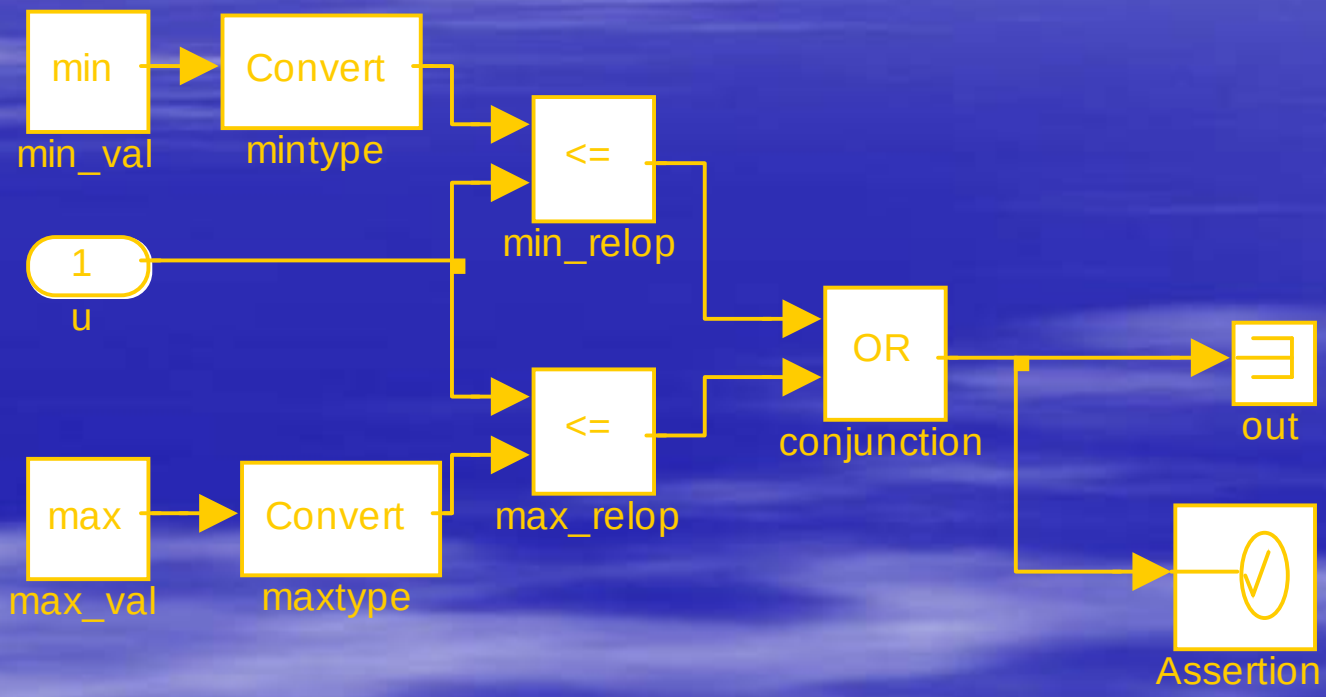
```
Block {
  BlockType                 Constant
  Name                      "Constant1"
  Position                  [155, 496, 240, 524]
  Value                     "FCS.lon.k5b"
}
Block {
  BlockType                 Constant
  Name                      "Constant2"
  Position                  [35, 411, 120, 439]
  Value                     "FCS.lon.k5c"
}
Block {
  BlockType                 DiscreteIntegrator
  Name                      "Discrete-Time\nIntegrator"
  Ports                     [1, 1]
  Position                  [395, 160, 430, 200]
  ShowName                  off
  IntegratorMethod          "Forward Euler"
  ExternalReset             "none"
  InitialConditionSource  "internal"
  SampleTime                "FCS.T_Samp"
}
Block {
  BlockType                 Product
  Name                      "Product"
  Ports                     [2, 1]
  Position                  [310, 383, 345, 552]
  InputSameDT               off
}
```

PARSED BLOCKS

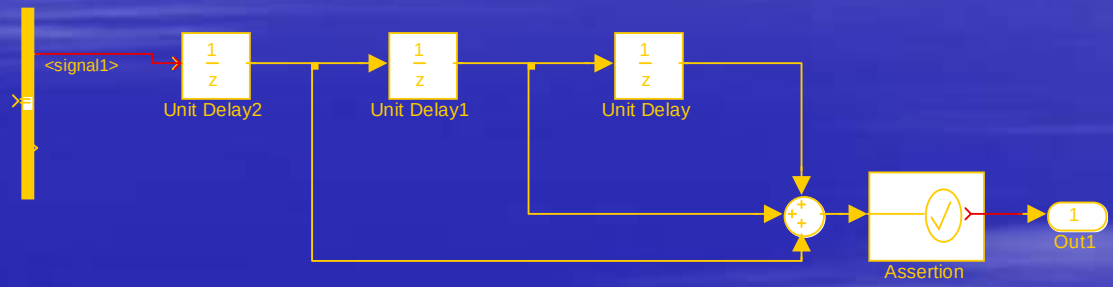
- 1 longitudinal_claw
- 1.1 Lon
- 1.1.1 Lon
- 1.1.1.1 Nz_cmd
- 1.1.1.2 Pitch_FB
- 1.1.1.3 Bus\nSelector
- 1.1.1.3.1 <Nz_g>
- 1.1.1.3.2 <Q_dps>
- 1.1.1.3.3 <AoA_deg>
- 1.1.1.4 Constant
- 1.1.1.5 Constant1
- 1.1.1.6 Constant2
- 1.1.1.7 Discrete-Time\nIntegrator
- 1.1.1.8 Product
- 1.1.1.9 Sum
- 1.1.1.10 Sum1
- 1.1.1.11 Sum2
- 1.1.1.12 Sum3
- 1.1.1.13 Sum4
- 1.1.1.14 Sum5
- 1.1.1.15 Zero-Order\nHold1



EXAMPLE OF DETECTION CHECK RANGE



EXAMPLE OF DETECTION DETECT ZERO OUTPUT



FMEA BY MOCET

ID	Item/Function	Failure Mode	Local Effect	Detection
1.1.1.1	N_z Command	a. Absent b. Jump c. > Limit	No output Hi rate None (limiter)	N-wait* Chck rate*
1.1.1.2	Pitch FB	See 1.1.1.3		
1.1.1.3	Bus selector	Stuck	No FB	N-wait*
1.1.1.3.1	N_z FB	a. Absent b. Jump c. Xtrm value	No signal Hi rate Hi/lo signal	N-wait Chck rate Chck range
1.1.1.7	Product	a. Absent b. Jump	No signal Hi rate	N-wait* Chck rate*

* Not in current model

CONCLUSIONS

- SOFTWARE CERTIFICATION BY DO-178B
  - IS UNNECESSARILY COSTLY
  - DOES NOT ADDRESS BASIC CERTIFICATION REQUIREMENTS
- MOCET WILL
  - SIMPLIFY THE CERTIFICATION EFFORT
  - ADDRESSES CERTIFICATION REQUIREMENTS MORE DIRECTLY

ACKNOWLEDGEMENT

MOCET is being developed under an AFRL contract for which Dave Hohman and Ray Bortner are the technical points of contact